Ethernet-коммутатор
RTT-A430-48XG-4QXG

Руководство по эксплуатации

Версия ПО 8.4.0.11.2

Версия документа	Дата выпуска	Содержание изменений
4.0	05.08.2026	Синхронизация с версией ПО 8.4.0.11.2
3.0	03.07.2025	Синхронизация с версией ПО 8.4.0.10.2
3.0	18.08.2024	Синхронизация с версией ПО 8.4.0.8.11
2.0	31.07.2020	Синхронизация с версией ПО 8.4.0.5
1.0	14.10.2019	Первая публикация
Версия программного обеспечения: 8.4.0.11.2		

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 42
2 ОПИСАНИЕ ИЗДЕЛИЯ 43
2.1 Назначение 43
2.2 Функции коммутатора 43
2.2.1 Базовые функции 43
2.2.2 Функции при работе с MAC–адресами 44
2.2.3 Функции второго уровня сетевой модели OSI 44
2.2.4 Функции третьего уровня сетевой модели OSI 46
2.2.5 Функции QoS 46
2.2.6 Функции обеспечения безопасности 47
2.2.7 Функции управления коммутатором 47
2.2.8 Функции ЦОД 49
2.2.9 Дополнительные функции 49
2.3 Основные технические характеристики 50
2.4 Конструктивное исполнение 52
2.4.1 Внешний вид и описание передней панели 52
2.4.2 Внешний вид и описание задней панели 53
2.4.3 Внешний вид и описание боковых панелей 54
2.4.4 Световая индикация 54
2.5 Комплект поставки 56
3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ 57
3.1 Крепление кронштейнов 57
3.2 Установка устройства в стойку 57
3.3 Установка модулей питания 59
3.4 Подключение питающей сети 60
3.5 Установка и удаление SFP-трансиверов 60
4 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА 62
4.1 Настройка терминала 62
4.2 Включение устройства 62
5 ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ (CLI) 64
5.1 Синтаксис команд 64
5.2 Условные обозначения в описании команд 65
5.3 Общие значения параметров 65
5.4 Unit/slot/port, правила именования 66
5.5 Использование отрицательной формы команд 67
5.6 Выполнение команд show 67
5.7 Фильтрация вывода данных CLI 67
5.8 Модули программного обеспечения 68
5.9 Режим ввода команд 69
5.10 Автоматическое дополнение и сокращение команд 73
5.11 Сообщения об ошибках в командном интерфейсе 73
5.12 Правила редактирования командной строки 74
5.13 Использование справки командного интерфейса 75
5.14 Доступ к командному интерфейсу 75
5.15 Программное управление кнопкой F 76
reset-button enable 76
reset-button disable 76
reset-button reload-only 76
no reset-button 76
6 КОМАНДЫ БАЗОВОЙ РАБОТЫ СИСТЕМЫ 77
6.1 Команды автоматической установки 77

boot autoinstall 78
boot host retrycount 78
boot host dhcp 78
boot host autosave 78
boot host autoreboot 79
erase startup-config 79
erase factory-defaults 79
copy <url> backup 80
boot system backup 80
exception protocol 80
exception switch-chip-register 80
exception dump stack-ip-address protocol 81
no debug crashlog verbose 81
6.2 Фильтрация вывода CLI 81
show xxx|include “string” 81
show xxx|include “string” exclude “string2” 81
show xxx|exclude “string” 81
show xxx|begin “string” 81
show xxx|section “string” 82
show xxx|section “string” “string2” 82
show xxx|section “string” include “string2” 82
show xxx|no-more 82
6.3 Команды работы с ПО 82
delete 82
boot system 83
show bootvar 83
filedescr 83
6.4 Вывод информации о системе и статистики 83
load-interval 83
show arp switch 84
show eventlog 84
show hardware 85
show version 85
show platform vpd 85
show interface 86
show interfaces status 88
show interfaces traffic 88
show interface counters 89
show interfaces description 89
show interface ethernet 90
show interface ethernet switchport 96
show fiber-ports optical-transceiver 96
show fiber-ports optical-transceiver-info 97
show mac-addr-table 98
process cpu threshold 99
show process app-list 99
show process app-resource-list 100
show process cpu 100
show process proc-list 101
show running-config 101
show running-config interface 102
show 103
dir 103
show sysinfo 103

show tech-support 104
length value 105
terminal length 105
show terminal length 106
memory free low-watermark processor 106
clear mac-addr-table 106
6.5 Команды бокс-сервисов 107
environment temprange 107
environment trap 107
show environment 108
6.6 Настройка системного журнала 108
logging buffered 108
logging buffered wrap 108
logging cli-command 109
logging console 109
logging host 109
logging host reconfigure 110
logging host remove 110
logging persistent 110
logging protocol 111
logging syslog 111
logging syslog port 111
logging syslog source-interface 112
show logging 112
show logging buffered 113
show logging hosts 113
show logging persistent 114
show logging traplogs 114
clear logging buffered 114
6.7 Настройка оповещений по электронной почте и почтового сервера 115
logging email 115
logging email urgent 115
logging email message-type to-addr 115
logging email from-addr 116
logging email message-type subject 116
logging email logtime 117
logging traps 117
logging email test message-type 117
show logging email config 118
show logging email statistics 118
clear logging email statistics 118
mail-server 119
security 119
port 119
username (в режиме конфигурирования почтового сервера) 119
password 120
show mail-server config 120
6.8 Служебные утилиты и команды очистки 120
traceroute 120
clear config 122
clear counters 122
clear igmpsnooping 123
clear ip access-list counters 123
clear ipv6 access-list counters 123

clear mac access-list counters 123
clear pass 123
clear traplog 123
clear vlan 124
logout 124
ping 124
quit 125
reload 125
copy 126
file verify 130
ip scp server enable 130
write memory 131
6.9 Управление лицензиями для расширенных функций 131
copy <url> nvram:license-key 131
delete license-key 131
show license 132
show license features 132
6.10 Настройка SNTP 132
sntp broadcast client poll-interval 132
sntp client mode 132
sntp client port 133
sntp unicast client poll-interval 133
sntp unicast client poll-timeout 133
sntp unicast client poll-retry 134
sntp source-interface 134
show sntp 135
show sntp client 135
show sntp server 136
show sntp source-interface 136
6.11 Настройка часов реального времени 137
clock set 137
clock summer-time date 137
clock summer-time recurring 138
clock timezone 138
show clock 139
show clock detail 139
6.12 Настройка DHCP-сервера 139
ip dhcp pool 139
client-identifier 139
client-name 140
default-router 140
dns-server 140
hardware-address 141
host 141
lease 142
network (в режиме конфигурации пула DHCP) 142
bootfile 142
domain-name 143
domain-name enable 143
netbios-name-server 143
netbios-node-type 144
next-server 144
option 144
ip dhcp excluded-address 145

ip dhcp ping packets 145
service dhcp 146
ip dhcp bootp automatic 146
ip dhcp conflict logging 146
clear ip dhcp binding 147
clear ip dhcp server statistics 147
clear ip dhcp conflict 147
show ip dhcp binding 147
show ip dhcp global configuration 147
show ip dhcp pool configuration 148
show ip dhcp server statistics 148
show ip dhcp conflict 149
6.13 Настройка DNS-клиента 149
ip domain lookup 150
ip domain name 150
ip domain list 150
ip name server 151
ip name source-interface 151
ip host 151
ipv6 host 152
ip domain retry 152
ip domain timeout 153
clear host 153
show hosts 153
show ip name source-interface 154
6.14 Управление конфликтами IP-адресов 154
ip address-conflict-detect run 154
show ip address-conflict 154
clear ip address-conflict-detect 155
6.15 Команды отслеживания служебных пакетов 156
capture start 156
capture stop 156
capture file | remote | line 156
capture remote port 157
capture file size 157
capture line wrap 158
capture usb 158
show capture packets 158
cpu-traffic direction interface 158
cpu-traffic direction match cust-filter 159
cpu-traffic direction match srcip 159
cpu-traffic direction match dstip 160
cpu-traffic direction match tcp 160
cpu-traffic direction match udp 160
cpu-traffic mode 161
cpu-traffic trace 161
show cpu-traffic 161
show cpu-traffic interface 162
show cpu-traffic summary 162
show cpu-traffic trace 162
clear cpu-traffic 162
debug aaa accounting 162
debug arp 163
debug authentication 163

debug auto-voip 163
debug clear 163
debug aaa authorization 164
debug console 164
debug crashlog 165
debug dcbx packet 165
debug debug-config 165
debug dhcp packet 166
debug dot1ag 166
debug dot1x packet 166
debug fip-snooping packet 167
debug igmpsnooping packet 167
debug igmpsnooping packet transmit 168
debug igmpsnooping packet receive 168
debug ip acl 169
debug ip bgp 169
debug ip vrrp 170
debug ipv6 dhcp 170
debug ipv6 ospfv3 packet 171
debug lacp packet 171
debug mldsnooping packet 171
debug ospf packet 172
debug ospfv3 packet 173
debug ping packet 173
debug rip packet 174
debug sflow packet 174
debug spanning-tree bpdu 175
debug spanning-tree bpdu receive 175
debug spanning-tree bpdu transmit 176
debug tacacs 176
debug telnetd start 176
debug telnetd stop 177
debug transfer 177
debug udld events 177
debug udld packet receive 177
debug udld packet transmit 177
show debugging 178
exception protocol 178
exception dump tftp-server 178
exception dump nfs 178
exception dump filepath 179
exception core-file 179
exception switch-chip-register 180
exception dump ftp-server 180
exception dump compression 180
exception dump stack-ip-address protocol 181
exception dump stack-ip-address add 181
exception dump stack-ip-address remove 181
exception nmi 181
write core 182
debug exception 182
show exception 182
show exception core-dump-file 182
show exception log 182

mbuf 183
show mbuf total 183
show msg-queue 184
debug packet-trace 184
session start 184
session stop 184
6.16 Команды тестирования кабеля 184
cablestatus 185
6.17 Команды sFlow 185
sflow poller 185
sflow receiver 186
sflow receiver owner timeout 187
sflow receiver owner notimeout 187
sflow sampler 187
sflow sampler rate 188
sflow source-interface 188
show sflow agent 189
show sflow pollers 189
show sflow receivers 189
show sflow source-interface 190
6.18 Команды настройки SDM-шаблонов 190
6.19 Команды удаленного мониторинга 192
rmon alarm 192
rmon hcalarm 193
rmon event 194
rmon collection history 195
show rmon 195
show rmon collection history 196
show rmon events 196
show rmon history 197
show rmon log 198
show rmon statistics interfaces 198
show rmon hcalarms 199
6.20 Управление приложением статистики 200
stats group 201
stats flow-based 201
stats flow-based reporting 202
stats group 202
stats flow-based 202
show stats group 203
show stats flow-based 203
6.21 Команды для резервирования конфигурации 203
backup url <url> 203
backup time-period 204
backup auto 204
backup write-memory 204
7 КОМАНДЫ РЕЖИМА СТЕКИРОВАНИЯ 205
7.1 Стекирование 205
stack 205
member 205
switch priority 206
switch renumber 206
movemanagement 206
standby 207

slot 207
set slot disable 208
set slot power 208
reload (Stack) 209
stack-status sample-mode 209
show slot 209
show stack-status 210
show supported cardtype 210
show switch 211
show supported switchtype 212
7.2 Команды настройки стек-портов 213
stack-port 213
show stack-port 213
show stack-port counters 213
show stack-port diag 214
show stack-port stack-path 215
7.3 Команды синхронизации ПО в стеке 215
boot auto-copy-sw 215
boot auto-copy-sw trap 215
boot auto-copy-sw allow-downgrade 215
show auto-copy-sw 216
Команды безостановочной обработки трафика (NSF) 216
nsf (Stack Global Config Mode) 217
show nsf 218
initiate failover 218
show checkpoint statistics 219
clear checkpoint statistics 219
7.4 Команды смешанного стекирования 220
stack-template 220
show stack-template list 220
show stack-template switch 221
7.5 Команды настройки протокола NETCONF 221
ip netconf server enable 221
8 КОМАНДЫ УПРАВЛЕНИЯ 222
8.1 Команды настройки интерфейса удалённого управления 222
enable (доступ в привилегированный режим) 222
do (выполнить команду в привилегированном режиме) 222
serviceport ip 222
serviceport protocol 223
serviceport protocol dhcp 223
network parms 223
network mgmt_vlan 223
network protocol 224
network protocol dhcp 224
network mac-address 224
network mac-type 225
network javamode 225
show network 225
show serviceport 226
8.2 Команды для настройки доступа с помощью консольного порта 227
configure 227
line 227
serial baudrate 228
serial timeout 228

show serial 228
session-limit 229
session-timeout 229
8.3 Команды настройки протокола Telnet 229
ip telnet server enable 230
ip telnet port 230
telnet 230
transport input telnet 231
transport output telnet 231
telnetcon maxsessions 231
telnetcon timeout 232
show telnet 232
show telnetcon 233
8.4 Команды настройки протокола SSH 233
ssh 233
transport output ssh 233
no transport output ssh 234
show ssh 234
clear ssh-client-knownhost 234
ip ssh 234
ip ssh port 235
ip ssh protocol 235
ip ssh server enable 235
sshcon maxsessions 235
sshcon timeout 236
show ip ssh 236
8.5 Команды управления ключами безопасности 237
crypto certificate generate 237
crypto key generate rsa 237
crypto key generate dsa 237
8.6 Команды настройки протоколов HTTP/HTTPS 238
ip http accounting exec, ip https accounting exec 238
ip http authentication 238
ip https authentication 239
ip http server 239
ip http secure-server 240
ip http java 240
ip http port 240
ip http rest-api port 241
ip http rest-api secure-port 241
ip http session hard-timeout 241
ip http session maxsessions 242
ip http session soft-timeout 242
ip http secure-session maxsessions 243
ip http secure-session soft-timeout 243
ip http secure-port 244
ip http secure-protocol 244
show ip http 244
8.7 Команды доступа 245
disconnect 245
linuxsh 245
show loginsession 246
show loginsession long 246
8.8 Команды настройки контроля учетных записей пользователя 246

aaa authentication login....246
aaa authentication enable....247
aaa authorization....249
authorization commands....251
authorization exec....251
authorization exec default....251
show authorization methods....252
enable authentication....252
username (режим глобальной конфигурации)....252
username nopassword....253
username unlock....253
username snmpv3 accessmode....253
username snmpv3 authentication....254
username snmpv3 encryption....254
username snmpv3 encryption encrypted....255
show users....255
show users long....256
show users accounts....256
show users login-history [long]....256
show users login-history [username]....256
login authentication....257
password....257
password (режим конфигурирования командной строки)....257
password (пользовательский режим)....258
password (режим конфигурации пользователя IAS aaa)....258
enable password (привилегированный режим)....258
passwords min-length....258
passwords history....259
passwords aging....259
passwords lock-out....259
passwords strength-check....260
passwords strength maximum consecutive-characters....260
passwords strength maximum repeated-characters....260
passwords strength minimum uppercase-letters....261
passwords strength minimum lowercase-letters....261
passwords strength minimum numeric-characters....261
passwords strength minimum special-characters....262
passwords strength minimum character-classes....262
passwords strength exclude-keyword....262
show passwords configuration....263
show passwords result....263
aaa accounting....264
aaa accounting update....265
accounting....265
no accounting....266
show accounting....266
show accounting methods....266
clear accounting statistics....266
show domain-name....266
aaa ias-user username....266
aaa session-id....267
password (режим конфигурации пользователя IAS aaa)....267
clear aaa ias-users....268
show aaa ias-users....268

8.9 Команды настройки протокола SNMP 268
snmp-server 268
snmp-server community 269
snmp-server community-group 269
snmp-server enable traps violation 270
snmp-server enable traps 270
snmp-server enable traps bgp 270
snmp-server enable traps fip-snooping 271
snmp-server port 271
snmp trap link-status 271
snmp trap link-status all 272
snmp-server enable traps linkmode 272
snmp-server enable traps multiusers 273
snmp-server enable traps stpmode 273
snmp-server engineID local 273
snmp-server filter 274
snmp-server group 275
snmp-server host 275
snmp-server user 276
snmp-server view 277
snmp-server v3-host 277
snmptrap source-interface 278
snmptrap ipaddr snmpversion 279
snmptrap ip6addr snmpversion[1] 279
show snmp 279
show snmp engineID 280
show snmp filters 280
show snmp group 281
show snmp-server 281
show snmp source-interface 281
show snmp user 281
show snmp views 282
show trapflags 282
8.10 Команды настройки протокола RADIUS 283
aaa server radius dynamic-author 283
authentication command bounce-port ignore 283
auth-type 283
authorization network radius 284
clear radius dynamic-author statistics 284
client 284
debug aaa coa 285
debug aaa pod 285
ignore server-key 285
ignore session-key 285
port 285
radius accounting mode 286
radius server attribute 4 286
radius server attribute 95 287
radius server attribute 31 287
radius server host 288
radius server key 289
radius server msgauth 289
radius server primary 290
radius server retransmit 290

radius source-interface 291
radius server timeout 291
server-key 292
no server-key 292
show radius servers 292
show radius 292
show radius servers 293
show radius accounting 294
show radius accounting statistics 294
show radius source-interface 295
show radius statistics 295
8.11 Команды настройки протокола TACACS+ 296
tacacs-server host 296
tacacs-server key 297
tacacs-server keystring 297
tacacs-server source-interface 297
tacacs-server timeout 298
key 298
keystring 299
port 299
priority (режим конфигурации TACACS) 299
timeout 299
show tacacs 299
show tacacs source-interface 300
8.12 Команды сценариев конфигурации 300
script apply 301
script delete 301
script list 301
script show 301
script validate 302
8.13 Команды настройки баннера, подсказки командной строки и имени устройства 302
copy (pre-login banner) 302
set prompt 302
hostname 302
show clibanner 303
set clibanner 303
9 КОМАНДЫ НАСТРОЙКИ КОММУТАЦИИ 304
9.1 Команды настройки порта 304
interface 304
auto-negotiate 304
auto-negotiate all 305
description 305
media-type 305
mtu 306
shutdown 307
shutdown all 307
speed 307
speed all 308
hardware profile portmode 308
show interface media-type 308
show interfaces status 309
show port 309
show port advertise 310
show port description 310

show interfaces hardware profile 311
9.2 Команды настройки протокола STP 311
spanning-tree 311
spanning-tree auto-edge 311
spanning-tree backbonefast 312
spanning-tree bpdufilter 313
spanning-tree bpdufilter default 313
spanning-tree bpduflood 314
spanning-tree bpduguard 314
spanning-tree bpdumigrationcheck 314
spanning-tree configuration name 314
spanning-tree configuration revision 315
spanning-tree cost 315
spanning-tree edgeport 315
spanning-tree forward-time 316
spanning-tree guard 316
spanning-tree max-age 316
spanning-tree max-hops 317
spanning-tree mode 317
spanning-tree mst 318
spanning-tree mst instance 319
spanning-tree mst priority 319
spanning-tree mst vlan 320
spanning-tree port mode 320
spanning-tree port mode all 321
spanning-tree port-priority 321
spanning-tree tcnguard 321
spanning-tree transmit 322
spanning-tree uplinkfast 322
spanning-tree vlan 323
spanning-tree vlan cost 323
spanning-tree vlan forward-time 323
spanning-tree vlan hello-time 323
spanning-tree vlan max-age 324
spanning-tree vlan root 324
spanning-tree vlan port-priority 324
spanning-tree vlan priority 325
show spanning-tree active 326
show spanning-tree backbonefast 326
show spanning-tree brief 326
show spanning-tree interface 327
show spanning-tree mst detailed 327
show spanning-tree mst port detailed 328
show spanning-tree mst port summary 329
show spanning-tree mst port summary active 330
show spanning-tree mst summary 330
show spanning-tree summary 331
show spanning-tree uplinkfast 331
show spanning-tree vlan 331
spanning-tree mac-address dot1d 332
spanning-tree mac-address dot1ad 332
spanning-tree mac-address auto 332
9.3 Команды настройки защиты от петель 333
keepalive (режим глобальной конфигурации) 333

keepalive (режим конфигурирования интерфейса) 333
keepalive action 333
keepalive disable-timer 334
keepalive disable-timer 334
keepalive retry 334
show keepalive 335
show keepalive statistics 335
clear counters keepalive 335
9.4 Команды настройки VLAN 335
vlan database 335
vlan 336
vlan acceptframe 336
vlan ingressfilter 336
vlan internal allocation 337
vlan makestatic 337
vlan name 337
vlan participation 338
vlan participation all 338
vlan port acceptframe all 338
vlan port ingressfilter all 339
vlan port pvid all 339
vlan port tagging all 340
vlan protocol group 340
vlan protocol group name 340
vlan protocol group add protocol 340
protocol group 341
protocol vlan group 341
protocol vlan group all 342
show port protocol 342
vlan pvid 342
vlan tagging 343
vlan association subnet 343
vlan association mac 343
remote-span 344
show vlan 344
show vlan tag 345
show vlan internal usage 345
show vlan brief 346
show vlan association subnet 346
show vlan association mac 346
9.5 Команды настройки Double VLAN 347
dvlan-tunnel ethertype (режим конфигурирования интерфейса) 347
dvlan-tunnel ethertype primary-tpid 347
mode dot1q-tunnel 348
mode dvlan-tunnel 348
show dot1q-tunnel 349
9.6 Команды настройки Private VLAN 349
switchport private-vlan 349
switchport mode private-vlan 350
private-vlan 350
9.7 Настройка портов коммутатора 351
switchport mode 351
switchport trunk allowed vlan 351
switchport trunk native vlan 352

switchport access vlan 353
show interfaces switchport 353
show interfaces switchport 353
9.8 Команды настройки Voice VLAN 353
voice vlan (режим глобальной конфигурации) 354
voice vlan (режим конфигурирования интерфейса) 354
voice vlan data priority 355
show voice vlan 355
9.9 Команды настройки моста провайдера 355
Команды настройки туннелирования данных 355
dot1ad mode 356
dot1ad service 356
subscribe match untagged–pkt 358
subscribe match priority 358
subscribe match cvid 358
subscribe match cvid priority 359
subscribe match svid 359
subscribe match svid cvid 359
subscribe 359
show dot1ad service 359
show dot1ad service-subscription 359
Команды настройки туннелирования протоколов L2 361
dot1ad l2tunnel 361
no dot1ad l2tunnel 362
show dot1ad mode 362
show dot1ad l2tunnel 362
9.10 Команды настройки распределения ресурсов (IEEE 802.1p) 362
vlan port priority all 362
vlan priority 362
9.11 Команды настройки сквозного режима (ASF) 362
cut-through mode 363
show cut-through mode 363
9.12 Настройки асимметричного управления потоком 363
flowcontrol {symmetric|asymmetric} 363
flowcontrol 364
show flowcontrol 364
9.13 Настройка защищенных портов 364
switchport protected (режим глобальной конфигурации) 365
switchport protected (режим конфигурирования интерфейса) 365
show switchport protected 365
show interfaces switchport 366
9.14 Команды настройки протокола GARP 366
set garp timer join 366
set garp timer leave 367
set garp timer leaveall 367
show garp 368
9.15 Команды настройки протокола GVRP 368
set gvrp adminmode 368
set gvrp interfacemode 369
show gvrp configuration 369
show mac-address-table gmrp 370
9.16 Команды настройки управления сетевым доступом на основе портов 370
aaa authentication dot1x default 370
clear dot1x statistics 371

clear dot1x authentication-history....371
clear radius statistics....371
dot1x eapolflood....371
dot1x dynamic-vlan enable....371
dot1x guest-vlan....372
dot1x initialize....372
dot1x max-req....372
dot1x max-users....372
dot1x port-control....373
dot1x port-control all....373
dot1x mac-auth-bypass....374
dot1x re-authenticate....374
dot1x re-authentication....374
dot1x system-auth-control....375
dot1x system-auth-control monitor....375
dot1x timeout....375
dot1x unauthenticated-vlan....376
dot1x user....377
authentication enable....377
authentication order....377
authentication priority....378
authentication timer restart....378
show authentication authentication-history....379
show authentication interface....379
show authentication statistics....380
show authentication methods....380
show authentication statistics....380
clear authentication statistics....380
clear authentication authentication-history....381
show dot1x....381
show dot1x authentication-history....384
show dot1x clients....384
show dot1x users....385
9.17 Команды клиента 802.1X....385
dot1x pae....385
dot1x supplicant port-control....385
dot1x supplicant max-start....386
dot1x supplicant timeout start-period....386
dot1x supplicant timeout held-period....387
dot1x supplicant timeout auth-period....387
dot1x supplicant user....387
show dot1x statistics....387
9.18 Авторизация на основе задач....388
usergroup....388
taskgroup....388
username usergroup....389
description (режим настройки групп пользователей)....389
inherit usergroup....389
taskgroup (режим настройки групп пользователей)....390
description (режим настройки групп задач)....390
inherit taskgroup....390
task [read] [write] [debug] [execute]....390
show aaa usergroup....391
show aaa taskgroup....391

show aaa userdb 391
9.19 Команды настройки контроля шторма 391
storm-control broadcast 392
storm-control broadcast action 392
storm-control broadcast level 393
storm-control broadcast rate 393
storm-control multicast 394
storm-control multicast action 394
storm-control multicast level 395
storm-control multicast rate 395
storm-control unicast 396
storm-control unicast action 396
storm-control unicast level 397
storm-control unicast rate 397
show storm-control 398
9.20 Команды настройки установления зависимости состояния соединений 398
no link state track 398
link state group 399
link state group downstream 399
link state group upstream 399
show link state group 400
show link state group detail 400
9.21 Команды настройки LLPF 400
llpf 400
show llpf interface 400
9.22 Команды настройки MVR 401
mvr 401
mvr group 401
mvr immediate 401
mvr mode 402
mvr querytime 402
mvr type 402
mvr vlan 403
mvr vlan group 403
show mvr 403
show mvr members 403
show mvr interface 403
show mvr traffic 404
debug mvr trace 404
debug mvr packet 404
9.23 Команды настройки агрегированного интерфейса (802.3ad) 404
port-channel 405
addport 405
deleteport (режим конфигурирования интерфейса) 405
deleteport (Global Config) 405
lacp admin key 406
lacp collector max-delay 406
lacp actor admin key 406
lacp actor admin state individual 407
lacp actor admin state longtimeout 407
lacp actor admin state passive 407
lacp actor admin state 408
lacp actor port priority 408
lacp partner admin key 409

lacp partner admin state individual 409
lacp partner admin state longtimeout 409
lacp partner admin state passive 410
lacp partner port id 410
lacp partner port priority 411
lacp partner system-id 411
lacp partner system priority 411
interface lag 412
port-channel static 412
port lacpmode 412
port lacpmode enable all 413
port lacptimeout (Interface Config) 413
port lacptimeout (Global Config) 413
port-channel adminmode 414
port-channel linktrap 414
port-channel load-balance 414
port-channel local-preference 415
port-channel min-links 416
port-channel name 416
port-channel system priority 416
show hashdest 416
show lacp actor 417
show lacp partner 417
show port-channel brief 418
show port-channel 418
show port-channel system priority 419
show port-channel counters 419
clear port-channel counters 420
clear port-channel all counters 420
9.24 Команды настройки протокола VPC 420
vpc domain 420
feature vpc 421
vpc isolate-orphans 421
vpc arp-synchronize 421
peer detection enable 421
peer detection interval 422
peer-keepalive destination 422
peer-keepalive enable 423
peer-keepalive timeout 423
role priority 423
system-mac 424
system-priority 424
vpc 425
vpc peer-link 425
show running-config vpc 425
show vpc 425
show vpc brief 426
show vpc consistency-parameters 426
show vpc peer-keepalive 426
show vpc role 426
show vpc statistics 426
clear vpc statistics 426
debug vpc peer-keepalive 427
debug vpc peer-link data-message 427

debug vpc peer-link control-message async 427
debug vpc peer-link control-message bulk 427
debug vpc peer-link control-message ckpt 427
debug vpc peer detection 427
9.25 Команды настройки зеркалирования интерфейсов 428
monitor session source 428
monitor session destination 428
monitor session filter 429
monitor session mode 430
no monitor session 430
no monitor 430
show monitor session 430
show vlan remote-span 431
9.26 Команды настройки статичной MAC-фильтрации 431
macfilter 431
macfilter adddest 432
macfilter adddest all 432
macfilter addsrc 433
macfilter addsrc all 433
show mac-address-table static 433
show mac-address-table staticfiltering 434
9.27 Настройка агента DHCP-ретранслятора уровня 2 434
dhcp l2relay 434
dhcp l2relay circuit-id subscription 435
dhcp l2relay remote-id subscription 435
dhcp l2relay subscription 436
dhcp l2relay trust 436
dhcp l2relay vlan 436
dhcp l2relay remote-id vlan 437
show dhcp l2relay all 437
show dhcp l2relay circuit-id vlan 437
dhcp l2relay circuit-id vlan 437
show dhcp l2relay interface 437
show dhcp l2relay remote-id vlan 438
show dhcp l2relay stats interface 438
show dhcp l2relay subscription interface 438
show dhcp l2relay agent-option vlan 438
show dhcp l2relay vlan 438
clear dhcp l2relay statistics interface 438
9.28 Команды настройки DHCP-клиента 439
dhcp client vendor-id-option 439
dhcp client vendor-id-option-string 439
show dhcp client vendor-id-option 439
9.29 Команды настройки DHCP Snooping 439
ip dhcp snooping 439
ip dhcp snooping vlan 440
ip dhcp snooping verify mac-address 440
ip dhcp snooping database 440
ip dhcp snooping database write-delay 441
ip dhcp snooping binding 441
ip dhcp filtering trust 441
ip verify binding 441
ip dhcp snooping limit 442
ip dhcp snooping log-invalid 442

ip dhcp snooping trust....442
ip verify source....443
show ip dhcp snooping....443
show ip dhcp snooping binding....443
show ip dhcp snooping database....444
show ip dhcp snooping interfaces....444
show ip dhcp snooping statistics....444
clear ip dhcp snooping binding....445
clear ip dhcp snooping statistics....445
show ip verify source....445
show ip verify interface....445
show ip source binding....446
9.30 Команды настройки Dynamic ARP Inspection....446
ip arp inspection vlan....446
ip arp inspection validate....447
ip arp inspection vlan logging....447
ip arp inspection trust....447
ip arp inspection limit....448
ip arp inspection filter....448
arp access-list....448
permit ip host mac host....449
show ip arp inspection....449
show ip arp inspection statistics....449
clear ip arp inspection statistics....450
show ip arp inspection interfaces....450
show arp access-list....450
9.31 Команды настройки IGMP Snooping....451
set igmp....451
set igmp header-validation....452
set igmp interfacemode....452
set igmp fast-leave....452
set igmp groupmembership-interval....453
set igmp maxresponse....453
set igmp mcrtrexpiretime....454
set igmp mrouter....454
set igmp mrouter interface....455
set igmp report-suppression....455
show igmpsnooping....455
show igmpsnooping mrouter interface....457
show igmpsnooping mrouter vlan....457
show igmpsnooping ssm....457
show mac-address-table igmpsnooping....457
9.32 Команды настройки опрашивающего устройства IGMP Snooping....458
set igmp querier....458
set igmp querier query-interval....459
set igmp querier timer expiry....459
set igmp querier version....459
set igmp querier election participate....460
show igmpsnooping querier....460
9.33 Команды настройки MLD Snooping....461
set mld....461
set mld interfacemode....462
set mld fast-leave....462
set mld groupmembership-interval....463

set mld maxresponse 463
set mld mcrtexpiretime 464
set mld mrouter 464
set mld mrouter interface 464
show mldsnooping 465
show mldsnooping mrouter interface 466
show mldsnooping mrouter vlan 466
show mldsnooping ssm entries 466
show mldsnooping ssm stats 467
show mldsnooping ssm groups 467
show mac-address-table mldsnooping 467
clear mldsnooping 468
9.34 Команды настройки опрашивающего устройства MLD Snooping 468
set mld querier 468
set mld querier query_interval 469
set mld querier timer expiry 469
set mld querier election participate 469
show mldsnooping querier 470
9.35 Команды настройки Port Security 471
port-security 471
port-security max-dynamic 471
port-security max-static 472
port-security mac-address 472
port-security mac-address move 472
port-security mac-address sticky 473
mac-address-table limit 473
show port-security 474
show port-security dynamic 474
show port-security static 474
show port-security violation 475
show mac-address-table limit 475
9.36 Команды настройки протокола LLDP (802.1AB) 475
lldp transmit 475
lldp receive 476
lldp timers 476
lldp transmit-tlv 476
lldp transmit-mgmt 477
lldp notification 477
lldp notification-interval 478
clear lldp statistics 478
clear lldp remote-data 478
show lldp 478
show lldp interface 479
show lldp statistics 479
show lldp remote-device 480
show lldp remote-device detail 480
show lldp local-device 481
show lldp local-device detail 481
9.37 Команды настройки LLDP-MED 481
lldp med 482
lldp med confignotification 482
lldp med transmit-tlv 482
lldp med all 483
lldp med confignotification all 483

lldp med faststartrepeatcount 483
lldp med transmit-tlv all 483
show lldp med 483
show lldp med interface 484
show lldp med local-device detail 484
show lldp med remote-device 484
show lldp med remote-device detail 484
9.38 Команды настройки управления DoS 484
dos-control all 485
dos-control sipdip 485
dos-control firstfrag 486
dos-control tcpfrag 486
dos-control tcpflag 486
dos-control l4port 487
dos-control smacdmac 487
dos-control tcpport 487
dos-control udpport 488
dos-control tcpflagseq 488
dos-control tcpoffset 488
dos-control tcpsyn 489
dos-control tcpsynfin 489
dos-control tcpfinurgpsh 489
dos-control icmpv4 490
dos-control icmpv6 490
dos-control icmpfrag 490
show dos-control 491
9.39 Команды настройки таблиц MAC-адресов 492
bridge aging-time 492
show forwardingdb agetime 492
show mac-address-table multicast 493
show mac-address-table stats 493
9.40 Команды настройки ISDP 493
isdp run 493
isdp holdtime 494
isdp timer 494
isdp advertise-v2 494
isdp enable 494
clear isdp counters 495
clear isdp table 495
show isdp 495
show isdp interface 497
show isdp entry 497
show isdp traffic 497
debug isdp packet 498
9.41 Команды настройки протокола EFM OAM 498
ethernet oam 498
ethernet oam timeout 498
ethernet oam min-rate 499
ethernet oam max-rate 499
ethernet oam mode 499
ethernet oam remote-loopback 500
ethernet oam remote-loopback start 500
ethernet oam remote-loopback stop 500
ethernet oam link-monitor supported 500

ethernet oam link-monitor 501
ethernet oam link-monitor frame 501
ethernet oam link-monitor frame-period 501
ethernet oam link-monitor frame-seconds 502
show ethernet oam statistics 502
show ethernet oam interface 502
show ethernet oam discovery 502
show ethernet oam status 503
show ethernet oam mode 503
show ethernet oam link-monitor 503
show ethernet oam summary 503
debug dot3ah packet 503
clear ethernet oam statistics 503
loopback-test 503
9.42 Команды настройки протокола CFM 504
ethernet cfm domain 504
service vlan 504
ethernet cfm enable 505
ethernet cfm cc level vlan interval 505
ethernet cfm mep archive-hold-time 505
ethernet cfm mep level 506
ethernet cfm mep enable 507
ethernet cfm mep active 507
ethernet cfm mip level 508
ping ethernet cfm mac 508
ping ethernet cfm remote–mpid 508
traceroute ethernet cfm mac 509
traceroute ethernet cfm remote–mpid 509
show ethernet cfm domain 510
show ethernet cfm domain brief 510
show ethernet cfm maintenance-points local domain 510
show ethernet cfm maintenance-points local interface 511
show ethernet cfm errors 511
show ethernet cfm errors domain 512
show ethernet cfm errors level 513
show ethernet cfm maintenance-points remote domain 513
show ethernet cfm maintenance-points remote level 514
show ethernet cfm maintenance-points remote detail mac 514
show ethernet cfm maintenance-points remote detail mpid 515
show ethernet cfm traceroute-cache 515
show ethernet cfm statistics 515
clear ethernet cfm maintenance-points remote 516
clear ethernet cfm traceroute-cache 516
9.43 Команды настройки функций Interface Error Disable и Auto Recovery 516
errdisable recovery cause 516
errdisable recovery interval 517
show errdisable recovery 517
show interfaces status err-disabled 518
9.44 Команды настройки UDLD 518
udld enable (Global Config) 518
udld message time 518
udld timeout interval 519
udld reset 519
udld enable (Interface Config) 519

udld port 519
show udld 519
show udld 520
10 КОМАНДЫ НАСТРОЙКИ ФУНКЦИОНАЛА DATA CENTER 521
10.1 Команды настройки протокола DCBX 521
lldp dcbx version 521
lldp tlv-select dcbxp 522
lldp dcbx port-role 522
show lldp tlv-select 523
show lldp dcbx interface 523
traffic-class-group max-bandwidth 524
traffic-class-group min-bandwidth 525
traffic-class-group strict 526
traffic-class-group weight 526
show classofservice traffic-class-group 527
Расширенный выбор режима передачи и Traffic Class Group 527
classofservice traffic-class-group 527
10.2 Команды настройки FIP Snooping 528
feature fip-snooping 528
fip-snooping enable 529
fip-snooping fc-map 529
fip-snooping port-mode 530
show fip-snooping 530
show fip-snooping enode 531
show fip-snooping fcf 532
show fip-snooping sessions 533
show fip-snooping statistics 534
show fip-snooping vlan 535
clear fip-snooping statistics 536
10.3 Команды настройки управления потоком на основании приоритета 536
priority-flow-control mode 537
priority-flow-control priority 537
clear priority-flow-control statistics 538
show interface priority-flow-control 538
10.4 Команды настройки QCN 539
qcn enable 539
qcn cnm-transmit-priority 539
qcn cnpv-priority (datacenter bridging config) 540
qcn cnpv-priority alternate-priority 540
qcn cnpv-priority cp-creation 541
qcn cnpv-priority defense-mode-choice 541
qcn cnpv-priority 541
qcn cnpv-priority alternate-priority 542
qcn transmit-tlv enable 542
clear qcn statistics 543
show qcn priority 543
show qcn active priority 543
show qcn interface 544
show qcn statistics 544
11 КОМАНДЫ НАСТРОЙКИ МАРШРУТИЗАЦИИ 545
11.1 Команды настройки протокола ARP 545
arp 545
ip proxy-arp 546
ip local-proxy-arp 546

arp cachesize 546
arp dynamicrenew 547
arp purge 547
arp resptime 548
arp retries 548
arp timeout 548
clear arp-cache 549
clear arp-switch 549
show arp 549
show arp brief 550
show arp switch 550
11.2 Команды настройки IP-маршрутизации 551
routing 551
ip routing 551
ip address 551
ip address dhcp 552
ip default-gateway 552
ip load-sharing 553
ip route 554
ip route default 554
ip route distance 555
ip route net-prototype 555
ip netdirbcast 556
ip mtu 556
release dhcp 557
renew dhcp 557
renew dhcp network-port 557
renew dhcp service-port 557
encapsulation 557
show dhcp lease 557
show ip brief 558
show ip interface 558
show ip interface brief 559
show ip load-sharing 560
show ip protocols 560
show ip route 562
show ip route ecmp-groups 563
show ip route hw-failure 564
show ip route net-prototype 564
show ip route summary 564
clear ip route counters 566
show ip route preferences 566
show ip stats 567
show routing heap summary 567
11.3 Команды настройки политик маршрутизации 567
ip policy route-map 567
ip prefix-list 568
ip prefix-list description 569
ipv6 prefix-list 569
route-map 571
match as-path 571
match community 572
match ip address 572
match ip address <access-list-number | access-list-name> 573

match ipv6 address 574
match length 574
match mac-list 574
set as-path 575
set comm-list delete 575
set community 576
set interface 577
set ip next-hop 577
set ip default next-hop 577
set ip precedence 578
set ipv6 next-hop (BGP) 578
set local-preference 579
set metric (BGP) 579
show ip policy 580
show ip prefix-list 580
show ipv6 prefix-list 581
show route-map 582
clear ip prefix-list 582
clear ipv6 prefix-list 582
11.4 Команды Router Discovery Protocol 583
ip irdp 583
ip irdp address 583
ip irdp holdtime 583
ip irdp maxadvertinterval 584
ip irdp minadvertinterval 584
ip irdp multicast 584
ip irdp preference 585
show ip irdp 585
11.5 Команды настройки виртуального маршрутизатора 586
ip vrf 586
maximum routes 586
description 587
ip vrf forwarding 587
show ip vrf 587
11.6 Команды настройки маршрутизации сети VLAN 588
vlan routing 588
interface vlan 588
show ip vlan 589
11.7 Команды настройки протокола VRRP 589
ip vrrp (режим глобальной конфигурации) 589
ip vrrp (режим конфигурирования интерфейса) 589
ip vrrp mode 590
ip vrrp ip 590
ip vrrp accept-mode 591
ip vrrp authentication 591
ip vrrp preempt 591
ip vrrp priority 592
ip vrrp timers advertise 592
ip vrrp track interface 593
ip vrrp track ip route 593
show ip vrrp interface stats 594
show ip vrrp 595
show ip vrrp interface 595
show ip vrrp interface brief 596

11.8 Команды настройки протокола VRRPv3 596
fhrp version vrrp v3 596
snmp-server enable traps vrrp 597
vrrp 597
preempt 598
accept-mode 598
priority 599
timers advertise 599
shutdown 600
address 600
track interface 601
track ip route 601
clear vrrp statistics 602
show vrrp 602
show vrrp brief 603
show vrrp statistics 603
11.9 Команды настройки DHCP- и BOOTP-ретрансляторов 604
bootpdhcprelay cidoptmode 604
bootpdhcprelay maxhopcount 604
bootpdhcprelay minwaittime 604
bootpdhcprelay serverip 605
bootpdhcprelay enable 605
show bootpdhcprelay 605
show ip bootpdhcprelay 606
11.10 Команды настройки IP Helper 606
clear ip helper statistics 608
ip helper-address (глобальная конфигурация) 608
ip helper-address (конфигурирование интерфейса) 609
ip helper enable 610
show ip helper-address 610
show ip helper statistics 611
11.11 Команды настройки протокола OSPF 612
Общие команды настройки OSPF 612
router ospf 612
enable 613
network area 613
1583compatibility 613
area default-cost 614
area nssa 614
area nssa default-info-originate 614
area nssa no-redistribute 614
area nssa no-summary 615
area nssa translator-role 615
area nssa translator-stab-intv 615
area range 616
area stub 617
area stub no-summary 617
area virtual-link 617
area virtual-link authentication 618
area virtual-link dead-interval 618
area virtual-link hello-interval 619
area virtual-link retransmit-interval 619
area virtual-link transmit-delay 619
auto-cost 620

capability opaque 620
clear ip ospf 621
clear ip ospf configuration....621
clear ip ospf counters 621
clear ip ospf neighbor....621
clear ip ospf neighbor interface 621
clear ip ospf redistribution 622
default-information originate 622
default-metric....622
distance ospf 622
distribute-list out....623
exit-overflow-interval....623
external-lsdb-limit 624
log-adjacency-changes 624
prefix-suppression....624
prefix-suppression....625
router-id 625
redistribute....625
maximum-paths 626
passive-interface default....626
passive-interface 627
timers pacing flood....627
timers pacing lsa-group....627
timers spf....628
trapflags....628
Команды настройки протокола на OSPF-интерфейсе 629
ip ospf area....629
bandwidth 630
ip ospf authentication 630
ip ospf cost 631
ip ospf database-filter all out 631
ip ospf dead-interval 631
ip ospf hello-interval 632
ip ospf network 632
ip ospf prefix-suppression 632
ip ospf priority 633
ip ospf retransmit-interval 633
ip ospf transmit-delay 634
ip ospf mtu-ignore....634
Команды настройки функции IP Event Dampening 635
dampening....635
show dampening interface....635
show interface dampening....635
Команды настройки OSPF Graceful Restart 636
nsf....636
nsf restart-interval....637
nsf helper....637
nsf ietf helper disable....638
nsf helper strict-lsa-checking....638
Команды настройки функции OSPFv2 Stub Router 639
max-metric router-lsa 639
clear ip ospf stub-router....640
Команды просмотра оперативного состояния устройства для протокола OSPF 640
show ip ospf 640

show ip ospf abr 643
show ip ospf area 643
show ip ospf asbr 644
show ip ospf database 644
show ip ospf database database-summary 645
show ip ospf interface 646
show ip ospf interface brief 647
show ip ospf interface stats 647
show ip ospf lsa-group 648
show ip ospf neighbor 649
show ip ospf range 651
show ip ospf statistics 652
show ip ospf stub table 652
show ip ospf traffic 653
show ip ospf virtual-link 653
show ip ospf virtual-link brief 654
11.12 Команды настройки протокола RIP 654
router rip 654
enable (RIP) 654
ip rip 655
auto-summary 655
default-information originate (RIP) 655
default-metric (RIP) 655
distance rip 656
distribute-list out (RIP) 656
ip rip authentication 656
ip rip receive version 657
ip rip send version 657
hostroutesaccept 658
split-horizon 658
redistribute (RIP) 658
show ip rip 659
show ip rip interface brief 659
show ip rip interface 660
11.13 Команды регулирования ICMP-сообщений 660
ip unreachables 661
ip redirects 661
ipv6 redirects 661
ip icmp echo-reply 662
ip icmp error-interval 662
11.14 Команды настройки BFD 663
feature bfd 663
bfd 663
bfd echo 663
bfd interval 664
bfd slow-timer 665
ip ospf bfd 665
ip ospf bfd 665
neighbor fall-over bfd 665
show bfd neighbors 666
debug bfd event 666
debug bfd packet 667
12 КОМАНДЫ НАСТРОЙКИ IP SLA 668
Ip sla 668

Ip sla schedule 669
track ip sla 670
12.1 Команды режима конфигурации Track 671
delay 671
12.2 Команды режима конфигурации IP SLA 672
icmp-echo 672
12.3 Команды режима конфигурации IP SLA ICMP ECHO 673
frequency 673
timeout 674
threshold 675
vrf (IP SLA) 675
12.4 Команды очистки 676
clear ip sla statistics 676
12.5 Команды show 676
show ip sla configuration 676
show ip sla statistics 677
show ip route track-table 678
show ipv6 route track-table 678
show ipv6 route track-table 678
show track 678
13 КОМАНДЫ BGP 681
address-family ipv4 681
address-family ipv6 682
address-family vpnv4 unicast 682
aggregate-address 682
bgp aggregate-different-meds 684
bgp always-compare-med 684
bgp bestpath as-path ignore 685
bgp client-to-client reflection 685
bgp cluster-id 686
bgp default local-preference 687
bgp fast-external-failover 687
bgp fast-internal-failover 688
bgp listen 688
bgp log-neighbor-changes 689
bgp maxas-limit 690
bgp router-id 690
default-information originate 691
default metric 691
distance (конфигурирование BGP-маршрутизатора) 692
distance BGP 693
distribute-list prefix in 694
distribute-list prefix out 694
enable (BGP) 695
ip bgp fast-external-failover 695
ip bgp fast-external-failover 696
maximum-paths 696
maximum-paths igbp 697
neighbor activate (конфигурирование семейства адресов IPv4 VRF) 698
neighbor activate (конфигурирование семейства адресов IPv6) 698
neighbor advertisement-interval 699
neighbor connect-retry-interval 700
neighbor default-originate 700
neighbor description 702

neighbor ebgp-multihop 702
neighbor filter-list 703
neighbor filter-list (конфигурирование семейства адресов IPv6) 704
neighbor inherit peer 704
neighbor local-as 705
neighbor maximum-prefix (конфигурирование BGP-маршрутизатора) 706
neighbor next-hop-self 707
neighbor password 707
neighbor prefix-list 708
neighbor remote-as 709
neighbor remove-private-as 710
neighbor rfc5549-support 710
neighbor route-map 711
neighbor route-reflector-client (конфигурирование BGP-маршрутизатора) 711
neighbor send-community 712
neighbor send-community extended 712
neighbor shutdown 713
neighbor timers 714
neighbor update-source 715
network (конфигурирование BGP-маршрутизатора) 716
rd 716
redistribute (конфигурирование BGP-маршрутизатора) 717
route-target 718
template peer 719
address-family 720
activate 721
connect-retry-interval 721
description 722
password 722
shutdown 722
no shutdown 723
timers 723
update-source 723
timers bgp 724
timers policy-apply delay 725
clear ip bgp 725
clear ip bgp counters 726
debug ip bgp 726
show ip bgp 727
show ip bgp aggregate-address 729
show ip bgp community 729
show ip bgp community-list 729
show ip bgp extcommunity-list 730
show ip bgp listen range 730
show ip bgp neighbors 730
show ip bgp neighbors advertised-routes 733
show ip bgp neighbors policy 734
show ip bgp neighbors {received-routes | routes | rejected-routes} 735
show ip bgp route-reflection 735
show ip bgp statistics 736
show ip bgp summary 737
show ip bgp template 738
show ip bgp traffic 738
show ip bgp update-group 739

show ip bgp vpnv4 740
show bgp ipv6 742
show bgp ipv6 aggregate-address 742
show bgp ipv6 community 743
show bgp ipv6 community-list 743
show bgp ipv6 listen range 743
show bgp ipv6 neighbors advertised-routes 744
show bgp ipv6 neighbors 744
show bgp ipv6 neighbors policy 744
show bgp ipv6 route-reflection 745
show bgp ipv6 statistics 745
show bgp ipv6 summary 745
show bgp ipv6 update-group 746
13.1 Команды настройки политики маршрутизации 746
ip as-path access-list 746
ip bgp-community new-format 748
ip community-list 748
show ip as-path-access-list 749
show ip community-list 749
clear ip community-list 749
14 КОМАНДЫ УПРАВЛЕНИЯ ПРОТОКОЛОМ IPV6 750
14.1 Команды настройки управления через протокол IPv6 750
serviceport ipv6 enable 750
network ipv6 enable 750
serviceport ipv6 address 751
serviceport ipv6 gateway 752
serviceport ipv6 neighbor 752
network ipv6 address 753
network ipv6 gateway 753
network ipv6 neighbor 754
show network ipv6 neighbors 754
show serviceport ipv6 neighbors 755
ping ipv6 755
ping ipv6 interface 756
14.2 Команды настройки туннельного интерфейса 756
interface tunnel 756
tunnel source 757
tunnel destination 757
tunnel mode ipv6ip 757
show interface tunnel 757
14.3 Команды настройки loopback-интерфейса 758
interface loopback 758
show interface loopback 758
14.4 Команды IPv6-маршрутизации 759
ipv6 hop-limit 759
ipv6 unicast-routing 759
ipv6 enable 760
ipv6 address 760
ipv6 address autoconfig 761
ipv6 address dhcp 761
ipv6 route 761
ipv6 route distance 762
ipv6 route net-prototype 763
ipv6 mtu 763

ipv6 nd dad attempts 764
ipv6 nd managed-config-flag 764
ipv6 nd ns-interval 764
ipv6 nd other-config-flag 765
ipv6 nd ra-interval 765
ipv6 nd ra-lifetime 765
ipv6 nd ra hop-limit unspecified 766
ipv6 nd reachable-time 766
ipv6 nd router-preference 767
ipv6 nd suppress-ra 767
ipv6 nd prefix 767
ipv6 neighbor 768
ipv6 neighbors dynamicrenew 768
ipv6 nud 769
ipv6 prefix-list 769
no ipv6 prefix-list 770
ipv6 unreachables 771
ipv6 unresolved-traffic 771
ipv6 icmp error-interval 771
show ipv6 brief 772
show ipv6 interface 773
show ipv6 interface vlan 774
show ipv6 dhcp interface 774
show ipv6 nd raguard policy 775
show ipv6 neighbors 775
clear ipv6 neighbors 776
show ipv6 protocols 776
show ipv6 route 777
show ipv6 route ecmp-groups 778
show ipv6 route hw-failure 779
show ipv6 route net-prototype 779
show ipv6 route preferences 779
show ipv6 route summary 779
show ipv6 snooping counters 781
show ipv6 vlan 781
show ipv6 traffic 782
clear ipv6 route counters 785
clear ipv6 snooping counters 785
clear ipv6 statistics 785
14.5 Команды настройки OSPFv3 786
Команды глобальной настройки OSPFv3 786
ipv6 router ospf 786
area default-cost 786
area nssa 786
area nssa default-info-originate 786
area nssa no-redistribute 787
area nssa no-summary 787
area nssa translator-role 787
area nssa translator-stab-intv 788
area range 788
area stub 789
area stub no-summary 789
area virtual-link 789
area virtual-link dead-interval 790

area virtual-link hello-interval 790
area virtual-link retransmit-interval 790
area virtual-link transmit-delay 791
auto-cost 791
clear ipv6 ospf 792
clear ipv6 ospf configuration 792
clear ipv6 ospf counters 792
clear ipv6 ospf neighbor 792
clear ipv6 ospf neighbor interface 792
clear ipv6 ospf redistribution 793
default-information originate 793
default-metric 793
distance ospf 793
enable 794
exit-overflow-interval 794
external-lsdb-limit 795
maximum-paths 795
passive-interface default 795
passive-interface 796
redistribute 796
router-id 797
timers pacing lsa-group 797
timers throttle spf 797
trapflags 798
no trapflags 799
Команды OSPFv3-интерфейса 799
ipv6 ospf area 799
ipv6 ospf cost 799
ipv6 ospf dead-interval 800
ipv6 ospf hello-interval 800
ipv6 ospf link-lsa-suppression 801
ipv6 ospf mtu-ignore 801
ipv6 ospf network 801
ipv6 ospf prefix-suppression 802
ipv6 ospf priority 802
ipv6 ospf retransmit-interval 803
ipv6 ospf transmit-delay 803
Команды настройки Graceful Restart в OSPFv3 804
nsf 804
nsf restart-interval 804
nsf helper 805
nsf ietf helper disable 805
nsf helper strict-lsa-checking 806
clear ipv6 ospf stub-router 807
Команды просмотра оперативного состояния OSPFv3 807
show ipv6 ospf 807
show ipv6 ospf abr 810
show ipv6 ospf area 810
show ipv6 ospf asbr 811
show ipv6 ospf database 811
show ipv6 ospf database database-summary 812
show ipv6 ospf interface 813
show ipv6 ospf interface brief 814
show ipv6 ospf interface stats 815

show ipv6 ospf lsa-group 816
show ipv6 ospf max-metric 816
show ipv6 ospf neighbor 816
show ipv6 ospf range 818
show ipv6 ospf statistics 818
show ipv6 ospf stub table 819
show ipv6 ospf virtual-link 819
show ipv6 ospf virtual-link brief 820
14.6 Команды настройки DHCPv6 820
service dhcpv6 820
ipv6 dhcp client pd 820
ipv6 dhcp server 821
ipv6 dhcp relay destination 821
ipv6 dhcp pool 822
address prefix (IPv6) 822
domain-name (IPv6) 823
dns-server (IPv6) 823
prefix-delegation (IPv6) 823
show ipv6 dhcp 824
show ipv6 dhcp statistics 824
show ipv6 dhcp interface 825
show ipv6 dhcp binding 825
show ipv6 dhcp pool 826
show network ipv6 dhcp statistics 826
show serviceport ipv6 dhcp statistics 827
clear ipv6 dhcp 828
clear ipv6 dhcp binding 828
clear network ipv6 dhcp statistics 828
clear serviceport ipv6 dhcp statistics 828
14.7 Команды настройки DHCPv6 Snooping 829
ipv6 dhcp snooping 829
ipv6 dhcp snooping vlan 829
ipv6 dhcp snooping verify mac-address 829
ipv6 dhcp snooping database 830
ip dhcp snooping database write-delay 830
ipv6 dhcp snooping binding 830
ipv6 dhcp snooping trust 830
ipv6 dhcp snooping log-invalid 831
ipv6 dhcp snooping limit 831
ipv6 verify source 831
ipv6 verify binding 832
show ipv6 dhcp snooping 832
show ipv6 dhcp snooping binding 832
show ipv6 dhcp snooping database 833
show ipv6 dhcp snooping statistics 833
clear ipv6 dhcp snooping binding 833
clear ipv6 dhcp snooping statistics 834
show ipv6 verify 834
show ipv6 verify source 834
show ipv6 source binding 834
15 КОМАНДЫ НАСТРОЙКИ QUALITY OF SERVICE 836
15.1 Команды управления Class of Service 836
classofservice dot1p-mapping 836
classofservice ip-dscp-mapping 836

classofservice trust 837
cos-queue max-bandwidth 837
cos-queue min-bandwidth 838
cos-queue random-detect 838
cos-queue strict 839
random-detect 839
random-detect exponential weighting-constant 839
random-detect queue-parms 840
traffic-shape 840
show classofservice dot1p-mapping 841
show classofservice ip-dscp-mapping 841
show classofservice trust 841
show interfaces cos-queue 842
show interfaces random-detect 842
show interfaces tail-drop-threshold 843
15.2 Команды настройки Differentiated Services 843
diffserv 844
15.3 Команды настройки класса DiffServ 844
class-map 845
class-map rename 845
match ethertype 845
match access-group 846
match access-group name 846
match any 846
match class-map 846
match cos 847
match secondary-cos 847
match destination-address mac 847
match dstip 848
match dstip6 848
match dstl4port 848
match ip dscp 848
match ip precedence 849
match ip tos 849
match ip6flowlbl 850
match protocol 850
match source-address mac 850
match srcip 851
match srcip6 851
match srcl4port 851
match vlan 851
match secondary-vlan 852
15.4 Команды настройки политики DiffServ 852
assign-queue 852
drop 853
mirror 853
redirect 853
conform-color 853
class 853
mark cos 854
mark secondary-cos 854
mark cos-as-sec-cos 854
mark ip-dscp 855
mark ip-precedence 855

police-simple 855
police-single-rate 856
police-two-rate 856
policy-map 856
policy-map rename 857
15.5 Команды настройки сервисов DiffServ 857
service-policy 857
15.6 Команды просмотра оперативного состояния DiffServ 858
show class-map 858
show diffserv 859
show policy-map 859
show diffserv service 861
show diffserv service brief 862
show policy-map interface 862
show service-policy 862
15.7 Команды настройки MAC ACL 863
mac access-list extended 863
mac access-list extended rename 863
mac access-list resequence 864
{deny | permit} (MAC ACL) 864
mac access-group 866
remark 867
show mac access-lists 867
15.8 Команды настройки IP ACL 868
access-list 869
ip access-list 872
ip access-list rename 872
ip access-list resequence 873
{deny | permit} (IP ACL) 873
ip access-group 876
acl-trapflags 878
show ip access-lists 878
show access-lists 880
show access-lists vlan 880
15.9 Команды настройки IPv6 ACL 881
IPv6 access-list 881
IPv6 access-list rename 881
IPv6 access-list resequence 881
{deny | permit} (IPv6) 882
IPv6 traffic-filter 885
show IPv6 access-lists 886
15.10 Команды управления функцией Management Access Control and Administration List 887
management access-list 887
{deny | permit} (Management ACAL) 887
management access-class 888
show management access-list 888
show management access-class 888
15.11 Команды настройки временного диапазона для ACL с ограничением по времени 889
time-range 889
time-range name 889
15.12 Команды Auto-Voice over IP 890
auto-voip 890
auto-voip oui 890
auto-voip oui-based priority 891

auto-voip protocol-based 891
auto-voip vlan 892
show auto-voip 892
show auto-voip oui-table 893
15.13 Команды оптимизации iSCSI 893
iscsi aging time 893
iscsi cos 894
iscsi enable 894
iscsi target port 895
show iscsi 895
show iscsi sessions 895
16 СИСТЕМНЫЕ СООБЩЕНИЯ 896
16.1 База 896
16.2 Утилиты 898
16.3 Управление 900
16.4 Коммутация 903
16.5 Качество обслуживания 909
16.6 Маршрутизация/Маршрутизация IPv6 910
16.7 Многоадресная рассылка 913
16.8 Стекирование 914
16.9 Технологии 914
16.10 Поддержка ОС 916

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение	Описание
[ ]	В квадратных скобках в командной строке указываются необязательные параметры, но их ввод предоставляет определенные дополнительные опции.
{}	В фигурных скобках в командной строке указываются возможные обязательные параметры. Необходимо выбрать один из параметров.
«,» **«-»**	Данные знаки в описании команды используются для указания диапазонов.
«|»	Данный знак в описании команды обозначает «или».
«/»	Данный знак в описание команды указывает на значение по умолчанию.
Курсив Calibri	Курсивом Calibri указываются переменные или параметры, которые необходимо заменить соответствующим словом или строкой.
Полужирный	Полужирным шрифтом выделены примечания и предупреждения.
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.
`Courier New`	Полужирным шрифтом Courier New записаны примеры ввода команд.
`Courier New`	Шрифтом Courier New в рамке с тенью указаны результаты выполнения команд.

Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

1 ВВЕДЕНИЕ

Ethernet-коммутатор RTT-A430-48XG-4QXG обеспечивает функциональность Layer 2 и Layer 3, что позволяет использовать его в качестве средства агрегации, а также в центрах обработки данных (ЦОД). Программное обеспечение коммутатора оптимизировано для масштабирования и повышения производительности ЦОД за счет удовлетворения требований к коммутаторам уровней Top-of-Rack и End-of-Row. Также данное изделие предназначено для применения в сетях агрегации и магистральных сетях операторов связи.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Ethernet-коммутатор RTT-A430-48XG-4QXG — это высокопроизводительное устройство, оснащенные интерфейсами 10GBASE-R/1000BASE-X и 40GBASE-R и предназначенное для использования в центрах обработки данных (ЦОД) в качестве Top-of-Rack или End-of-Row коммутаторов, а также в сетях агрегации и магистральных сетях операторов связи.

Неблокируемая коммутационная матрица устройства позволяет осуществлять корректную обработку пакетов на максимальных скоростях, сохраняя при этом минимальные и предсказуемые задержки на всех типах трафика.

Схема вентиляции front-to-back обеспечивает эффективное охлаждение при использовании устройств в условиях современных ЦОД.

Коммутаторы имеет возможность горячей замены модулей питания и вентиляции, обеспечивая бесперебойность функционирования сети.

2.2 Функции коммутатора

2.2.1 *Базовые функции*

В таблице 2.1 приведен список базовых функций коммутатора, доступных для администрирования.

Таблица 2.1 – Базовые функции устройства

Защита от блокировки очереди (HOL)	Блокировка возникает в случаях перегрузки выходных портов устройства трафиком от нескольких входных портов. Это приводит к задержкам передачи данных и потере пакетов.
Поддержка сверхдлинных кадров (Jumbo frames)	Способность поддерживать передачу сверхдлинных кадров, что позволяет передавать данные меньшим числом пакетов. Это снижает объем служебной информации и, как следствие, время обработки пакетов.
Управление потоком (IEEE 802.3x)	Управление потоком позволяет соединять низкоскоростное устройство с высокоскоростным. Для предотвращения переполнения буфера низкоскоростное устройство имеет возможность отправлять пакет PAUSE, тем самым информируя высокоскоростное устройство о необходимости сделать паузу при передаче пакетов.
Работа в стеке устройств	Коммутатор поддерживает объединение нескольких устройств в стек. В этом случае коммутаторы рассматриваются как единое логическое устройство с общими настройками. Возможны две топологии построения стека – кольцо и цепочка. При этом параметры портов всех устройств, включенных в стек, можно задать с коммутатора, работающего в режиме «мастер». Стекирование устройств позволяет снизить трудоемкость управления сетью и повысить ее отказоустойчивость.

2.2.2 *Функции при работе с MAC–адресами*

В таблице 2.2 приведены функции устройств при работе с MAC–адресами.

Таблица 2.2 – Функции работы с MAC-адресами

Таблица MAC-адресов	Коммутатор составляет в памяти таблицу, в которой устанавливается соответствие между MAC-адресами и портами коммутатора.
Режим обучения	В отсутствие обучения данные, поступающие на какой-либо порт, передаются на все остальные порты коммутатора. В режиме обучения коммутатор анализирует кадры и, определив MAC-адрес отправителя, заносит его в таблицу коммутации. Впоследствии кадр Ethernet, предназначенный для хоста, MAC-адрес которого уже есть в таблице, перенаправляется на указанный в таблице порт.
Поддержка передачи на несколько MAC-адресов (MAC Multicast Support)	Данная функция позволяет устанавливать соединения «один ко многим» и «многие ко многим». Таким образом, кадр, адресованный многоадресной группе, передается на каждый порт, входящий в группу.
Автоматическое время хранения MAC-адресов (Automatic Aging for MAC Addresses)	Если от устройства с определенным MAC-адресом за определенный период времени не поступают пакеты, то запись для данного адреса устаревает и удаляется. Это позволяет поддерживать таблицу коммутации в актуальном состоянии.

2.2.3 *Функции второго уровня сетевой модели OSI*

В таблице 2.3 приведены функции и особенности *второго уровня (уровень 2 OSI)*

Таблица 2.3 – Описание функций второго уровня (уровень 2 OSI)

Функция IGMP Snooping	Реализация протокола IGMP позволяет на основе информации, полученной при анализе содержимого IGMP-пакетов, определить, какие устройства в сети участвуют в группах многоадресной рассылки, и адресовать трафик на соответствующие порты.
Функция MLD Snooping	Реализация протокола MLD позволяет устройству минимизировать многоадресный IPv6-трафик.
Функция MVR	Функция, позволяющая перенаправлять многоадресный трафик из одной VLAN в другую на основании IGMP-сообщений, что позволяет уменьшить нагрузку на uplink-порту. Применяется в решениях Triple Play.
Защита от «шторма» (Broadcast, multicast, unknown unicast Storm Control)	«Шторм» — это размножение broadcast-, multicast-, unknown unicast-пакетов в каждом узле, которое приводит к лавинообразному росту их числа и парализует работу сети. Коммутаторы имеют функцию, позволяющую ограничить скорость передачи многоадресных и широковещательных кадров, принятых и переданных коммутатором.
Зеркалирование портов (Port Mirroring)	Зеркалирование портов позволяет дублировать трафик наблюдаемых портов, пересылая входящие и/или исходящие пакеты на контролирующий порт. У пользователя коммутатора есть возможность задать контролирующий и контролируемые порты и выбрать тип трафика (входящий и/или исходящий), который будет передан на контролирующий порт.
Изоляция портов (Protected ports)	Данная функция позволяет создать изолированную группу портов, которые могут обмениваться трафиком только друг с другом. За пределы группы трафик выйти не может.

Поддержка Private VLAN	Технология Private VLAN (PVLAN) позволяет производить разграничение трафика на втором уровне модели OSI между портами коммутатора, которые находятся в одном широковещательном домене.
Поддержка протокола STP (Spanning Tree Protocol)	Spanning Tree Protocol — сетевой протокол, основной задачей которого является приведение сети Ethernet с избыточными соединениями к древовидной топологии, исключающей петли. Коммутаторы обмениваются конфигурационными сообщениями, используя кадры специального формата, на основе которых включают и отключают передачу трафика через порты.
Поддержка протокола RSTP (IEEE 802.1w Rapid spanning tree protocol)	Rapid (быстрый) STP (RSTP) – является усовершенствованием протокола STP, характеризуется меньшим временем приведения сети к древовидной топологии.
Поддержка протокола MSTP (IEEE 802.1w Rapid spanning tree protocol)	Протокол Multiple Spanning Tree Protocol (MSTP) – является усовершенствованием протокола RSTP, который позволяет настраивать отдельное связующее дерево для отдельных VLAN или групп VLAN.
Поддержка протокола PVSTP (Per-VLAN Spanning Tree protocol)	Per-VLAN Spanning Tree protocol (PVSTP) – является усовершенствованием протокола STP, позволяющий запускать отдельные экземпляры протокола STP в отдельных VLAN.
Поддержка VLAN	VLAN – это виртуальная группа портов коммутатора, образующих один широковещательный домен. Коммутатор поддерживает различные средства классификации пакетов для определения их принадлежности к определенной VLAN.
Поддержка 802.1Q	IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. Позволяет использовать несколько групп VLAN на одном порту.
Поддержка протокола OAM (Operation, Administration, and Maintenance, IEEE 802.3ah)	Ethernet OAM (Operation, Administration, and Maintenance), IEEE 802.3ah – функции уровня канала передачи данных представляют собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah.
Поддержка GVRP (GARP VLAN)	Протокол регистрации GARP VLAN обеспечивает динамическое добавление/удаление групп VLAN на портах коммутатора. Если включен протокол GVRP, коммутатор определяет, а затем распространяет данные о принадлежности к VLAN на все порты, являющиеся частью активной топологии.
Поддержка VLAN на основе физических портов (Port-Based VLAN)	Функция позволяет назначить пакету метку VLAN на основе физического порта, с которого он был принят.
Создание групп LAG	В устройствах поддерживается функция создания групп каналов. Агрегация каналов (Link aggregation, trunking) – технология объединения нескольких физических каналов в один логический. Это способствует не только увеличению пропускной способности магистральных каналов коммутатор–коммутатор или коммутатор–сервер, но и повышению их надежности. Возможны варианты балансировки трафика на основе MAC-адресов, IP-адресов, VLAN, TCP/UDP-портов. Группа LAG состоит из портов с одинаковой скоростью, работающих в дуплексном режиме.
Объединение каналов с использованием LACP	Протокол LACP (IEEE 802.3ad) обеспечивает автоматическое объединение нескольких физических портов коммутатора в единый канал передачи данных. В протоколе постоянно определяется возможность объединения каналов, и, в случае отказа порта, входящего в объединенный канал, его трафик автоматически перераспределяется по не отказавшим компонентам объединенного канала.

Поддержка Auto Voice VLAN	Предоставляет возможность идентифицировать голосовой трафик на основании OUI (Organizationally Unique Identifier – первые 24 бита MAC-адреса) либо L4-порта. Если в MAC-таблице коммутатора присутствует MAC-адрес с OUI голосового шлюза или же IP-телефона, то данный порт автоматически добавляется в voice vlan (идентификация по протоколу SIP или же по MAC-адресу получателя не поддерживается).
Dot1ad	Реализация QinQ-туннелей, согласно которой трафик, идущий от пользователя в сеть провайдера, тегируется двумя VLAN-тегами. Внутренним тегом является пользовательский тег (C-tag), а внешним – провайдерский (S-tag).

2.2.4 *Функции третьего уровня сетевой модели OSI*

В таблице 2.4 приведены функции третьего уровня (уровень 3 OSI)

Таблица 2.4 – Описание функций третьего уровня (Layer 3)

Клиенты BootP и DHCP (Dynamic Host Configuration Protocol)	Устройства способны автоматически получать IP-адрес по протоколу BootP/ DHCP.
Статические IP-маршруты	Администратор коммутатора имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Протокол ARP (Address Resolution Protocol)	ARP – протокол сопоставления IP-адреса и физического адреса устройства. Соответствие устанавливается на основе анализа ответа от узла сети, адрес узла запрашивается в широковещательном пакете.
Протокол RIP (Routing Information Protocol)	Протокол динамической маршрутизации, который позволяет маршрутизаторам обновлять маршрутную информацию, получая ее от соседних маршрутизаторов. В задачи протокола входит определение оптимального маршрута на основании данных о количестве промежуточных узлов.
Протокол OSPF	Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.
Протокол VRRP	Протокол VRRP предназначен для резервирования маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения IP-интерфейсов группы маршрутизаторов в один виртуальный, который будет использоваться как шлюз по умолчанию для компьютеров в сети.
BFD (Bidirectional Forwarding Detection)	Протокол BFD обеспечивает двунаправленную связность между маршрутизаторами, которые могут отстоять друг от друга более чем на один хоп. BFD имеет очень низкое время (гибко настраиваемое) определения неисправности канала связи и, как следствие, быстрое переключение на резервный маршрут.
Протокол BGP	BGP (Border Gateway Protocol, протокол граничного шлюза) — протокол динамической маршрутизации, относящийся к классу протоколов маршрутизации внешнего шлюза. Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами, то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие автономные системы.

2.2.5 *Функции QoS*

В таблице 2.5 приведены основные функции качества обслуживания (Quality of Service)

Таблица 2.5 – Основные функции качества обслуживания

Поддержка приоритетных очередей	Устройство поддерживает приоритизацию исходящего трафика по очередям на каждом порту. Распределение пакетов по очередям может производиться в результате классификации пакетов по различным полям в заголовках пакетов.
Поддержка класса обслуживания 802.1p	Стандарт 802.1p специфицирует метод указания приоритета кадра и алгоритм использования приоритета в целях своевременной доставки чувствительного к временным задержкам трафика. Стандарт 802.1p определяет восемь уровней приоритетов. Коммутаторы могут использовать значение приоритета 802.1p для распределения кадров по приоритетным очередям.

2.2.6 *Функции обеспечения безопасности*

Таблица 2.6 – Функции обеспечения безопасности

DHCP snooping	Функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Обеспечивает фильтрацию DHCP-сообщений, поступивших с ненадежных портов путем построения и поддержания базы данных привязки DHCP (DHCP snooping binding database). DHCP snooping выполняет действия брандмауэра между ненадежными портами и серверами DHCP.
UDP relay	Перенаправление широковещательного UDP-трафика на указанный IP-адрес.
Функции DHCP-сервера	DHCP-сервер осуществляет централизованное управление сетевыми адресами и соответствующими конфигурационными параметрами, автоматически предоставляя их клиентам.
IP Source address guard	Функция коммутатора, которая ограничивает IP-трафик, фильтруя его на основании таблицы соответствий IP- и MAC-адресов в базе данных DHCP snooping либо статически сконфигурированных связок. Функция используется для борьбы с подменой IP-адресов.
Dynamic ARP Inspection (Protection)	Функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Сообщение, которое поступает с ненадежного порта, подвергается проверке – соответствует ли IP-адрес в теле принятого ARP-пакета IP-адресу отправителя. Если адреса не совпадают, то коммутатор отбрасывает пакет.
L2 – L3 – L4 ACL (Access Control List)	На основе информации, содержащейся в заголовках уровней 2, 3 и 4, у администратора есть возможность настроить политики, согласно которым пакет будет обработан либо отброшен.
Time-Based ACL	Позволяет сконфигурировать временные рамки, в течение которых данный ACL будет действовать.
Port Security	Функция коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт. После этого порт передает пакеты, если MAC-адрес отправителя не указан как разрешенный.
Проверка подлинности на основе порта (802.1x)	Проверка подлинности IEEE 802.1x представляет собой механизм контроля доступа к ресурсам через внешний сервер. Прошедшие проверку подлинности пользователи получают доступ к ресурсам сети.

2.2.7 *Функции управления коммутатором*

Таблица 2.7 – Основные функции управления коммутаторами

Загрузка и выгрузка файла конфигурации	Параметры устройства сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства.

Протокол TFTP (Trivial File Transfer Protocol)	Протокол TFTP используется для операций записи и чтения файлов. Протокол основан на транспортном протоколе UDP. Устройства поддерживают загрузку и выгрузку по данному протоколу файлов конфигурации и образов программного обеспечения.
Протокол SCP (Secure Copy)	Протокол SCP используется для операций записи и чтения файлов. Протокол основан на сетевом протоколе SSH. Устройства поддерживают загрузку и передачу по данному протоколу файлов настройки и образов программного обеспечения.
Протокол FTP (File Transfer Protocol)	Протокол FTP используется для операций записи и чтения файлов. Протокол основан на транспортном протоколе TCP. Устройства поддерживают загрузку и выгрузку по данному протоколу файлов конфигурации и образов программного обеспечения.
Протокол SFTP (SSH File Transfer Protocol)	SFTP – протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения. Устройства поддерживают загрузку и выгрузку по данному протоколу файлов конфигурации и образов программного обеспечения.
Удаленный мониторинг (RMON)	Удаленный мониторинг (RMON) – средство мониторинга компьютерных сетей, расширение SNMP. Совместимые устройства позволяют собирать диагностические данные с помощью станции управления сетью. RMON – это стандартная база MIB, в которой определены текущая и предыдущая статистика уровня MAC и объекты управления, предоставляющие данные в реальном времени.
Протокол SNMP	Протокол SNMP используется для мониторинга и управления сетевым устройством. Он состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.
Интерфейс командной строки (CLI)	Управление коммутаторами посредством CLI осуществляется локально через последовательный порт RS-232, либо удаленно через Telnet/SSH. Интерфейс командной строки консоли (CLI) является промышленным стандартом. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению объема вводимых данных.
Syslog	Syslog – протокол, обеспечивающий передачу сообщений о происходящих в системе событиях, а также уведомлений об ошибках удаленным серверам.
SNTP (Simple Network Time Protocol)	Протокол SNTP – протокол синхронизации времени. Гарантирует точность синхронизации времени сетевого устройства с сервером до миллисекунды.
Traceroute	Traceroute – служебная функция, предназначенная для определения маршрутов передачи данных в IP-сетях.
Управление контролируемым доступом – уровни привилегий	Администратор может определить уровни привилегий доступа для пользователей устройства и характеристики для каждого уровня привилегий (только для чтения – 1 уровень, полный доступ – 15 уровень).
Блокировка интерфейса управления	Коммутатор способен устанавливать запрет доступа к каждому интерфейсу управления (SNMP, CLI). Запрет может быть установлен отдельно для каждого интерфейса доступа: Telnet (CLI over Telnet Session) Secure Shell (CLI over SSH) TFTP HTTP HTTPS SNMP SNTP
Локальная аутентификация	Для локальной аутентификации поддерживается хранение паролей в базе данных коммутатора.

Клиент RADIUS	Протокол RADIUS используется для аутентификации, авторизации и учета. Сервер RADIUS использует базу данных пользователей, которая содержит данные проверки подлинности для каждого пользователя. Коммутаторы содержат клиентскую часть протокола RADIUS.
TACACS+ (Terminal Access Controller Access Control System)	Устройство предоставляет поддержку проверки подлинности клиентов посредством протокола TACACS+. Протокол TACACS+ обеспечивает централизованную систему безопасности для проверки пользователей, получающих доступ к устройству, а также централизованную систему управления при соблюдении совместимости с RADIUS и другими процессами проверки подлинности.
Сервер SSH	Функция сервера SSH позволяет клиенту SSH установить с устройством защищенное соединение для управления им.
Поддержка макрокоманд	Данная функция предоставляет возможность создавать макрокоманды, представляющие собой набор команд, и применять их для конфигурации устройства.

2.2.8 *Функции ЦОД*

Таблица 2.8 – Основные функции для центров обработки данных

FIP Snooping	Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) – это функция безопасности, предназначенная для предотвращения неавторизованного доступа и передачи данных в сетях Fibre Channel (FC). Функция фильтрует трафик, разрешая только те серверы хранения данных, которые имеют на это право.
LLDP DCBX	Протокол Data Center Bridging Exchange (DCBX) используется устройствам для обмена конфигурационной информацией с напрямую подключенными узлами. Является расширением протокола LLDP.
PFC (Priority Flow Control)	Функция Priority-based flow control (PFC) предоставляет средства для приостановки трафика определенного приоритета (802.1p) при наступлении переполнения (congestion) в исходящей очереди.
QCN (Quantized Congestion Notification)	Стандарт 802.1Qau решает проблему переполнения исходящих очередей с помощью протокола Quantized Congestion Notification (QCN). Коммутаторы постоянно анализируют загрузку своих исходящих очередей. Когда размер очереди превышает определённый порог и продолжает увеличиваться, коммутатор отправляет источнику трафика с определённой частотой специальные служебные сообщения.
ETS (Enhanced Transmission Selection)	Данный протокол предоставляет возможность гибкой настройки полосы пропускания для трафика определённого приоритета.
Cut-Through	Режим Cut-Through позволяет коммутатору начать пересылку пакета еще до того, как его приём был полностью завершён. Это позволяет сократить задержки при пересылке больших и сверхбольших пакетов.

2.2.9 *Дополнительные функции*

В таблице 2.9 приведены дополнительные функции устройства.

Таблица 2.9 – Дополнительные функции устройства

Виртуальное тестирование кабеля (VCT)	Сетевые коммутаторы имеют в своём составе программные и аппаратные средства, позволяющие выполнять функции виртуального тестера кабеля – VCT. Тестер позволяет определить состояние медного кабеля связи.
Диагностика оптического трансивера	Устройство позволяет тестировать оптический трансивер (DDM). При тестировании отслеживаются такие параметры, как ток и напряжение питания, температура трансивера, мощность сигнала. Для реализации требуется поддержка этих функций в трансивере.

2.3 Основные технические характеристики

Основные технические параметры коммутаторов приведены в таблице 2.10.

Таблица 2.10 – Основные технические характеристики

Общие параметры	
Интерфейсы	1 × 10/100/1000BASE-T (OOB) 48 × 10GBASE-R (SFP+)/1000BASE-X (SFP) 4 × 40GBASE-SR4/LR4 (QSFP+) 1 × USB 2.0 1 × Консольный порт RS-232 (RJ-45)
Пропускная способность	1,28 Тбит/с
Производительность на пакетах длиной 64 байта[1]	943,5 MPPS
Объем буферной памяти	9 МБ
Объем ОЗУ (DDR3)	4 ГБ
Объем ПЗУ (SATA SSD)	8 ГБ
Таблица MAC-адресов	131072
Количество ARP-записей	6144
Таблица VLAN	4094
Количество групп L2 Multicast	2048
Количество правил SQinQ	4090
Количество правил ACL	1023 входных, 1023 выходных
Количество ACL	100
Количество правил ACL в одном ACL	1023
Количество IPv4 Unicast-маршрутов	8200
Количество IPv6 Unicast-маршрутов[2]	4096
Количество VRRP-маршрутизаторов	128
Количество VRF	64 (включая VRF по умолчанию)
Количество L3-интерфейсов	256

[1] Значения указаны для односторонней передачи.

[2] Маршруты IPv4/IPv6 Unicast/Multicast используют общие аппаратные ресурсы.

Максимальное количество OSPF соседств	1
Максимальное количество BGP соседств	208
Количество виртуальных Loopback-интерфейсов	64
Агрегация каналов (LAG)	64, до 32 портов в каждом LAG
Количество экземпляров MSTP	64
Количество экземпляров PVSTP/RPVSTP	256
Количество DHCP pool	128, всего 4096 IP-адресов
Качество обслуживания QoS	7 очередей
Сверхдлинные кадры (jumbo frames)	12270 байт
Стекирование	До 8 юнитов
Соответствие стандартам	IEEE 802.3ac IEEE 802.3ad – агрегация каналов IEEE 802.3ae – 10 GbE IEEE 802.1ak – MRP IEEE 802.1S – множество связующих деревьев (MST) IEEE 802.1W – быстрое связующее дерево (RSTP) IEEE 802.1D – связующее дерево (STP) IEEE 802.1Qat – MSRP IEEE 802.1Qav – Time-Sensetive Streams IEEE 801.1Qbb IEEE 802.1v – классификация VLAN IEEE 802.1p – приоритизация трафика IEEE 802.1X IEEE 802.3x – Flow Control IEEE 802.1AB – LLDP IEEE 802.1Qbb – Priority-based Flow Control IEEE 802.1ad – Double VLAN tagging IEEE 802.1ag – Connectivity Fault Management (CFM) IEEE 802.3ah – Operations, Administration, and Maintenance (OAM) IEEE 802.1Qau – Congestion Notification IEEE 802.1Qaz – Enhanced Transmission Selection (ETS)
Управление	
Локальное управление	Console
Удаленное управление	Telnet, SSH, SNMP, Netconf, HTTP/HTTPS
Физические характеристики и условия окружающей среды	
Источники питания	Сеть переменного тока: 220 В +- 20 %, В, 50 Гц Сеть постоянного тока: 36 – 72 В Варианты питания: - один источник питания постоянного или переменного тока; - два источника питания постоянного или переменного тока, с возможностью горячей замены
Макс. потребляемая мощность	Не более 160 Вт
Тепловыделение	Не более 160 Вт
Пусковые токи	AC: RTT-PS220-12-350, 45 А, 5.5 мс DC: RTT-PS048-12-350, 320 А, 0.14 мс

Габариты (Ш × В × Г)	440 × 425 × 44 мм
Рабочая температура	От 0 до 45 °С
Температура хранения	От -40 до +70 °С
Относительная влажность при эксплуатации	Не более 80 % (без образования конденсата)
Максимальный уровень акустического шума	С передней панели, max < 62,4 дБ С задней панели, max < 69,8 дБ
Срок службы	10 лет

2.4 Конструктивное исполнение

В данном разделе описано конструктивное исполнение коммутатора, представлены изображения передней, задней и боковых панелей устройства, описаны разъемы, светодиодные индикаторы и органы управления.

Коммутатор выполнен в металлическом корпусе с возможностью установки в 19” каркас, высота корпуса 1U.

2.4.1 *Внешний вид и описание передней панели*

Внешний вид передней панели коммутатора приведен на рисунке (*Рисунок 1*).

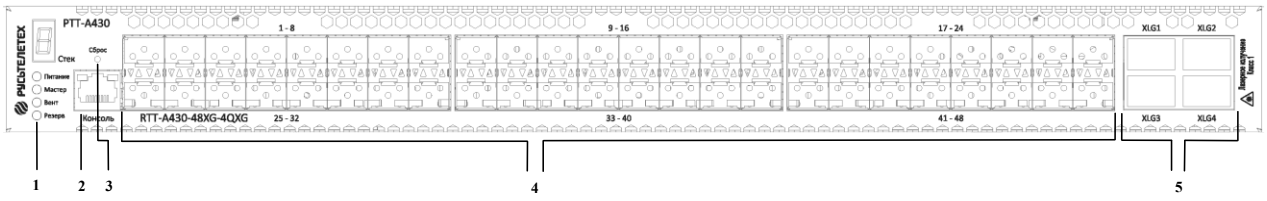

Рисунок 1 – Передняя панель

В таблице (Таблица 2.11) приведен перечень разъемов, светодиодных индикаторов и органов управления, расположенных на передней панели коммутатора.

Таблица 2.11 – Описание разъемов, индикаторов и органов управления передней панели

№	Элемент передней панели	Описание
1	Стек	Индикатор номера устройства в стеке
	Питание	Индикатор питания устройства
	Мастер	Индикатор режима работы устройства (ведущий/ведомый)
	Вент.	Индикатор работы вентиляторов
	Резерв	Индикатор резервного электропитания

2	Консоль	Консольный порт для локального управления устройством. Распиновка разъема следующая: 1 не используется 2 не используется 3 RX 4 GND 5 GND 6 TX 7 не используется 8 не используется 9 не используется
3	Сброс	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: - при нажатии на кнопку длительностью менее 10 с происходит перезагрузка устройства; - при нажатии на кнопку длительностью более 10 с происходит сброс настроек устройства до заводской конфигурации.
4	[1-48]	Слоты для установки трансиверов 10G SFP+/ 1G SFP.
5	XLG1, XLG2 XLG3, XLG4	Слоты XLG1-XLG4 для установки трансиверов 40G QSFP+.

2.4.2 *Внешний вид и описание задней панели*

Внешний вид задней панели коммутатора приведен на рисунке (*Рисунок 2*).

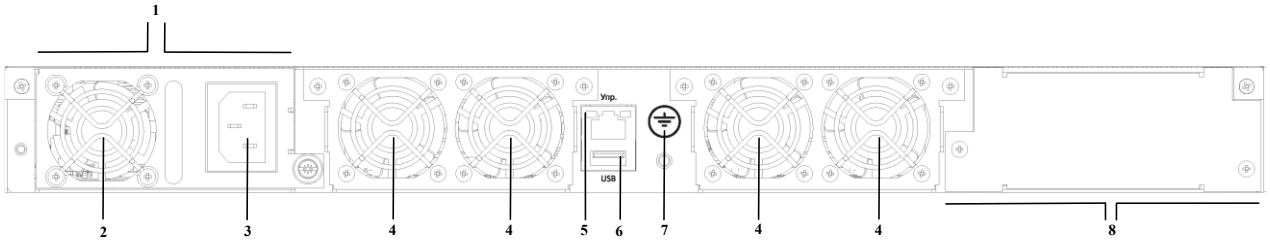

Рисунок 2 – Задняя панель

В таблице приведен перечень разъемов, расположенных на задней панели коммутатора.

Таблица 2.12 – Описание разъемов задней панели коммутатора

№	Элемент задней панели	Описание
1		Источник питания RTT-PS220-12-350
2		Вентилятор источника питания
3	~220 VAC 50 Hz max 3.5A	Разъем для подключения к источнику электропитания переменного тока.
4	Съемные вентиляторы	Съемные вентиляционные модули с возможностью горячей замены
5	Упр.	Порт (out-of-band) 10/100/1000BASE-T (RJ-45) для удаленного управления устройством. Управление осуществляется по сети, изолированной от канала передачи данных.
6	USB	USB-порт
7	Клемма заземления ⏚	Клемма для заземления устройства

8		Слот для резервного источника питания

2.4.3 *Внешний вид и описание боковых панелей*

Внешний вид боковых панелей коммутатора приведен на рисунках (*Рисунок 3*, *Рисунок 4*).

Рисунок 3 – Правая боковая панель

Рисунок 4 – Левая боковая панель

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. Рекомендации по установке устройства приведены в разделе «Установка и подключение».

2.4.4 *Световая индикация*

Состояние интерфейсов Ethernet индицируется двумя светодиодными индикаторами, *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение светодиодов показано на рисунках (*Рисунок 5*, *Рисунок 6*).

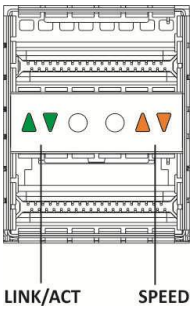

Рисунок 5 – Внешний вид разъема QSFP+

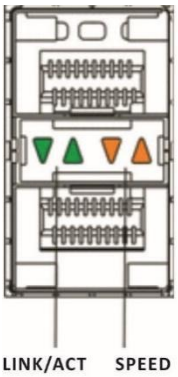

Рисунок 6 – Внешний вид разъема SFP/SFP+

Таблица 2.13 – Световая индикация состояния XLG-портов

Свечение индикатора SPEED	*Свечение индикатора LINK/ACT*	*Состояние интерфейса Ethernet*
Выключен	Выключен	Порт выключен или соединение не установлено
Горит постоянно	Горит постоянно	Установлено соединение на скорости 40/10 Гбит/с
Горит постоянно	Мигание	Идет передача данных

Таблица 2.14 – Световая индикация состояния XG-портов

Свечение индикатора SPEED	*Свечение индикатора LINK/ACT*	*Состояние интерфейса Ethernet*
Выключен	Выключен	Порт выключен или соединение не установлено
Выключен	Горит постоянно	Установлено соединение на скорости 1 Гбит/с
Горит постоянно	Горит постоянно	Установлено соединение на скорости 10 Гбит/с
X	Мигание	Идет передача данных

Индикатор *Стек ID* (1-8) служит для обозначения номера устройства в стеке.

Системные индикаторы (Питание, Мастер, Вент., Резерв) служат для определения состояния работы узлов коммутатора.

Таблица 2.15 – Световая индикация системных индикаторов

Название индикатора	**Функция индикатора**	**Состояние индикатора**	**Состояние устройства**
Питание	Состояние источников питания	Выключен	Питание выключено
		Зеленый, горит постоянно	Питание включено, штатная работа устройства
Мастер	Признак ведущего устройства при работе в стеке	Зеленый, горит постоянно	Устройство является «мастером» стека
		Выключен	Устройство не является «мастером» в стеке или не задан режим стекирования
Вент.	Состояние вентилятора охлаждения	Зеленый, горит постоянно	Все вентиляторы исправны
		Красный, горит постоянно	Отказ одного или более вентиляторов
Резерв	Режим работы резервного источника питания	Зеленый, горит постоянно	Резервный источник подключен и работает в штатном режиме
		Красный, горит постоянно	Отсутствие первичного питания резервного источника либо его неисправность, либо отказ вентилятора.
		Выключен	Резервный источник не подключен

2.5 Комплект поставки

В базовый комплект поставки входят:

- Ethernet-коммутатор;
- Комплект крепежа в стойку;
- Памятка о документации;
- Сертификат соответствия;
- Паспорт.

По заказу покупателя в комплект поставки опционально могут быть включены:

- Руководство по эксплуатации на CD-диске (опционально);
- Консольный кабель;
- Модуль питания RTT-PS220-12-350;
- Шнур питания Евровилка-C13 1.8м (в случае комплектации модулем питания);
- Модуль питания RTT-PS048-12-350;
- Шнур питания ПВС 2х1.5 2м (в случае комплектации модулем питания RTT-PS048-12-350);
- SFP/SFP+/QSFP+/QSFP28 трансиверы.

3 УСТАНОВКА И ПОДКЛЮЧЕНИЕ

В данном разделе описаны процедуры установки оборудования в стойку и подключения к питающей сети.

3.1 Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. Для установки кронштейнов:

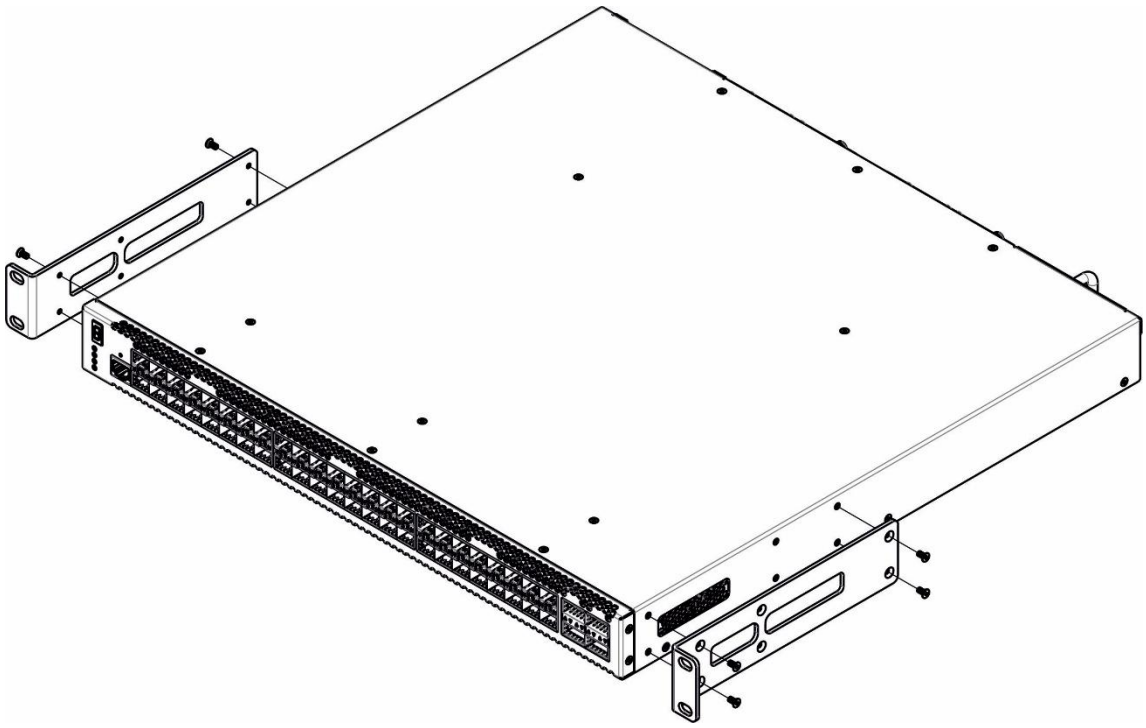

Рисунок 7 – Крепление кронштейнов

1. Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства.
2. С помощью отвертки прикрепите кронштейн винтами к корпусу.
3. Повторите действия 1, 2 для второго кронштейна.

3.2 Установка устройства в стойку

Для установки устройства в стойку:

1. Приложите устройство к вертикальным направляющим стойки.
2. Совместите отверстия кронштейнов с отверстиями на направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки, для того чтобы устройство располагалось горизонтально.
3. С помощью отвертки прикрепите коммутатор к стойке винтами.

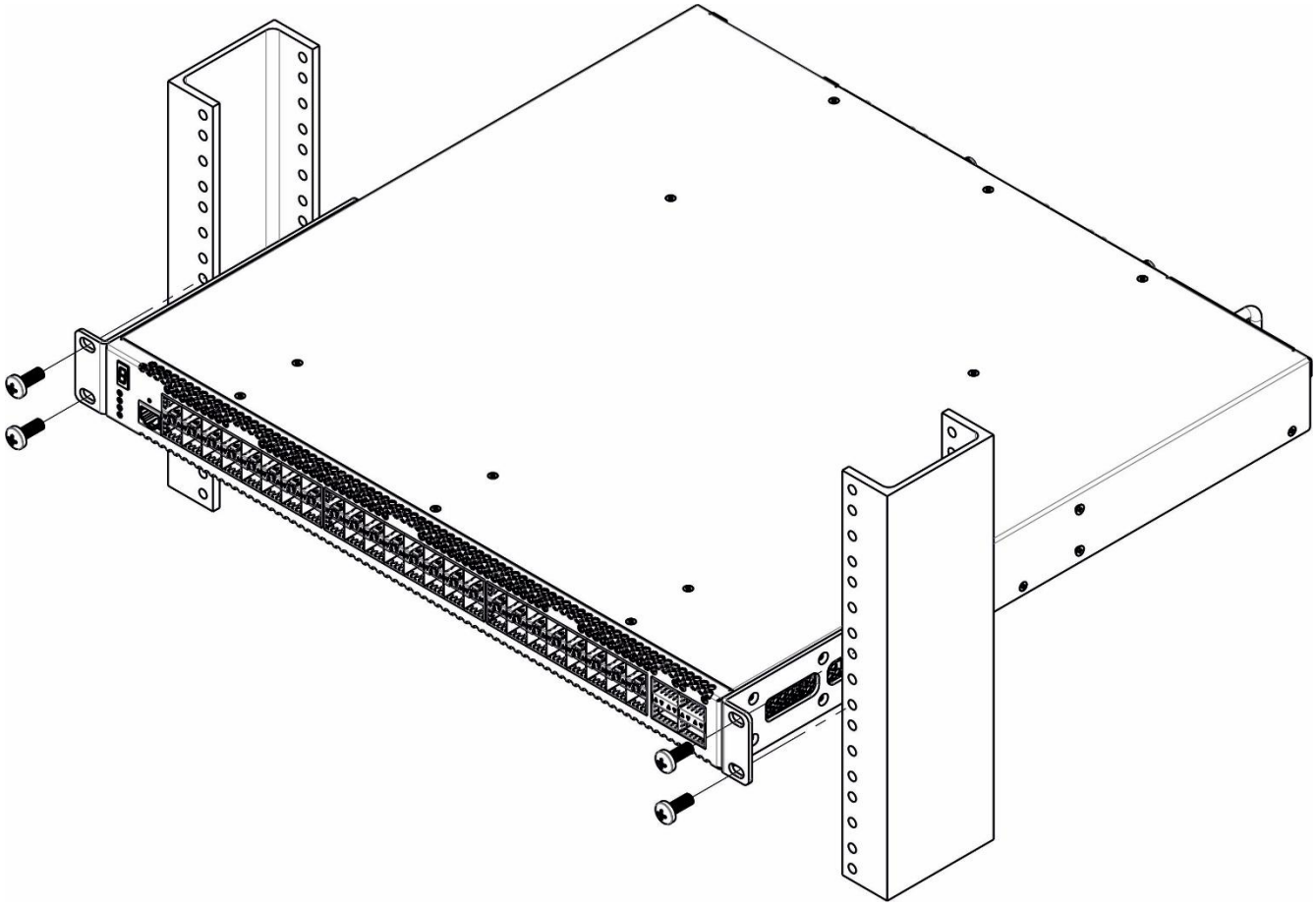

Рисунок 8 – Установка устройства в стойку

На рисунке 9 приведен пример размещения коммутатора в стойке.

Рисунок 9 – Размещение коммутатора в стойке

Не закрывайте вентиляционные отверстия, а также вентиляторы, расположенные на задней панели, посторонними предметами во избежание перегрева компонентов коммутатора и нарушения его работы.

3.3 Установка модулей питания

Коммутатор может работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Места для установки модулей питания с электрической точки зрения равноценны. С точки зрения устройства, модуль питания, находящийся слева (если смотреть на заднюю стенку коммутатора), считается основным, справа – резервным. Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания коммутатор продолжает работу без перезапуска.

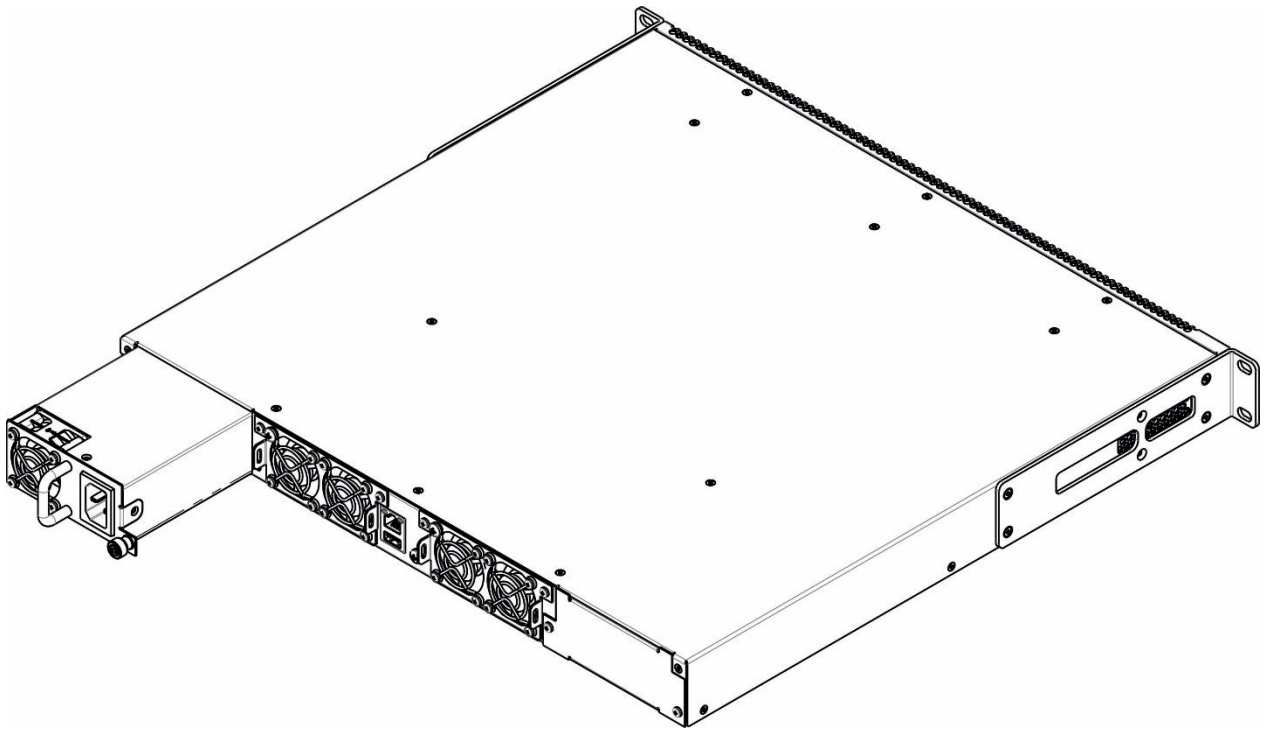

Рисунок 10 – Установка модулей питания

Состояние модулей питания может быть проверено по индикации на передней панели коммутатора (см. раздел **Световая индикация**) или по диагностике, доступной через интерфейсы управления коммутатором.

Индикация аварии модуля питания может быть вызвана не только отказом модуля, но и отсутствием первичного питания.

3.4 Подключение питающей сети

1. Прежде чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиям ПУЭ.

Подключение должно осуществляться квалифицированным специалистом.

2. Если предполагается подключение компьютера или иного оборудования к консольному порту коммутатора, это оборудование также должно быть надежно заземлено.
3. Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока либо от сети постоянного тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. При подключении к сети постоянного тока используйте провод сечением не менее 1 мм^2 и соблюдайте полярность, указанную на блоке питания.

Во избежание возникновения короткого замыкания при подключении к сети постоянного тока рекомендуется произвести зачистку провода на длину 9 мм.

Цепь питания постоянным током должна содержать устройство отключения питания с физическим разъединением соединения (выключатель, разъем, контактор, автоматический выключатель и т. п.).

4. Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

3.5 Установка и удаление SFP-трансиверов

Установка оптических модулей может производиться как при выключенном, так и при включенном устройстве.

1. Вставьте верхний SFP-модуль в слот открытой частью разъема вниз, а нижний SFP-модуль открытой частью разъема вверх.

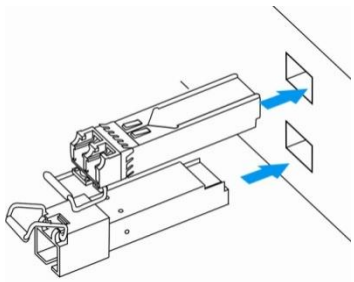

Рисунок 11 – Установка SFP-трансиверов

2. Надавите на модуль. Когда он встанет на место, вы услышите характерный щелчок.

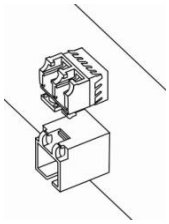

Рисунок 12 – Установленные SFP-трансиверы

Для удаления трансивера:

1. Откройте защелку модуля.

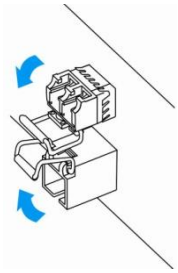

Рисунок 13 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

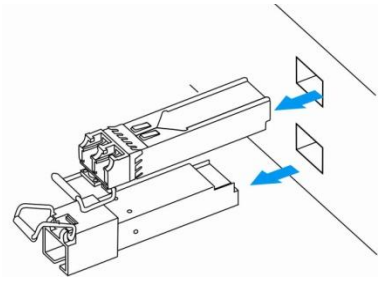

Рисунок 14 – Извлечение SFP-трансиверов

4 НАЧАЛЬНАЯ НАСТРОЙКА КОММУТАТОРА

4.1 Настройка терминала

На компьютере запустить программу эмуляции терминала (HyperTerminal, TeraTerm, Minicom) и произвести следующие настройки:

- выбрать соответствующий последовательный порт;
- установить скорость передачи данных — 115200 бод;
- задать формат данных: 8 бит данных, 1 стоповый бит, без контроля четности;
- отключить аппаратное и программное управление потоком данных;
- задать режим эмуляции терминала VT100 (многие терминальные программы используют данный режим эмуляции терминала в качестве режима по умолчанию).

4.2 Включение устройства

Установить соединение консоли коммутатора (порт «Console») с разъемом последовательного интерфейса компьютера, на котором установлено программное обеспечение эмуляции терминала.

Включить устройство. При каждом включении коммутатора запускается процедура тестирования системы при включении, которая позволяет определить работоспособность устройства перед загрузкой исполняемой программы в оперативную память (ОЗУ).

Отображение хода выполнения процедуры тестирования системы:

```
Stopping network: OK
Saving random seed... done.
Unloading kernel modules: OK
Stopping logging: OK
umount: /: not mounted.
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
[78648.185579] reboot: Restarting system

Booting Rusteletech RTT-A430-48XG-4QXG BIOS version 3.5...


U-Boot RTT-A430-48XG-4QXG (Mar 31 2021 - 12:59:35 +0700)

CPU: x86_64, device 406d8h
DRAM:  4 GiB
SF: Detected MX25L12805 with page size 256 Bytes, erase size 64 KiB, total 16 MiB
Model: RTT-A430-48XG-4QXG
SF: Detected MX25L12805 with page size 256 Bytes, erase size 64 KiB, total 16 MiB
Loading FPGA image: ..............................OK.
SF: Detected MX25L12805 with page size 256 Bytes, erase size 64 KiB, total 16 MiB
SCSI:  scanning bus for devices...
  Device 0: (1:0) Vendor: ATA Prod.: 8GB SATA Flash D Rev: SFPS
            Type: Hard Disk
            Capacity: 7641.2 MB = 7.4 GB (15649200 x 512)
Found 1 device(s).
Net:   eth0: e1000#0
Autoboot in 5 seconds
```

Через 5 секунд после завершения процедуры проверки начинается автозагрузка программного обеспечения коммутатора.

После успешной загрузки коммутатора появится системное приглашение интерфейса командной строки CLI.

```
 Applying Global configuration, please wait ...

Applying Interface configuration, please wait ...



User Name:admin
Password:
console>enable

console#
```

Пользователь по умолчанию «admin», пароля нет. Пароль для пользователя «admin» можно настроить, но удалить данного пользователя нельзя. Пароль для привилегированного режима по умолчанию отсутствует.

Для быстрого вызова справки о доступных командах используйте комбинацию клавиш *<Shift>* и *<?>*.

5 ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ (CLI)

Интерфейс командной строки (Command Line Interface, CLI) – это средство для управления и мониторинга системы, основанное на текстовых командах. Вы можете получить доступ к CLI с помощью прямого подключения через последовательный интерфейс либо с помощью удаленного логического подключения с использованием Telnet или SSH.

В данном разделе описаны синтаксис CLI, условные обозначения и режимы.

5.1 Синтаксис команд

Команда – одно или несколько слов, которые могут сопровождаться одним или несколькими параметрами. Параметры могут быть обязательными и опциональными.

Некоторые команды, как, например, `show network` или `clear vlan`, не требуют параметров. Другие команды, как `network parms`, требуют ввода значений после команды. Значения параметров необходимо вводить в определенном порядке: сначала обязательные, затем опциональные параметры. Так, следующий пример описывает синтаксис команды `network parms`:

`network parms` **ipaddr netmask** *[gateway]*

`network parms` имя команды.

`ipaddr` и `netmask` — обязательные параметры, представляющие собой значения, которые необходимо ввести после введения ключевых слов команды.

`[gateway]` — опциональный параметр, который не является необходимым для выполнения команды.

Справочник команд CLI содержит список команд (упорядоченный по имени команды) и предоставляет краткое описание каждой команды. В описании каждой команды также содержится следующая информация:

- «Формат» — ключевые слова команды, а также обязательные и опциональные параметры.
- «Режим ввода команд» — режим ввода команд, в котором появляется доступ к данной команде.
- «Значение по умолчанию» — значение конфигурируемых настроек по умолчанию (если есть) на данном устройстве.

Описание команд `show` также содержит указание на информацию, выводимую каждой такой командой.

5.2 Условные обозначения в описании команд

Параметры команды могут включать в себя обязательные и опциональные значения, а также список ключевых слов. Параметры вводятся в определенном порядке. Таблица 5.1 описывает условные обозначения, используемые в этом документе для различия между типами значений.

Таблица 5.1 – Условные обозначения параметров

Символ	***Пример***	***Описание***
[] квадратные скобки	`[value]`	Опциональный параметр.
параметр, написанный курсивом.	`value` или `[value]`	Переменное значение. Вместо текста курсивом и скобок необходимо ввести соответствующее значение (имя или число).
{} фигурные скобки	`{choice1 | choice2}`	Требуется выбрать параметр из списка вариантов.
| Вертикальная черта	`choice1 | choice2`	Взаимоисключающие варианты.
[{}] Фигурные скобки в квадратных	`[{choice1 | choice2}]`	Выбор опционального элемента из предложенных.

5.3 Общие значения параметров

Значения параметров могут быть именами (последовательностями букв) или числами. При использовании пробела в качестве части параметра следует заключить значение в двойные кавычки. Например, система будет учитывать пробелы, если вы используете выражение “System Name with Spaces”. Задание пользователем пустых последовательностей (““) недопустимо. Таблица 5.2 описывает общие значения параметров и правила задания формата значений.

Таблица 5.2 – Описание параметров

Параметр	***Описание***
ipaddr	Допустимый IP-адрес. IP-адрес может быть задан следующими способами: `a` (32 бит) `a.b` (8.24 бит) `a.b.c` (8.8.16 бит) `a.b.c.d` (8.8.8.8) Помимо вышеперечисленных форматов CLI допускает десятичный, шестнадцатеричный и восьмеричный форматы ввода (где n – любое действительное шестнадцатеричное, восьмеричное или десятичное число), осуществляемые следующим образом: `0x`n (CLI предполагает шестнадцатеричный формат); `0`n (CLI предполагает восьмеричный формат с ведущими нулями); n (CLI предполагает десятичный формат).
ipv6-address	`FE80:0000:0000:0000:020F:24FF:FEBF:DBCB`,или `FE80:0:0:0:20F:24FF:FEBF:DBCB`,или `FE80::20F24FF:FEBF:DBCB`,или `FE80:0:0:0:20F:24FF:128:141:49:32`
Интерфейс или `unit/slot/port`	Допустимые номера слота и порта, разделенные косой чертой. Например, 0/1 означает номер слота 0 и номер порта 1.
Логический интерфейс	Логический номер слота и порта. Применимо для агрегированного интерфейса (LAG). Логические unit/slot/port могут использоваться для конфигурирования агрегированного интерфейса.

Последовательности символов	Двойные кавычки используются для оформления последовательности символов, например, “System Name with Spaces”. Пустая последовательность (“”) недопустима.

5.4 Unit/slot/port, правила именования

Программное обеспечение обращается к физическим объектам (карты и порты), используя правило именования `unit/slot/port`. ПО также использует это сокращение для идентификации определенных логических объектов, таких как логический интерфейс агрегированного типа.

Номер слота может использоваться двумя способами. При обращении к физическому порту он идентифицирует карту, содержащую порты. При обращении к логическому порту и порту CPU он также идентифицирует тип интерфейса или порта.

Таблица 5.3 – Типы слотов

Тип слота	*Описание*
Номера физических слотов	Номера физических слотов начинаются с нуля и присваиваются до достижения максимального количества физических слотов.
Номера логических слотов	Логические слоты следуют за физическими слотами и идентифицируют логический агрегированный интерфейс (LAG) или интерфейсы маршрутизаторов. Значение номера логического слота зависит от типа логического интерфейса и может различаться в зависимости от платформы.
Номера слотов CPU	Слоты CPU следуют сразу за логическими слотами.

Порт определяет либо физический порт устройства, либо логический интерфейс, управление которым осуществляется в данном слоте.

Таблица 5.4 – Типы портов

Тип порта	*Описание*
Физические порты	Физические порты для каждого слота последовательно пронумерованы, начиная с единицы. Так, порт 1 на слоте 0 (внутренний порт) для коммутатора в автономном режиме (вне стека) – 1/0/1, порт 2 – 1/0/2, порт 3 – 1/0/3 и т. д.
Логические интерфейсы	Интерфейсы группы агрегации каналов (Link Aggregation Group, LAG) – логические интерфейсы, которые используются только для функций коммутации трафика. Например, LAG 1 = 0/3/1, LAG 2 = 0/3/2 и т.д. Интерфейсы маршрутизации VLAN используются только для функций маршрутизации. Loopback-интерфейсы – логические интерфейсы, которые всегда включены. Туннельные интерфейсы – логические двухточечные (p2p) соединения, которые пропускают инкапсулированные пакеты.
Порты CPU	Порты CPU обрабатываются драйвером как один или несколько физических объектов, расположенных на физических слотах.

CLI не использует формат unit/slot/port для loopback- и туннельных интерфейсов. Чтобы задать loopback-интерфейс, используйте loopback-идентификатор. Чтобы задать туннельный интерфейс – туннельный идентификатор.

5.5 Использование отрицательной формы команд

Ключевое слово no представляет собой отрицательную форму существующей команды и не является самостоятельной командой. Почти у каждой команды конфигурации есть отрицательная форма. В основном она используется, чтобы отменить действие команды или вернуться к значению по умолчанию. Например, команда конфигурации `no shutdown` отменяет завершение работы интерфейса. Используйте команду без ключевого слова no для повторного включения отключенной опции или активации опции, отключенной по умолчанию. Отрицательная форма доступна только для команд конфигурации.

5.6 Выполнение команд show

Все команды просмотра оперативного состояния устройства (команды `show`) выполняются в любом режиме конфигурации (режимы глобальной конфигурации, конфигурирования интерфейса, конфигурирования VLAN и т. д.). Команды show предоставляют информацию о системе и особенностях конкретной конфигурации, ее состоянии и статистике. Ранее команды `show` были доступны только в пользовательском или привилегированном режимах.

5.7 Фильтрация вывода данных CLI

Многие show-команды CLI выводят значительные объемы данных, что может осложнить поиск желаемой информации. Функция «Фильтрация вывода данных CLI» позволяет пользователю при выполнении команд CLI `show display` дополнительно определить параметры фильтрации выходных данных с целью выведения только необходимой информации. Суть состоит в том, чтобы уменьшить объемы выводимых на дисплей данных и упростить поиск интересующей пользователя информации.

Основные функции фильтрации вывода данных CLI:

- Управление постраничным выводом
  - Поддержка включения/отключения постраничного вывода данных для всех команд просмотра CLI. Когда функция отключена, производится вывод всей совокупности данных. Когда функция включена, вывод данных на экран идёт постранично, для просмотра дальнейшей информации требуется нажать клавишу. В конце каждой страницы отображается --More-- (Дальше) или (q)uit (Q, выход).
  - При включенном постраничном выводе: нажмите клавишу Enter, чтобы продвинуться по одной строке; нажмите «q» или «Q», чтобы отменить постраничный вывод; нажмите любую другую клавишу, чтобы перейти на следующую страницу. Изменить эти клавиши нельзя.

Некоторые команды show уже поддерживают функцию постраничного вывода, некоторые – нет, и она применима не ко всем командам.

- Фильтрация вывода данных
  - Управление отображением данных по принципу grep для вывода желаемой информации.

- Отфильтровать отображаемые данные, включив только строки, содержащие заданную последовательность.
- Отфильтровать отображаемые данные, исключив строки, содержащие заданную последовательность.
- Отфильтровать отображаемые данные, включив только строки, включающие в себя заданную последовательность, и все, следующие за ними.
- Отфильтровать отображаемые данные, включив заданный раздел содержимого вывода (например, “interface 0/1”) с конфигурируемым ограничителем.
- При нахождении последовательности регистр не учитывается.
- Включенный постраничный вывод также применяется к фильтрации выходных данных.

5.8 Модули программного обеспечения

ПО состоит из множества независимых друг от друга модулей, которые можно компоновать в произвольной комбинации для разработки передовых продуктов уровней 2/3/4+. Команды и режимы ввода команд, доступные на вашем коммутаторе, зависят от установленных модулей. Кроме того, для некоторых show-команд поля вывода могут меняться в зависимости от модулей, включенных в конкретную сборку.

Комплект программного обеспечения включает следующие модули:

- Коммутация (уровень 2);
- Маршрутизация (уровень 3);
- IPv6-маршрутизация;
- Multicast (мультикаст, мультивещание);
- BGP-4;
- Качество обслуживания (QoS);
- Управление (CLI, Web UI и SNMP);
- IPv6-управление — позволяет управлять устройством через протокол IPv6 (не требует наличия модуля IPv6-маршрутизации в системе). Адрес управления IPv6 может быть привязан к сетевому порту (порты передней панели коммутатора), интерфейсу VLAN и служебному порту;
- Metro;
- Стекирование;
- Центр обработки и хранения данных (DataCenter);
- Secure Management (безопасное управление).

Некоторые модули недоступны для некоторых платформ или версий программного обеспечения.

5.9 Режим ввода команд

Команды CLI сгруппированы по режимам ввода в соответствии с функцией команды. Каждый из режимов ввода команд поддерживает определенные команды программного обеспечения. Команды того или иного режима будут недоступны, пока вы не переключитесь на этот режим, за исключением команд пользовательского режима. Команды пользовательского режима выполняются и в привилегированном режиме.

В каждом режиме подсказки командной строки изменяются, чтобы помочь вам определить текущий режим. Таблица 5.5 содержит режимы ввода команд и подсказки, видимые в этих режимах.

Режимы ввода команд, доступные на вашем коммутаторе, зависят от установленных модулей ПО. Например, коммутатор, который не поддерживает BGPv4, не имеет режима ввода команд BGPv4-маршрутизатора.

Таблица 5.5 – Командные режимы CLI

Режим ввода команд	***Подсказка***	***Описание режима***
Пользовательский режим	`Switch>`	Содержит ограниченный набор команд для просмотра базовой информации о системе.
Привилегированный режим	`Switch#`	Позволяет выполнить любую команду пользовательского/привилегированного режима, войти в режим VLAN или в режим глобальной конфигурации
Режим глобальной конфигурации	`Switch (Config)#`	Объединяет общие команды установки и позволяет вносить изменения в текущую конфигурацию.
Режим конфигурации VLAN	`Switch (Vlan)#`	Объединяет все команды VLAN.

Режим конфигурирования интерфейса	`Switch (Interface` *`unit/slot/ port`*`)#`
	`Switch (Interface Loopback id)#`
	`Switch (Interface Tunnel id)#`
	`Switch (Interface unit/slot/port (startrange)-unit/slot/ port(endrange)#`
	`Switch (Interface lag` *`lag-intf-num`*`)#`
	`Switch (Interface vlan` *`vlan-id`*`)#`
		Управляет работой интерфейса и обеспечивает доступ к командам конфигурирования интерфейса коммутатора.
		Используйте этот режим, чтобы настроить физический порт для операций через логическое соединение.
		Также этот режим используется для настройки диапазона интерфейсов. Подсказка может отобразиться так:
		Switch (Interface 1/0/1-1/0/4) #
		Вход в режим конфигурирования интерфейса LAG для заданного LAG.
		Вход в режим конфигурирования интерфейса маршрутизации VLAN для заданного идентификатора VLAN.

Line Console	`Switch (config-line)#`	Содержит команды конфигурирования настроек исходящего трафика Telnet и интерфейса консоли, а также настройки аутентификации

		пользователя при входе/запуске консоли.
Line SSH	`Switch (config-ssh)#`	Содержит команды конфигурирования аутентификации при входе/включении SSH.
Line Telnet	`Switch (config-telnet)#`	Содержит команды конфигурирования аутентификации при входе/включении Telnet.
Конфигурирование пользователя IAS AAA	`Switch (Config-IAS-User)#`	Позволяет сконфигурировать пароль для пользователя в базе данных IAS.
Конфигурирование почтового сервера	`Switch (Mail-Server)#`	Позволяет сконфигурировать сервер электронной почты.
Конфигурирование Policy Map	`Switch (Config-policy-map)#`	Содержит команды конфигурирования QoS Policy-Map.
Конфигурирование Policy Class	`Switch (Config-policy-class-map)#`	Состоит из команд создания класса, удаления и соответствия. Команды соответствия класса задают L2, L3 и общие критерии соответствия.
Конфигурирование Class Map	`Switch (Config-class-map)#`	Содержит команды конфигурирования карты класса QoS для IPv4.
Конфигурирование Ipv6_Class-Map	`Switch (Config-class-map)#`	Содержит команды конфигурирования карты класса QoS для IPv6.
Конфигурирование OSPF маршр.	`Switch (Config-router)#`	Содержит команды конфигурирования OSPF.
Конфигурирование OSPFv3 маршр.	`Switch (Config rtr)#`	Содержит команды конфигурирования OSPFv3.
Конфигурирование RIP маршр.	`Switch (Config-router)#`	Содержит команды конфигурирования RIP.
Конфигурирование BGP маршр.	`Switch (Config-router)#`	Содержит команды конфигурирования BGP4.
Конфигурирование маршрутной карты	`Switch (config-route-map)#`	Содержит команды конфигурирования маршрутной карты.
Конфигурирование семейства адресов IPv6	`Switch (Config-router-af)#`	Содержит команды конфигурирования семейства IPv6-адресов.
Конфигурирование шаблона узла сети (Peer Template)	`(Config-rtr-tmplt)#`	Содержит команды конфигурирования шаблона BGP-узла.
Конфигурирование динамической авторизации RADIUS	`(Config-radius-da)`	Содержит команды динамической авторизации RADIUS.
Конфигурирование MAC Access-list	`Switch (Config-mac-access-list)#`	Позволяет создавать ACL MAC и использовать команды конфигурирования списка доступа MAC.
Конфигурирование IPv4 Access-list	`Switch (Config-ipv4-acl)#`	Позволяет создавать именованный или расширенный список доступа

		IPv4 и использовать команды конфигурации списка доступа IPv4.
Конфигурирование IPv6Access-list	`Switch (Config-ipv6-acl)#`	Позволяет создавать список доступа IPv6 и использовать команды конфигурации списка доступа IPv6.
Конфигурирование списка доступа управления (Management Access-list)	`Switch (config-macal)#`	Позволяет создавать список доступа управления и использовать команды конфигурации списка доступа управления.
Конфигурирование TACACS	`Switch (Tacacs)#`	Содержит команды конфигурации свойств TACACS-серверов
Режим конфигурирования группы пользователей	`Switch (config-usergroup)`	Содержит команды группы пользователей.
Режим конфигурирования группы заданий	`Switch (config-taskgroup)`	Содержит команды группы заданий.
Конфигурирование пула DHCP (DHCP Pool)	`Switch (Config dhcp-pool)#`	Содержит команды конфигурирования пула IP-адреса сервера DHCP.
Конфигурирование пула DHCPv6	`Switch (Config dhcp6-pool)#`	Содержит команды конфигурирования пула адресов IPv6 сервера DHCPv6.
Режим глобальной конфигурации стека	`Switch (Config stack)#`	Позволяет получать доступ к режиму глобальной конфигурации стека.
Режим конфигурирования списка доступа ARP	`Switch (Config-arp-access-list)#`	Содержит команды для добавления правил в список доступа ARP.
Режим поддержки (Support Mode)	`Switch (Support)#`	Позволяет получить доступ к командам поддержки, которые должны использоваться только персоналом технической поддержки производителя, поскольку неправильное использование может вызвать сбой системы и/или аннулировать гарантию продукта.

Таблица 5.6 объясняет, как войти/выйти из любого режима. Чтобы выйти из режима и возвратиться к предыдущему режиму, введите “exit”. Чтобы перейти к привилегированному режиму, используйте сочетание клавиш Ctrl+Z.

Нажатие Ctrl+Z позволяет перейти из привилегированного режима в пользовательский режим. Чтобы выйти из пользовательского режима, воспользуйтесь "выходом из системы".

Таблица 5.6 – Режимы ввода команд CLI (Доступ и выход)

Режим ввода команд	***Как получить доступ***
Пользовательский режим	Это первый уровень доступа.
Привилегированный режим	В пользовательском режиме введите: `enable`.
Режим глобальной конфигурации	В привилегированном режиме введите: `configure`.
Конфигурация VLAN	В привилегированном режиме введите: `vlan database`.

Конфигурация интерфейса	В режиме глобальной конфигурации введите:
	`interface unit/slot/port or`
	`interface loopback id or`
	`interface tunnel id`
	`interface unit/slot/port(startrange)-unit/slot/port(endrange)`
	`interface lag lag-intf-num`
	`interface vlan vlan-id`

Line Console	В режиме глобальной конфигурации введите: `line console`.
Line SSH	В режиме глобальной конфигурации введите: `line ssh`.
Line Telnet	В режиме глобальной конфигурации введите: `line telnet`.
AAA IAS User Config	В режиме глобальной конфигурации введите: `aaa ias-user username name`.
Конфигурация почтового сервера	В режиме глобальной конфигурации введите: `mail-server address`.
Конфигурация Policy-Map	В режиме глобальной конфигурации введите: `policy-map`.
Конфигурация Policy-Class-Map	В режиме глобальной конфигурации введите `class-map`, и укажите дополнительное ключевое слово **`ipv4`**, чтобы задать протокол уровня 3 для этого класса.
VPC	В режиме глобальной конфигурации введите `vpc`.
Конфигурация Ipv6-Class-Map	В режиме глобальной конфигурации введите `class-map` и укажите дополнительное ключевое слово **`ipv6`** чтобы задать протокол уровня 3 для этого класса.
Конфигурация OSPF маршр.	В режиме глобальной конфигурации введите: `router ospf`.
Конфигурация OSPFv3 маршр.	В режиме глобальной конфигурации введите: `ipv6 router ospf`.
Конфигурация RIP маршр.	В режиме глобальной конфигурации введите: `router rip`.
Конфигурация BGP маршр.	В режиме глобальной конфигурации введите: `router bgp`.
Конфигурация карты маршрутизации	В режиме глобальной конфигурации введите: `route-map map-tag`.
Конфигурация семейства адресов IPv6	В режиме конфигурирования BGP маршрутизатора введите: `address-family ipv6`.
Конфигурация шаблона узла	В режиме конфигурирования BGP маршрутизатора введите: `template peer name` для создания шаблона BGP-узла.

Конфигурация MAC Access-list	В режиме глобальной конфигурации введите: `mac access-list extended name.`
Конфигурация IPv4 Access-list	В режиме глобальной конфигурации введите: `ip access-list name.`
Конфигурация IPv6 Access-list	В режиме глобальной конфигурации введите: `ipv6 access-list name.`
Конфигурация Management Access-list	В режиме глобальной конфигурации введите: `management access-list name.`
Конфигурация TACACS	В режиме глобальной конфигурации введите: `tacacs-server host ip-addr`, где ip-addr – IP- адрес сервера TACACS вашей сети.
Режим конфигурации пользовательской группы	В режиме глобальной конфигурации введите: `usergroup <usergroup-name>.`
Режим конфигурации группы заданий	В режиме глобальной конфигурации введите: `taskgroup <taskgroup-name>.`
Конфигурация пула DHCP	В режиме глобальной конфигурации введите: `ip dhcp pool pool-name.`
Конфигурация пула DHCPv6	В режиме глобальной конфигурации введите: `ip dhcpv6 pool pool-name.`
Режим глобальной конфигурации стека	В режиме глобальной конфигурации введите: `stack.`
Режим конфигурации ARP Access-List	В режиме глобальной конфигурации введите: `arp access-list.`
Режим поддержки	В привилегированном режиме введите: `support.` **Команда** `support`**доступна только при выполненной команде** `techsupport enable.`

5.10 Автоматическое дополнение и сокращение команд

Автоматическое дополнение команды завершает ее ввод, когда введено достаточное количество букв для однозначной идентификации ключевого слова команды. Как только набрано достаточное количество символов, нажмите клавишу пробел (SPACEBAR) или клавишу Tab, чтобы дополнить слово до его полной формы.

Сокращенные команды могут быть выполнены, когда введено достаточное количество символов для однозначной идентификации команды. Нужно ввести все необходимые ключевые слова и параметры перед отправкой команды на исполнение (нажатием клавиши Enter).

5.11 Сообщения об ошибках в командном интерфейсе

Сообщение об ошибке появляется в случае введения команды, которую система не может выполнить. Таблица 5.7 описывает наиболее распространенные сообщения об ошибках в CLI.

Таблица 5.7 – Сообщения об ошибках в командном интерфейсе

Текст сообщения	***Описание***
`% Invalid input detected at '^' marker.`	Команда введена неверно или невыполнима.Знак (^) показывает, где был введен недопустимый текст. Также это сообщение появляется, если распознаны не все параметры или значения.
`Command not found/ Incomplete command. Use ? to list commands.`	Не введены требуемые ключевые слова или значения.
`Ambiguous command`	Не введено достаточное количество знаков для однозначной идентификации команды.

5.12 Правила редактирования командной строки

Таблица 5.8 содержит сочетания клавиш, которые можно использовать для редактирования команд или увеличения скорости ввода команды. Получить доступ к данному списку возможно через CLI, введя `help` в пользовательском или привилегированном режиме.

Таблица 5.8 – Правила редактирования командной строки

Сочетание клавиш	***Описание***
DEL or Backspace	Удалить предыдущий символ.
Ctrl-A	Вернуться к началу строки.
Ctrl-E	Вернуться к концу строки.
Ctrl-F	Продвинуться вперед на один символ.
Ctrl-B	Продвинуться назад на один символ.
Ctrl-D	Удалить данный символ.
Ctrl-U, X	Удалить начало строки до символа.
Ctrl-K	Удалить конец строки после символа.
Ctrl-W	Удалить предыдущее слово.
Ctrl-T	Переместить предыдущий символ.
Ctrl-P	Перейти к предыдущей строке в истории команд.
Ctrl-R	Перезаписать или вставить строку.
Ctrl-N	Перейти к следующей строке в истории команд.
Ctrl-Y	Ввести последний удаленный символ.
Ctrl-Q	Включить последовательный поток.
Ctrl-S	Выключить последовательный поток.
Ctrl-Z	Возврат к корневому режиму CLI.
Tab, <SPACE>	Дополнить команду.
Exit	Переход к предыдущему режиму конфигурирования CLI.
?	Вывести список доступных команд, ключевых слов или параметров.

5.13 Использование справки командного интерфейса

Введите вопросительный знак (?) в поле командной строки для отображения команд, доступных в текущем режиме.

```
(switch) >?

enable                        Enter into user privilege mode.
help                          Display help for various special keys.
logout                        Exit this session. Any unsaved changes are lost.
password                      Change an existing user’s password.
ping                          Send ICMP echo packets to a specified IP address.
quit                          Exit this session. Any unsaved changes are lost.
show                          Display Switch Options and Settings.
telnet                        Telnet to a remote host.
```

Введите вопросительный знак (?) после любого введенного слова, чтобы отобразить доступные ключевые слова и параметры команды.

```
(switch) #network ?

ipv6                          Configure IPv6 parameters for system network.
javamode                      Enable/Disable.
mac-address                   Configure MAC Address.
mac-type                      Select the locally administered or burnedin MAC address.
mgmt_vlan                     Configure the Management VLAN ID of the switch.
parms                         Configure Network Parameters of the device.
protocol                      Select DHCP, BootP, or None as the network config protocol.
```

Если при выводе справки параметр указан в угловых скобках, необходимо заменить данный параметр значением.

```
(Routing) #network parms ?

<ipaddr>                      Enter the IP Address.
none                          Reset IP address and gateway on management interface
```

Если нет никаких дополнительных ключевых слов или параметров команды, либо дополнительные параметры необязательны, появляется следующее сообщение:

```
<cr>                      Press Enter to execute the command
```

Вы можете также ввести вопросительный знак (?) после набора одной или более букв слова, чтобы отобразить список доступных команд или параметров, начинающихся с этих букв, как показано ниже:

```
(switch) #show m?

mac                           mac-addr-table                mac-address-table
mail-server                   mbuf                          monitor
```

5.14 Доступ к командному интерфейсу

Получить доступ к CLI можно с помощью прямого подключения через консоль или с помощью соединения через Telnet или SSH с устройства удаленного управления.

При первом подключении используйте прямое подключение к порту консоли. Нельзя получить удаленный доступ к системе, пока она не имеет IP-адрес, маску подсети и шлюз по умолчанию.

Установить информацию о конфигурации сети можно вручную или сконфигурировав систему для приема этих настроек с сервера BOOTP или DHCP в вашей сети. Для получения дополнительной информации см. раздел "Команды настройки интерфейса удалённого управления".

5.15 Программное управление кнопкой F

reset-button enable

Программное включение кнопки F. Удерживанием кнопки F в течении 10 секунд можно произвести сброс конфигурации устройства к заводским настройкам.

Значение по умолчанию	Включено
Формат	`reset-button enable`
Режим ввода команды	Режим глобальной конфигурации

reset-button disable

Программное отключение кнопки F.

Значение по умолчанию	Выключено
Формат	`reset-button disnable`
Режим ввода команды	Режим глобальной конфигурации

no reset-button

Программно активировать кнопку F.

Формат	`no reset-button`
Режим ввода команд	Привилегированный режим

reset-button reload-only

Программное отключение кнопки F. Перезагрузка произойдет после отжатия кнопки или по прошествии 10 секунд. Конфигурация останется без изменений.

Значение по умолчанию	Выключено
Формат	`reset-button reload-only`
Режим ввода команды	Режим глобальной конфигурации

no reset-button

Программно активировать кнопку F.

Формат	`no reset-button`
Режим ввода команд	Привилегированный режим

6 КОМАНДЫ БАЗОВОЙ РАБОТЫ СИСТЕМЫ

В этой главе описываются команды работы с системой и настройками мониторинга, доступные в CLI.

Команды этого раздела делятся на 2 функциональные группы:

- **Команды просмотра оперативного состояния (команды show) отображают настройки коммутации, статистику и другую информацию.**
- **Команды конфигурации настраивают функции и параметры коммутатора. Каждой команде конфигурации соответствует команда show, которая показывает настройки конфигурации.**

6.1 Команды автоматической установки

Функция автоматической установки (AutoInstall) позволяет автоматически обновлять образ ПО и конфигурацию коммутатора. Она дает возможность производить автоматическое обновление ПО и загрузку конфигурации коммутатора без участия пользователя либо с минимальным участием.

Автоматическая установка включает в себя следующие возможности:

- Загрузка образа ПО с TFTP-сервера с использованием DHCP-опции 125. В результате обновления образа программное обеспечение коммутатора может быть обновлено либо возвращено к более ранней версии.
- Автоматическая загрузка файла конфигурации с TFTP-сервера при загрузке коммутатора без сохраненного в постоянной памяти файла конфигурации.
- Автоматическая загрузка образа ПО с TFTP-сервера в следующих случаях:
  - если при загрузке коммутатора не найдена сохраненная конфигурация;
  - при загрузке коммутатора, в сохраненной конфигурации которого включена функция автоматического обновления.

Если при загрузке коммутатора не найден файл конфигурации, выполняется попытка получить IP-адрес от DHCP-сервера сети. Ответ от DHCP-сервера включает в себя IP-адрес TFTP-сервера, где хранится образ ПО и файлы конфигурации.

После получения от DHCP-сервера IP-адреса и сопутствующей информации коммутатор загружает с TFTP-сервера образ ПО или файл конфигурации. Загруженный образ устанавливается автоматически. Загруженный файл конфигурации сохраняется в энергозависимой памяти коммутатора.

Автоматическая установка с использованием TFTP-сервера может выполняться на любом IP-интерфейсе, включая сетевой порт, сервисный порт и интерфейсы маршрутизации. Для поддержки автоматической установки DCHP-клиент включается по ходу работы на сервисном порте либо на сетевом порте.

boot autoinstall

Команда предназначена для оперативного запуска или остановки процесса автоматической установки на коммутаторе. Не является конфигурационной, поэтому не сохраняется в текущем или загрузочном файле конфигурации.

Значение по умолчанию: остановлено

Формат: `boot autoinstall {start | stop}`

Режим ввода команд: привилегированный

boot host retrycount

Команда устанавливает количество попыток загрузки файла конфигурации с TFTP-сервера.

Значение по умолчанию: 3

Формат: `boot host retrycount` *`1-3`*

Режим ввода команд: привилегированный

no boot host retrycount

Команда используется, чтобы установить количество попыток загрузки файла конфигурации в значение по умолчанию.

Формат: `no boot host retrycount`

Режим ввода команд: привилегированный

boot host dhcp

Команда включает функцию автоматической установки на коммутаторе при следующей перезагрузке. Команда не влияет на текущие настройки автоматической установки и сохраняется в энергонезависимой памяти коммутатора.

Значение по умолчанию: включено

Формат: `boot host dhcp`

Режим ввода команд: привилегированный

no boot host dhcp

Команда выключает функцию автоматической установки на коммутаторе при следующей перезагрузке.

Формат: `no boot host dhcp`

Режим ввода команд: привилегированный

boot host autosave

Команда для автоматического сохранения загруженного файла конфигурации в качестве файла стартовой конфигурации коммутатора. Если автоматическое сохранение выключено, требуется явным образом сохранять загруженную конфигурацию в энергонезависимой памяти с помощью команды `write memory` или `copy system:running-config nvram:startup-config`. Если загруженная конфигурация не была сохранена, после перезагрузки коммутатора с включенной функцией AutoInstall снова начинается процесс автоматической установки.

Значение по умолчанию: выключено

Формат: `boot host autosave`

Режим ввода команд: привилегированный

no boot host autosave

Команда используется для отмены автоматического сохранения загруженного файла конфигурации на коммутаторе.

Формат: `no boot host autosave`

Режим ввода команд: привилегированный

boot host autoreboot

Команда разрешает автоматическую перезагрузку коммутатора после успешной загрузки образа ПО. Разрешение на автоматическую перезагрузку позволяет активировать образ ПО и перезагрузить коммутатор без дополнительных административных действий.

Значение по умолчанию: включено

Формат: `boot host autoreboot`

Режим ввода команд: привилегированный

no boot host autoreboot

Команда используется для запрета автоматической перезагрузки коммутатора после загрузки образа ПО с использованием функции автоматической установки.

Формат: `no boot host autoreboot`

Режим ввода команд: привилегированный

erase startup-config

Команда удаляет текстовый файл конфигурации, сохраненный в энергонезависимой памяти. Если при загрузке коммутатора не найден файл стартовой конфигурации, запускается процесс автоматической установки.

Формат: `erase startup-config`

Режим ввода команд: привилегированный

erase factory-defaults

Команда удаляет текстовый файл с заводскими настройками конфигурации, сохраненный в энергонезависимой памяти.

Значение по умолчанию: выключено

Формат: `erase factory-defaults`

Режим ввода команд: привилегированный

show autoinstall

Команда для отображения текущего состояния процесса автоматической установки.

Формат: `show autoinstall`

Режим ввода команд: привилегированный

copy <url> backup

Загрузить новый резервный образ ПО. Загрузка устройства осуществляется из файла системного программного обеспечения (ПО), который хранится во flash-памяти. При обновлении новый файл системного ПО сохраняется в специально выделенной области памяти.

Значение по умолчанию: выключено

Формат: `copy<tftp|ftp|scp|sftp|usb://<ipaddr>/<filepath>/<filename>> |xmodem | ymodem | zmodem | backup`

Режим ввода команды: привилегированный режим

boot system backup

Переключиться на резервный образ после перезагрузки**.** При загрузке устройство запускает активный файл системного ПО.

Значение по умолчанию: выключено

Формат: `boot system backup`

Режим ввода команды привилегированный режим

exception protocol

Команда для указания протокола, используемого для хранения файла coredump. Всего локально может быть сохранено не более 4 coredump-файлов.

Значение по умолчанию: выключено

Формат: `exception protocol {nfs| tftp | ftp | local | usb | none}`

Режим ввода команды: режим глобальной конфигурации

no exception protocol

Отключить сохранение coredump-файла.

Значение по умолчанию: выключено

Формат: `exception protocol {nfs| tftp | ftp | local | usb | none}`

Режим ввода команды: режим глобальной конфигурации

exception switch-chip-register

Включает сохранение при падении дампа регистров свитча. Дамп сохраняется отдельно в файл reg_core_<timestamp>.x.{bz2,bin} Регистрация дампа берется только для ведущего устройства, а не для backup.

Значение по умолчанию: выключено

Формат: `exception switch-chip-register {enable | disable}`

Режим ввода команды: режим глобальной конфигурации

exception dump stack-ip-address protocol

Эта команда настраивает протокол (DHCP или static), который будет использоваться для настройки служебного порта при сбое устройства. Если он настроен как DHCP, то устройство получает IP-адрес с сервера DHCP, доступного в сети.

Значение по умолчанию: выключено

Формат: `exception dump stack-ip-address protocol {dhcp | static}`

Режим ввода команды: режим глобальной конфигурации

no debug crashlog verbose

Отключить генерацию файла о потоках и системе.

Значение по умолчанию: выключено

Формат: `copy nvram:errorlog <tftp|ftp|scp|sftp|usb:// <ipaddr>/ <filepath>/<filename>> |xmodem | ymodem | zmodem`

Режим ввода команды: режим глобальной конфигурации

6.2 Фильтрация вывода CLI

show xxx|include “string”

Команда ***xxx*** выполняется, при выводе результаты фильтруются следующим образом: отображаются только строки, содержащие совпадение ***string***. Строки, не соответствующие этому условию, при выводе скрываются.

show xxx|include “string” exclude “string2”

Команда ***xxx*** выполняется, при выводе результаты фильтруются следующим образом: отображаются только строки, содержащие совпадение ***string*** и не содержащие совпадение ***string2***. Строки, не соответствующие этим условиям, при выводе скрываются. Если строка вывода соответствует только одному из условий и не соответствует другому, она будет скрыта.

show xxx|exclude “string”

Команда ***xxx*** выполняется, при выводе результаты фильтруются следующим образом: отображаются только строки, не содержащие совпадение ***string***. Строки, содержащие выражение ***string***, при выводе скрываются.

show xxx|begin “string”

Команда ***xxx*** выполняется, при выводе результаты фильтруются следующим образом: отображаются только строки, начинающиеся с совпадения ***string***, а также следующие за первой строкой, соответствующей данному условию. Все предшествующие строки при выводе скрываются.

show xxx|section “string”

Команда ***xxx*** выполняется, при выводе результаты фильтруются следующим образом: отображаются только строки, которые входят в определенные разделы. Разделы (один или несколько) определяются по наличию строк, содержащих совпадение ***string***, и заканчиваются первой строкой с идентификатором конечной позиции по умолчанию (например, exit).

show xxx|section “string” “string2”

Команда ***xxx*** выполняется, при выводе результаты фильтруются следующим образом: отображаются только строки, которые входят в определенные разделы. Разделы (один или несколько) определяются по наличию строк, содержащих совпадение ***string***, и заканчиваются первой строкой, содержащей совпадение ***string2***. Если заданным условиям для строк соответствует несколько сессий, являющихся частью базового вывода, отображаются все копии.

show xxx|section “string” include “string2”

Команда ***xxx*** выполняется, и при выводе результаты фильтруются следующим образом: отображаются только строки, которые входят в определенные разделы. Разделы (один или несколько) определяются по наличию строк, содержащих совпадение ***string***, и заканчиваются первой строкой с идентификатором конечной позиции по умолчанию (например, exit), содержащей также совпадение ***string2***. Данный тип команд фильтрации также может включать параметр exclude или заданный пользователем идентификатор конца раздела.

show xxx|no-more

Команда ***xxx*** выполняется, при выводе результаты отображаются в консоли не порционно, а в полном объеме, без потребности в нажатии дополнительных клавиш для полного отображения необходимой информации.

6.3 Команды работы с ПО

Программное обеспечение поддерживает функцию использования двух образов ПО, что позволяет коммутатору хранить в энергонезависимой памяти сразу два образа. При этом можно указать, какой из образов будет активен при последующих перезагрузках. Эта функция позволяет сократить время простоя при обновлении или возврате к более ранней версии ПО.

delete

Команда удаляет файл резервного образа из энергонезависимой памяти коммутатора или файл с дампом памяти из локальной файловой системы. Необязательный параметр unit работает только для стека. Если использовать данный параметр для систем в автономном режиме, команда возвратит сообщение об ошибке. В стеке параметр unit определяет, на каком узле будет выполнена команда. Если данный параметр не указан, команда будет выполнена на всех узлах стека.

Формат: `delete [unit] backup`
`delete core-dump-file file-name | all`

Режим ввода команд: привилегированный

boot system

Эта команда активирует определенный образ ПО. Данный образ при последующих перезагрузках будет оставаться активным и загружаться начальным загрузчиком. Текущий активный образ ПО отмечается как резервный образ для последующих перезагрузок. Если указанный образ в системе отсутствует, команда возвращает сообщение об ошибке. Необязательный параметр *unit* работает только для стеков. При наличии стека параметр *unit* определяет узел, на котором будет выполнена команда. Если данный параметр не указан, команда будет выполнена на всех узлах стека.

Формат: `boot system [unit] {active | backup}`

Режим ввода команд: привилегированный

show bootvar

Команда для вывода информации о версии и статусе активации для текущего активного образа ПО и резервного образа на поставляемом элементе (узле) стека. Если номер узла не указан, команда отображает сведения об образах ПО всех узлов стека. Данная команда также выводит текстовое описание, связанное с образом ПО. При использовании в автономном режиме команда отображает статус активации коммутатора. В автономном режиме параметр *unit* не работает.

Формат: `show bootvar [unit]`

Режим ввода команд: привилегированный

filedescr

Данная команда связывает заданное текстовое описание с образом ПО. Заданное описание заменяет любое ранее существовавшее. Команда выполняется на всех узлах стека.

Формат: `filedescr {active | backup} text-description`

Режим ввода команд: привилегированный

6.4 Вывод информации о системе и статистики

В этой части описаны команды, которые можно использовать для просмотра системных функций, компонентов и конфигураций.

load-interval

Команда изменяет период времени, в течение которого измеряется загрузка (утилизация) интерфейса. Значение задается в секундах и должно быть кратно 30. Допустимый диапазон значений для параметра *interval* составляет от 30 до 600 секунд. Чем меньше значение интервала загрузки, тем точнее определяется мгновенная утилизация. При этом слишком маленькое значение интервала может снизить производительность системы.

Значение по умолчанию: 300 секунд

Формат: `load-interval interval`

Режим ввода команд: конфигурирование интерфейса

no load-interval

Данная команда возвращает значение интервала загрузки на интерфейсе к значению по умолчанию.

Формат: `no load-interval`

Режим ввода команд: конфигурирование интерфейса

show arp switch

Команда для отображения содержимого ARP-таблицы (Address Resolution Protocol). IP-стек изучает только записи ARP, связанные с интерфейсами управления (сетевыми или сервисными портами). Записи ARP, связанные с интерфейсами маршрутизации, не выводятся.

Формат: `show arp switch`
Режим ввода команд: привилегированный

Термин	*Значение*
IP Address	IP-адрес интерфейса управления или другого устройства в сети управления.
MAC Address	Физический MAC-адрес данного устройства.
Interface	Вывод для сервисного порта – *Management*. Вывод для сетевого порта – *unit/slot/port* физического интерфейса.

show eventlog

Команда для отображения журнала событий, который содержит сообщения об ошибках в системе. При перезагрузке системы журнал событий не очищается. Параметр *unit* представляет собой идентификатор коммутатора.

Формат: `show eventlog [unit]`

Режим ввода команд: привилегированный

Термин	*Значение*
File	Файл, в котором произошло событие.
Line	Номер строки события.
Task ID	Идентификатор задачи события.
Code	Код события.
Time	Время, когда произошло событие.
Unit	Связанный с событием элемент.

При сбросе настроек, перезагрузке коммутатора журнал событий сохраняется.

show hardware

Команда отображает инвентарную информацию о коммутаторе.

Команда show version и команда show hardware отображают одинаковую информацию. В новых версиях программного обеспечения команда show hardware будет недоступна.

Формат: `show hardware`

Режим ввода команд: привилегированный

show version

Команда отображает инвентарную информацию о коммутаторе.

В новых версиях программного обеспечения команда show version заменит команду show hardware.

Формат: `show version`

Режим ввода команд: привилегированный

Термин	*Значение*
System Description	Текст для идентификации названия коммутатора и его типа.
Machine Type	Тип устройства в соответствии с Vital Product Data.
Machine Model	Модель устройства в соответствии с Vital Product Data.
Serial Number	Уникальный серийный номер коммутатора, указанный на корпусе.
FRU Number	Номер сборочного узла элемента.
Part Number	Заводской номер детали.
Maintenance Level	Аппаратные изменения, значимые для ПО.
Manufacturer	Поле дескриптора производителя.
Burned in MAC Address	Общий назначаемый сетевой адрес.
Software Version	Номер (релиз.версия редакция) текущего ПО коммутатора.
Operating System	Текущая ОС на коммутаторе.
Network Processing Device	Тип микрокода процессора.
Additional Packages	Дополнительные пакеты, включенные в систему.

show platform vpd

Данная команда отображает Vital Product Data (VPD) для коммутатора.

Формат: `show platform vpd`

Режим ввода команд: пользовательский привилегированный

Отображается информация, представленная ниже.

Термин	*Значение*
Operational Code Image File Name	Подпись сборки ПО, загруженного в коммутатор.
Software Version	Информация о версии ПО, уровне обслуживания и сборке коммутатора.
Timestamp	Временная метка данной сборки образа ПО.

show interface

Данная команда отображает сводную статистику определенного интерфейса или подсчет всего трафика CPU в зависимости от аргумента.

Формат: `show interface {`*`unit/slot/port`* `| switchport | lag` *`lag-id`*`}`

Режим ввода команд: привилегированный

При значении аргумента `unit/slot/port` или указании `lag` *`lag-id`* отображаются следующие параметры.

Термин	*Значение*
Interface index	Идентификатор интерфейса в системе.
Hardware	Тип интерфейса.
Interface MTU	Максимальный MTU поддерживаемый на данном интерфейсе.
Link type	Пропускная способность интерфейса и состояние дуплекса. Если в качестве аргумента указан lag выводится следующая информация: • Link aggregation type — тип LAG; • No. of members in this port-channel — количество интерфейсов входящих в LAG; • No. of active members in this port-channel — количество активных интерфейсов входящих в состав LAG; • Active bandwidth — суммарная пропускная способность LAG; • Member — информация о конкретных интерфейсах входящих в состав LAG.
Media type	Тип среды передачи для интерфейса. Не выводится для LAG-интерфейса.
Link downs	Количество переходов в состояние Down. Не учитывает переходы по команде shutdown. Не выводится для LAG-интерфейса.
Time since counters last cleared	Время с момента последней очистки статистики интерфейса.
Flow control	Состояние контроля потока на интерфейсе. Не выводится для LAG-интерфейса.
Input rate	Средняя скорость входящего потока за указанный интервал времени (Load Interval).
Output rate	Средняя скорость исходящего потока за указанный интервал времени (Load Interval).
Packets input	Количество входящих пакетов.

Bytes received	Количество принятых данных в байтах.
Oversize errors	Количество пакетов принятых интерфейсом, превышающих предельно допустимый MTU.
Internal MAC errors	Количество пакетов, принятых с ошибками.
Broadcast frames	Общее количество широковещательных пакетов, принятых и переданных данным интерфейсом.
Multicast frames	Общее количество многоадресных пакетов, принятых и переданных данным интерфейсом.
Total input errors	Общее количество пакетов, принятых с ошибками.
FCS errors	Количество принятых пакетов с ошибками контрольной суммы и целым числом октетов.
Alignment errors	Количество принятых пакетов с ошибками контрольной суммы и не целым числом октетов.
Pause frames received	Количество принятых запросов остановки передачи потока.
Snmp input frames discarded	Количество отброшенных входящих SNMP-пакетов.
Packets output	Количество исходящих пакетов.
Bytes sent	Количество переданных данных в байтах.
Broadcast errors	Общее количество широковещательных пакетов, принятых и переданных данным интерфейсом с ошибками.
Multicast errors	Общее количество многоадресных пакетов, принятых и переданных данным интерфейсом с ошибками.
Output errors	Общее количество пакетов переданных с ошибками.
Total collisions	Общее количество коллизий.
Excessive collisions	Общее количество символов, переданных с коллизиями.
Late collisions	Количество пакетов, переданных с коллизиями на последних этапах передачи.
Pause frames transmitted	Количество отправленных запросов остановки передачи потока.
Snmp out frames discarded	Количество отброшенных исходящих SNMP-пакетов.
Output queues	QoS-статистика исходящих очередей интерфейса (передано/ отброшено). Не выводится для LAG-интерфейса.

Параметры отображения при аргументе `switchport`.

Термин	***Значение***
Packets Received Without Error	Общее количество пакетов (включая широковещательные и многоадресные пакеты), принятых процессором.
Broadcast Packets Received	Общее количество принятых пакетов, направленных на широковещательный адрес. Многоадресные пакеты в данный параметр не включаются.
Packets Received With Error	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке на протокол более высокого уровня.
Packets Transmitted Without Error	Общее количество пакетов, переданных из интерфейса.

Broadcast Packets Transmitted	Общее количество пакетов, запрашиваемых протоколами более высокого уровня для передачи на широковещательный адрес, включая удаленные или не отправленные.
Transmit Packet Errors	Число исходящих пакетов, которые не могут быть переданы из-за ошибок.
Time Since Counters Last Cleared	Истекшее время (дни, часы, минуты и секунды) с момента последнего обнуления статистики данного коммутатора.

show interfaces status

Команда для отображения информации об интерфейсе, включая описание, состояние порта, скорость и функцию автосогласования. Данная команда похожа на команду `show port all`, но она выводит дополнительные поля, такие как описание интерфейса и возможности порта.

Описание интерфейса можно настроить с помощью существующей команды `description <name>`. Максимальная длина — 64 символа, при выводе сокращается до 28 символов. Полную форму описания можно отобразить с помощью команды `show port description`. Данная команда отображает физические интерфейсы, LAG-интерфейсы и интерфейсы маршрутизации VLAN.

Формат: `show interfaces status [{`*`unit/slot/port`*` | vlan `*`id`*`}]`

Режим ввода команд: привилегированный

Поле	*Описание*
Port	Интерфейс, связанный с остальными данными в строке.
Name	Настраиваемое пользователем описание для интерфейса.
Admin Mode	Административное состояние порта.
Link State	Оперативное состояние порта.
Physical Mode	Настройки скорости и дуплекса на интерфейсе.
Physical Status	Показывает скорость порта и режим дуплекса для физических интерфейсов. Физический статус LAG-интерфейсов не отображается. Если порт не поднят, физический статус неизвестен.
Media Type	Тип среды передачи для интерфейса.
Flow Control Status	Статус управления потоком 802.3x.
Flow Control	Настраиваемый режим управления потоком 802.3x

show interfaces traffic

Команда используется для отображения информации о прохождении трафика через интерфейс.

Формат: `show interfaces traffic [`*`unit/slot/port`*`]`

Режим ввода команд: привилегированный

Поле	*Описание*
Interface Name	Интерфейс, связанный с остальными данными в строке.
Queue	Номер очереди.

Total Pass (Pkts)	Общее количество пакетов переданных для указанной очереди.
Congestion Drops	Количество пакетов, отброшенных в очереди по причине перегрузки.
TX Queue	Количество ячеек в исходящей очереди.
RX Queue	Количество ячеек во входящей очереди.
Color Drops: Yellow	Количество отброшенных желтых (подтвержденных) пакетов.
Color Drops: Red	Количество отброшенных красных (избыточных) пакетов.
WRED TX Queue	Количество пакетов в исходящей очереди WRED.

show interface counters

Данная команда отображает сводные данные об основной статистике для всех портов (физических, CPU, агрегированного интерфейса).

Формат: `show interface counters`

Режим ввода команд: привилегированный

Поле	*Описание*
Port	Интерфейс, связанный с остальными данными в строке.
InOctects	Общее количество октетов, принятых на интерфейсе.
InUcastPkts	Общее количество одноадресных пакетов, принятых на интерфейсе.
InMcastPkts	Общее количество многоадресных пакетов, принятых на интерфейсе.
InBcastPkts	Общее количество широковещательных пакетов, принятых на интерфейсе.
OutOctects	Общее количество октетов, переданных через интерфейс.
OutUcastPkts	Общее количество одноадресных пакетов, переданных через интерфейс.
OutMcastPkts	Общее количество многоадресных пакетов, переданных через интерфейс.
OutBcastPkts	Общее количество широковещательных пакетов, переданных через интерфейс.

show interfaces description

Эта команда отображает описание интерфейсов, их административное и текущее состояние.

Формат: `show interfaces description {unit/slot/port | all | lag | vlan}`

Режим ввода команд: привилегированный

show interface ethernet

Данная команда отображает подробную статистику определенного интерфейса или весь трафик через CPU в зависимости от аргумента.

Формат: `show interface ethernet {`*`unit/slot/port`* `| switchport | all}`

Режим ввода команд: привилегированный

Если задано значение для `unit/slot/port`, на выходе отображается информация, приведенная в таблице ниже.

Термин	*Значение*
Packets Received	**Total Packets Received (Octets).** Общее количество октетов данных (включая поврежденные пакеты), принятых по сети (исключая кодирующие биты, но с учетом октетов контрольной суммы пакета). Данный объект может использоваться для практической оценки использования Ethernet. Если требуется более высокая точность, следует оценить объекты etherStatsPkts и etherStatsOctets по состоянию до и после стандартного интервала. Результатом такой оценки станет значение Utilization, представляющее собой процентное выражение утилизации данного сегмента Ethernet (от 0 до 100 процентов). **Packets Received 64 Octets.** Общее количество принятых пакетов (включая поврежденные пакеты) длиной в 64 октета (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Received 65–127 Octets.** Общее количество принятых пакетов (включая поврежденные пакеты) длиной от 65 до 127 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Received 128–255 Octets.** Общее количество принятых пакетов (включая поврежденные пакеты) длиной от 128 до 255 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Received 256–511 Octets.** Общее количество принятых пакетов (включая поврежденные пакеты) длиной от 256 до 511 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Received 512–1023 Octets.** Общее количество принятых пакетов (включая поврежденные пакеты) длиной от 512 до 1023 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Received 1024–1518 Octets.** Общее количество принятых пакетов (включая поврежденные пакеты) длиной от 1024 до 1518 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Received > 1518 Octets.** Общее количество принятых пакетов длиной более 1518 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета), не содержащих ошибок. **Packets RX and TX 64 Octets.** Общее количество принятых и отправленных пакетов (включая поврежденные пакеты) длиной в 64 октета (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets RX and TX 65–127 Octets.** Общее количество принятых и отправленных пакетов (включая поврежденные пакеты) длиной от 65 до 127 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета).

	Packets RX and TX 128–255 Octets. Общее количество принятых и отправленных пакетов (включая поврежденные пакеты) длиной от 128 до 255 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets RX and TX 256–511 Octets.** Общее количество принятых и отправленных пакетов (включая поврежденные пакеты) длиной от 256 до 511 октетов включительно (без учета межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets RX and TX 512–1023 Octets.** Общее количество принятых и отправленных пакетов (включая поврежденные пакеты) длиной от 512 до 1023 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets RX and TX 1024–1518 Octets.** Общее количество принятых и отправленных пакетов (включая поврежденные пакеты) длиной от 1024 до 1518 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets RX and TX 1519–2047 Octets.** Общее количество принятых и отправленных пакетов длиной от 1519 до 2047 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета), не содержащих ошибок. **Packets RX and TX 1523–2047 Octets.** Общее количество принятых и отправленных пакетов длиной от 1523 до 2047 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета), не содержащих ошибок. **Packets RX and TX 2048–4095 Octets.** Общее количество принятых пакетов длиной от 2048 до 4095 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета), не содержащих ошибок.
Packets Received Successfully	**Packets RX and TX 4096–9216 Octets.** Общее количество принятых пакетов длиной от 4096 до 9216 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета), не содержащих ошибок. **Total Packets Received Without Error.** Общее количество принятых пакетов, не содержащих ошибок. **Unicast Packets Received.** Количество одноадресных пакетов подсети, доставленных на протокол более высокого уровня. **Multicast Packets Received.** Общее количество принятых неповрежденных пакетов, переданных на групповой адрес. В это количество не входят пакеты, переданные на широковещательный адрес. **Broadcast Packets Received.** Общее количество принятых неповрежденных пакетов, переданных на широковещательный адрес. Многоадресные пакеты в данный параметр не включаются.
Receive Packets Discarded	Многоадресные пакеты в данный параметр не включаются. Количество полученных пакетов, помеченных для удаления, несмотря на отсутствие в них обнаруженных ошибок, которые могли бы препятствовать их доставке на протокол более высокого уровня. Одной из возможных причин для удаления таких пакетов может быть освобождение пространства буфера.
Packets Received with MAC Errors	**Total Packets Received with MAC Errors.** Общее количество входящих пакетов, которые содержат ошибки, препятствующие их доставке на протокол более высокого уровня. **Jabbers Received.** Общее количество полученных пакетов длиной более 1518 октетов (без учёта межкадрового интервала, но с учетом октетов

	контрольной суммы пакета), в которых содержалась либо ошибочная контрольная сумма с целым количеством октетов (ошибка FCS) либо ошибочная контрольная сумма с нецелым числом октетов (ошибка выравнивания). **Примечание:** Данное определение сбойных пакетов отличается от определения в IEEE-802.3, раздел 8.2.1.5 (10BASE5) и раздел 10.3.1.4 (10BASE2). Указанные документы определяют сбой пакета как состояние, когда пакет превышает 20 мс. Допустимые значения для определения сбоя пакета — от 20 до 150 мс. **Fragments/Undersize Received.** Общее количество принятых пакетов данных длиной менее 64 октетов (без учёта межкадрового интервала, исключая кодирующие биты, но с учетом октетов контрольной суммы пакета). **Alignment Errors.** Общее количество принятых пакетов длиной от 64 до 1518 октетов включительно (без учёта межкадрового интервала исключая кодирующие биты, но с учетом октетов контрольной суммы пакета), в которых содержалась ошибочная контрольная сумма пакета представляла собой дробное число с нецелым числом октетов. **FCS Errors.** Общее количество принятых пакетов длиной от 64 до 1518 октетов включительно (без учёта межкадрового интервала, исключая кодирующие биты, но с учетом октетов контрольной суммы пакета), в которых содержалась ошибочная контрольная сумма пакета с целым количеством октетов. **Overruns.** Общее количество кадров, отклоненных по причине того, что данный порт был перегружен входящими пакетами и не справлялся с нагрузкой.
Received Packets Not Forwarded	**Total Received Packets Not Forwarded.** Количество полученных кадров без ошибок, которые были отклонены (отфильтрованы) в процессе передачи. **802.3x Pause Frames Received**. Количество принятых через интерфейс контрольных кадров MAC с кодом операции PAUSE. Данное значение не фиксируется при работе интерфейса в полудуплексном режиме. **Unacceptable Frame Type**. Количество кадров, удаленных на данном порте из-за неприемлемого типа кадра.
Packets Transmitted Octets	**Total Packets Transmitted (Octets).** Общее количество октетов данных (включая поврежденные пакеты), переданных по сети (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). Данный объект может использоваться для практической оценки использования Ethernet. Если требуется более высокая точность, следует использовать объекты etherStatsPkts и etherStatsOctets по состоянию до и после стандартного интервала. **Packets Transmitted 64 Octets.** Общее количество переданных пакетов (включая поврежденные пакеты) длиной в 64 октета (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Transmitted 65–127 Octets.** Общее количество переданных пакетов (включая поврежденные пакеты) длиной от 65 до 127 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Transmitted 128–255 Octets.** Общее количество переданных пакетов (включая поврежденные пакеты) длиной от 128 до 255 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Transmitted 256–511 Octets.** Общее количество переданных пакетов (включая поврежденные пакеты) длиной от 256 до 511 октетов

	включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Transmitted 512–1023 Octets.** Общее количество переданных пакетов (включая поврежденные пакеты) длиной от 512 до 1023 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета). **Packets Transmitted 1024–1518 Octets.** Общее количество переданных пакетов (включая поврежденные пакеты) длиной от 1024 до 1518 октетов включительно (без учёта межкадрового интервала, но с учетом октетов в контрольной сумме пакета) **Packets Transmitted > 1518 Octets.** Общее количество переданных пакетов длиной более 1518 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета), не содержащих ошибок. **Max Frame Size.** Максимальный размер полезной нагрузки (не включая MAC-заголовок), который может быть принят или передан портом. **Maximum Transmit Unit.** Максимальный объем полезной нагрузки Ethernet.
Packets Transmitted Successfully	**Total Packets Transmitted Successfully.** Количество кадров, переданных через данный порт в соответствующий сегмент. **Unicast Packets Transmitted**. Общее число одноадресных пакетов, которые протокол верхнего уровня отправил, включая удаленные и неотправленные пакеты. **Multicast Packets Transmitted.** Общее количество пакетов, которые протокол верхнего уровня должен был передать по групповым адресам (включая отклоненные и неотправленные пакеты). **Broadcast Packets Transmitted.** Общее количество пакетов, которые протокол верхнего уровня должен был передать по широковещательным адресам (включая отклоненные и неотправленные пакеты).
Transmit Packets Discarded	Общее количество исходящих пакетов, помеченных для удаления, несмотря на отсутствие в них обнаруженных ошибок, которые могли бы препятствовать их доставке на протокол более высокого уровня. Одной из возможных причин удаления пакета может быть освобождение пространства буфера.
Transmit Errors	**Total Transmit Errors.** Общее количество единичных, множественных и частых коллизий. **FCS Errors**. Общее количество переданных пакетов длиной от 64 до 1518 октетов включительно (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета), в которых содержалась ошибочная контрольная сумма пакета с целым количеством октетов. Underrun Errors. Общее количество кадров, отклоненных из-за того, что передающий буфер FIFO в процессе передачи кадра оказался пустым.
Transmit Discards	**Total Transmit Packets Discards.** Общее количество кадров, отклоненных в силу единичных и множественных коллизий, а также избыточных пакетов. **Single Collision Frames.** Счетчик количества успешно переданных через конкретный интерфейс кадров, передача которых была приостановлена в силу одной коллизии. **Multiple Collision Frames.** Счетчик количества успешно переданных через конкретный интерфейс кадров, передача которых была приостановлена в силу нескольких коллизий. **Excessive Collisions.** Счетчик количества кадров, передача которых через конкретный интерфейс не удается из-за частых коллизий.

	Port Membership Discards. Количество кадров, отклоненных на выходе данного порта в силу включенной фильтрации. **Total Transmit Packets Discards.** Общее количество кадров, отклоненных в силу единичных и множественных коллизий, а также избыточных пакетов. **Single Collision Frames.** Счетчик количества успешно переданных через конкретный интерфейс кадров, передача которых была приостановлена в силу одной коллизии. **Multiple Collision Frames.** Счетчик количества успешно переданных через конкретный интерфейс кадров, передача которых была приостановлена в силу нескольких коллизий. **Excessive Collisions.** Счетчик количества кадров, передача которых через конкретный интерфейс не удается из-за частых коллизий. **Port Membership Discards.** Количество кадров, отклоненных на выходе данного порта в силу включенной фильтрации.
Protocol Statistics	**802.3x Pause Frames Transmitted.** Счетчик контрольных кадров MAC с кодом операции PAUSE, переданных через конкретный интерфейс. Данное значение не фиксируется при работе интерфейса в полудуплексном режиме. **GVRP PDUs Received.** Счетчик пакетов GVRP PDU, принятых на уровне GARP. **GVRP PDUs Transmitted.** Счетчик пакетов GVRP PDU, переданных с уровня GARP. **GVRP Failed Registrations.** Количество попыток регистрации GVRP, которые не удалось завершить. **GMRP PDUs Received.** Счетчик пакетов GMRP PDU, принятых на уровне GARP. **GMRP PDUs Transmitted.** Счетчик пакетов GMRP PDU, переданных с уровня GARP. **GMRP Failed Registrations.** Количество попыток регистрации GMRP, которые не удалось завершить. **STP BPDUs Transmitted.** Отправленные пакеты Spanning Tree Protocol Bridge Protocol Data Units. **STP BPDUs Received.** Принятые пакеты Spanning Tree Protocol Bridge Protocol Data Units. **RST BPDUs Transmitted.** Отправленные пакеты Rapid Spanning Tree Protocol Bridge Protocol Data Units. **RSTP BPDUs Received.** Принятые пакеты Rapid Spanning Tree Protocol Bridge Protocol Data Units. **MSTP BPDUs Transmitted.** Отправленные пакеты Multiple Spanning Tree Protocol Bridge Protocol Data Units. **MSTP BPDUs Received.** Принятые пакеты Multiple Spanning Tree Protocol Bridge Protocol Data Units. **SSTP BPDUs Transmitted.** Отправленные пакеты Shared Spanning Tree Protocol Bridge Protocol Data Units. **SSTP BPDUs Received.** Принятые пакеты Shared Spanning Tree Protocol Bridge Protocol Data Units.
Dot1x Statistics	**EAPOL Frames Transmitted.** Количество кадров EAPOL любого типа, которые были переданы данным аутентификатором. **EAPOL Start Frames Received.** Количество стартовых кадров EAPOL без ошибок, которые были приняты данным аутентификатором.

Traffic Load Statistics	**Load Interval.** Период времени, в течение которого вычисляется загрузка интерфейса. Значение задается в секундах и должно быть кратно 30. Допустимый диапазон значений — от 30 до 600 секунд. **Bits Per Second Received.** Приблизительное количество битов, принятых за секунду. Это экспоненциально взвешенное среднее значение, которое зависит от настроенного интервала загрузки. **Bits Per Second Transmitted.** Приблизительное количество битов, переданных за секунду. Это экспоненциально взвешенное среднее значение, которое зависит от настроенного интервала загрузки. **Packets Per Second Received.** Приблизительное количество пакетов, полученных за секунду. Это экспоненциально взвешенное среднее значение, которое зависит от настроенного интервала загрузки. **Packets Per Second Transmitted.** Приблизительное количество пакетов, переданных за секунду. Это экспоненциально взвешенное среднее значение, которое зависит от настроенного интервала загрузки. **Percent Utilization Received.** Значение загруженности соединения для RX-линии, представленное в процентах. **Percent Utilization Transmitted.** Значение загруженности соединения для TX-линии, представленное в процентах.
Time Since Counters Last Cleared	Истекшее время (дни, часы, минуты и секунды) с момента последнего обнуления статистики данного порта.

При использовании ключевого слова switchport появится информация, приведенная в таблице ниже.

Термин	***Значение***
Packets Received Without Error	Общее количество пакетов (включая широковещательные и многоадресные пакеты), принятых процессором.
Broadcast Packets Received	Общее количество принятых пакетов, которые были направлены на широковещательный адрес. Многоадресные пакеты в данный параметр не включаются
Packets Received With Error	Общее количество пакетов с ошибками (включая широковещательные и многоадресные пакеты), принятых процессором.
Packets Transmitted without Errors	Общее количество пакетов, переданных из интерфейса.
Broadcast Packets Transmitted	Общее количество пакетов, отправленных протоколами верхнего уровня для передачи на широковещательный адрес, включая отброшенные или неотправленные.
Transmit Packet Errors	Количество исходящих пакетов, которые не могут быть переданы из-за ошибок.
Time Since Counters Last Cleared	Истекшее время (дни, часы, минуты и секунды) с момента последнего обнуления статистики данного коммутатора.

При использовании ключевого слова `all` для всех интерфейсов коммутатора выводится информация, приведенная в таблице ниже.

Термин	*Значение*
Port	Идентификатор интерфейса.
Bytes Tx	Общее количество байтов, переданных через интерфейс.
Bytes Rx	Общее количество байтов, принятых через интерфейс.
Packets Tx	Общее количество пакетов, переданных через интерфейс.
Packets Rx	Общее количество пакетов, принятых через интерфейс.
Utilization Tx (%)	Общая загрузка передачи интерфейса за интервал времени `load interval`.
Utilization Rx (%)	Общая загрузка приёма интерфейса за интервал времени `load interval`.

show interface ethernet switchport

Данная команда отображает настройки private VLAN для интерфейсов коммутатора.

Формат: `show interface ethernet` *`interface-id`* `switchport`

Режим ввода команд: привилегированный

Команда отображает следующую информацию:

Термин	*Значение*
Private-vlan host association	Настройки ассоциаций для host-портов private VLAN.
Private-vlan mapping	Настройки соответствий для promiscuous-портов private VLAN.

show fiber-ports optical-transceiver

Данная команда отображает диагностическую информацию SFP: температура, напряжение, ток, входная мощность, выходная мощность, ошибка передатчика, потеря сигнала (LOS). Значения берутся из SFP-трансивера по адресу A2 (Diagnostics) по интерфейсу I2C.

Формат: `show fiber-ports optical-transceiver {all | `*`unit/slot/port`*`}`

Режим ввода команд: привилегированный

Поле	*Описание*
Temp	Температура трансивера, измеренная внутренним датчиком.
Voltage	Напряжение питания, измеренное внутренним датчиком.
Current	Данные о текущем токе смещения.
Output Power	Выходная мощность оптического сигнала по отношению к 1 мВт.
Input Power	Входная мощность оптического сигнала по отношению к 1 мВт.
TX Fault	Отказ трансмиттера.
LOS	Потеря сигнала.

show fiber-ports optical-transceiver-info

Команда для вывода информации о производителе SFP, такой как наименование производителя, серийный номер SFP, номер компонента SFP. Значения берутся из SFP-трансивера по адресу A0 по интерфейсу I2C.

Формат: `show fiber-ports optical-transceiver-info {all | slot/port}`

Режим ввода команд: привилегированный

Поле	*Описание*
Vendor Name	Наименование производителя состоит из 16 символов ASCII, выровненных по левому краю дополненных справа пробелами ASCII (20h). Наименование производителя должно представлять собой полное наименование компании, его узнаваемую аббревиатуру, SCSI-код или биржевой код компании.
Length (50um, OM2)	Данное значение указывает длину канала, поддерживаемого трансивером при работе в рамках применимых стандартов с использованием 50-микронного многомодового оптоволоконного подключения OM2 [500 МГц*км при 850 нм]. Ноль в данном поле означает, что трансивер не поддерживает 50-микронное многомодовое оптоволоконное подключение или что информация о длине канала определяется в соответствии с технологией трансивера.
Length (62.5um, OM1)	Данное значение указывает длину канала, поддерживаемого трансивером при работе в рамках применимых стандартов с использованием 62,5-микронного многомодового оптоволоконного подключения OM1 [200 МГц*км при 850 нм, 500 МГц*км при 1310 нм]. Ноль в данном поле означает, что трансивер не поддерживает 62,5-микронное многомодовое оптоволоконное подключение или что информация о длине канала определяется в соответствии с технологией трансивера.
Vendor SN	Серийный номер производителя располагается в поле из 16 символов, содержащем выравненные по левому краю символы ASCII, дополненные справа пробелами ASCII (20h). Значение поля определяет серийный номер производителя трансивера. Ноль в данном поле означает, что серийный номер производителя не указан.
Vendor PN	Номер компонента производителя располагается в поле из 16 символов, содержащем выравненные по левому краю символы ASCII, дополненные справа пробелами ASCII (20h). Значение поля определяет производственный номер компонента или наименование продукта. Ноль в данном поле означает, что номер компонента не указан.
BR, nominal	Номинальная скорость передачи данных определяется в единицах по 100 MBD и округляется до ближайшего значения, кратного 100 MBD. Скорость передачи данных включает не только биты полезной нагрузки, но и биты, необходимые для кодирования и ограничения сигнала. Нулевая величина параметра означает, что скорость цифрового потока не указана и должна определяться в соответствии с технологией трансивера. Фактическая скорость передачи данных будет зависеть от кодирования данных, как определено в значении кодирования.
Vendor Rev	Номер редакции производителя содержит символы ASCII с выравниванием по левому краю, дополненные справа пробелами ASCII (20h). и определяет номер редакции продукта, присвоенный производителем. Ноль в данном поле означает, что номер редакции не указан.

show mac-addr-table

Команда для отображения записей таблицы коммутации. Эти записи используются при прозрачной коммутации трафика для определения, куда требуется переслать принятый кадр.

Чтобы отобразить всю таблицу, введите `all` или не указывайте дополнительные параметры. Чтобы отобразить записи таблицы с запрашиваемым MAC-адресом в определенной VLAN, укажите значение параметров MAC Address и VLAN ID. Для просмотра обзорной информации о таблице коммутации введите параметр `count`. Для просмотра MAC-адресов, связанных с определенным интерфейсом, используйте параметр `interface unit/slot/port`.

Вместо параметра `unit/slot/port` можно использовать `lag` *`lag-intf-num`* для указания LAG-интерфейса, где `lag-intf-num` — это номер LAG-интерфейса. Для отображения информации о MAC-адресах в определенной VLAN используется параметр `vlan` *`vlan_id`*.

Формат: `show mac-addr-table [{`*`macaddr vlan_id`*` | all | count | interface {`*`unit/slot/port`*` | lag `*`lag-id`*` | vlan `*`vlan_id`*`} }]`

Режим ввода команд: привилегированный

Если параметры, ключевое слово `all` или значения MAC-адреса и VLAN ID не указаны, команда выводит следующую информацию.

Поле	*Описание*
VLAN ID	VLAN, в рамках которой определен MAC-адрес.
MAC Address	MAC-адрес одноадресной передачи, для которого на коммутаторе есть данные для отправки или фильтрации. Формат представляет собой 6 шестнадцатеричных чисел из двух цифр, разделенных двоеточиями, например 01:23:45:67:89:AB.
Interface	Порт, на котором был изучен адрес.
Interface Index	Указывает индекс записи таблицы интерфейса, связанной с данным портом.
Status	Статус записи. Значения могут быть следующими: **Static** — значение было добавлено системой или пользователем в процессе определения статического MAC-фильтра. Переобучению не подлежит. **Learned** — значение было определено в процессе наблюдения исходных MAC-адресов входящего трафика и используется в данный момент. **Management** — значение (системный MAC-адрес) также является значением для существующего параметра dot1dStaticAddress. Этот адрес определён на интерфейсе и используется для сетевой маршрутизации. **Self** — значение представляет собой адрес одного из физических интерфейсов коммутатора (собственный MAC-адрес системы). **GMRP Learned** — значение было определено посредством GMRP и применяется для многоадресной рассылки. **Other** — значение не подходит ни под одну из указанных категорий.

При указании vlan vlan_id будут отображены только поля MAC Address, Interface и Status. При указании параметра `interface unit/slot/port` в дополнение к полям MAC Address и Status будет отображаться поле VLAN ID. При использовании параметра count отобразится следующая информация.

Поля	*Описание*
Dynamic Address count	Количество MAC-адресов в таблицах коммутации, определенных автоматически.
Static Address (User-defined) count	Количество MAC-адресов в таблицах коммутации, введенных пользователем вручную.
Total MAC Addresses in use	Количество MAC-адресов, в настоящее время находящихся в таблицах коммутации.
Total MAC Addresses available	Количество MAC-адресов, допустимое для таблиц коммутации.

process cpu threshold

Используйте данную команду для настройки порогов использования CPU. Значения порогов Rising (порог при повышении) и Falling (порог при понижении) указываются в процентах от ресурсов CPU. Время наблюдения за использованием CPU можно настроить в диапазоне от 5 до 86400 секунд с шагом в 5 секунд. Конфигурация порога утилизации CPU сохраняется при перезагрузке коммутатора. Настройка порога при понижении не обязательна, если он не настроен, то он принимает то же значение, что и порог при повышении.

Формат: `process cpu threshold type total rising` *`1-100`* `interval`

Режим ввода команд: глобальная конфигурация

Поле	*Описание*
rising threshold	Настроенный верхний порог утилизации CPU в процентах, при пересечении которого в течение времени rising interval генерируется уведомление. От 1 до 100%. Значение по умолчанию — 0 (выключено).
rising interval	Время в секундах, в течение которого загрузка CPU должны быть выше порога rising threshold, чтобы сгенерировалось уведомление. От 5 до 86400 секунд. Значение по умолчанию — 0 (выключено).
falling threshold	Нижний порог утилизации CPU в процентах, при понижении до которого в течение времени falling interval генерируется уведомление. От 1 до 100%. Значение по умолчанию — 0 (выключено). Уведомление создается, когда использование CPU падает ниже заданного уровня на установленный период времени. Уведомление о достижении нижнего порога при понижении использования создается генерируется только в случае, если ранее было настроено сгенерировано уведомление о превышении верхнего порога использования. Нижний порог использования необходимо всегда устанавливать на уровне не выше верхнего порога. CLI не позволяет настроить нижний порог использования, превышающий значение верхнего порога.
falling interval	Время в секундах, в течение которого загрузка CPU должна быть ниже порогового falling threshold, чтобы сгенерировалось уведомление. От 5 до 86400 секунд. Значение по умолчанию — 0 (выключено).

show process app-list

Команда для отображения пользовательских и системных приложений.

Формат: `show process app-list`

Режим ввода команд: привилегированный

Поле	*Описание*
ID	Идентификатор приложения.
Name	Имя, идентифицирующее процесс.
PID	Номер, который программное обеспечение использует для идентификации процесса.
Admin Status	Административный статус процесса.
Auto Restart	Показывает, требуется ли автоматически перезапускать процесс в случае остановки.
Running Status	Показывает активен ли процесс в данный момент.

show process app-resource-list

Данная команда отображает настроенные и потребляемые ресурсы для каждого приложения.

Формат: `show process` *app-resource-list*

Режим ввода команд: привилегированный

Параметр	*Описание*
ID	Идентификатор приложения.
Name	Имя, идентифицирующее процесс.
PID	Номер, который программное обеспечение использует для идентификации процесса.
Memory Limit	Максимальный объем памяти для использования процессом.
CPU Share	Максимальный уровень использования CPU (в процентах) для процесса
Memory Usage	Объем памяти, потребляемый процессом в данный момент.
Max Mem Usage	Максимальный объем памяти, который был использован процессом когда-либо с момента запуска.

show process cpu

Эта команда предоставляет процентные сведения об использовании CPU различными задачами.

Высокая загрузка CPU не обязательно вызвана трафиком на CPU — это могут быть различные задачи, создающие нагрузку на CPU.

Формат: `show process cpu [`*1-n* `|` `all]`

Режим ввода команд: привилегированный

Ключевое слово	*Описание*
Free	Свободная память системы.
Alloc	Выделенная память всей системы (за исключением объема кэша, используемого файловой системой).
Pid	Идентификатор процесса или потока.
Name	Имя процесса или потока.
5Secs	Процент использования CPU за 5-секундный интервал.
60Secs	Процент использования CPU за 60-секундный интервал.
300Secs	Процент использования CPU за 300-секундный интервал.
Total CPU Utilization	Общий процент использования CPU за промежуток времени продолжительностью 5, 60 и 300 секунд.

show process proc-list

Отображает процессы приложений, созданных менеджером процессов.

Формат: `show process proc-list`

Режим ввода команд: привилегированный

Параметр	*Описание*
PID	Номер, который программное обеспечение, использует для идентификации процесса.
Process Name	Имя, идентифицирующее процесс.
Application ID- Name	Идентификатор приложения и связанное с ним имя.
Child	Показывает, был ли запущен дочерний процесс.
VM Size	Объем виртуальной памяти.
VM Peak	Максимальное число виртуальной памяти, использованное процессом за всё время.
FD Count	Количество файловых дескрипторов процесса.

show running-config

Команда для отображения или сохранения текущих настроек протоколов, поддерживаемых коммутатором. Данная команда отображает или сохраняет команды с конфигурацией и настройками, отличными от значений по умолчанию. Для отображения или сохранения команд с настройками и конфигурацией по умолчанию включите опцию `all`.

Команда show running-config не отображает пароль пользователя, даже если пароль отличен от значения по умолчанию.

Вывод отображается в виде сценария, который можно использовать для настройки другого коммутатора с такой же конфигурацией. Если указан необязательный параметр scriptname с определенным именем файла и расширением .scr, вывод команды сохраняется в виде файла сценария.

При запуске команды show running-config через последовательный интерфейс управления, доступ к коммутатору через удаленные соединения (например, Telnet) будет заблокирован на время исполнения команды и вывода результатов.

При использовании текстового файла конфигурации команда show running-config отобразит только настроенные физические интерфейсы (т. е. если интерфейс содержит только значения по умолчанию, он будет пропущен в выводе команды show running-config). Это касается всех режимов конфигурирования, где не содержится ничего, кроме конфигурации по умолчанию. Таким образом, если за командой входа в определенный режим конфигурации сразу следует команда выхода из него, в выводе команды show running-config обе команды будут пропущены (и, следовательно, они не будут добавлены в файл стартовой конфигурации при сохранении системных настроек).

Используйте ключи, приведенные в таблице ниже, для навигации по выводу команды.

Ключ	*Действие*
Enter	На одну строку вперед.
Space Bar	На одну страницу вперед.
q	Остановить вывод и вернуться к командной строке.

Обратите внимание, что строка `--More-- or (q)uit` отображается внизу экрана вывода, пока он не дойдет до конца.

Формат: `show running-config [all | scriptname]`

Режим ввода команд: привилегированный

show running-config interface

Команда для отображения текущей конфигурации определенного интерфейса, например, физического, туннельного, LAG-интерфейса, loopback-интерфейса или VLAN-интерфейса.

Формат: `show running-config interface {interface | lag {lag-intf-num} | loopback {loopback- id} | tunnel {tunnel-id} | vlan {vlan-id}}`

Режим ввода команд: привилегированный

Параметр	*Описание*
interface	Текущая конфигурация указанного интерфейса.
lag-intf-num	Текущая конфигурация LAG-интерфейса.
loopback-id	Текущая конфигурация loopback-интерфейса.
tunnel-id	Текущая конфигурация туннельного интерфейса.
vlan-id	Текущая конфигурация виртуального интерфейса маршрутизации.

В рамках данной команды отображается информация, приведенная в таблице ниже.

Параметр	*Описание*
unit|slot|port	Интерфейс в формате unit/slot/port.
lag	Отображает текущую конфигурацию указанного LAG-интерфейса.
loopback	Отображает текущую конфигурацию указанного loopback-интерфейса.
tunnel	Отображает текущую конфигурацию указанного туннельного интерфейса.
vlan	Отображает текущую конфигурацию указанного виртуального интерфейса маршрутизации.

show

Данная команда выводит содержимое текстовых файлов конфигурации в CLI. Текстовые файлы конфигурации (стартовой и резервной конфигурации, а также заводских настроек) в сжатом виде хранятся в памяти. С помощью данной команды можно распаковать данные файлы и сразу отобразить их содержимое.

Формат: `show { startup-config | backup-config | factory-defaults }`

Режим ввода команд: привилегированный

Параметр	*Описание*
startup-config	Отображает содержимое файла стартовой конфигурации.
backup-config	Отображает содержимое файла резервной конфигурации.
factory-defaults	Отображает содержимое файла заводских настроек.

dir

Команда выводит список файлов, сохранённых во flash-памяти.

Формат: `dir`

Режим ввода команд: привилегированный

show sysinfo

Команда отображает информацию о коммутаторе.

Формат: `show sysinfo`

Режим ввода команд: привилегированный

Термин	*Значение*
System Description	Текстовое описания коммутатора.
System Name	Наименование для идентификации данного коммутатора. По умолчанию пустое.
System Location	Текстовое описание местоположения коммутатора. По умолчанию пустое.

System Contact	Информация о контактном лице для данного коммутатора. По умолчанию пустое.
System ObjectID	Базовый MIB ObjectID данного коммутатора.
System Up Time	Время (дни, часы и минуты) с момента последней перезагрузки коммутатора.
Current SNTP Synchronized Time	Системное время, полученное от SNTP-сервера сети.
MIBs Supported	Список MIB, поддерживаемых данным агентом.

show tech-support

Команда `show tech-support` используется для отображения системной и конфигурационной информации во время общения с технической поддержкой. Вывод команды `show tech-support` представляет собой комбинацию выводов перечисленных ниже команд и включает файлы журналов их прошлого выполнения.

Если в команде указан один из необязательных параметров [bgp|dot1q|dot1s|dot3ad|file||isdp|layer3|link_dependency|lldp|log|routing|sim|stacking|switching|system], то вывод отображает часть информации из полного вывода команды show tech-support только для указанного параметра.

- `show version`
- `show version`
- `show bootvar`
- `show switch`
- `show switch detail`
- `show environment`
- `show running-config`
- `show serviceport`
- `show process cpu`
- `show process proc-list`
- `show process memory`
- `show mbuf total`
- `show port all`
- `show interface ethernet all`
- `show fiber-ports optical-transceiver-info all`
- `show fiber-ports optical-transceiver all`
- `show interface all`
- `show interfaces hardware profile`
- `show interfaces status err-disabled`
- `show interface debounce`
- `show mac-addr-table`
- `show mac-addr-table count`
- `show vlan brief`
- `show port-channel all`
- `show ip interface brief`
- `show ipv6 interface brief`
- `show arp`
- `show ip stats`
- `show ip route`

- `show routing heap summary`
- `show ip bgp summary`
- `show ip bgp neighbors`
- `show ip bgp statistics`
- `show ip bgp update-group`
- `show bgp ipv6 summary`
- `show bgp ipv6 neighbors`
- `show bgp ipv6 statistics`
- `show bgp ipv6 update-group`
- `show spanning-tree active`
- `show stack-port`
- `show stack-port counters all`
- `show stack-port diag all`
- `show logging`
- `show logging buffered`
- `show logging traplogs`
- `show lldp remote-device all`
- `show isdp neighbors`
- `show link state group`

Формат: `show tech-support [bgp|dot1q|dot1s|dot3ad|file|isdp|layer3|`
`|link_dependency|lldp|log|routing|sim|stacking|switching|system]`

Режим ввода команд: привилегированный

length value

Команда устанавливает количество строк на страницу при постраничном выводе для разных видов консольных сессий (telnet/ssh/console). Эта команда сохраняется в текущей конфигурации.

Значение по умолчанию: 24

Формат: `length value`

Режим ввода команд: line-конфигурация

no length value

Команда возвращает количеством строк на страницу при постраничном выводе в значение по умолчанию.

Формат: `no length` *`value`*

Режим ввода команд: line-конфигурация

terminal length

Команда устанавливает количество строк на страницу при постраничном выводе для текущей сессии в значение `value`. Применяется мгновенно для текущей сессии и не сохраняется в текущей конфигурации.

Значение по умолчанию: 24 строки на страницу

Формат: `terminal length` *value*

Режим ввода команд: привилегированный

no terminal length

Команда возвращает количество строк на страницу при постраничном выводе в текущей сессии в значение по умолчанию.

Формат: `no terminal length` *value*

Режим ввода команд: привилегированный

show terminal length

Команда для отображения всех настроенных значений количества строк на страницу.

Формат: `show terminal length`

Режим ввода команд: привилегированный

memory free low-watermark processor

Команда для настройки уведомлений в случае, когда объем свободной памяти CPU оказывается ниже указанного порога. Уведомление создается, когда объем свободной памяти оказывается ниже настроенного порога. Еще одно уведомление создается, как только объем свободной памяти оказывается на 10 % выше настроенного порога. Чтобы предотвратить чрезмерное количество уведомлений в ситуациях, когда объем свободной памяти CPU колеблется на близком к порогу уровне, в течение 60 секунд может быть создано только одно уведомление об увеличении или уменьшении объема памяти. Пороговое значение указывается в килобайтах. Конфигурация порога свободной памяти CPU при перезагрузке коммутатора сохраняется.

Формат: `memory free low-watermark processor` *1-1034956*

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
low-watermark	Когда объем свободной памяти CPU оказывается ниже этого порога, инициируется уведомление. Диапазон значения: от 1 до максимального объема доступной памяти на коммутаторе. Значение по умолчанию — 0 (выключено).

clear mac-addr-table

Используйте команду, чтобы динамически удалять изученные записи из таблиц коммутации. Используя следующие опции, можно задать группу динамически изученных записей таблиц коммутации для удаления.

Значение по умолчанию: отсутствует

Формат: `clear mac-addr-table {all | vlan` *vlanId* `| interface` *unit/slot/port* `|` *macAddr* `[`*macMask*`]}`

Режим ввода команд: привилегированный

Параметр	*Описание*
all	Удаляет динамически изученные записи в таблице коммутации
vlan vlanId	Удаляет динамически изученные записи таблиц коммутации, связанные с указанным vlanId.
interface unit/slot/port	Удаляет записи таблиц коммутации, изученные для указанного интерфейса.
macAddr **macMask**	Удаляет динамически изученные записи таблиц коммутации, связанные с диапазоном, который определен маской MAC и MAC-адресом. Если маска MAC не указана, из таблиц коммутации удаляется только указанный MAC-адрес.

6.5 Команды бокс-сервисов

Ниже описаны команды бокс-сервисов. Бокс-сервисы обеспечивают поддержку таких функций, как контроль температуры и состояния источника питания, управление вентилятором и другие.

environment temprange

Эта команда позволяет задать допустимый диапазон температур для нормальной работы.

Формат: `environment temprange min` *`-100-100`* `max` *`-100-100`*

Режим ввода команд: глобальная конфигурация

Параметр	*Значение*
min	Устанавливает минимально допустимую температуру. Диапазон значений: от -100 °C до 100 °C. По умолчанию: 0 °C
max	Устанавливает максимально допустимую температуру. Диапазон значений: от -100 °C до 100°C. По умолчанию: 0 °C

environment trap

Команда для настройки трапов, основанных на состоянии среды.

Формат: `environment trap {fan | powersupply | temperature}`

Режим ввода команд: глобальная конфигурация

Параметр	*Значение*
fan	Включает или выключает отправку трапов при смене состояния вентиляторов. По умолчанию: включено.
powersupply	Включает или выключает отправку трапов при смене состояния источников питания. По умолчанию: включено.
temperature	Включает или выключает отправку трапов при изменении показателей температуры. По умолчанию: включено.

show environment

Команда для отображения сводной информации об объеме системного диска и его использовании, показаний датчиков температуры, состояния вентиляторов и блоков питания.

Формат: `show environment`

Режим ввода команд: привилегированный

6.6 Настройка системного журнала

В этой части описываются команды для настройки системного журнала, а также просмотра как самого журнала, так и его настроек.

logging buffered

Команда включает ведение журнала в памяти.

Значение по умолчанию: включено; уровень notice

Формат: `logging buffered`

Режим ввода команд: глобальная конфигурация

no logging buffered

Выключение ведения журнала в памяти.

Формат: `no logging buffered`

Режим ввода команд: глобальная конфигурация

logging buffered wrap

Данная команда разрешает постепенную перезапись информации, когда файл журнала достигает предельного объема. Если перезапись не разрешена, при достижении предельного объема файла запись журнала останавливается.

Значение по умолчанию: включено

Формат: `logging buffered wrap`

Режим ввода команд: привилегированный

no logging buffered wrap

Команда выключает постепенную перезапись информации и отключает ведение журнала, когда файл достигает предельного объема.

Формат: `no logging buffered wrap`

Режим ввода команд: привилегированный

logging cli-command

Команда для включения функции ведения журнала CLI, которая позволяет ПО фиксировать все команды, переданные в систему. Журнал команд сохраняется в постоянном хранилище. Для отображения сохраненной истории команд CLI используйте команду show logging persistent.

Значение по умолчанию: выключено

Формат: `logging cli-command`

Режим ввода команд: глобальная конфигурация

no logging cli-command

Эта команда выключает функцию ведения журнала CLI.

Формат: `no logging cli-command`

Режим ввода команд: глобальная конфигурация

logging console

Команда включает ведение журнала в консоли. Значение severitylevel можно задать как целыми числами от 0 до 7, так и описательно, с использованием следующих ключевых слов: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) или debug (7).

Значение по умолчанию: включено; уровень info

Формат: `logging console` *`[severitylevel]`*

Режим ввода команд: глобальная конфигурация

no logging console

Эта команда выключает ведение журнала в консоли.

Формат: `no logging console`

Режим ввода команд: глобальная конфигурация

logging host

Команда для настройки параметров серверов syslog. Настроить можно до 8 серверов.

Значение по умолчанию: `port: 514 (для UDP) и 6514 (для TLS)`
`authentication mode: анонимно`
`certificate index: 0`
`level: critical (2)`

Формат: `logging host {hostaddress | hostname} addresstype tls [anon|x509name] certificate-index {port severitylevel}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*

hostaddress| hostname	IP-адрес сервера syslog.
address-type	Указывает тип указанного адреса: DNS или IPv4.
tls	Включает защищённый протокол TLS.
anon|x509name	Тип режима аутентификации: анонимный или x509name.
certificate-index	Номер сертификата, который будет использоваться для аутентификации. Диапазон допустимых значений: 0–8. Индекс 0 используется для файла по умолчанию.
port	Номер порта от 1 до 65535.
severitylevel	Значение можно задать как целыми числами от 0 до 7, так и описательно, с использованием следующих ключевых слов: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) или debug (7).

logging host reconfigure

Эта команда разрешает изменение адреса сервера syslog.

Формат: `logging host reconfigure` *`hostindex`*

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
hostindex	Укажите индекс сервера syslog, для которого требуется изменить IP-адрес.

logging host remove

Команда для выключения ведения журнала для указанного сервера syslog. См. команду show logging hosts для вывода списка индексов серверов.

Формат: `logging host remove` *`hostindex`*

Режим ввода команд: глобальная конфигурация

logging persistent

Команда включает ведение журнала постоянного хранения. Значение severitylevel можно задать как целыми числами от 0 до 7, так и описательно, с использованием следующих ключевых слов: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) или debug (7).

Значение по умолчанию: включено; уровень notice

Формат: `logging persistent [severitylevel]`

Режим ввода команд: глобальная конфигурация

no logging persistent

Эта команда выключает ведение журнала постоянного хранения.

Формат: no `logging persistent`

Режим ввода команд: глобальная конфигурация

logging protocol

Используйте команду для настройки версии протокола syslog (0 или 1). RFC 3164 использует версию 0, а RFC 5424 — версию 1.

Значение по умолчанию: версия 0 (RFC 3164).

Формат: `logging protocol {0|1}`

Режим ввода команд: глобальная конфигурация

logging syslog

Команда включает отправку журнала на сервер syslog. Необязательный параметр facility назначает объект по умолчанию для использования в сообщениях тех компонентов, что не имеют встроенной привязки к объекту. Значение facility может быть задано одним из следующих ключевых слов: kernel, user, mail, system, security, syslog, lpr, nntp, uucp, cron, auth, ftp, ntp, audit, alert, clock, local0, local1, local2, local3, local4, local5, local6, local7. Объект по умолчанию: local7.

Значение по умолчанию: отключено

Формат: `logging syslog [facility` *`facility`*`]`

Режим ввода команд: глобальная конфигурация

no logging syslog

Выключает отправку журнала на сервер syslog.

Формат: `no logging syslog [facility]`

Режим ввода команд: глобальная конфигурация

logging syslog port

Команда включает отправку журнала на сервер syslog. Параметр portid представляет собой целое число в диапазоне от 1 до 65535.

Значение по умолчанию: выключено

Формат: `logging syslog port` *`portid`*

Режим ввода команд: глобальная конфигурация

no logging syslog port

Выключает отправку журнала на сервер syslog.

Формат: `no logging syslog port`

Режим ввода команд: глобальная конфигурация

logging syslog source-interface

Эта команда настраивает интерфейс, IP-адрес которого будет использоваться в качестве IP-адреса источника для сообщений syslog. Выбранный IP-адрес источника используется для заполнения заголовка IP-пакетов протокола управления. Это позволяет устройствам безопасности (брандмауэрам) идентифицировать исходные пакеты, идущие от определенного коммутатора. Если указан интерфейс, в качестве адреса источника используется основной IP-адрес инициирующего (исходящего) интерфейса.

Формат: `logging syslog source-interface {`*`unit/slot/port`*`|{loopback` *`loopback-id`*`}|{vlan` *`vlan-id`*`}}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
unit/slot/port	VLAN или интерфейс маршрутизации на базе порта.
loopback-id	Настраивает loopback-интерфейс в качестве IP-адреса источника. Диапазон идентификатора loopback-интерфейса: от 0 до 7.
tunnel-id	Настраивает туннельный интерфейс в качестве IP-адреса источника. Диапазон идентификатора туннельного интерфейса: от 0 до 7.
vlan-id	Настраивает интерфейс VLAN в качестве IP-адреса источника Диапазон идентификатора VLAN: 1–4094.

no logging syslog source-interface

Выключает отправку журнала на сервер syslog.

Формат: `no logging syslog`

Режим ввода команд: глобальная конфигурация

show logging

Команда показывает информацию о настройках журнала.

Формат: `show logging`

Режим ввода команд: привилегированный

Термин	*Значение*
Logging Client Local Port	Порт для отправки сообщений syslog.
Logging Client USB File Name	Имя файла на USB-носителе для хранения журнала.
Logging Client Source Interface	Показывает интерфейс, адрес которого используется в качестве IP-адреса источника для syslog.
CLI Command Logging	Показывает, включено ли ведение журнала вводимых команд .
Logging Protocol	Номер версии протокола syslog. 0: RFC 3164 1: RFC 5424
Console Logging	Показывает, включено ли ведение журнала в консоли.

Console Logging Severity Filter	Минимальный уровень критичности для регистрации в журнале в консоли. Регистрируются сообщения с равным или меньшим числовым значением уровня критичности.
Buffered Logging	Показывает, включен ли журнал в памяти.
Persistent Logging	Показывает, включено ли ведение журнала с сохранением в память.
Persistent Logging Severity Filter	Минимальный уровень кричитности для регистрации в журнале с постоянным сохранением в память.
Syslog Logging	Показывает, включена ли отправка журнала на сервер syslog.
Syslog Logging Facility	Показывает значение для объекта syslog.
Log Messages Received	Количество записей, полученных в процессе ведения журнала. Включает сообщения, которые были отброшены или проигнорированы.
Log Messages Dropped	Количество сообщений, которые не удалось обработать из-за ошибки или отсутствия ресурсов.
Log Messages Relayed	Количество сообщений, отправленных на коллектор/реле.

show logging buffered

Команда отображает журналы в буфере (журналы запуска и работы системы).

Формат: `show logging buffered`

Режим ввода команд: привилегированный

Термин	*Значение*
Buffered (In- Memory) Logging	Показывает, включен ли журнал в памяти.
Buffered Logging Wrapping Behavior	Действия журнала в памяти при достижении максимального объема.
Buffered Log Count	Количество действительных записей журнала в буфере.

show logging hosts

Команда вывода всех настроенных серверов syslog.

Формат: `show logging hosts`

Режим ввода команд: привилегированный

Термин	*Значение*
Host Index	Используется для удаления серверов.
IP Address / Hostname	IP-адрес или имя сервера syslog.
Severity Level	Минимальный уровень критичности для регистрации по указанному адресу. Возможные значения: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) или debug (7).
Port	Номер порта удалённого коллектора/реле, на который отправляются сообщения журнала syslog.
Status	Поле статуса, которое показывает текущий статус (Active, Not in Service, Not Ready).

Mode	Тип безопасности: UDP или TLS.
Auth	Тип аутентификации: anonymous или x509name.
Cert #	Номер сертификата, используемый для аутентификации. Диапазон допустимых значений: 0–8. Индекс 0 используется по умолчанию.

show logging persistent

Команда отображает записи в журнале постоянного хранения. Если указан параметр log-files, выводятся список файлов журналов постоянного хранения.

Формат: `show logging persistent [log-files]`

Режим ввода команд: привилегированный

Параметр	*Описание*
Persistent Logging	Показывает, включено или выключено ведение журнала с постоянным хранением.
Persistent Log Count	Количество записей в журнале постоянного хранения.
Persistent Log Files	Список файлов журналов постоянного хранения в системе. Отображается, если указан параметр `log-files`.

show logging traplogs

Команда отображает события и статистику SNMP-трапов.

Формат: `show logging traplogs`

Режим ввода команд: привилегированный

Параметр	*Значение*
Number of Traps Since Last Reset	Количество трапов с момента последней загрузки.
Trap Log Capacity	Количество трапов, которые система может хранить.
Number of Traps Since Log Last Viewed	Количество новых трапов с прошлого исполнения данной команды.
Log	Номер журнальной записи.
System Time Up	Время работы системы на момент отправки трапа.
Trap	Текст сообщения трапа.

clear logging buffered

Команда очищает журналы в буфере (журналы запуска и работы системы).

Формат: `clear logging buffered`

Режим ввода команд: привилегированный

6.7 Настройка оповещений по электронной почте и почтового сервера

logging email

Эта команда включает оповещения по электронной почте и устанавливает минимальный уровень критичности для отправки системных сообщений. Если уровень критичности задан, системные сообщения с критичностью выше этого уровня, но ниже уровня срочной отправки будут отправляться в рабочем порядке, объединенные за определенное время. Значение severitylevel можно задать как целыми числами от 0 до 7, так и описательно, с использованием следующих ключевых слов: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) или debug (7).

Значение по умолчанию: выключено; если включено, ведется отправка сообщений уровня Warning (4) или выше

Формат: `logging email` *`[severitylevel]`*

Режим ввода команд: глобальная конфигурация

no logging email

Команда выключает почтовые оповещения.

Формат: `no logging email`

Режим ввода команд: глобальная конфигурация

logging email urgent

Команда устанавливает минимальный уровень критичности, на котором системные сообщения отправляются по электронной почте мгновенно, отдельными письмами. Значение `severitylevel` можно задать как целыми числами от 0 до 7, так и описательно, с использованием следующих ключевых слов: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) или debug (7). Значение none указывает, что системные сообщения будут отправляться в объединенном виде с указанным интервалом.

Значение по умолчанию: мгновенно отправляются сообщения уровня alert (1) и emergency (0).

Формат: `logging email urgent {`*`severitylevel`* `|` `none}`

Режим ввода команд: глобальная конфигурация

no logging email urgent

Эта команда устанавливает уровень критичности для срочных сообщений в значение по умолчанию.

Формат: `no logging email urgent`

Режим ввода команд: глобальная конфигурация

logging email message-type to-addr

Команда позволяет настроить адрес электронной почты для отправки сообщений. Типы сообщений можно задать как *`urgent`*, *`non-urgent`* и *`both`*. Для каждого уровня критичности можно указать

несколько адресов электронной почты. Переменная *to-email-addr* — стандартный адрес электронной почты, например admin@yourcompany.com.

Формат: `logging email message-type {urgent |non-urgent |both} to-addr` *to-email-addr*

Режим ввода команд: глобальная конфигурация

no logging email message-type to-addr

Команда удаляет настроенное значение электронной почты для отправки.

Формат: `no logging email message-type {urgent |non-urgent |both} to-addr` *to-email-addr*

Режим ввода команд: глобальная конфигурация

logging email from-addr

Настройка адреса электронной почты отправителя (коммутатора).

Значение по умолчанию: switch@rusteletech.ru

Формат: `logging email from-addr` *from-email-addr*

Режим ввода команд: глобальная конфигурация

no logging email from-addr

Команда удаляет настроенный адрес отправителя.

Формат: `no logging email from-addr` *from-email-addr*

Режим ввода команд: глобальная конфигурация

logging email message-type subject

Команда позволяет настроить тему отправляемых писем по типам.

Значение по умолчанию: Для срочных сообщений: Urgent Log Messages

Для несрочных сообщений: Non Urgent Log Messages

Формат: `logging email message-type {urgent |non-urgent |both} subject` *subject*

Режим ввода команд: глобальная конфигурация

no logging email message-type subject

Команда удаляет настроенные значения тем для отправляемых писем и возвращает настройки тем по умолчанию.

Формат: `no logging email message-type {urgent |non-urgent |both} subject`

Режим ввода команд: глобальная конфигурация

logging email logtime

Позволяет настроить частоту отправки несрочных сообщений электронной почты. Несрочные системные сообщения отправляются в объединенном виде одним письмом с указанным интервалом. Допустимый диапазон значений: от 30 до 1440 минут.

Значение по умолчанию: 30 минут

Формат: `logging email logtime` *`minutes`*

Режим ввода команд: глобальная конфигурация

no logging email logtime

Эта команда возвращает частоту отправки несрочных сообщений электронной почты в значение по умолчанию.

Формат: `no logging email logtime`

Режим ввода команд: глобальная конфигурация

logging traps

Команда устанавливает уровень критичности, при котором SNMP-трапы заносятся в журнал и отправляются по электронной почте. Значение *`severitylevel`* можно задать как целыми числами от 0 до 7, так и описательно, с использованием следующих ключевых слов: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6) или debug (7).

Значение по умолчанию: фиксируются сообщения уровня Info (6) и выше.

Формат: `logging traps` *`severitylevel`*

Режим ввода команд: глобальная конфигурация

no logging traps

Возвращает значение уровня критичности, при котором SNMP-трапы заносятся в журнал в значение по умолчанию.

Формат: `no logging traps`

Режим ввода команд: глобальная конфигурация

logging email test message-type

Команда для отправки сообщения электронной почты на сервер SMTP с целью тестирования функции отправки оповещений.

Формат: `logging email test message-type {urgent |non-urgent |both} message-body` *`message-body`*

Режим ввода команд: глобальная конфигурация

show logging email config

Данная команда выводит информацию о настройках оповещений по электронной почте.

Формат: `show logging email config`

Режим ввода команд: привилегированный

Термин	*Значение*
Email Alert Logging	Административное состояние функции: включена или выключена.
Email Alert From Address	Электронная почта отправителя (коммутатора).
Email Alert Urgent Severity Level	Минимальный уровень критичности, который считается срочным. Сообщения этого типа отправляются сразу.
Email Alert Non Urgent Severity Level	Минимальный уровень критичности, который считается несрочным. Сообщения этого типа, за исключением сообщений срочного уровня, отправляются в объединенном письме. Системные сообщения более низкого уровня не отправляются совсем.
Email Alert Trap Severity Level	Минимальный уровень критичности для регистрации трапов в журнале.
Email Alert Notification Period	Интервал времени между отправками несрочных сообщений.
Email Alert To Address Table	Настроенные получатели электронной почты.
Email Alert Subject Table	Строки тем для срочных (Type 1) и несрочных (Type 2) сообщений электронной почты.
For Msg Type urgent, subject is	Настроенная тема для отправки срочных сообщений.
For Msg Type non-urgent, subject is	Настроенная тема для отправки несрочных сообщений.

show logging email statistics

Команда вывода статистики оповещений по электронной почте.

Формат: `show logging email statistics`

Режим ввода команд: привилегированный

Термин	*Значение*
Email Alert Operation Status	Оперативный статус функции оповещений по электронной почте.
No of Email Failures	Количество писем, при отправке которых произошли ошибки.
No of Email Sent	Количество писем, отправленных с коммутатора с момента последнего сброса счетчика.
Time Since Last Email Sent	Время, прошедшее с момента отправки последнего письма с коммутатора.

clear logging email statistics

Команда для сброса статистики почтовых оповещений.

Формат: `clear logging email statistics`

Режим ввода команд: привилегированный

mail-server

Эта команда настраивает SMTP-сервер, через который коммутатор отправляет оповещения по электронной почте. Режим при этом меняется на режим конфигурирования почтового сервера. Адрес сервера может быть указан в формате IPv4, IPv6 или DNS.

Формат: `mail-server {`*`ip-address`* | *`ipv6-address`* | *`hostname`*`}`

Режим ввода команд: глобальная конфигурация

no mail-server

Команда для удаления указанного SMTP-сервера из конфигурации.

Формат: `no mail-server {`*`ip-address`* | *`ipv6-address`* | *`hostname`*`}`

Режим ввода команд: глобальная конфигурация

security

Команда для установки протокола безопасности для отправки оповещений по электронной почте: включает на коммутаторе аутентификацию TLS для SMTP-сервера. Если TLS на коммутаторе включен, а SMTP-сервер не поддерживает режим TLS, отправка электронной почты будет невозможна.

Значение по умолчанию: отсутствует

Формат: `security {tlsv1 | none}`

Режим ввода команд: конфигурирование почтового сервера

port

Команда настройки TCP-порта для связи с SMTP-сервером. Рекомендуемый порт для TLS версии 1 — 465, при отсутствии настроек безопасности — 25. Допустимо также использовать любой нестандартный порт в диапазоне 1–65535.

Значение по умолчанию: 25

Формат: `port {465 | 25 | 1–65535}`

Режим ввода команд: конфигурирование почтового сервера

username (в режиме конфигурирования почтового сервера)

Настраивает идентификатор логина, который коммутатор использует при аутентификации на SMTP-сервере.

Значение по умолчанию: admin

Формат: `username` *`name`*

Режим ввода команд: конфигурирование почтового сервера

password

Настраивает пароль, который коммутатор использует при аутентификации на SMTP-сервере.

Значение по умолчанию: admin

Формат: `password` *`password`*

Режим ввода команд: конфигурирование почтового сервера

show mail-server config

Данная команда выводит информацию о настройках оповещений по электронной почте.

Формат: `show mail-server {`*`ip-address`* | *`hostname`* | `all} config`

Режим ввода команд: привилегированный

Термин	*Значение*
No of mail servers configured	Количество SMTP-серверов, настроенных на коммутаторе.
Email Alert Mail Server Address	Настройка адреса IPv4/IPv6 или имени узла DNS для SMTP-сервера.
Email Alert Mail Server Port	Порт TCP, используемый коммутатором для отправки электронной почты SMTP-серверу.
Email Alert Security Protocol	Протокол безопасности (TLS или отсутствует), используемый коммутатором при аутентификации на SMTP-сервере.
Email Alert Username	Имя пользователя (логин), которое коммутатор использует при аутентификации на SMTP-сервере.
Email Alert Password	Пароль, который коммутатор использует при аутентификации на SMTP-сервере.

6.8 Служебные утилиты и команды очистки

В этой части описаны команды для диагностики проблем связи, а также для сброса конфигурации к заводским настройкам.

traceroute

Команда `traceroute` используется для поэтапного обнаружения маршрутов, которыми в действительности следуют пакеты IPv4 или IPv6 при перемещении по сети в место назначения. Данная команда продолжает выводить синхронный ответ, когда инициируется в CLI.

Для проверки с помощью этой команды можно задать IP-адрес источника или виртуальный маршрутизатор. Следует помнить, что команда traceroute отправляет пакеты, которые заведомо не должны достигать места назначения, вызывая вместо этого сообщения об ошибках ICMP, которые на каждом хопе маршрута к месту назначения возвращаются в адрес источника. Задавая адрес источника, можно определить, на каком участке маршрута к месту назначения отсутствует обратная связь с адресом источника. Это применимо лишь в тех случаях, когда маршрут от источника до места назначения и обратно является симметричным. К примеру, часто команду traceroute запускают на периферийном маршрутизаторе, чтобы получить отклик от целевого узла более высокого уровня, при этом в качестве адреса источника используется узел в подсети периферийного маршрутизатора. Это

позволяет протестировать доступность маршрутов из сети к узлам, подключенным к периферийному маршрутизатору. Как вариант, можно выполнить команду traceroute с адресом источника в loopback-интерфейсе, чтобы протестировать доступность обратного маршрута к адресу loopback-интерфейса.

Источник в CLI можно определить как адрес IPv4 или IPv6, виртуальный маршрутизатор или как интерфейс маршрутизации. Когда источник задан как интерфейс маршрутизации, traceroute отправляется с использованием основного адреса IPv4 заданного интерфейса. При использовании SNMP необходимо задать источник как адрес. При работе через веб-интерфейс источник задать нельзя.

ПО не примет входящий пакет, например, ответ traceroute, на интерфейсе маршрутизации, если адрес назначения пакета относится к сервисному (out-of-band) интерфейсу управления (сервисный или сетевой порт). Аналогичным образом ПО не примет пакет в сервисном интерфейсе, если его адрес назначения принадлежит к интерфейсу маршрутизации. Соответственно, бесполезно отправлять traceroute на интерфейс управления, используя в качестве источника адрес интерфейса маршрутизации, или отправлять traceroute на интерфейсе маршрутизации, используя в качестве источника интерфейс управления. При отправке traceroute на интерфейс маршрутизации источник должен принадлежать этому или иному интерфейсу маршрутизации. При отправке traceroute на интерфейс управления источник должен принадлежать этому интерфейсу управления. Соответственно, нельзя задать источник как интерфейс управления или принадлежащий к нему адрес. При отправке traceroute на интерфейсе управления указывать адрес источника не нужно, система сама выбирает адрес источника на основании исходящего интерфейса.

Значение по умолчанию: count: 3 попытки
interval: 3 секунды
size: 0 байт
port: 33434
maxTtl: 30 хопов
maxFail: 5 попыток
initTtl: 1 хоп

Формат: `traceroute [vrf` *`vrf-name`*`] {`*`ip-address`*` | [ipv6] {`*`ipv6-address`*` | `*`hostname`*`}} [initTtl` *`initTtl`*`][maxTtl` *`maxTtl`*`] [maxFail` *`maxFail`*`] [interval` *`interval`*`] [count` *`count`*`] [port` *`port`*`] [size` *`size`*`] [source {`*`ip-address`*` | | `*`ipv6-address`*` | `*`unit/slot/port`*`}]`

Режим ввода команд: привилегированный

Используя опции, описанные ниже, можно указать стартовое и максимальное значение TTL для тестовых пакетов, максимальное количестве отказов до завершения, количество попыток отправки на каждом TTL и размер тестового пакета.

Параметр	*Описание*
vrf-name	Имя объекта виртуальной маршрутизации (VRF), с которого происходит запуск traceroute. Запускать traceroute можно только для узлов, доступных для данного объекта VRF. Если в дополнение к параметру VRF также указан параметр source, то источник также должен относится к указанному VRF. Параметры IPv6 нельзя использовать в сочетании с настройками VRF.
ipaddress	Значение ipaddress должно быть действительным IP-адресом.
ipv6-address	Значение ipv6-address должно быть действительным IPv6-адресом.
hostname	Значение hostname должно быть действительным именем узла.
ipv6	Необязательное ключевое слово ipv6 можно использовать перед параметрами ipv6-address или hostname. При указании ключевого слова ipv6

	перед hostname команда пытается разрешить указанное имя узла как IPv6-адрес.
initTtl	Задает начальное время жизни (TTL), максимальное количество хопов маршрутизатора между локальной и удаленной системой. Допустимые значения: от 0 до 255.
maxTtl	Задает максимальное значение TTL. Допустимые значения: от 1 до 255.
maxFail	Завершает выполнение traceroute после заданного количества неудачных попыток получить ответ подряд. Допустимые значения: от 0 до 255.
interval	Необязательный параметр interval определяет время между попытками в секундах. Если ответ не получен за указанное время, traceroute считает попытку неудачной (отображает знак *) и отправляет следующий тестовый пакет. Если traceroute получает ответ в заданном интервале, сразу же происходит отправка следующего пакета. Допустимые значения: от 1 до 60 секунд.
count	Необязательный параметр count определяет количество попыток для каждого значения TTL. Допустимые значения: 1–10 попыток
port	Необязательный параметр port определяет целевой UDP-порт для отправки тестовых пакетов. Это должен быть неиспользуемый порт в удаленной системе назначения. Допустимые значения: от 1 до 65535.
size	Необязательный параметр size определяет размер полезной нагрузки (в байтах) для отправляемых запросов. Допустимые значения от 0 до 13000 байт.
source	Необязательный параметр source определяет IP-адрес или интерфейс источника для traceroute.

clear config

Эта команда сбрасывает конфигурацию к заводским настройкам, не выключая коммутатор. При выполнении данной команды выводится запрос на подтверждение сброса конфигурации. При ответе y (да) текущая конфигурация на коммутаторе сбрасывается до значений по умолчанию. Перезагрузка коммутатора не происходит.

Формат: `clear config`

Режим ввода команд: привилегированный

clear counters

В зависимости от используемых аргументов данная команда сбрасывает статистику (включая счетчики функции защиты от петель) для конкретного объекта unit/slot/port, для всех портов или для интерфейса VLAN. Если указан виртуальный маршрутизатор, сбрасывается статистика портов на виртуальном маршрутизаторе. Если маршрутизатор не указан, будет использован маршрутизатор по умолчанию.

Формат: `clear counters {`*`unit/slot/port`* `| all [vrf` *`vrf-name`*`] | vlan` *`id`*`}`

Режим ввода команд: привилегированный

clear igmpsnooping

Данная команда очищает таблицы, которыми управляет функция IGMP Snooping, и пытается удалить эти записи из таблицы коммутации многоадресного трафика.

Формат: `clear igmpsnooping`

Режим ввода команд: привилегированный

clear ip access-list counters

Команда сброса счетчиков списка ACL для указанного имени IP ACL и номера правила IP ACL.

Формат: `clear ip access-list counters` *`acl-ID | acl-name rule-id`*

Режим ввода команд: привилегированный

clear ipv6 access-list counters

Команда сброса счетчиков списка ACL для указанного имени IP ACL и номера правила IP ACL.

Формат: `clear ipv6 access-list counters` *`acl-name rule-id`*

Режим ввода команд: привилегированный

clear mac access-list counters

Команда сброса счетчиков списка ACL для указанного имени MAC ACL и номера правила MAC ACL.

Формат: `clear mac access-list counters` *`acl-name rule-id`*

Режим ввода команд: привилегированный

clear pass

Команда сбрасывает все пользовательские пароли к заводским настройкам, не выключая коммутатор. При исполнении выводится запрос на подтверждение сброса паролей.

Формат: `clear pass`

Режим ввода команд: привилегированный

clear traplog

Команда очищает журнал трапов.

Формат: `clear traplog`

Режим ввода команд: привилегированный

clear vlan

Эта команда сбрасывает параметры конфигурации VLAN к заводским настройкам. У сброса конфигурации VLAN есть несколько последствий, касающихся GVRP:

1. Статические VLAN удаляются.
2. GVRP восстанавливается до заводских настроек в результате обработки события VLAN RESTORE NOTIFY. Так как GVRP по умолчанию выключен, в результате GVRP выключается, а все его динамические VLAN — удаляются.

Формат: `clear vlan`

Режим ввода команд: привилегированный

logout

Эта команда закрывает текущее соединение Telnet или сбрасывает текущее последовательное соединение.

Перед выполнением команды сохраните изменения конфигурации.

Формат: `logout`

Режимы ввода команд: привилегированный
пользовательский

ping

Используйте эту команду, чтобы определить, есть ли другой компьютер в сети. Ping выводит синхронный ответ при запуске в CLI и веб-интерфейсах.

Количество по умолчанию: 3 пакета

Интервал по умолчанию: 3 секунды

Размер по умолчанию: 0 байт

Формат: `ping [vrf vrf-name] {ip-address| hostname | {ipv6 {interface {unit/slot/port | vlan 1-4093 | loopback loopback-id | network | serviceport | tunnel tunnel-id } link-local- address} | ip6addr | hostname} [count count] [interval interval] [size size] [source ip- address | ip6addr | {unit/slot/port | vlan 1-4093 | serviceport | network}] [outgoing-interface {unit/slot/port | vlan 1-4093 | serviceport | network}]`

Режимы ввода команд: привилегированный
пользовательский

Используя описанные ниже опции, можно задать количество и размер запросов, а также интервал между ними.

Параметр	*Описание*
vrf-name	Имя виртуального маршрутизатора, на котором будет инициирована команда ping. Если виртуальный маршрутизатор не указан, команда инициируется на маршрутизаторе по умолчанию.
address	IPv4- или IPv6-адреса для отправки запроса.

count	Параметр count используется, чтобы задать количество пакетов ping (запросов ICMP) для отправки по адресу назначения, который указан в поле ip-address. Диапазон значений: 1–15 запросов.
interval	Параметр interval определяет время между запросами в миллисекундах. Допустимые значения: от 100 до 60000 миллисекунд.
size	Параметр size определяет размер полезной нагрузки (в байтах) для отправляемых запросов. Допустимые значения от 0 до 13000 байт.
source	Параметр source задает IP/IPv6-адрес или интерфейс источника, который будет использован при отправке запросов.
hostname	Параметр hostname используется для разрешения адреса IPv6 или IPv4. Ключевое слово ipv6 указывает, что имя узла требуется разрешить к IPv6-адресу. Адрес IPv4 используется, если ключевое слово не задано.
ipv6	Необязательное ключевое слово ipv6 может использоваться перед параметрами ipv6-address или hostname. Если необязательное ключевое слово ipv6 стоит перед hostname, имя узла требуется разрешить к IPv6-адресу. Ключевое слово также используется для проверки link-local IPv6-адреса.
interface	Ключевое слово interface используется для проверки с помощью ping-запросов link-local IPv6-адреса через данный интерфейс
link-local- address	link-local IPv6-адрес для проверки с помощью ping-запросов.
outgoing- interface	Используйте параметр outgoing-interface, чтобы определить исходящий интерфейс при отправке запросов ping на многоадресный IP/IPv6-адрес.

quit

Эта команда закрывает текущее соединение Telnet или сбрасывает текущее последовательное соединение. Система выдает запрос на сохранение изменений конфигурации перед выходом.

Формат: `quit`

Режимы ввода команд: привилегированный
пользовательский

reload

Эта команда перезагружает коммутатор. Перезагрузка означает, что все сетевые соединения завершаются и выполняется начальный загрузчик. Коммутатор использует для инициализации сохраненную конфигурацию. При выполнении без параметров выводится запрос на подтверждение сохранения конфигурации и подтверждение перезагрузки.

Формат: `reload [configuration [`*`scriptname`*`]]`
Режим ввода команд: привилегированный

Параметр	*Описание*
configuration	Перезагружает конфигурацию без перезагрузки коммутатора. Если имя файла конфигурации не определен, загружается файл стартовой конфигурации.
scriptname	Имя файла конфигурации для загрузки. Имя файла должно включать расширение scr.

copy

Команда загружает файлы на коммутатор и выгружает их с него. Использовать команду copy можно для управления в файловой системе двойными образами ПО (активным и резервным). Выгрузка и загрузка файлов с сервера происходит с использованием FTP, TFTP, Xmodem, Ymodem или Zmodem. SFTP и SCP доступны как дополнительные методы передачи, если пакет программного обеспечения поддерживает безопасное управление. Если используется FTP, требуется пароль.

Формат: `copy source destination {verify | noverify}`

Режим ввода команд: привилегированный

Замените параметры *source* и *destination* опциями из таблицы ниже. Для url источника или места назначения используйте одно из следующих значений:

{xmodem | ymodem | zmodem |

tftp://<ipaddress|hostname>/<filepath>/<filename>|

ftp://<*username*>@<ipaddr|hostname>/< filepath>/<filename> |

scp://<*username*>@<ipaddr|hostname>/< filepath>/<filename> |

sftp://<*username* >@<ipaddr|hostname>/< filepath>/<filename>

| usb://<filepath>/<filename>}

Параметр `verify | noverify` доступен, только если для образа ПО/конфигурации включена функция проверки цифровой подписи (см. «file verify»). verify определяет, что для указанного загруженного образа или файла конфигурации будет выполняться проверка цифровой подписи. noverify определяет, что проверка не будет выполняться.

Ключевое слово `ias-users` поддерживает загрузку пользовательского файла базы данных IAS. После загрузки этого файла пользовательская база данных для IAS коммутатора будет заменена пользователями и связанными атрибутами из загруженного файла. В команде `copy url ias-users` используется для одно из следующих значений URL пользовательского файла IAS:

{ tftp://<ipaddress|hostname>/<filepath>/<filename>|

ftp://<username >@<ipaddr|hostname>/<filepath>/<filename> |

scp://<username >@<ipaddr|hostname>/<filepath>/<filename> |

sftp://<username >@<ipaddr|hostname>/<filepath>/<filename> |

usb://<filepath>/<filename>}

Максимальная длина пути к файлу — 160 символов, максимальная длина для имени файла — 128 символов.

Для FTP, TFTP, SFTP и SCP параметр `ipaddr|hostname` — это IP-адрес или имя сервера, `filepath` — путь к файлу, `filename` — имя файла, который требуется выгрузить или загрузить. Для SFTP и SCP параметр username — это имя пользователя для входа на удаленный сервер по SSH.

В стеке можно использовать необязательный параметр [unit unit id] (если доступен), чтобы указать юнит стека, используемый в качестве источника при копировании. Если юнит не задан, элемент копируется с главного юнита стека.

В целях резервного копирования не забудьте выгрузить существующий файл конфигурации с коммутатора до загрузки образа нового релиза.

Source	***Destination***	***Описание***
nvram:application:*sourcefilename*	url	Исходное имя файла приложения
nvram:backup-config	nvram:startup-config	Копирование резервной конфигурации в стартовую конфигурацию.
nvram:clibanner	url	Копирует баннер CLI на сервер.
nvram: core-dump [unit *unit id*]	tftp:// <ipaddress|hostname>/ <filepath>/<filename>| ftp:// <user>@<ipaddr|hostnam e>/<path>/<filename> | scp:// <user>@<ipaddr|hostnam e>/<path>/<filename> | sftp:// <user>@<ipaddr|hostnam e>/<path>/<filename>}	Выгружает файл дампа памяти локальной системы на внешний сервер TFTP/FTP/SCP/SFTP.
nvram:cpupktcapture.pcap [unit *unit id*]	url	Выгружает файл захвата пакетов CPU.
nvram:crash-log	url	Копирует журнал сбоев на сервер.
nvram:errorlog	url	Копирует журнал ошибок на сервер.
nvram:factory-defaults	url	Выгружает файл заводских настроек.
nvram:fastpath.cfg	url	Выгружает двоичный файл конфигурации на сервер.
nvram:log	url	Копирует файл журнала на сервер.
nvram:operational-log [unit unit id]	url	Копирует файл операционного журнала на сервер.
nvram:persistent-log	url	Копирует текущий файл и все архивы на сервер одним архивом.
nvram:script scriptname	url	Копирует указанный файл сценария конфигурации на сервер.
nvram:startup-config	nvram:backup-config	Копирует стартовую конфигурацию в резервную конфигурацию.
nvram:startup-config	url	Копирует стартовую конфигурацию на сервер.

nvram:startup-log [unit unit id]	url	Выгружает файл журнала запусков.
nvram: tech-support [unit *unit id*]	url	Выгружает системную и конфигурационную информацию для технической поддержки.
nvram:traplog	url	Копирует файл журнала трапов на сервер.
system:running-config	nvram:startup-config	Сохраняет текущую конфигурацию в энергонезависимой памяти.
system:running-config	nvram:factory-defaults	Сохраняет текущую конфигурацию в энергонезависимой памяти в файл заводских настроек.
system:image	url	Сохраняет образ системы на сервер.
tftp:// <ipaddress>/ <filename>	system:packet.pcap	Копирует файл PCAP в RAM. Файл PCAP используется для инъекции пакетов в микросхему в целях трассировки.
url	nvram:application destfilename	Имя целевого файла для файла приложения.
url	nvram:backup-config	Загружает файл резервной конфигурации.
url	nvram:ca-root index	Загружает файл сертификата CA во флеш-память и устанавливает имя сохранённого файла в CAindex.pem.
url	nvram:clibanner	Загружает баннер CLI в систему.
url	nvram:client-key index	Загружает клиентский файл ключей во флеш-память и устанавливает имя сохранённого файла в CAindex.key.
url	nvram:client-ssl-cert *1-8*	Загружает клиентский сертификат во флеш-память и устанавливает имя.
url	nvram:factory-defaults	Загружает файл заводских настроек.
url	nvram:fastpath.cfg	Загружает в систему двоичный файл конфигурации.
url	nvram:license-key	Загружает файл лицензии.
url	nvram:publickey-config	Загружает публичный ключ для проверки сценария конфигурации.
url	nvram:publickey-image	Загружает публичный ключ для проверки образа ПО.

url	nvram:script destfilename	Загружает файл сценария конфигурации в систему. Во время загрузки сценария конфигурации команда копирования проверяет сценарий. В случае любой ошибки команда составляет список всех строк в конце процесса проверки и запрашивает подтверждение перед копированием файла сценария.
url	nvram:script *destfilename* noval	При использовании этой опции команда копирования не будет проверять загруженный файл сценария. Пример команды CLI: (Routing) #copy tftp://1.1.1.1/file.scr nvram:script file.scr noval
url	nvram:sshkey-dsa	Загружает файл SSH-ключей.
url	nvram:sshkey-rsa1	Загружает файл SSH-ключей.
url	nvram:sshkey-rsa2	Загружает файл SSH-ключей.
url	nvram:sslpem-dhweak	Загружает сертификат защищенного HTTP-сервера.
url	nvram:sslpem-dhstrong	Загружает сертификат защищенного HTTP-сервера.
url	nvram:sslpem-root	Загружает сертификат защищенного HTTP-сервера.
url	nvram:sslpem-server	Загружает сертификат защищенного HTTP-сервера.
url	nvram:startup-config	Загружает в систему файл стартовой конфигурации.
url	ias-users	Загружает в систему пользовательский файл базы данных IAS. Когда пользовательский файл IAS загружен, база данных IAS на коммутаторе заменяется пользователями и их атрибутами, доступными в загруженном файле.
url	nvram:tech-support-cmds	Загружает файл со списком команд, которые будут выводиться при выполнении команды show tech-support.
url	{active | backup}	Загружает с удаленного сервера образ в качестве любого из образов ПО. В среде стекирования загруженный образ ПО распространяется на все узлы стека.
{active | backup}	url	Выгружает любой из образов ПО на удаленный сервер.

active	backup	Копирует активный образ ПО в резервный образ.
backup	active	Копирует резервный образ ПО в активный образ.
{active | backup}	unit://unit/{active | backup}	Копирует образ ПО с узла управления в определенный узел стека. Используйте параметр unit, чтобы задать узел, в который требуется скопировать образ.
{active | backup}	unit://unit/{active | backup}	Копирует образ ПО с узла управления на все узлы стека.

file verify

Эта команда включает проверку цифровой подписи в процессе загрузки образа ПО и/или файла конфигурации на коммутатор.

Формат: `file verify {all | image | none | script}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
All	Проверяет цифровую подпись образа ПО и файлов конфигурации.
Image	Проверяет только цифровую подпись файлов образов.
None	Выключает проверку цифровой подписи для образов ПО и файлов конфигурации.
Script	Проверяет только цифровую подпись файлов конфигурации.

no file verify

Сбрасывает настройку проверки цифровой подписи к значению по умолчанию.

Формат: `no file verify`

Режим ввода команд: глобальная конфигурация

ip scp server enable

Команда включает функциональность SCP-сервера для push-операций SCP на коммутаторе, что позволяет передавать файлы с хост-устройства на коммутатор по протоколу SCP. Во время передачи SCP-файла операции управления на коммутаторе блокируются. После завершения загрузки файла коммутатор выполняет его проверку аналогично другим операциям загрузки, выполняемым при помощи команды copy.

Чтобы разрешить передачу файлов по SCP от хост-системы к коммутатору, на нем должен быть включен сервер SCP.

Значение по умолчанию: выключено

Формат: `ip scp server enable`

Режим ввода команд: привилегированный

Передача инициируется через CLI в хост-системе, а не из CLI коммутатора. В следующих примерах показан синтаксис push-команд SCP, исполняемых на хосте ПК для файлов конфигурации и прошивки:

```
scp <config file> user@<scp server IP>:startup-config
scp <config file> user@<scp server IP>:backup-config
scp <config file> user@<scp server IP>:factory-defaults
scp <config file> user@<scp server IP>:<scriptfile.scr>
scp <image file> user@<scp server IP>:active
scp <image file> user@<scp server IP>:backup
```

no ip scp server enable

Эта команда сбрасывает функционал SCP-сервера для push-операций SCP на коммутаторе на значение по умолчанию (отключено).

Формат: `no ip scp server enable`

Режим ввода команд: привилегированный

write memory

Команда позволяет сохранить текущие изменения конфигурации в энергонезависимую память, чтобы все изменения сохранились после перезагрузки. Результат выполнения совпадает с командой `copy system:running-config nvram:startup-config`. Используйте ключевое слово confirm, чтобы сохранить конфигурацию в энергонезависимую память без подтверждения.

Формат: `write memory [confirm]`

Режим ввода команд: привилегированный

6.9 Управление лицензиями для расширенных функций

В этой части описаны команды, которые используются для загрузки лицензионных ключей и доступа к расширенным функциям. Доступ к расширенным функциям без лицензионного ключа невозможен.

copy <url> nvram:license-key

Загрузить файл лицензии на устройство**.**

Значение по умолчанию: отсутствует

Формат: `copy <tftp|ftp|scp|sftp|usb://<ipaddr>/<filepath>/<filename>> |xmodem|ymodem|zmodem nvram:license-key`

Режим ввода команды: привилегированный режим

delete license-key

С помощью этой команды можно удалить файл лицензии.

Значение по умолчанию: выключено

Формат: `delete license-key`

Режим ввода команды: режим глобальной конфигурации

show license

Просмотреть состояние лицензии на текущий момент.

Формат: `show license`

Режим ввода команды: привилегированный режим

show license features

Просмотреть список лицензируемых компонентов.

Формат: `show license features`

Режим ввода команды: привилегированный режим

6.10 Настройка SNTP

В этой части приведены команды автоматической настройки системного времени и даты с помощью Simple Network Time Protocol (SNTP).

sntp broadcast client poll-interval

Команда задает интервал опроса широковещательного клиента SNTP в секундах, равный двум в степени poll-interval. Значение poll-interval может быть от 6 до 10.

Значение по умолчанию: 6

Формат: `sntp broadcast client poll-interval` *`poll-interval`*

Режим ввода команд: глобальная конфигурация

no sntp broadcast client poll-interval

Сброс интервал опроса широковещательного клиента SNTP к значению по умолчанию.

Формат: `no sntp broadcast client poll-interval`

Режим ввода команд: глобальная конфигурация

sntp client mode

Команда включает режим SNTP-клиента и может установить режим широковещательной или одноадресной передачи.

Значение по умолчанию: выключено

Формат: `sntp client mode [`*`broadcast`* `|` *`unicast`*`]`

Режим ввода команд: глобальная конфигурация

no sntp client mode

Команда выключает режим SNTP-клиента.

Формат: `no sntp client mode`

Режим ввода команд: глобальная конфигурация

sntp client port

Команда устанавливает идентификатор порта SNTP-клиента в значение 0, 123 или иное значение между 1025 и 65535. Значение по умолчанию 0 (порт SNTP не настроен пользователем). В этом случае фактическое значение порта клиента, используемое в пакетах SNTP будет назначено ОС.

Значение по умолчанию: 0

Формат: `sntp client port` *`portid`*

Режим ввода команд: глобальная конфигурация

no sntp client port

Сброс клиентского порта SNTP к значению по умолчанию.

Формат: `no sntp client port`

Режим ввода команд: глобальная конфигурация

sntp unicast client poll-interval

Команда задает интервал опроса одноадресного клиента SNTP в секундах, равный двум в степени poll-interval. Значение poll-interval может быть от 6 до 10.

Значение по умолчанию: 6

Формат: `sntp unicast client poll-interval` *`poll-interval`*

Режим ввода команд: глобальная конфигурация

no sntp unicast client poll-interval

Эта команда сбрасывает интервал опроса для одноадресного SNTP-клиента к значению по умолчанию.

Формат: `no sntp unicast client poll-interval`

Режим ввода команд: глобальная конфигурация

sntp unicast client poll-timeout

Команда устанавливает интервал опроса для одноадресного SNTP-клиента в секундах. Значение poll-timeout может быть от 1 до 30.

Значение по умолчанию: 5

Формат: `sntp unicast client poll-timeout` *`poll-timeout`*

Режим ввода команд: глобальная конфигурация

no sntp unicast client poll-timeout

Команда для сброса интервала опроса к значению по умолчанию.

Формат: `no sntp unicast client poll-timeout`

Режим ввода команд: глобальная конфигурация

sntp unicast client poll-retry

Команда устанавливает количество повторных попыток опроса для одноадресного SNTP-клиента в значение от 0 до 10.

Значение по умолчанию: 1

Формат: `sntp unicast client poll-retry` *`poll-retry`*

Режим ввода команд: глобальная конфигурация

no sntp unicast client poll-retry

Эта команда сбрасывает количество повторных попыток опроса для одноадресного SNTP-клиента к значению по умолчанию.

Формат: `no sntp unicast client poll-retry`

Режим ввода команд: глобальная конфигурация

sntp server

Команда настраивает сервер SNTP (максимум три). Адрес сервера может быть адресом IPv4 или IPv6 или Hostname. Необязательный приоритет может иметь значение от 1 до 3; значение версии — 1–4; идентификатор порта — 1–65535.

Формат: `sntp server {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`} [`*`priority`* `[`*`version`* `[`*`portid`*`]]]`

Режим ввода команд: глобальная конфигурация

no sntp server

Эта команда удаляет сервер из числа настроенных серверов SNTP.

Формат: `no sntp server remove {`*`ipaddress`* `|` *`ipv6address`* `|` *`hostname`*`}`

Режим ввода команд: глобальная конфигурация

sntp source-interface

Используйте эту команду, чтобы задать физический или логический интерфейс, адрес которого будет использоваться в качестве IP-адреса источника в настройке одноадресного SNTP-сервера. Настроенный адрес источника используется в любом SNTP-соединении между сервером и клиентом SNTP. Выбранный IP-адрес источника используется для заполнения заголовка IP-пакетов протокола управления. Это позволяет устройствам безопасности (брандмауэрам) идентифицировать исходные пакеты, идущие от определенного коммутатора. Если интерфейс не задан, в качестве адреса источника используется основной IP-адрес инициирующего (исходящего) интерфейса. При сбое настроенного интерфейса SNTP-клиент возвращается к алгоритму действий по умолчанию.

Формат: `sntp source-interface {`*`unit/slot/port`* `|` `loopback` *`loopback-id`* `|` `vlan` *`vlan-id`*`}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
unit/slot/port	Идентификатор юнита, присвоенный коммутатору.
loopback-id	Конфигурирует loopback-интерфейс. Диапазон идентификатора loopback от 0 до 7.
tunnel-id	Конфигурирует туннельный интерфейс IPv6. Диапазон туннельного ID от 0 до 7.
vlan-id	Конфигурирует VLAN-интерфейс, чтобы использовать в качестве исходного IP-адреса. Диапазон ID VLAN: 1-4093.

no sntp source-interface

Команда используется, чтобы сбросить IP-адрес источника SNTP к значениям по умолчанию.

Формат: `no sntp source-interface`

Режим ввода команд: глобальная конфигурация

show sntp

Команда отображения настроек SNTP и его состояния.

Формат: `show sntp`

Режим ввода команд: привилегированный

Термин	*Значение*
Last Update Time	Время последнего обновления часов.
Last Attempt Time	Время последнего запроса передачи (в одноадресном режиме).
Last Attempt Status	Состояние последнего запроса SNTP (в одноадресном режиме) или не запрошенного сообщения (в широковещательном режиме).
Broadcast Count	Текущее количество не запрошенных широковещательных сообщений, которые были получены и обработаны SNTP-клиентом с момента последней перезагрузки.

show sntp client

Команда отображения настроек SNTP-клиента.

Формат: `show sntp client`

Режим ввода команд: привилегированный

Термин	*Значение*
Client Supported Modes	Поддерживаемые режимы SNTP (широковещательная или одноадресная передача).
SNTP Version	Последняя версия SNTP, поддерживаемая клиентом.
Port	Порт SNTP-клиента. Значение 0 является значением по умолчанию. Когда значение порта клиента 0, если клиент находится в

	широковещательном режиме, связывается с портом 123; если клиент находится в одноадресном режиме, значение связывается с портом, назначенным ОС.
Client Mode	Настроенный режим SNTP-клиента.

show sntp server

Эта команда используется, чтобы отобразить настройки SNTP-сервера и сконфигурированные серверы.

Формат: `show sntp server`

Режим ввода команд: привилегированный

Термин	*Значение*
Server Host Address	IP-адрес или имя узла сконфигурированного SNTP-сервера.
Server Type	Тип адреса сервера (IPv4, IPv6 или DNS).
Server Stratum	Заявленный уровень часовой слой сервера для последнего полученного действительного пакета.
Server Reference ID	Справочный идентификатор часов сервера для последнего полученного допустимого пакета.
Server Mode	Режим SNTP-сервера.
Server Maximum Entries	Максимальное количество SNTP-серверов.
Server Current Entries	Общее количество сконфигурированных SNTP-серверов.

Параметры для каждого сконфигурированного сервера:

Термин	*Значение*
IP Address / Hostname	IP-адрес или имя узла сконфигурированного SNTP-сервера.
Address Type	Тип адреса сконфигурированного SNTP-сервера (IPv4, IPv6 или DNS).
Priority	Значение приоритета сконфигурированного сервера.
Version	Номер версии SNTP-сервера. Версия протокола, используемая при опросах сервера в одноадресном режиме.
Port	Номер порта сервера.
Last Attempt Time	Время последней попытки для указанного сервера.
Last Update Status	Статус последней попытки для указанного сервера.
Total Unicast Requests	Количество запросов к серверу.
Failed Unicast Requests	Число неудачных запросов к серверу.

show sntp source-interface

Команда отображения адреса источника SNTP-клиента, настроенного на коммутаторе.

Формат: `show sntp source-interface`

Режим ввода команд: привилегированный

Поле	*Описание*
SNTP Client Source Interface	Идентификатор физического или логического интерфейса, адрес которого используется, как IP-адрес источника SNTP-клиента.
SNTP Client Source IPv4 Address	IP-адрес источника SNTP-клиента.

6.11 Настройка часов реального времени

Команды настройки часовых поясов позволяют настроить системное время и дату, часовой пояс и переход на летнее время. Переход на летнее время может выполняться периодически или нет.

clock set

Команда устанавливает системное время и дату.

Формат: `clock set` *`hh:mm:ss`*
`clock set` *`mm/dd/yyyy`*

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
hh:mm:ss	Текущее системное время в 24-часовом формате (часы, минуты, секунды) Диапазон для часов: от 0 до 23, для минут: от 0 до 59, для секунд: от 0 до 59.
mm/dd/yyyy	Текущая системная дата. (месяц, день, год). Диапазон для месяца: от 1 до 12. Диапазон для дня: от 1 до 31. Диапазон для года: от 2010 до 2079.

clock summer-time date

Данная команда позволяет установить смещение летнего времени относительно UTC. Если необязательные параметры не определены, они считываются как 0 или как \0.

Формат: `clock summer-time date {`*`date month year hh:mm date month year hh:mm`*`}[offset` *`offset`*`] [zone` *`acronym`*`]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
date	День месяца. Допустимые значения: от 1 до 31.
month	Месяц. Указываются первые три буквы месяца (например, Jan).
year	Год. Допустимые значения: от 2000 до 2097.
hh:mm	Время в 24-часовом формате (час:мин). Диапазон для часов: от 0 до 23, для минут: от 0 до 59.
offset	Число дополнительных минут к летнему времени. Допустимые значения: от 1 до 1440.
acronym	Обозначение летнего времени для отображения в период действия летнего времени. Длина: до четырех символов.

clock summer-time recurring

Команда устанавливает параметры цикличного включения летнего времени.

Формат: `clock summer-time recurring {`*`week day month hh:mm week day month hh:mm`*`} [offset `*`offset`*`] [zone `*`acronym`*`]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
EU	Системные часы используют стандартные повторяющиеся настройки летнего времени, используемые в странах Евросоюза.
USA	Системные часы используют стандартные повторяющиеся настройки летнего времени, используемые в США.
week	Неделя месяца. Диапазон значений: 1–5, first, last.
day	День недели. Обозначение: первые три буквы (например, «sun»).
month	Месяц. Обозначение: первые три буквы (например, «jan»).
hh:mm	Время в 24-часовом формате (час:мин). Диапазон для часов: от 0 до 23, для минут: от 0 до 59.
offset	Число дополнительных минут к летнему времени. Допустимые значения: от 1 до 1440.
acronym	Обозначение летнего времени для отображения в период действия летнего времени. Длина: до четырех символов.

no clock summer-time

Эта команда выключает настройки летнего времени.

Формат: `no clock summer-time`

Режим ввода команд: глобальная конфигурация

clock timezone

Используйте эту команду, чтобы установить смещение относительно UTC. Если дополнительные параметры не будут определены, они считываются как 0 или как \0.

Формат: `clock timezone {`*`hours`*`} [minutes `*`minutes`*`] [zone `*`acronym`*`]`

Режим ввода команд: глобальная конфигурация

no clock timezone

Команда для сброса настроек часового пояса.

Формат: `no clock timezone`

Режим ввода команд: глобальная конфигурация

show clock

Команда отображает время и дату системных часов.

Формат: `show clock`

Режим ввода команд: привилегированный

show clock detail

Эта команда отображает подробное системное время вместе с часовым поясом и конфигурацией летнего времени.

Формат: `show clock detail`

Режим ввода команд: привилегированный

6.12 Настройка DHCP-сервера

В этой части показаны команды конфигурирования настроек DHCP-сервера для коммутатора. DHCP-сервер в качестве транспортного протокола использует UDP и поддерживает функции, которые упрощают распределение административных адресов.

ip dhcp pool

Эта команда настраивает имя пула DHCP-адресов на DHCP-сервере и выполняет вход в режим конфигурирования DHCP-пула.

Значение по умолчанию: отсутствует

Формат: `ip dhcp pool` *name*

Режим ввода команд: глобальная конфигурация

no ip dhcp pool

Данная команда удаляет пул DHCP адресов. Используемое имя пула должно быть одним из ранее настроенных.

Формат: `no ip dhcp pool` *name*

Режим ввода команд: глобальная конфигурация

client-identifier

Команда для установки уникального идентификатора DHCP-клиента. Уникальный идентификатор представляет собой действительное выражение в шестнадцатеричном формате. Некоторые системы, например, DHCP-клиенты Microsoft, запрашивают идентификатор клиента вместо аппаратных адресов. Уникальный идентификатор устанавливает связь между типом носителя и MAC-адресом. Например, идентификатор клиента Microsoft для Ethernet-адреса c819.2488.f177 выглядит как 01c8.1924.88f1.77, где 01 обозначает тип носителя (Ethernet). Подробнее об этом см. в разделе «Address Resolution Protocol Parameters» стандарта RFC 1700, где приводится список номерных кодов по типам носителей.

Значение по умолчанию: отсутствует

Формат: `client-identifier uniqueidentifier`

Режим ввода команд: конфигурация пула DHCP

no client-identifier

Удаляет идентификатор клиента.

Формат: `no client-identifier`

Режим ввода команд: конфигурация пула DHCP

client-name

Команда задает имя для DHCP-клиента. Имя должно представлять собой строку из стандартных символов ASCII.

Значение по умолчанию: отсутствует

Формат: `client-name name`

Режим ввода команд: конфигурация пула DHCP

no client-name

Удаляет имя клиента.

Формат: `no client-name`

Режим ввода команд: конфигурация пула DHCP

default-router

Данная команда задает список маршрутизаторов по умолчанию для DHCP-клиента. {address1, address2… address8} — действительные IP-адреса, каждый из которых составлен из четырех десятичных байтов в пределах от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

Значение по умолчанию: отсутствует

Формат: `default-router address1 [address2....address8]`

Режим ввода команд: конфигурация пула DHCP

no default-router

Команда удаляет список маршрутизаторов по умолчанию.

Формат: `no default-router`

Режим ввода команд: конфигурация пула DHCP

dns-server

Эта команда задает DNS-серверы, доступные для DHCP-клиента. Параметры адреса — действительные IP-адреса, каждый из которых составлен из четырех десятичных байтов в пределах от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

Значение по умолчанию: отсутствует

Формат: `dns-server address1 [address2....address8]`

Режим ввода команд: конфигурация пула DHCP

no dns-server

Команда для удаления списка DNS-серверов.

Формат: `no dns-server`

Режим ввода команд: конфигурация пула DHCP

hardware-address

Данная команда задает аппаратный адрес DHCP-клиента. Аппаратный адрес — это MAC-адрес аппаратной платформы клиента, состоящий из 6 байт в шестнадцатеричном формате с точками. Тип указывает протокол, используемый аппаратной платформой. (1 для Ethernet 10 МБ и 6 для IEEE 802).

Значение по умолчанию: Ethernet

Формат: `hardware-address hardwareaddress type`

Режим ввода команд: конфигурация пула DHCP

no hardware-address

Команда удаляет аппаратный адрес DHCP-клиента.

Формат: `no hardware-address`

Режим ввода команд: конфигурация пула DHCP

host

С помощью этой команды можно указать IP-адрес и маску сети для привязки к DHCP-клиенту вручную. Адрес и маска должны представлять собой действительные IP-адреса; каждый из которых составлен из четырех десятичных байтов в пределах от 0 до 255. IP-адрес 0.0.0.0 не является действительным. Префикс — целое число от 0 до 32.

Значение по умолчанию: отсутствует

Формат: `host address [{mask | prefix-length}]`

Режим ввода команд: конфигурация пула DHCP

no host

Команда удаляет IP-адрес DHCP-клиента.

Формат: `no host`

Режим ввода команд: конфигурация пула DHCP

lease

Эта команда настраивает срок аренды для IP-адреса, который DHCP-сервер назначил DHCP-клиенту. Срок аренды должен быть установлен в пределах от 1 до 86400 минут. При указании значения infinite срок аренды устанавливается на 60 дней. Можно указать точный срок действия аренды с помощью следующих параметров. Days — целое число от 0 до 59. Hours —целое число от 0 до 23. Minutes —целое число от 0 до 59.

Значение по умолчанию: 1 (день)

Формат: `lease [{days [hours] [minutes] | infinite}]`

Режим ввода команд: конфигурация пула DHCP

no lease

Эта команда восстанавливает значение по умолчанию для срока аренды DHCP-сервера.

Формат: `no lease`

Режим ввода команд: конфигурация пула DHCP

network (в режиме конфигурации пула DHCP)

Команду для настройки номера подсети и маски для пула DHCP-адресов на сервере. Номер сети — действительный IP-адрес из четырех десятичных байтов в пределах от 0 до 255. IP-адрес 0.0.0.0 не является действительным. Маска — маска подсети IP для указанного пула адресов. Префикс — целое число от 0 до 32.

Значение по умолчанию: отсутствует

Формат: `network networknumber [{mask | prefixlength}]`

Режим ввода команд: конфигурация пула DHCP

no network

Удаляет номер подсети и маску.

Формат: `no network`

Режим ввода команд: конфигурация пула DHCP

bootfile

Команда задает имя загрузочного образа ПО по умолчанию для DHCP-клиента. Параметр `filename` задает имя загрузочного образа ПО.

Формат: `bootfile filename`

Режим ввода команд: конфигурация пула DHCP

no bootfile

Команда удаляет имя загрузочного образа ПО.

Формат: `no bootfile`

Режим ввода команд: конфигурация пула DHCP

domain-name

Эта команда задает доменное имя для DHCP-клиента. Строка доменного имени определяется в параметре `domain`.

Значение по умолчанию: отсутствует

Формат: `domain-name` *`domain`*

Режим ввода команд: конфигурация пула DHCP

no domain-name

Команда удаления доменного имени.

Формат: `no domain-name`

Режим ввода команд: конфигурация пула DHCP

domain-name enable

Эта команда включает возможность использования доменного имени.

Формат: `domain-name enable [name` *`name`*`]`

Режим ввода команд: глобальная конфигурация

no domain-name enable

Команда выключает возможность использования доменного имени.

Формат: `no domain-name enable`

Режим ввода команд: глобальная конфигурация

netbios-name-server

Команда позволяет настроить NetBIOS серверы имен Windows Internet Naming Service (WINS), доступные DHCP-клиентам.

Один IP-адрес обязателен; в одной командной строке можно определить до восьми адресов. Серверы перечисляются в порядке предпочтения (address1 — самый предпочтительный сервер, address2 — следующий по предпочтению и т. д.).

Значение по умолчанию: отсутствует

Формат: `netbios-name-server` *`address`* [*`address2...address8`*]

Режим ввода команд: конфигурация пула DHCP

no netbios-name-server

Эта команда удаляет список серверов имен NetBIOS.

Формат: `no netbios-name-server`

Режим ввода команд: конфигурация пула DHCP

netbios-node-type

Команда настраивает тип узла NetBIOS для DHCP-клиентов. Допустимые типы:

- b-node — широковещательная сеть
- p-node — одноранговая сеть
- m-node — смешанная сеть
- h-node — гибридная сеть (рекомендуемое значение)

Значение по умолчанию: отсутствует

Формат: `netbios-node-type` *`type`*

Режим ввода команд: конфигурация пула DHCP

no netbios-node-type

Команда удаляет тип узла NetBIOS.

Формат: `no netbios-node-type`

Режим ввода команд: конфигурация пула DHCP

next-server

Эта команда настраивает следующий сервер в процессе загрузки клиента DHCP. Параметр `address` — это IP-адрес следующего сервера в процессе загрузки (обычно это TFTP-сервер).

Значение по умолчанию: inbound interface helper addresses

Формат: `next-server` *`address`*

Режим ввода команд: конфигурация пула DHCP

no next-server

Команда удаляет список серверов начальной загрузки.

Формат: `no next-server`

Режим ввода команд: конфигурация пула DHCP

option

Команда `option` настраивает опции DHCP-сервера. Параметр `code` определяет код опции DHCP в диапазоне от 1 до 254. Параметр `ascii string` определяет строку символов NVT ASCII. Строки символов ASCII, в которых содержится пробел, необходимо заключать в кавычки. Параметр `hex string` определяет шестнадцатеричные данные. Шестнадцатеричные символьные строки содержат два шестнадцатеричных знака. Разделить байты между собой можно с помощью точки (например, a3.4f.22.0c), двоеточия (например, a3:4f:22:0c) или пробела (например, a3 4f 22 0c).

Значение по умолчанию: отсутствует

Формат: `option code {ascii string | hex string1 [string2...string8] | ip address1[address2...address8]}`

Режим ввода команд: конфигурация пула DHCP

no option

Команда удаляет опции DHCP-сервера. Параметр code определяет код удаляемой опции DHCP.

Формат: `no option code`

Режим ввода команд: конфигурация пула DHCP

ip dhcp excluded-address

Данная команда определяет IP-адреса, которые DHCP-сервер не должен назначать DHCP-клиентам. Параметры low-address и high-address должны представлять собой действительные IP-адреса; каждый из которых составлен из четырех десятичных байтов в пределах от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

Значение по умолчанию: отсутствует

Формат: `ip dhcp excluded-address lowaddress [highaddress]`

Режим ввода команд: глобальная конфигурация

no ip dhcp excluded-address

Команда для удаления списка исключенных IP-адресов для DHCP-клиента. Параметры `low-address` и `high-address` должны представлять собой действительные IP-адреса; каждый из которых составлен из четырех десятичных байтов в пределах от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

Формат: `no ip dhcp excluded-address lowaddress [highaddress]`

Режим ввода команд: глобальная конфигурация

ip dhcp ping packets

Команда задает количество пакетов (в диапазоне от 2 до 10), которые DHCP-сервер отправляет на адрес пула в процессе выполнения операции ping. По умолчанию количество пакетов равно 2 (наименьшее допустимое количество пакетов для отправки). При установке числа пакетов, равного 0, команда выключается.

Значение по умолчанию: 2

Формат: `ip dhcp ping packets 0,2-10`

Режим ввода команд: глобальная конфигурация

no ip dhcp ping packets

Эта команда восстанавливает количество пакетов для операции ping до значения по умолчанию.

Формат: `no ip dhcp ping packets`

Режим ввода команд: глобальная конфигурация

service dhcp

Команда включает DHCP-сервер.

Значение по умолчанию: выключено

Формат: `service dhcp`

Режим ввода команд: глобальная конфигурация

no service dhcp

Команда выключает DHCP-сервер.

Формат: `no service dhcp`

Режим ввода команд: глобальная конфигурация

ip dhcp bootp automatic

Эта команда включает выделение адресов клиентам протокола BOOTP. Адреса берутся из автоматического пула адресов.

Значение по умолчанию: выключено

Формат: `ip dhcp bootp automatic`

Режим ввода команд: глобальная конфигурация

no ip dhcp bootp automatic

Команда выключает выделение адресов клиентам протокола BOOTP. Адреса берутся из автоматического пула адресов.

Формат: `no ip dhcp bootp automatic`

Режим ввода команд: глобальная конфигурация

ip dhcp conflict logging

Данная команда включает ведение журнала конфликтов на DHCP-сервере.

Значение по умолчанию: включено

Формат: `ip dhcp conflict logging`

Режим ввода команд: глобальная конфигурация

no ip dhcp conflict logging

Команда выключает ведение журнала конфликтов на DHCP-сервере.

Формат: `no ip dhcp conflict logging`

Режим ввода команд: глобальная конфигурация

clear ip dhcp binding

Эта команда удаляет автоматическую привязку адресов из базы данных DHCP-сервера. Если указан параметр *, удаляется привязка для всех адресов. address — действительный IP-адрес из четырех десятичных байтов в пределах от 0 до 255. IP-адрес 0.0.0.0 не является действительным.

Формат: `clear ip dhcp binding {address | *}`

Режим ввода команд: привилегированный

clear ip dhcp server statistics

Сброс счетчиков статистики DHCP-сервера.

Формат: `clear ip dhcp server statistics`

Режим ввода команд: привилегированный

clear ip dhcp conflict

Команда для удаления конфликта адресов от базы данных DHCP-сервера. Сервер обнаруживает конфликты с помощью операции ping. Если в качестве параметра адреса используется символ звездочки (*), DHCP-сервер удаляет все конфликты.

Значение по умолчанию: отсутствует

Формат: `clear ip dhcp conflict {address | *}`

Режим ввода команд: привилегированный

show ip dhcp binding

Команда отображает привязки адресов для определенного IP-адреса на DHCP-сервере. Если IP-адрес не указан, отображается привязка для всех адресов.

Формат: `show ip dhcp binding [address]`

Режимы ввода команд: привилегированный
пользовательский

Термин	*Значение*
IP address	IP-адрес клиента.
Hardware Address	MAC-адрес или идентификатор клиента.
Lease expiration	Срок аренды IP-адреса, присвоенного клиенту.
Type	Способ, которым IP-адрес был назначен клиенту.

show ip dhcp global configuration

Команда отображает привязки адресов для определенного IP-адреса на DHCP-сервере. Если IP-адрес не указан, отображается привязка для всех адресов.

Формат: `show ip dhcp global configuration`

Режимы ввода команд: привилегированный
пользовательский

Термин	*Значение*
Service DHCP	Поле указывает состояние DHCP-протокола.
Number of Ping Packets	Максимальное количество пакетов, которые будут отправлены в ходе операции ping, чтобы проверить что данный идентификатор IP-адреса еще не используется.
Conflict Logging	Показывает, включено ли ведение журнала конфликтов.
BootP Automatic	Показывает, включен ли BootP для динамических пулов.

show ip dhcp pool configuration

Команда отображает конфигурацию пула. При указании `all` отображается конфигурация для всех пулов.

Формат: `show ip dhcp pool configuration {`*`name`*` | all}`

Режимы ввода команд: привилегированный
пользовательский

Поле	*Значение*
Pool Name	Имя настроенного пула.
Pool Type	Тип пула.
Lease Time	Срок аренды IP-адреса, присвоенного клиенту.
DNS Servers	Список DNS-серверов, доступных DHCP-клиенту.
Default Routers	Список маршрутизаторов по умолчанию, доступных DHCP-клиенту.

Для динамического типа пулов отображается следующее дополнительное поле.

Поле	*Значение*
Network	Номер и маска сети для пула адресов DHCP.

Для пулов ручной настройки отображается следующие дополнительные поля.

Поле	*Значение*
Client Name	Имя DHCP-клиента.
Client Identifier	Уникальный идентификатор DHCP-клиента.
Hardware Address	Аппаратный адрес DHCP-клиента.
Hardware Address Type	Протокол аппаратной платформы.
Host	IP-адрес и маска для привязки к DHCP-клиенту вручную.

show ip dhcp server statistics

Команда отображает статистику DHCP-сервера.

Формат: `show ip dhcp server statistics`

Режимы ввода команд: привилегированный
пользовательский

Поле	*Значение*
Automatic Bindings	Количество IP-адресов, которые были автоматически распределены по MAC-адресам узлов, найденных в базе данных DHCP.
Expired Bindings	Количество IP-адресов с истекшим сроком аренды.
Malformed Bindings	Количество неполных или поврежденных сообщений, полученных DHCP-сервером.

Полученные сообщения.

Сообщение	*Значение*
DHCP DISCOVER	Количество сообщений DHCPDISCOVER, полученных сервером.
DHCP REQUEST	Количество сообщений DHCPREQUEST, полученных сервером.
DHCP DECLINE	Количество сообщений DHCPDECLINE, полученных сервером.
DHCP RELEASE	Количество сообщений DHCPRELEASE, полученных сервером.
DHCP INFORM	Количество сообщений DHCPINFORM, полученных сервером.
DHCP OFFER	Количество сообщений DHCPOFFER, отправленных сервером.
DHCP ACK	Количество сообщений DHCPACK, отправленных сервером.
DHCP NACK	Количество сообщений DHCPNACK, отправленных сервером.

show ip dhcp conflict

Команда отображает конфликты адресов, попавшие в журнал DHCP-сервера. Если конкретный IP-адрес не указан, отображаются все конфликтующие адреса.

Формат: `show ip dhcp conflict [`*`ip-address`*`]`

Режимы ввода команд: привилегированный
Пользовательский

Термин	*Значение*
IP address	IP-адрес узла, зарегистрированный на DHCP-сервере.
Detection Method	Способ, которым IP-адреса узлов были найдены на DHCP-сервере.
Detection time	Время обнаружения конфликта.

6.13 Настройка DNS-клиента

Ниже приведены команды, которые используются в Domain Name System (DNS), интернет-сервисе каталогов. DNS определяет, как доменные имена превращаются в IP-адреса. Когда функция включена, DNS-клиент предоставляет сервис поиска имени узла другим компонентам ПОН.

ip domain lookup

Команда включения DNS-клиента.

Значение по умолчанию: включено

Формат: `ip domain lookup`

Режим ввода команд: глобальная конфигурация

no ip domain lookup

Команда выключения DNS-клиента.

Формат: `no ip domain lookup`

Режим ввода команд: глобальная конфигурация

ip domain name

Эта команда задает доменное имя по умолчанию, которое ПО использует для дополнения неполных имен узлов (имен без доменного имени). По умолчанию в системе нет настроенных доменных имен. Параметр name может включать не более 255 символов и не должен начинаться с точки. Это значение name используется, только когда список доменных имен по умолчанию, настраиваемый командой `ip domain list`, пуст.

Значение по умолчанию: отсутствует

Формат: `ip domain name` *name*

Режим ввода команд: глобальная конфигурация

Пример

Команда CLI ip domain name yahoo.com настроит yahoo.com как имя домена по умолчанию. Для неполного имени узла xxx будет выполняться запрос DNS на поиск IP-адреса, соответствующего xxx.yahoo.com.

no ip domain name

Удаляет доменное имя по умолчанию, настроенное с помощью команды ip domain name.

Формат: `no ip domain name`

Режим ввода команд: глобальная конфигурация

ip domain list

Эта команда задает список доменных имен по умолчанию, используемых для дополнения неполных имен. По умолчанию список пуст. Каждое имя может включать не более 256 символов и не должно начинаться с точки. Доменное имя по умолчанию, заданное командой ip domain name, используется только тогда, когда список доменных имен по умолчанию пуст. Максимальное количество имен в списке — 32.

Значение по умолчанию: отсутствует

Формат: `ip domain list` *name*

Режим ввода команд: глобальная конфигурация

no ip domain list

Команда удаляет имя из списка.

Формат: `no ip domain list` *`name`*

Режим ввода команд: глобальная конфигурация

ip name server

Команда позволяет настроить доступные серверы имен. Настроить можно до 8 серверов, используя одну команду или несколько последовательных команд. Параметр `server-address` — действительный адрес сервера (IPv4 или IPv6). Приоритет серверов определяется последовательностью ввода.

Формат: `ip name-server` *`server-address1`* [*`server-address2...server-address8`*]

Режим ввода команд: глобальная конфигурация

no ip name server

Команда для удаления сервера имен.

Формат: `no ip name-server` [*`server-address1...server-address8`*]

Режим ввода команд: глобальная конфигурация

ip name source-interface

Команда позволяет указать физический или логический интерфейс, адрес которого будет использоваться в качестве IP-адреса источника для DNS. Настроенный адрес источника используется для всех DNS-соединений между сервером и клиентом DNS. Выбранный IP-адрес источника используется для заполнения заголовка IP-пакетов протокола управления. Это позволяет устройствам безопасности (брандмауэрам) идентифицировать исходные пакеты, идущие от определенного коммутатора. Если интерфейс не задан, в качестве адреса источника используется основной IP-адрес инициирующего (исходящего) интерфейса. При сбое настроенного интерфейса DNS-клиент возвращается к алгоритму действий по умолчанию.

Формат: `ip name source-interface {`*`unit/slot/port`* | `loopback` *`loopback-id`* | `tunnel` *`tunnel-id`* | `vlan` *`vlan-id`*`}`

Режим ввода команд: глобальная конфигурация

no ip name source-interface

Команда используется, чтобы сбросить адрес источника DNS к настройкам по умолчанию.

Формат: `no ip name source-interface`

Режим ввода команд: глобальная конфигурация

ip host

Команда, которая определяет статическую привязку имени узла к адресу в кэше узлов. Параметр name является именем хоста, ip address — это IP-адрес узла. Имя узла может включать 1–255 буквенно-цифровых символов, точки, дефисы, подчеркивания и одиночные пробелы. Имена

узлов, в которые входит один или несколько пробелов, должны быть заключены в кавычки, например, “lab-pc 45”.

Значение по умолчанию: отсутствует

Формат: `ip host name ipaddress`

Режим ввода команд: глобальная конфигурация

no ip host

Эта команда удаляет привязку имени узла к адресу.

Формат: `no ip host name`

Режим ввода команд: глобальная конфигурация

ipv6 host

Команда, которая определяет статическую привязка имени узла к IPv6-адресу в кэше узлов. Параметр name является именем хоста, v6 address — это IPv6-адрес узла. Имя узла может включать 1–255 буквенно-цифровых символов, точки, дефисы и пробелы. Имена узлов, в которые входит один или несколько пробелов, должны быть заключены в кавычки, например, “lab-pc 45”.

Значение по умолчанию: отсутствует

Формат: `ipv6 host name v6 address`

Режим ввода команд: глобальная конфигурация

no ipv6 host

Команда позволяет удалить статическую привязку имени узла к IPv6-адресу в кэше узлов.

Формат: `no ipv6 host name`

Режим ввода команд: глобальная конфигурация

ip domain retry

Используйте эту команду, чтобы определить количество попыток отправки запросов DNS. Параметр number задает количество попыток отправить запрос DNS к DNS-серверу. Диапазон значений: от 0 до 100.

Значение по умолчанию: 2

Формат: `ip domain retry number`

Режим ввода команд: глобальная конфигурация

no ip domain retry

Команда возврата к настройкам по умолчанию.

Формат: `no ip domain retry number`

Режим ввода команд: глобальная конфигурация

ip domain timeout

Эта команда задает время ожидания ответа на запрос DNS. Параметр seconds определяет время (в секундах) ожидания ответа на запрос DNS. Значение параметра: от 0 до 3600.

Значение по умолчанию: 3

Формат: `ip domain timeout` *`seconds`*

Режим ввода команд: глобальная конфигурация

no ip domain timeout

Команда возвращает время ожидания к настройке по умолчанию.

Формат: `no ip domain timeout` *`seconds`*

Режим ввода команд: глобальная конфигурация

clear host

Команда для удаления записей из кэша привязки имен к адресам. Эта команда очищает записи программно обслуживаемого кэша DNS. Удаление касается адресов IPv4 и IPv6.

Формат: `clear host {`*`name`*` | all}`

Режим ввода команд: привилегированный

Поле	*Описание*
Name	Удаление записи определенного узла. Параметр name может иметь значение от 1 до 255 символов.
all	Удаление всех записей.

show hosts

Команда отображает доменное имя по умолчанию, список узлов сервера имен, а также статический и кэшируемый список имен узлов и адресов. Параметр name может иметь значение от 1 до 255 символов. Эта команда отображает записи IPv4 и IPv6.

Формат: `show hosts` *`[name]`*

Режим ввода команд: привилегированный, пользовательский

Поле	*Описание*
Host Name	Доменное имя узла.
Default Domain	Доменное имя по умолчанию.
Default Domain List	Список доменов по умолчанию.
Domain Name Lookup	Состояние DNS-клиента (включен/выключен).
Number of Retries	Количество повторов при отправке DNS.
Retry Timeout Period	Время ожидания ответа на запрос DNS.
Name Servers	Настроенные серверы имен.

DNS Client Source Interface	Показывает настроенный интерфейс, IP-адрес которого используется в качестве адреса источника для DNS-клиента. IP-адрес выбранного интерфейса используется в качестве IP-адреса источника для всех соединений с сервером.

show ip name source-interface

Эта команда отображает подробные настройки адреса источника, используемого DNS-клиентом. IP-адрес выбранного интерфейса используется в качестве IP-адреса источника для всех соединений с сервером.

Формат: `show ip name source-interface`

Режим ввода команд: привилегированный

6.14 Управление конфликтами IP-адресов

В этой части приведены команды, которые помогают выявлять и устранять конфликты IP-адресов.

ip address-conflict-detect run

Команда инициирует на коммутаторе запуск операции по обнаружению конфликтов активных адресов путем отправки Gratuitous ARP-пакетов на IPv4-адреса коммутатора.

Формат: `ip address-conflict-detect run`

Режим ввода команд: глобальная конфигурация
Virtual Router Config

show ip address-conflict

Эта команда отображает информацию о состоянии последнего обнаруженного конфликта адресов.

Формат: `show ip address-conflict`

Режим ввода команд: привилегированный

Термин	*Значение*
Address Conflict Detection Status	Показывает, были ли обнаружены конфликты адресов по какому-либо IP-адресу.
Last Conflicting IP Address	Последний IP-адрес, который был обнаружен как конфликтующий в любом из интерфейсов.
Last Conflicting MAC Address	MAC-адрес последнего конфликтующего узла, который был обнаружен как конфликтующий в любом из интерфейсов.
Time Since Conflict Detected	Время в днях, часах, минутах и секундах с момента обнаружения последнего конфликта адресов.

clear ip address-conflict-detect

Эта команда очищает информацию о статусах обнаруженных конфликтов адресов для указанного виртуального маршрутизатора. Если маршрутизатор не указан, команда выполняется для маршрутизатора по умолчанию.

Формат: `clear ip address-conflict-detect [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

6.15 Команды отслеживания служебных пакетов

Эти команды упрощают для сетевых администраторов диагностику возможных проблем в работе ПО.

Вывод команд группы debug может занимать много времени и отрицательно сказываться на производительности системы.

capture start

Команда используется, чтобы вручную запустить захват пакетов CPU для отслеживания.

Захват пакетов может выполняться в трех режимах:

- захват в файл;
- удаленный захват;
- захват в виде строк.

Команда не является конфигурационной и не сохраняется при перезагрузке.

Формат: `capture start [{all | receive | transmit}]`

Режим ввода команд: привилегированный

Параметр	*Описание*
all	Захват всего трафика.
receive	Захват только принятого трафика.
transmit	Захват только переданного трафика.

capture stop

Команда позволяет вручную остановить захват пакетов CPU для отслеживания.

Формат: `capture stop`

Режим ввода команд: привилегированный

capture file | remote | line

Команда для настройки опций захвата. Является конфигурационной и сохраняется при перезагрузке.

Формат: `capture {file|remote|line|usb}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
file	В режиме файла захвата в файл захваченные пакеты сохраняются в файле в энергонезависимой памяти. По умолчанию максимальный размер такого файла составляет 524288 байт. Коммутатор может передать файл на сервер по протоколам TFTP, SFTP, SCP через CLI или SNMP.

	Файл сохраняется в формате pcap (с именем cpuPktCapture.pcap) и может быть просмотрен с помощью инструментов сетевого анализа (Wireshark или Ethereal). Запуск захвата в файл автоматически останавливает любые удаленные сессии захвата и захвата в виде строк. После того, как захват пакетов активирован, он продолжается до тех пор, пока файл захвата не достигнет максимального размера или пока захват не будет остановлен вручную (команда CLI capture stop).
remote	В режиме удаленного захвата захваченные пакеты в режиме реального времени перенаправляются на внешний PC, где работает инструмент Wireshark для Microsoft Windows. Сервер захвата пакетов работает на коммутаторе и отправляет захваченные пакеты через TCP-соединение в инструмент Wireshark. Режим удаленного захвата можно включить или выключить через CLI. Чтобы просмотреть полученный файл, требуется PC с ОС Windows и установленным инструментом Wireshark. При использовании режима удаленного захвата коммутатор не сохраняет захваченные данные в файловой системе. Можно настроить номер порта IP для подключения Wireshark к коммутатору. Номер порта по умолчанию — 2002. Если между PC с Wireshark и коммутатором установлен брандмауэр, необходимо открыть используемые порты для передачи данных. Настройки брандмауэра должны позволять инструменту Wireshark инициировать TCP-соединение с коммутатором. Если клиент успешно соединяется с коммутатором, пакеты CPU отправляются на PC-клиент, а Wireshark получает пакеты и может отображать их. Такое взаимодействие продолжается до тех пор, пока сессия не остановлена одной из сторон. Запуск сессии удаленного захвата автоматически останавливает работу захвата в файл и захвата в виде строк
line	В режиме захвата в виде строк захваченные пакеты сохраняются в памяти коммутатора и могут быть отображены средствами CLI. Запуск захвата в виде строк автоматически завершает любую удаленную сессию захвата и работу захвата в файл. В режиме захвата в виде строк можно принять и отобразить до 128 пакетов максимальным размером 128 байт.
usb	В режиме файла захвата на USB, захваченные пакеты сохраняются в файле на USB-носителе.

capture remote port

Команда для настройки опций удалённого захвата. Является конфигурационной и сохраняется при перезагрузке. Параметр id представляет собой номер TCP-порта (1024–49151).

Формат: `capture remote port` *`id`*

Режим ввода команд: глобальная конфигурация

capture file size

Команда для настройки опций захвата в файл. Является конфигурационной и сохраняется при перезагрузке. Параметр max-file-size задает максимальный размер, которого может достигнуть файл .pcap (2–512 КБ).

Формат: `capture file size` *`max file size`*

Режим ввода команд: глобальная конфигурация

capture line wrap

Эта команда позволяет перезапись захваченных пакетов в режиме строк, когда количество пакетов достигает максимума.

Формат: `capture line wrap`

Режим ввода команд: глобальная конфигурация

no capture line wrap

Команда выключает перезапись захваченных пакетов и включает остановку захвата при достижении предельно допустимого количества пакетов.

Формат: `no capture line wrap`

Режим ввода команд: глобальная конфигурация

capture usb

Команда для настройки опций захвата на USB-носитель. Является конфигурационной и сохраняется при перезагрузке. Параметр <file-name> задает имя файла на USB-носителе, в который записываются захваченные пакеты.

Формат: `capture usb <file-name>`

Режим ввода команд: глобальная конфигурация

show capture packets

Команда отображения пакетов, полученных и сохраненных в RAM. Получить и сохранить в RAM можно пакеты, полученные или переданные CPU. Максимальное количество пакетов для сохранения за одну сессию — 128. Максимальный размер сохраняемого в RAM пакета — 128 байт. Если объем пакета более 128 байт, сохраняются только первые 128 байт; остальные данные пропускаются и не отображаются в CLI.

Захват пакетов останавливается автоматически, когда 128 пакетов были получены, но еще не выведены на экран. Захваченные пакеты после перезагрузки не сохраняются.

Формат: `show capture packets`

Режим ввода команд: привилегированный

cpu-traffic direction interface

Команда для привязки фильтров CPU к интерфейсу или списку интерфейсов. Использовать можно физические или логические LAG-интерфейсы. Счетчики статистики обновляются только для настроенных интерфейсов. Результаты трассировки могут также быть получены только для настроенных интерфейсов.

Необходимо учитывать смещение заголовков тега VLAN, поскольку получаемые пакеты CPU всегда содержат теги.

Значение по умолчанию: отсутствует

Формат: `cpu-traffic direction {tx|rx|both} interface` *`interface-range`*

Режим ввода команд: глобальная конфигурация

no cpu-traffic direction interface

Используйте эту команду, чтобы удалить все интерфейсы из фильтров CPU.

Формат: `no cpu-traffic direction {tx|rx|both} interface` *`interface-range`*

Режим ввода команд: глобальная конфигурация

cpu-traffic direction match cust-filter

Команда для настройки пользовательского фильтра. Статистика и/или результаты трассировки для настроенных фильтров выводятся для пакетов, содержащих настроенные данными по определенному смещению. Если иная маска не определена, маска по умолчанию — 0xFF. В качестве условий соответствия можно использовать три различных смещения. При каждой настройке пользовательского фильтра коммутатор выполняет перезапись предыдущей конфигурации.

Необходимо учитывать смещение заголовков тега VLAN, поскольку получаемые пакеты CPU всегда содержат теги.

Значение по умолчанию: отсутствует

Формат: `cpu-traffic direction {tx|rx|both} match cust-filter` *`offset1 data1`* `[mask1` *`mask1`*`]` *`offset2 data2`* `[mask2` *`mask2`*`]` *`offset3 data3`* `[mask3` *`mask3`*`]`

Режим ввода команд: глобальная конфигурация

no cpu-traffic direction match cust-filter

Команда для удаления настроенного пользовательского фильтра.

Формат: `no cpu-traffic direction {tx|rx|both} match cust-filter` *`offset1 data1`* `[mask1` *`mask1`*`]` *`offset2 data2`* `[mask2` *`mask2`*`]` *`offset3 data3`* `[mask3` *`mask3`*`]`

Режим ввода команд: глобальная конфигурация

cpu-traffic direction match srcip

Команда для настройки фильтра на основе IP-адреса источника. Статистика и/или результаты трассировки для настроенных фильтров выводятся для пакетов с соответствующим IP-адресом/маской источника.

Значение по умолчанию: отсутствует

Формат: `cpu-traffic direction {tx|rx|both} match srcip` *`ipaddress`* `[mask` *`mask`*`]`

Режим ввода команд: глобальная конфигурация

no cpu-traffic direction match srcip

Эта команда выключает фильтр на основе IP-адреса источника.

Формат: `no cpu-traffic direction {tx|rx|both} match srcip` *`ipaddress`* `[mask` *`mask`*`]`

Режим ввода команд: глобальная конфигурация

cpu-traffic direction match dstip

Команда для настройки фильтра на основе IP-адреса адресата. Статистика и/или результаты трассировки для настроенных фильтров выводятся для пакетов с соответствующим IP-адресом/маской адресата.

Значение по умолчанию: отсутствует

Формат: `cpu-traffic direction {tx|rx|both} match dstip` *`ipaddress`* `[mask` *`mask`*`]`

Режим ввода команд: глобальная конфигурация

no cpu-traffic direction match dstip

Эта команда выключает фильтр на основе IP-адреса адресата.

Формат: `no cpu-traffic direction {tx|rx|both} match dstip` *`ipaddress`* `[mask` *`mask`*`]`

Режим ввода команд: глобальная конфигурация

cpu-traffic direction match tcp

Команда для настройки фильтра на основе TCP-порта источника или адресата. Статистика и/или результаты трассировки для настроенных фильтров выводятся для пакетов с соответствующим TCP-портом источника или адресата.

Значение по умолчанию: отсутствует

Формат: `cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp}` *`port`* `[mask` *`mask`*`]`

Режим ввода команд: глобальная конфигурация

no cpu-traffic direction match tcp

Команда для удаления фильтра на основе TCP-порта источника или адресата.

Формат: `no cpu-traffic direction {tx|rx|both} match {srctcp|dsttcp}` *`port`* `[mask` *`mask`*`]`

Режим ввода команд: глобальная конфигурация

cpu-traffic direction match udp

Команда для настройки фильтра на основе UDP-порта источника или адресата. Статистика и/или результаты трассировки для настроенных фильтров выводятся для пакетов с соответствующим UDP-портом источника или адресата.

Значение по умолчанию: отсутствует

Формат: `cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`

Режим ввода команд: глобальная конфигурация

no cpu-traffic direction match udp

Команда для удаления фильтра на основе UDP-порта источника или адресата.

Формат: `no cpu-traffic direction {tx|rx|both} match {srcudp|dstudp} port [mask mask]`

Режим ввода команд: глобальная конфигурация

cpu-traffic mode

Команда для включения режима фильтрации трафика CPU. При включении пакеты RX/TX проверяются на соответствие установленным фильтрам.

Значение по умолчанию: выключено

Формат: `cpu-traffic mode`

Режим ввода команд: глобальная конфигурация

no cpu-traffic mode

Выключение режима фильтрации трафика CPU.

Формат: `no cpu-traffic mode`

Режим ввода команд: глобальная конфигурация

cpu-traffic trace

Используйте эту команду, чтобы настроить трассировку пакетов CPU. Пакет может быть получен различными компонентами. Если данная функция активирована и настроена трассировка, пакеты отслеживаются по заданному фильтру. Если включен режим dump-pkt, наряду со статистикой трассировки отображаются первые 64 байт пакета.

Значение по умолчанию: выключено

Формат: `cpu-traffic trace {dump-pkt}`

Режим ввода команд: глобальная конфигурация

no cpu-traffic trace

Команда выключает трассировку пакетов CPU и режим dump-pkt (если настроен).

Формат: `no cpu-traffic trace {dump-pkt}`

Режим ввода команд: глобальная конфигурация

show cpu-traffic

Команда отображает текущие параметры конфигурации.

Значение по умолчанию: отсутствует

Формат: `show cpu-traffic`

Режим ввода команд: привилегированный

show cpu-traffic interface

Команда вывода статистики по интерфейсам для настроенных фильтров. Статистику можно отобразить для определенного фильтра (например, stp, udld, arp и др.). Если фильтр не указан, отображается статистика для всех настроенных фильтров.

Аналогично можно использовать IP-адрес источника/адресата, TCP, UDP или MAC-адрес вместе с пользовательским фильтром в качестве опции команды для вывода статистики.

Значение по умолчанию: отсутствует

Формат: `show cpu-traffic interface {all | unit/slot/port | cpu } filter`

Режим ввода команд: привилегированный

show cpu-traffic summary

Команда вывода сводной статистики для настроенных фильтров по всем интерфейсам.

Значение по умолчанию: отсутствует

Формат: `show cpu-traffic summary`

Режим ввода команд: привилегированный

show cpu-traffic trace

Команда для отображения результатов трассировки. Результаты трассировки могут быть выведены как для всех доступных пакетов, так и для определенного фильтра (например, STP, UDLD, ARP и т. д.). Аналогично можно использовать IP-адрес источника/адресата или MAC-адрес вместе с пользовательским фильтром в качестве опции команды для частичного вывода истории трассировки. Если функция включена, информация дампа пакетов отображается вместе со статистикой трассировки пакетов. По умолчанию размер буфера дампа настроен на сохранение первых 64 байт пакета.

Значение по умолчанию: отсутствует

Формат: `show cpu-traffic trace filter`

Режим ввода команд: привилегированный

clear cpu-traffic

Данная команда удаляет статистику трафика CPU и информацию трассировки для всех интерфейсов.

Значение по умолчанию: отсутствует

Формат: `clear cpu-traffic {counters | traces}`

Режим ввода команд: глобальная конфигурация

debug aaa accounting

Команда для отладки конфигурации и функционала диспетчера учёта пользователей.

Формат: `debug aaa accounting`

Режим ввода команд: привилегированный

no debug aaa accounting

Выключение отладки конфигурации и функционала диспетчера учёта пользователей.

Формат: `no debug aaa accounting`

Режим ввода команд: привилегированный

debug arp

Команда включает сообщения отладки протокола ARP. Дополнительно можно определить виртуальный маршрутизатор, в котором выполняется команда.

Значение по умолчанию: выключено

Формат: `debug arp [vrf vrf-name]`

Режим ввода команд: привилегированный

no debug arp

Выключает сообщения отладки протокола ARP.

Формат: `no debug arp`

Режим ввода команд: привилегированный

debug authentication

Команда отображает сообщения отладки аутентификации для отдельного события или для всех событий интерфейса

Значение по умолчанию: отсутствует

Формат: `debug authentication packet {all | event} interface`

Режим ввода команд: привилегированный

debug auto-voip

Команда включает сообщения отладки функции Auto VOIP. Используйте дополнительные параметры, чтобы отслеживать пакеты H323, SCCP или SIP соответственно.

Значение по умолчанию: выключено

Формат: `debug auto-voip [H323|SCCP|SIP|oui]`

Режим ввода команд: привилегированный

no debug auto-voip

Эта команда выключает сообщения отладки функции Auto VOIP.

Формат: `no debug auto-voip`

Режим ввода команд: привилегированный

debug clear

Эта команда выключает все ранее включенные сообщения отладки.

Значение по умолчанию: выключено

Формат: `debug clear`

Режим ввода команд: привилегированный

debug aaa authorization

Эта команда включает трассировку AAA-функционала диспетчера пользователей. Используется для отладки настроек и функционала авторизации диспетчера пользователей. Каждый из параметров используется для настройки флагов отладки авторизации.

Формат: `debug aaa authorization commands|exec`

Режим ввода команд: привилегированный

no debug aaa authorization

Команда выключает отладку функционала авторизации диспетчера пользователей.

Формат: `no debug aaa authorization`

Режим ввода команд: привилегированный

Параметр	*Описание*
kernel	Просмотр журнала сбоев для ядра.
crashlog-number	Задает номер файла для просмотра. Система сохраняет до четырех копий файла, допустимый диапазон 1–4.
upload url	Чтобы выгрузить журнал сбоев (или дамп сбоя) на сервер TFTP, используйте ключевое слово upload и укажите необходимую информацию TFTP-сервера.
proc	Просмотр журнала сбоев в работе приложения.
verbose	Включение подробного журнала.
deleteall	Удаление всех файлов журналов сбоев в системе.
data	Устройство записи данных журнала.
crashdump-number	Номер дампа журнала для просмотра. Диапазон допустимых значений: 0–2.
download url	Чтобы загрузить дамп сбоя на коммутатор, используйте ключевое слово download и укажите необходимую информацию TFTP-сервера.
component-id	Идентификатор компонента, который стал причиной сбоя.
item-number	Номер позиции.
additional-parameter	Дополнительные параметры для включения.

debug console

Эта команда включает отображение трассировок команды debug в текущей сессии, в рамках которой она выполняется. Вывод трассировок команды debug появится для всех сессий, для которых включена эта команда. Конфигурация этой команды сохраняется на время сессии. Команда не сохраняется после перезагрузки.

Значение по умолчанию: выключено

Формат: `debug console`

Режим ввода команд: привилегированный

no debug console

Эта команда выключает отображение вывода трассировок команды debug в сессии входа, в рамках которой она выполняется.

Формат: `no debug console`

Режим ввода команд: привилегированный

debug crashlog

Используйте эту команду, чтобы просмотреть информацию в файле журнала сбоев, который формирует система, когда происходит непредвиденная перезагрузка. Файл журнала сбоев содержит следующую информацию.

- Информацию о стеке вызовов в простой и подробной форме;
- Состояние журнала;
- Журнал в буфере;
- Журнал событий;
- Сохраняемый журнал;
- Системную информация (вывод sysapiMbufDump);
- Отладочную информацию об очередях сообщений;
- Отладочную информацию о памяти;
- Отладочный статус памяти;
- Информацию об ОС (вывод osapiShowTasks);
- Информацию из /proc (meminfo, cpuinfo, interrupts, version и net/sockstat).

Значение по умолчанию: выключено

Формат: `debug crashlog {[kernel] crashlog-number [upload url] | proc | verbose | deleteall}`

Режим ввода команд: привилегированный

debug dcbx packet

Эта команда включает отладочную трассировку для переданных или полученных пакетов DCBX.

Значение по умолчанию: выключено

Формат: `debug dcbx packet {receive | transmit}`

Режим ввода команд: привилегированный

debug debug-config

Команда выгрузки/загрузки файла debug-config.ini. Файл debug-config.ini выполняет команды CLI (включая команды devshell и drivshell) при определенных событиях. Данный файл создается вручную и загружается на коммутатор.

Значение по умолчанию: выключено

Формат: `debug debug-config {download <url> | upload <url>}`

Режим ввода команд: привилегированный

debug dhcp packet

Команда выводит отладочную информацию о действиях DHCPv4-клиента и трассировки пакетов DHCPv4, поступающих на локальный DHCPv4-клиент и передаваемых с него.

Значение по умолчанию: выключено

Формат: `debug dhcp packet [transmit | receive]`

Режим ввода команд: привилегированный

no debug dhcp

Выключает вывод отладочной информации о действиях DHCPv4-клиента.

Формат: `no debug dhcp packet [transmit | receive]`

Режим ввода команд: привилегированный

debug dot1ag

Команда включает отладку сообщений, отправленных между MP и MEP.

Значение по умолчанию: выключено

Формат: `debug dot1ag {all | ccm | events | lbm | lbr | ltm | ltr | pdu}`

Режим ввода команд: привилегированный

Параметр	*Описание*
all	Отладка всех типов сообщений dot1ag.
ccm	Включает флаги отладки для получения информации о сообщениях проверки целостности (Continuity Check Message, CCM). Многоадресные PDU CFM периодически передаются MEP, чтобы гарантировать непрерывность по MA, которому принадлежат передающий MEP. В ответ на сообщения CCM MP не отправляет ответ.
ltm	Включает флаги отладки для получения информации о сообщениях Linktrace (LTM). PDU CFM, инициируемых MEP для определения пути к целевому MAC-адресу, передающихся от MIP до MIP, до точки, в которой LTM достигает своей цели или не может передаваться далее. Каждый MP вдоль пути к цели генерирует LTR.
ltr	Включает флаги отладки для получения информации об ответах Linktrace. Одноадресные PDU CFM передаются от MP к MEP в ответ на получение LTM от MEP.
lbm	Включает флаги отладки для получения информации о loopback-сообщениях. Одноадресные PDU CFM передаются MEP, адресованные определенному MP в ожидании получения loopback-ответа.
lbr	Включает флаги отладки для получения информации о loopback-ответах. Одноадресный PDU CFM передаются от MP к MEP, в ответ на loopback-сообщение, полученное от MEP.
pdu	Включает флаги отладки для получения информации о всех PDU CFM.

debug dot1x packet

Включение отладочной трассировки пакетов dot1x.

Значение по умолчанию: выключено

Формат: `debug dot1x`

Режим ввода команд: привилегированный

no debug dot1x packet

Выключение отладочной трассировки пакетов dot1x.

Формат: `no debug dot1x`

Режим ввода команд: привилегированный

debug fip-snooping packet

Используйте команду `debug fip-snooping packet` в привилегированном режиме, чтобы включить отладочную трассировку FIP-пакетов в процессе передаче или получения с различными настройками фильтра.

Значение по умолчанию: выключено

Формат: `debug fip-snooping packet [{transmit | receive | filter {dst-mac` *`mac-addr`* `| fip-proto-code` *`1-15`* `| src-intf` *`unit/slot/port`* `| src-mac` *`mac-addr`* `| vlan` *`1-4093`*`}]`

Режим ввода команд: пользовательский

привилегированный

Параметр	*Описание*
dst-mac	Если задана опция фильтра dst-mac, вывод трассировки фильтруется на предмет соответствия указанному целевому MAC-адресу.
fip-proto-code	Если задана опция фильтра fip-proto-code, вывод трассировки фильтруется на предмет соответствия поддерживаемым типам.
src-intf	Если задана опция фильтра src-intf, вывод трассировки фильтруется на предмет соответствия входящему интерфейсу источника.
src-mac	Если задана опция фильтра src-mac, вывод трассировки фильтруется на предмет соответствия указанному MAC-адресу источника.
vlan	Если задана опция фильтра vlan, вывод трассировки фильтруется на предмет соответствия указанному идентификатору VLAN.

no debug fip-snooping packet

Данная команда используется в привилегированном режиме, чтобы выключить отладочную трассировку FIP-пакетов в процессе передачи или получения с различными настройками фильтра.

Формат: `no debug fip-snooping packet [{transmit | receive | filter {dst-mac` *`mac-addr`* `| fip- proto-code` *`1-15`* `| src-intf` *`unit/slot/port`* `| src-mac` *`mac-addr`* `| vlan` *`1-4093`*`}]`

Режим ввода команд: пользовательский

привилегированный

debug igmpsnooping packet

Эта команда включает отслеживание пакетов IGMP Snooping, полученных и переданных коммутатором.

Значение по умолчанию: выключено

Формат: `debug igmpsnooping packet`

Режим ввода команд: привилегированный

no debug igmpsnooping packet

Выключение отслеживания пакетов IGMP Snooping.

Формат: `no debug igmpsnooping packet`

Режим ввода команд: привилегированный

debug igmpsnooping packet transmit

Эта команда позволяет отслеживать пакеты IGMP Snooping, переданные коммутатором. Чтобы отслеживать пакеты для определенного интерфейса, функция Snooping должна быть включена на устройстве и интерфейсе.

Значение по умолчанию: выключено

Формат: `debug igmpsnooping packet transmit`

Режим ввода команд: привилегированный

Параметр	*Значение*
TX	Пакет, отправленный устройством.
Intf	Интерфейс, из которого пакет вышел. Используемый формат — unit/slot/port (внутренний номер интерфейса). Для интерфейсов устройств вне стека юнит всегда отображается как 1.
Src_Mac	MAC-адрес источника пакета.
Dest_Mac	Групповой MAC-адрес назначения пакета.
Src_IP	IP-адрес источника в IP-заголовке пакета.
Dest_IP	Групповой IP-адрес назначения пакета.
Type	Тип IGMP-пакета. Тип может иметь одно из следующих значений: • Membership Query – IGMP Membership Query; • V1_Membership_Report – IGMP Membership Report, версия 1; • V2_Membership_Report – IGMP Membership Report, версия 2; • V3_Membership_Report – IGMP Membership Report, версия 3; • V2_Leave_Group – IGMP Leave Group, версия 2.
Group	Групповой адрес многоадресной передачи в заголовке IGMP.

no debug igmpsnooping transmit

Эта команда выключает трассировку переданных пакетов IGMP Snooping.

Формат: `no debug igmpsnooping transmit`

Режим ввода команд: привилегированный

debug igmpsnooping packet receive

Команда позволяет отслеживать пакеты IGMP Snooping, полученные коммутатором. Чтобы отслеживать пакеты для определенного интерфейса, функция Snooping должна быть включена на устройстве и интерфейсе.

Значение по умолчанию: выключено

Формат: `debug igmpsnooping packet receive`

Режим ввода команд: привилегированный

Параметры, отображаемые в сообщении трассировки

Параметр	*Значение*
TX	Пакет, отправленный устройством.
Intf	Интерфейс, из которого пакет вышел. Используемый формат — unit/slot/port (внутренний номер интерфейса). Для интерфейсов устройств вне стека юнит всегда отображается как 1.
Src_Mac	MAC-адрес источника пакета.
Dest_Mac	Групповой MAC-адрес назначения пакета.
Src_IP	IP-адрес источника в IP-заголовке пакета.
Dest_IP	Групповой IP-адрес назначения пакета.
Type	Тип IGMP-пакета. Тип может иметь одно из следующих значений: • Membership Query – IGMP Membership Query; • V1_Membership_Report – IGMP Membership Report, версия 1; • V2_Membership_Report – IGMP Membership Report, версия 2; • V3_Membership_Report – IGMP Membership Report, версия 3; • V2_Leave_Group – IGMP Leave Group, версия 2.
Group	Групповой адрес многоадресной передачи в заголовке IGMP.

no debug igmpsnooping receive

Эта команда выключает трассировку полученных пакетов IGMP Snooping.

Формат: `no debug igmpsnooping receive`

Режим ввода команд: привилегированный

debug ip acl

Команда включения отладки пакетов IP-протокола, соответствующих критериям ACL.

Значение по умолчанию: выключено

Формат: `debug ip acl` *`acl Number`*

Режим ввода команд: привилегированный

no debug ip acl

Выключение отладки пакетов IP-протокола, соответствующих критериям ACL.

Формат: `no debug ip acl` *`acl Number`*

Режим ввода команд: привилегированный

debug ip bgp

Используйте команду, чтобы включить отладочную трассировку BGP-пакетов. Сообщения отладки отправляются в системный журнал с уровнем критичности DEBUG. Чтобы вывести сообщения отладки в консоль, включите ведение консольного журнала на уровне DEBUG, используя команду logging console debug. Опции отладки для конкретного соединения являются объединением

опций, включенных глобально, и опций, включенных для данного соединения. Включение одной из опций типа пакета включает пакетную трассировку во входящем и в исходящем направлении.

Значение по умолчанию: выключено

Формат: `debug ip bgp [vrf vrf-name] {ipv4-address|ipv6-address} [ events | in | interface {unit/slot/port | vlan 1-4093} | keepalives | notification | open | out | refresh | updates ]`

Режим ввода команд: привилегированный

Параметр	*Описание*
peer-address	(Необязательно.) Адрес IPv4 BGP-соединения. Отладочные трассировки включены для определенного соединения, когда эта опция задана. Команда может быть выполнена многократно, чтобы включить одновременную трассировку для нескольких соединений.
events	(Необязательно.) Трассировка событий состояния смежности.
keepalives	(Необязательно.) Трассировка передачи и получение пакетов KEEPALIVE.
notification	(Необязательно.) Трассировка передачи и получения пакетов NOTIFICATION.
open	(Необязательно.) Трассировка передачи и получения пакетов OPEN.
refresh	(Необязательно.) Трассировка передачи и получения пакетов ROUTE REFRESH
updates	(Необязательно.) Трассировка передачи и получения пакетов UPDATE.

no debug bgp

Команда выключения отладочной трассировки событий BGP.

Формат: `no debug ip bgp [peer-address|events|keepalives|notification |open|refresh|updates]`

Режим ввода команд: привилегированный

debug ip vrrp

Команда включает отладочные сообщения протокола VRRP.

Значение по умолчанию: выключено

Формат: `debug ip vrrp`

Режим ввода команд: привилегированный

no debug ip vrrp

Выключает отладочные сообщения протокола VRRP.

Формат: `no debug ip vrrp`

Режим ввода команд: привилегированный

debug ipv6 dhcp

Команда выводит отладочную информации о действиях DHCPv6-клиента и трассировки пакетов DHCPv6, поступающих на локальный DHCPv6-клиент и передаваемых с него.

Значение по умолчанию: выключено

Формат: `debug ipv6 dhcp`

Режим ввода команд: привилегированный

no debug ipv6 dhcp

Выключает вывод отладочной информации о действиях DHCPv6-клиента.

Формат: `no debug ipv6 dhcp`

Режим ввода команд: привилегированный

debug ipv6 ospfv3 packet

Используйте команду, чтобы включить отладочную трассировку пакетов IPv6 OSPFv3.

Значение по умолчанию: выключено

Формат: `debug ipv6 ospfv3 packet`

Режим ввода команд: привилегированный

no debug ipv6 ospfv3 packet

Выключение отладочной трассировки пакетов IPv6 OSPFv3.

Формат: `no debug ipv6 ospfv3 packet`

Режим ввода команд: привилегированный

debug lacp packet

Эта команда позволяет отследить пакеты LACP, полученные и переданные коммутатором.

Значение по умолчанию: выключено

Формат: `debug lacp packet`

Режим ввода команд: привилегированный

no debug lacp packet

Выключает трассировку пакетов LACP.

Формат: `no debug lacp packet`

Режим ввода команд: привилегированный

debug mldsnooping packet

Используйте эту команду, чтобы отслеживать прием и передачу пакетов MLD Snooping. При использовании ключевого слова **receive** отслеживаются только полученные пакеты MLD Snooping, при использовании **transmit** отслеживаются только переданные пакеты MLD Snooping. Когда ключевое слово не используется, выводятся все трассировки пакетов MLD Snooping. Важная информация (исходный адрес, адрес назначения, тип управляющего пакета, длина пакета и интерфейс, в котором пакет получен или передан) выводится в консоли.

Значение по умолчанию: выключено

Формат: `debug mldsnooping packet [receive | transmit]`

Режим ввода команд: привилегированный

no debug mldsnooping packet

Команда выключения отладочной трассировки приема и передачи пакета MLD snooping.

debug ospf packet

Команда позволяет отслеживать пакеты OSPF, полученные и переданные коммутатором. Дополнительно можно задать используемый виртуальный маршрутизатор.

Значение по умолчанию: выключено

Формат: `debug ospf packet [vrf vrf-name]`

Режим ввода команд: привилегированный

Параметры, отображаемые в сообщении трассировки, приведены в таблице ниже.

Параметр	*Значение*
TX/RX	TX — пакеты, переданные устройством. RX — пакеты, полученные устройством.
Intf	Интерфейс, через который пакет вошел или из которого вышел. Используемый формат — unit/slot/port (внутренний номер интерфейса).
SrcIp	IP-адрес источника в IP-заголовке пакета
DestIp	IP-адрес назначения в IP-заголовке пакета
AreaId	Идентификатор зоны в OSPF-заголовке пакета.
Type	Может быть одним из следующих: • HELLO – Hello packet; • DB_DSCR – Database descriptor; • LS_REQ – LS Reques; • LS_UPD – LS Update; • LS_ACK – LS Acknowledge.

Оставшиеся поля в трассировке связаны с типами пакетов OSPF. Описания полей для пакета HELLO приведены в таблице ниже.

Параметр	*Значение*
Netmask	Маска сети в пакете hello.
DesignRouter	IP-адрес назначенного маршрутизатора.
Backup	IP-адрес резервного маршрутизатора.

Описания полей для пакета DB_DSCR приведены в таблице ниже.

Поле	*Значение*
MTU	MTU
Options	Опции в пакете OSPF.
Flags	Флаг (или несколько флагов) из приведенных ниже: • I – Init; • M – More; • MS – Master/Slave.
Seq	Порядковый номер пакета DD.

Описания полей для пакета LS_REQ приведены в таблице ниже.

Поле	*Значение*
Length	Длина пакета

Описания полей для пакета LS_UPD приведены в таблице ниже.

Поле	*Значение*
Length	Длина пакета

Описания полей для пакета LS_ACK приведены в таблице ниже.

Поле	*Значение*
Length	Длина пакета

no debug ospf packet

Выключает трассировку пакетов OSPF.

Формат: `no debug ospf packet`

Режим ввода команд: привилегированный

debug ospfv3 packet

Используйте команду, чтобы включить отладочную трассировку пакетов OSPFv3.

Значение по умолчанию: отключено

Формат: `debug ospfv3 packet`

Режим ввода команд: привилегированный

no debug ospfv3 packet

Отключает отладочную трассировку пакетов OSPFv3.

Формат: `no debug ospfv3 packet`

Режим ввода команд: привилегированный

debug ping packet

Эта команда позволяет отслеживать запросы и ответы ICMP. Команда отслеживает операции ping на сетевом/сервисном порте. Возможно отслеживание на виртуальном маршрутизаторе.

Значение по умолчанию: отключено

Формат: `debug ping packet [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

Параметр	*Значение*
TX/RX	TX — пакеты, переданные устройством. RX — пакеты, полученные устройством.
Intf	Интерфейс, через который пакет вошел или из которого вышел. Используемый формат — unit/slot/port (внутренний номер интерфейса). Для интерфейсов устройств вне стека юнит всегда отображается как 1.
SRC_IP	IP-адрес источника в IP-заголовке пакета.
DEST_IP	IP-адрес назначения в IP-заголовке пакета.

Type	Определяет тип сообщения ICMP (REQUEST или RESPONSE).

no debug ping packet

Выключает трассировку запросов и ответов ICMP.

Формат: `no debug ping packet`

Режим ввода команд: привилегированный

debug rip packet

Данная команда включает трассировку запросов и ответов RIP. Дополнительных опций нет. Вывод направлен в файл журнала.

Значение по умолчанию: отключено

Формат: `debug rip packet`

Режим ввода команд: привилегированный

Параметры, отображаемые в сообщении трассировки, приведены в таблице ниже.

Поле	***Значение***
TX/RX	TX — пакеты, переданные устройством. RX — пакеты, полученные устройством.
Intf	Интерфейс, через который пакет вошел или из которого вышел. Используемый формат — unit/slot/port (внутренний номер интерфейса). Для интерфейсов устройств вне стека юнит всегда отображается как 1.
SRC_IP	IP-адрес источника в IP-заголовке пакета.
DEST_IP	IP-адрес назначения в IP-заголовке пакета.
Rip_Version	Используемая версия RIP: RIPv1 или RIPv2.
Packet_Type	Тип пакета RIP: RIP_REQUEST или RIP_RESPONSE.
Routes	Выводится до 5 маршрутов на пакет в следующем формате: Network: a.b.c.d Mask a.b.c.d Next_Hop a.b.c.d Metric a Следующий хоп отображается, если он отличен от 0.0.0.0. Для пакетов RIPv1 маска всегда казана как 0.0.0.0.
Number of routes not printed	В трассировку включены только первые пять маршрутов пакета. Это уведомление о количестве дополнительных маршрутов в пакете, которые не были включены в трассировку.

no debug rip packet

Команда выключает трассировку запросов и ответов RIP.

Формат: `no debug rip packet`

Режим ввода команд: привилегированный

debug sflow packet

Включить отладочную трассировку пакетов sFlow.

Значение по умолчанию: выключено

Формат: `debug sflow packet`

Режим ввода команд: привилегированный

no debug sflow packet

Выключить отладочную трассировку пакетов sFlow.

Формат: `no debug sflow packet`

Режим ввода команд: привилегированный

debug spanning-tree bpdu

Эта команда позволяет отслеживать BPDU-пакеты протокола STP, полученные и переданные коммутатором.

Значение по умолчанию: выключено

Формат: `debug spanning-tree bpdu`

Режим ввода команд: привилегированный

no debug spanning-tree bpdu

Выключение трассировки BPDU-пакетов протокола остовного дерева.

Формат: `no debug spanning-tree bpdu`

Режим ввода команд: привилегированный

debug spanning-tree bpdu receive

Команда отслеживания BPDU-пакетов протокола STP, полученных коммутатором. Чтобы отслеживать пакеты для определенного интерфейса, протокол STP должен быть включен на устройстве и интерфейсе.

Значение по умолчанию: выключено

Формат: `debug spanning-tree bpdu receive`

Режим ввода команд: привилегированный

Поле	*Значение*
TX/RX	TX — пакеты, переданные устройством. RX — пакеты, полученные устройством.
Intf	Интерфейс, через который пакет вошел или из которого вышел. Используемый формат — unit/slot/port (внутренний номер интерфейса). Для интерфейсов устройств вне стека юнит всегда отображается как 1.
Source_Mac	MAC-адрес источника пакета.
Version	Версия протокола остовного дерева (0–3). 0 означает STP, 2 — RSTP, 3 — MSTP.
Root_Mac	MAC-адрес корневого моста CIST.
Root_Priority	Приоритет корневого моста CIST. Допустимое значение: от 0 до 61440. Выводится как шестнадцатеричное число, кратное 4096.
Path_Cost	Стоимость внешнего корневого пути, указанная в BPDU.

no debug spanning-tree bpdu receive

Выключить трассировку получаемых BPDU-пакетов протокола остовного дерева.

Формат: `no debug spanning-tree bpdu receive`

Режим ввода команд: привилегированный

debug spanning-tree bpdu transmit

Эта команда позволяет отслеживать BPDU-пакеты протокола STP, отправленных коммутатором. Чтобы отслеживать пакеты на определенном интерфейсе, протокол STP должен быть включен на устройстве и интерфейсе.

Значение по умолчанию: выключено

Формат: `debug spanning-tree bpdu transmit`

Режим ввода команд: привилегированный

Поле	*Значение*
TX/RX	TX — пакеты, переданные устройством. RX — пакеты, полученные устройством.
Intf	Интерфейс, через который пакет вошел или из которого вышел. Используемый формат — unit/slot/port (внутренний номер интерфейса). Для интерфейсов устройств вне стека юнит всегда отображается как 1.
Source_Mac	MAC-адрес источника пакета.
Version	Версия протокола остовного дерева (0–3). 0 означает STP, 2 — RSTP, 3 — MSTP.
Root_Mac	MAC-адрес корневого моста CIST.
Root_Priority	Приоритет корневого моста CIST. Допустимое значение: от 0 до 61440. Выводится как шестнадцатеричное число, кратное 4096.
Path_Cost	Компонент затрат BPDU: стоимость корневого пути BPDU.

no debug spanning-tree bpdu transmit

Выключение трассировки отправляемых BPDU-пакетов протокола остовного дерева.

Формат: `no debug spanning-tree bpdu transmit`

Режим ввода команд: привилегированный

debug tacacs

Команда debug tacacs packet используется для включения отладки TACACS+.

Формат: `debug tacacs {packet [receive | transmit] | accounting | authentication}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
packet receive	Включить отладку для принимаемых пакетов TACACS +.
packet transmit	Включить отладку для передаваемых пакетов TACACS +.
accounting	Включить отладку аутентификации TACACS+.
authentication	Включить отладку авторизации TACACS+.

debug telnetd start

Используйте эту команду, чтобы запустить отладочный демон Telnet. Отладочный демон Telnet предоставляет доступ к командной оболочке Linux. Идентификатор пользователя Telnet: root. Если на момент выполнения команды демон Telnet уже работает, команда останавливает и перезапускает демон. Команда доступна при наличии debug-ключа.

Формат: `debug telnetd start [password][port]`

Режим ввода команд: привилегированный

Параметр	*Описание*
password	Необязательный пароль Telnet. Если пароль не задан, используется пароль по умолчанию: lvl7dbg.
port	Необязательный номер порта Telnet. Если порт Telnet не указан, используется порт по умолчанию: 2323.

debug telnetd stop

Команда остановки демона Telnet, ранее запущенного командой debug telnetd start.

Формат: `debug telnetd stop`

Режим ввода команд: привилегированный

debug transfer

Команда включает отладку передачи файлов.

Формат: `debug transfer`

Режим ввода команд: привилегированный

no debug transfer

Выключает отладку передачи файлов.

Формат: `no debug transfer`

Режим ввода команд: привилегированный

debug udld events

Команда включает отладку событий UDLD.

Значение по умолчанию: выключено

Формат: `debug udld events`

Режим ввода команд: привилегированный

debug udld packet receive

Команда включает отладочные сообщения при получении PDU UDLD.

Значение по умолчанию: выключено

Формат: `debug udld packet receive`

Режим ввода команд: привилегированный

debug udld packet transmit

Команда включает отладочные сообщения при отправке PDU UDLD.

Значение по умолчанию: выключено

Формат: `debug udld packet transmit`

Режим ввода команд: привилегированный

show debugging

Команда отображает текущую конфигурацию отслеживания пакетов.

Формат: `show debugging`

Режим ввода команд: привилегированный

exception protocol

Команда задает протокол, используемый для хранения файла дампа памяти.

Значение по умолчанию: отсутствует

Формат: `exception protocol {nfs | tftp | ftp | local | usb | none}`

Режим ввода команд: глобальная конфигурация

no exception protocol

Используйте эту команду, чтобы сбросить конфигурацию протокола дампа памяти к заводским настройкам

Формат: `no exception protocol`

Режим ввода команд: глобальная конфигурация

exception dump tftp-server

Используйте эту команду для настройки IP-адреса удаленного TFTP-сервера, чтобы сохранить файлы дампа памяти на внешнем сервере

Значение по умолчанию: отсутствует

Формат: `exception dump tftp-server {`*`ip-address`*`}`

Режим ввода команд: глобальная конфигурация

no exception dump tftp-server

Используйте эту команду, чтобы сбросить конфигурацию удаленного сервера для дампов к заводским настройкам.

Формат: `no exception dump tftp-server`

Режим ввода команд: глобальная конфигурация

exception dump nfs

Используйте эту команду, чтобы настроить точку подключения NFS и сохранение файла дампа памяти в файловой системе NFS.

Значение по умолчанию: отсутствует

Формат: `exception dump nfs ip-address/dir`

Режим ввода команд: глобальная конфигурация

no exception dump nfs

Сброс конфигурации точки подключения NFS для дампа к заводским настройкам.

Формат: `no exception dump nfs`

Режим ввода команд: глобальная конфигурация

exception dump filepath

Команда для настройки пути к файлу при сохранении дампа памяти на TFTP или FTP-сервере, в подключенной системе NFS или подкаталоге USB-устройства.

Значение по умолчанию: отсутствует

Формат: `exception dump filepath dir`

Режим ввода команд: глобальная конфигурация

no exception dump filepath

Команда сброса конфигурации пути к файлу дампа к заводским настройкам.

Формат: `exception dump filepath`

Режим ввода команд: глобальная конфигурация

exception core-file

Настраивает префикс для имени файла дампа памяти. Имя файла дампа памяти генерируется с префиксом следующим образом.

При выборе hostname:

```
file-name-prefix_hostname_Time_Stamp.bin
```

Если hostname не выбран:

```
file-name-prefix_MAC_Address_Time_Stamp.bin
```

Если hostname указан, имя файла ядра использует значение hostname, в остальных случаях имя файла ядра использует MAC-адрес при генерации файла дампа ядра. Длина префикса — 15 символов.

Значение по умолчанию: core

Формат: `exception core-file {file-name-prefix | [hostname] | [time-stamp]}`

Режим ввода команд: глобальная конфигурация

no exception core-file

Команда сброса конфигурации префикса файла дампа памяти исключения к заводским настройкам. Опции имени узла и метки времени также отключаются.

Значение по умолчанию: core

Формат: `no exception core-file`

Режим ввода команд: глобальная конфигурация

exception switch-chip-register

Команда включает или выключает дамп регистров микросхемы коммутатора в случае исключения. Дамп регистров микросхемы коммутатора выполняется только для основного юнита, для остальных юнитов стека не выполняется.

Значение по умолчанию: выключено

Формат: `exception switch-chip-register {enable | disable}`

Режим ввода команд: глобальная конфигурация

exception dump ftp-server

Команда настраивает IP-адрес удаленного FTP-сервера, чтобы сохранить файлы дампа памяти на внешнем сервере. Если имя пользователя и пароль не настроены, коммутатор использует анонимное FTP-подключение (FTP-сервер должен принимать анонимные подключения).

Значение по умолчанию: отсутствует

Формат: `exception dump ftp-server` *`ip-address`* `[{username` *`user-name`* `password` *`password`*`}]`

Режим ввода команд: глобальная конфигурация

no exception dump ftp-server

Команда сброса настроек удаленного FTP-сервера для дампа исключения к заводским настройкам. Команда также сбрасывает имя пользователя и пароль FTP.

Значение по умолчанию: отсутствует

Формат: `no exception dump ftp-server`

Режим ввода команд: глобальная конфигурация

exception dump compression

Команда включает режим сжатия.

Значение по умолчанию: включено

Формат: `exception dump compression`

Режим ввода команд: глобальная конфигурация

no exception dump compression

Команда выключает режим сжатия.

Значение по умолчанию: отсутствует

Формат: `no exception compression`

Режим ввода команд: глобальная конфигурация

exception dump stack-ip-address protocol

Команда настраивает протокол (DHCP или статический) для использования при конфигурации сервисного порта в случае отказа юнита. Если настроен DHCP, модуль получает IP-адрес от DHCP-сервера, доступного в сети.

Значение по умолчанию: DHCP

Формат: `exception dump stack-ip-address protocol {dhcp | static}`

Режим ввода команд: глобальная конфигурация

no exception dump stack-ip-address protocol

Сброс конфигурации IP-протокола стека (DHCP или статического) к настройкам по умолчанию.

Значение по умолчанию: отсутствует

Формат: `no exception dump stack-ip-address protocol`

Режим ввода команд: глобальная конфигурация

exception dump stack-ip-address add

Команда добавляет статический IP-адрес, который будет присвоен сервисному порту отдельного юнита в стеке в случае отказа коммутатора. Этот IP-адрес используется для дампа памяти.

Значение по умолчанию: отсутствует

Формат: `exception dump stack-ip-address add` *`ip-address netmask`* [*`gateway`*]

Режим ввода команд: глобальная конфигурация

exception dump stack-ip-address remove

Удаление конфигурации IP-адреса стека. Если данный IP-адрес присвоен какому-либо модулю в стеке, он удаляется из модуля.

Значение по умолчанию: отсутствует

Формат: `exception dump stack-ip-address remove` *`ip-address netmask`*

Режим ввода команд: глобальная конфигурация

exception nmi

Эта команда включает или выключает дамп памяти в случае NMI.

Значение по умолчанию: выключено

Формат: `exception nmi {enable | disable}`

Режим ввода команд: глобальная конфигурация

write core

Используйте команду write core, чтобы создать файл дампа памяти. Команда write core test полезна при тестировании настроек дампа памяти. Например, если протокол TFTP сконфигурирован, write core test пытается связаться с сервером TFTP и сообщает, можно ли с ним связаться. Аналогичным образом, если протокол сконфигурирован как nfs, эта команда подключает и выключает файловую систему и сообщает пользователю о ее состоянии.

`write core` перезагружает коммутатор, что может быть полезно, если он работает неправильно, но не отказал.

Для write core test целевое имя файла используется для теста TFTP. Дополнительно можно задать целевое имя файла, если протокол сконфигурирован как TFTP.

Значение по умолчанию: отсутствует

Формат: `write core [test [dest_file_name]]`

Режим ввода команд: привилегированный

debug exception

Команда отображает поддержку функций дампа памяти.

Значение по умолчанию: отсутствует

Формат: `debug exception`

Режим ввода команд: привилегированный

show exception

Эта команда отображает параметры конфигурации для создания файла дампа памяти.

Значение по умолчанию: отсутствует

Формат: `show exception`

Режим ввода команд: привилегированный

show exception core-dump-file

Команда отображает файлы дампа памяти, существующие в локальной файловой системе.

Значение по умолчанию: отсутствует

Формат: `show exception core-dump-file`

Режим ввода команд: привилегированный или режим конфигурации

show exception log

Команда отображает результаты трассировки дампа памяти в локальной файловой системе.

Значение по умолчанию: отсутствует

Формат: `show exception log [previous]`

Режим ввода команд: привилегированный или режим конфигурации

mbuf

Используйте эту команду, чтобы настроить пороговые ограничения для буфера памяти (MBUF) и генерировать уведомления при достижении этих пределов.

Формат: `mbuf {falling-threshold | rising threshold | severity}`

Режим ввода команд: глобальная конфигурация

Поле	*Описание*
Rising Threshold	Уровень использования ресурсов памяти в процентах, при превышении которого отправляется уведомление. Допустимые значения: от 1 до 100. Значение по умолчанию — 0 (выключено).
Falling Threshold	Нижний уровень использования ресурсов памяти в процентах, при потреблении менее которого создается уведомление. Допустимые значения: от 1 до 100. Значение по умолчанию — 0 (выключено).
Severity	Уровень критичности, на котором Mbuf выдает системные сообщения. Допустимые значения: от 1 до 7. Значение по умолчанию: 5 (L7_LOG_SEVERITY_NOTICE).

show mbuf total

Команда отображает информацию буфера памяти (MBUF).

Формат: `show mbuf total`

Режим ввода команд: привилегированный

Поле	*Описание*
Mbufs Total	Общее количество сообщений в системном буфере.
Mbufs Free	Количество доступных буферов сообщений.
Mbufs Rx Used	Количество использующихся в настоящее время буферов сообщений.
Total Rx Norm Alloc Attempts	Число попыток системы выделить буфер под сообщения класса RX Norm.
Total Rx Mid2	Число попыток системы выделить буфер под сообщения класса RX Mid2.
Total Rx Mid1 Alloc Attempts	Число попыток системы выделить буфер под сообщения класса RX Mid1.
Total Rx Mid0 Alloc Attempts	Число попыток системы выделить буфер под сообщения класса RX Mid0.
Total Rx High Alloc Attempts	Число попыток системы выделить буфер под сообщения класса RX High.
Total Tx Alloc Attempts	Число попыток системы выделить буфер под сообщения класса TX.
Total Rx Norm Alloc Failures	Количество отказов при выделении буфер под сообщения класса RX Norm.
Total Rx Mid2 Alloc Failures	Количество отказов при выделении буфер под сообщения класса RX Mid2
Total Rx Mid1 Alloc Failures	Количество отказов при выделении буфер под сообщения класса RX Mid1.
Total Rx Mid0 Alloc Failures	Количество отказов при выделении буфер под сообщения класса RX Mid0.

Total Rx High Alloc Failures	Количество отказов при выделении буфер под сообщения класса RX High.
Total Tx Alloc Failures	Количество отказов при выделении буфер под сообщения класса TX.

show msg-queue

Команда для отображения очередей сообщений.

Значение по умолчанию: отсутствует

Формат: `show msg-queue`

Режим ввода команд: привилегированный

debug packet-trace

Используйте эту команду, чтобы включить вывод сообщений функции трассировки пакетов.

Значение по умолчанию: отсутствует

Формат: `debug packet-trace`

Режим ввода команд: привилегированный

session start

Команда инициирует консольную сессию от ведущего устройства стека к другому юниту в стеке, или от второстепенного юнита до управляющего или другого второстепенного юнита. Во время сессии на задействованном юните могут быть использованы команды для поиска неисправностей и отладки с выводом релевантной информации от задействованного юнита, определенного в сессии. Команды отображаются на задействованном юните с помощью опции help.

Значение по умолчанию: выключено

Формат: `session start {unit` *`unit-number`* `| manager}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
unit	Подключение к указанному юниту от главного юнита стека.
manager	Подключение непосредственно к управляющему юниту от любого второстепенного юнита без ввода номера управляющего юнита.

session stop

Используйте эту команду, чтобы завершить сессию, запущенную командой session start от управляющего юнита к второстепенному, от второстепенного юнита к такому же юниту или от юнита к управляющему юниту.

Значение по умолчанию: выключено

Формат: `session stop`

Режим ввода команд: глобальная конфигурация

6.16 Команды тестирования кабеля

Функция тестирования кабеля позволяет определить состояние кабельного соединения на выбранном порту.

Функция тестирования кабеля поддерживается только для медного кабеля. Для оптоволоконного кабеля тестирование не поддерживается.

Если у порта есть активное соединение, в процессе тестирования кабеля соединение может быть прервано.

cablestatus

Эта команда возвращает состояние указанного порта.

Формат: `cablestatus` *`unit/slot/port`*
Режим ввода команд: привилегированный

Поле	*Описание*
Cable Status	Возвращает один из следующих статусов. • **Normal:** Кабель работает исправно; • **Open:** Кабель разъединен или есть неисправный разъем; • **Short:** Короткое замыкание кабеля; • **Cable Test Failed:** Состояние кабеля не определено. Не исключено, что он исправен; • **Crosstalk:** Перекрестные помехи на кабеле; • **No Cable:** Кабель не найден.
Cable Length	Если эта функция поддерживается PHY для текущей скорости соединения, длина кабеля отображается как диапазон между самой короткой предполагаемой длиной и самой продолжительно предполагаемой длиной. Обратите внимание: если соединение поднято и кабель присоединен к адаптеру Ethernet 10/100, отображается состояние кабеля Open или Short, потому что некоторые адаптеры Ethernet оставляют неиспользованные проводные пары включенными или заземленными. Значение unknown отображается, если длина кабеля не определена.

6.17 Команды sFlow

sFlow — стандарт для мониторинга высокоскоростных коммутируемых и маршрутизируемых сетей. Технология sFlow встроена в сетевое оборудование и обеспечивает полную видимость сетевой активности, обеспечивая эффективное управление и контроль сетевых ресурсов.

sflow poller

Источник данных, настроенный для сбора показаний счётчиков, называется поллером. Используйте эту команду, чтобы включить новый поллер sFlow на интерфейсе или диапазоне интерфейсов, rcvr_idx должен быть индексом настроенного принимающего устройства.

Формат: `sflow poller {`*`rcvr-indx`* `|` `interval` *`poll-interval`*`}`
Режим ввода команд: конфигурирование интерфейса

Поле	*Описание*
Receiver Index	Принимающее устройство sFlow, связанное с регистратором. Значение 0 означает, что принимающее устройство не настроено. Диапазон: 1–8. Значение по умолчанию: 0.

Poll Interval	Интервал опроса счётчиков для поллера sFlow. Интервал опроса 0 выключает встречную выборку показаний счётчиков. Когда установлено нулевое значение (0), все параметры регистраторов поллера принимают значения по умолчанию. Диапазон: 0–86400. Значение по умолчанию: 0. Значение N значит, что встречная выборка показаний счётчиков происходит один раз в N секунд.

Процесс sFlow загружен больше всего, когда интервал опроса sFlow настроен на минимальное значение (т. е. одна секунда для всех поддерживаемых интерфейсов sFlow). В этом случае процесс sFlow постоянно занят сбором показаний счетчиков во всех сконфигурированных интерфейсах. Устройство может зависнуть на некоторое время при попытке конфигурации или использования show-команд для sFlow. Для предотвращения этой ситуации доступные интервалы для интерфейсов ограничены следующим образом:
Максимальное количество допустимых интерфейсов для интервалов опроса от максимального (1, (interval – 10)) до минимального ((interval + 10), 86400):интервал * 5.
При каждом увеличении интервала опроса на одну секунду количество допустимых интерфейсов, которые могут быть сконфигурированы увеличивается на 5.

no sflow poller

Используйте эту команду, чтобы удалить поллер sFlow с интерфейса или диапазона интерфейсов.

Формат: `no sflow poller [interval]`

Режим ввода команд: конфигурирование интерфейса

sflow receiver

Команда устанавливает параметры принимающего устройства sFlow.

Формат: `no sflow receiver index {ip ip-address | maxdatagram size | owner string timeout interval | port 14-port}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
index	Индекс принимающего устройства. Допустимые значения: от 1 до 8
owner	Строка, идентифицирующая запись таблицы sFlowRcvrTable для данного принимающее устройства. Диапазон: 127 символов. Значение по умолчанию: пустая строка. Пустая строка указывает, что запись не используется и конфигурация принимающего устройства сбрасывается к значениям по умолчанию. Перед использованием записи sFlowRcvrTable необходимо убедиться, что запись еще не используется. Запись считается используемой, если имеет значение, отличное от пустой строки. Запись должна быть создана до того, как принимающее устройство будет связано с поллером или самплером.
timeout	Время (в секундах), через которое сэмплер или поллер будет отсоединён и перестанет отсылать информацию. Управляющее устройство, обеспечивающее контроль над сэмплером/поллером, ответственно за установку нового значения, прежде чем истечет старое. Допустимый диапазон: 0–2147483647 секунд. Значение по умолчанию: 0.

notimeout	Настроенная запись сохраняется в конфигурации, пока не будет явно удалена.
maxdatagram	Максимальное количество байтов данных, которые могут быть отправлены в одной дейтаграмме. Управляющее устройство должно установить это значение, чтобы избежать фрагментации sFlow-дейтаграмм. Диапазон: 200–9116. Значение по умолчанию: 1400.
ip	IP-адрес принимающего устройства sFlow. При значении 0.0.0.0 sFlow-дейтаграммы не будут отправлены. Значение по умолчанию: 0.0.0.0.
port	UDP-порт назначения Layer4 для sFlow-дейтаграмм. Диапазон: 1–65535. Значение по умолчанию: 6343.

no sflow receiver

Команда возвращает параметры принимающего устройства sFlow к значениям по умолчанию.

Формат: `no sflow receiver indx {ip ip-address | maxdatagram size | owner string timeout interval | port 14-port}`

Режим ввода команд: глобальная конфигурация

sflow receiver owner timeout

Используйте эту команду, чтобы настроить принимающее устройство как запись с заданным временем жизни. Если принимающее устройство sFlow настроено с заданным временем жизни, информация, связанная с регистраторами, не отображается в текущей конфигурации и не сохраняется после перезагрузки.

Формат: `sflow receiver` *`index`* `owner` *`owner-string`* `timeout`

Режим ввода команд: глобальная конфигурация

sflow receiver owner notimeout

Используйте эту команду, чтобы настроить принимающее устройство как запись без заданного времени жизни. В отличие от записей, сконфигурированных с определенным значением времени жизни, эта команда будет отображаться в текущей конфигурации и сохраняться после перезагрузки. Если принимающее устройство sFlow настроено как запись без заданного времени жизни, информация о самплерах и поллерах, связанных с этим принимающим устройством также будет отображаться в текущей конфигурации и сохраняться после перезагрузки.

Формат: `sflow receiver` *`index`* `owner` *`owner-string`* `notimeout`
Режим ввода команд: глобальная конфигурация

sflow sampler

Источник данных, настроенный для выборки образцов потока, называется сэмплером. Используйте эту команду, чтобы настроить новый сэмплером sFlow на интерфейсе или диапазоне интерфейсов, rcvr_idx должен быть индексом настроенного принимающего устройства.

Формат: `sflow sampler {`*`rcvr-indx`* `| rate` *`sampling-rate`* `| maxheadersize` *`size`*`}`

Режим ввода команд: конфигурирование интерфейса

Поле	*Описание*
rcvr-indx	Принимающее устройство sFlow для данного sFlow-сэмплера, на который требуется отправлять выборки потока. Значение 0 означает,

	что принимающее устройство не настроено и пакеты с выборкой пакетов не будут отправляться. Можно настроить только активные принимающие устройства. Если принимающее устройство будет становится неактивным, то все сэмплеры, связанные с этим принимающим устройством, также будут становятся неактивными. Возможные значения: 1–8. Значение по умолчанию: 0.
maxheadersize	Максимальное количество байт, которые требуется копировать из сэмплируемого пакета. Диапазон: 20–256. Значение по умолчанию: 128. Если установлено нулевое значение (0), все параметры сэмплера принимают значения по умолчанию.
rate	Частота сэмплирования пакетов из данного источника. Значение 0 выключает сэмплирование. Значение N означает, что из N входящих пакетов будет выбран 1 пакет. Диапазон: 1024–65536 и 0. Значение по умолчанию: 0.

no sflow sampler

Используйте эту команду, чтобы сбросить sFlow-сэмплер к настройкам по умолчанию.

Формат: `no sflow sampler {`*`rcvr-indx`* `| rate` *`sampling-rate`* `| maxheader-size` *`size`*`}`

Режим ввода команд: конфигурирование интерфейса

sflow sampler rate

Команда устанавливает частоту сэмплирования входящих пакетов.

Значение по умолчанию: 0 для частоты сэмплирования входящих пакетов

Формат: `sflow sampler rate` *`value`*

Режим ввода команд: конфигурирование интерфейса

no sflow sample rate

Удаляет частоту сэмплирования входящих пакетов.

Формат: `no sflow sampler rate`

Режим ввода команд: конфигурирование интерфейса

sflow source-interface

Команда для определения физического или логического интерфейса, адрес которого будет использоваться в качестве адреса источника sFlow-клиента. Если настроен, адрес источника используется для любых связей между принимающим устройством sFlow и sFlow-клиентом (если нет, изменения не вносятся). Если настроенный интерфейс не поднят, sFlow-клиент возвращается в режим по умолчанию.

Формат: `sflow source-interface {`*`unit/slot/port`* `| loopback` *`loopback-id`* `| tunnel` *`tunnel-id`* `| vlan` *`vlan-id`*`}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
unit/slot/port	VLAN или интерфейс маршрутизации на базе порта.
loopback-id	Настраивает loopback-интерфейс в качестве IP-адреса источника. Диапазон идентификатора обратной петли: от 0 до 7.
tunnel-id	Настраивает туннельный интерфейс в качестве IP-адреса источника. Диапазон идентификатора туннеля: от 0 до 7.

vlan-id	Настраивает интерфейс VLAN в качестве IP-адреса источника. Диапазон идентификатора VLAN: 1–4093.

no sflow source-interface

Сбрасывает настройки адреса источника sFlow к настройкам по умолчанию.

Формат: `no sflow source-interface`

Режим ввода команд: глобальная конфигурация

show sflow agent

Используйте эту команду, чтобы отобразить информацию об агенте sFlow.

Формат: `show sflow agent`

Режим ввода команд: привилегированный

Поле	*Описание*
sFlow Version	Однозначно определяет версию и реализацию этого MIB. У строки версии должна быть следующая структура: версия MIB; организация; редакция ПО, где версия MIB: 1.3, версия данного MIB. Организация: Corp. Редакция: 1.0.
IP address	IP-адрес, связанный с этим агентом.

show sflow pollers

Используйте эту команду, чтобы отобразить поллеры sFlow, созданные на коммутаторе.

Формат: `show sflow pollers`

Режим ввода команд: привилегированный

Поле	*Описание*
Poller Data Source	sFlowDataSource (slot/port) для этого sFlow-поллера. Этот агент поддерживает только физические порты.
Receiver Index	Принимающее устройство sFlow, связанное с этим поллером sFlow.
Poller Interval	Время в секундах между последовательными опросами счетчиков, связанных с этим источником данных.

show sflow receivers

Используйте эту команду для отображения конфигурационной информации, связанной с принимающими устройствами sFlow.

Формат: `show sflow receivers [`*index*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
Receiver Index	Принимающее устройство sFlow, связанное с сэмплером/поллером.
Owner String	Строка, идентифицирующая запись таблицы sFlowRcvrTable для данного принимающее устройства.
Time Out	Время (в секундах), через которое сэмплер или поллер будет отсоединён и перестанет отсылать информацию. Значение параметра no timeout означает, что принимающее устройство sFlow настроено как запись без заданного времени жизни.

Max Datagram Size	Максимальное количество байтов, которые могут быть отправлены в одной дейтаграмме.
Port	UDP-порт назначения для sFlow-дейтаграмм.
IP adress	IP-адрес принимающего устройства sFlow.
Address Type	Тип IP-адреса принимающего устройства sFlow. Для IPv4-адреса используется значение 1, для IPv6-адреса — 2.
Datagram Version	Версия протокола sFlow, которая будет использоваться при отправке выборок на принимающее устройство sFlow.

show sflow source-interface

Используйте эту команду, чтобы отобразить интерфейс, адрес которого используется в качестве адреса источника sFlow, настроенный на коммутаторе.

Формат: `show sflow source-interface`

Режим ввода команд: привилегированный

Поле	*Описание*
sFlow Client Source Interface	Идентификатор физического или логического интерфейса, адрес которого используется в качестве адреса источника sFlow-клиента.
sFlow Client Source IPv4 Address	IP-адрес интерфейса, сконфигурированного как исходный интерфейс использующийся в качестве адреса источника sFlow-клиента.

6.18 Команды настройки SDM-шаблонов

Шаблон Switch Database Management (SDM) — это описание максимальных ресурсов, которые коммутатор или маршрутизатор может использовать для различных функций. Различные шаблоны SDM позволяют различные комбинации коэффициентов масштабирования, включая различные примеры распределения ресурсов в зависимости от того, как используется устройство. Другими словами, шаблоны SDM позволяют перераспределить системные ресурсы, чтобы поддерживать различное сочетание функций для конкретных сетевых требований.

При подключении юнита к стеку, если его шаблон не соответствует шаблону стека, новый юнит автоматически перезагружается с использованием шаблона, аналогичного используемым другими юнитами стека. Чтобы избежать автоматической перезагрузки, можно предварительно установить на юните шаблон, используемый существующими юнитами стека. Затем выключите новый юнит, присоедините его к стеку и включите.

sdm prefer

Используйте эту команду, чтобы изменить шаблон, который будет активен после следующей перезагрузки. Ключевые слова:

- **dual-ipv4-and-ipv6** — ограничивает выбор шаблонов теми шаблонами, что поддерживают и IPv4, и IPv6. Шаблон default увеличивает до максимума количество одноадресных маршрутов IPv4 и IPv6, параллельно ограничивая количество ближайших ECMP на каждом маршруте до 4. Шаблон data-center поддерживание увеличение количества ближайших ECMP до 16.
- **ipv4-routing** — ограничивает выбор шаблонов теми шаблонами, что поддерживают только IPv4. Шаблон default для IPv4-маршрутизации увеличивает до максимума количество одноадресных маршрутов IPv4, параллельно ограничивая количество ближайших ECMP на каждом маршруте до 4. Шаблон data-center default поддерживает увеличение количества ближайших ECMP до 16 и сокращает количество маршрутов. Шаблон data-center plus увеличивает количество ближайших ECMP до 16 и сохраняет максимальное количество маршрутов IPv4.

После установки шаблона требуется выполнить перезагрузку, чтобы изменения конфигурации вступили в силу.

Значение по умолчанию: dual-ipv4-and-ipv6

Формат: `sdm prefer {dual-ipv4-and-ipv6 {default | data-center } | ipv4-routing {default | {data-center {default | plus}}}`

Режим ввода команд: глобальная конфигурация

no sdm prefer

Используйте эту команду, чтобы после следующей перезагрузки вернуться к шаблону по умолчанию.

Формат: `no sdm prefer`

Режим ввода команд: глобальная конфигурация

show sdm prefer

Команда позволяет просмотреть активный SDM-шаблон и его параметры масштабирования или просмотреть параметры масштабирования для неактивного шаблона. Без дополнительных ключевых слов команда выводит активный шаблон и шаблон, который будет активен после перезагрузки, если он отличен от активного шаблона. Если система загружена не с использованием шаблона по умолчанию и выполняется сброс конфигурации шаблона (с помощью no sdm prefer или удаления стартовой конфигурации), команда show sdm prefer выведет шаблон по умолчанию как следующий активный шаблон. Чтобы вывести коэффициенты масштабирования определенного шаблона, используйте ключевое слово этого шаблона в качестве параметра к команде.

Используйте дополнительные ключевые слова, чтобы вывести коэффициенты масштабирования определенного шаблона.

Формат: `show sdm prefer [dual-ipv4-and-ipv6 {default | data-center} | ipv4-routing {default | data-center {default | plus}} ]`

Режим ввода команд: привилегированный

Параметр	*Описание*
dual-ipv4-and-ipv6 default	(Не обязательно.) Список коэффициентов масштабирования для шаблона с поддержкой IPv4 и IPv6.
dual-ipv4-and-ipv6 data-center	(Не обязательно.) Список коэффициентов масштабирования для шаблона Dual IPv4 и IPv6, поддерживающего больше ближайших ECMP.
ipv4-routing default	(Не обязательно.) Список коэффициентов масштабирования для шаблона, поддерживающего только IPv4 с максимальным количеством одноадресных маршрутов
ipv4-routing data-center default	(Не обязательно.) Список коэффициентов масштабирования для шаблона поддержки только IPv4 и большего количества ближайших ECMP.
ipv4-routing data-center plus	(Не обязательно.) Список коэффициентов масштабирования для шаблона, поддерживающего только IPv4 с максимальным количеством одноадресных маршрутов, а также большее количества ближайших ECMP.

Поле	*Описание*
ARP Entries	Максимальное количество записей в кэше Address Resolution Protocol (ARP) IPv4 для интерфейсов маршрутизации.

IPv4 Unicast Routes	Максимальное количество записей таблицы маршрутизации для одноадресного трафика IPv4.
IPv6 NDP Entries	Максимальное количество записей кэша Neighbor Discovery Protocol (NDP) для IPv6.
IPv6 Unicast Routes	Максимальное количество записей таблицы маршрутизации для одноадресного трафика IPv6.
ECMP Next Hops	Максимальное количество ECMP маршрутов, которые могут быть установлены в одноадресных таблицах маршрутизации IPv4 и IPv6.

6.19 Команды удаленного мониторинга

Удаленный мониторинг (RMON) является методом сбора разнообразных данных о сетевом трафике. RMON поддерживает 64-разрядные счетчики (RFC 3273) и High Capacity Alarm Table (RFC 3434).

Не существует команды конфигурации для статистики ethernet и статистики ethernet большой разрядности. Источник данных для статистики ethernet и статистики ethernet большой разрядности настраиваются во время инициализации.

rmon alarm

Команда устанавливает запись оповещения RMON в таблице оповещений RMON MIB.

Формат: `rmon alarm` *`alarm number variable sample interval`* {absolute|delta} `rising-threshold` *`value`* [*`rising-event-index`*] `falling-threshold` *`value`* [*`falling-event-index`*] [`startup` {*`rising`*|*`falling`*|*`rising-falling`*}] [`owner` *`string`*]

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
Alarm Index	Индекс, который однозначно определяет запись в таблице оповещений. Каждая запись определяет диагностическую выборку по определенному интервалу времени для объекта на устройстве. Допустимые значения: от 1 до 65535.
Alarm Variable	Идентификатор объекта переменной для выборки. Допускаются только переменные, которые имеют тип примитивного целого числа ASN.1.
Alarm Interval	Интервал в секундах, по которому происходит выборка данных и их сравнение с нижним и верхним порогом. Допустимые значения: от 1 до 2147483647. Значение по умолчанию: 1.
Alarm Rising Threshold	Верхний порог для оповещения. Допустимые значения: от 2147483648 до 2147483647. Значение по умолчанию: 1.
Alarm Rising Event Index	Индекс объекта события eventEntry, использующегося при пересечении верхнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 1.
Alarm Falling Threshold	Нижний порог для оповещения. Допустимые значения: от 2147483648 до 2147483647. Значение по умолчанию: 1.
Alarm Falling Event Index	Индекс объекта события eventEntry, использующегося при пересечении нижнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 2.
Alarm Startup Alarm	Оповещение, которое должно быть отправлено. Возможные значения: `rising`, `falling` или `rising-falling`. По умолчанию: `rising-falling`.
Alarm Owner	Строка имени владельца, связанная с записью оповещения. Значение по умолчанию: `monitorAlarm`.

no rmon alarm

Удаляет запись оповещения RMON.

Формат: `no rmon alarm` *`alarm number`*

Режим ввода команд: глобальная конфигурация

rmon hcalarm

Команда устанавливает запись RMON hcalarm в MIB-таблице оповещений RMON для переменных большой разрядности.

Формат: `rmon hcalarm` *`alarm number variable sample interval`* {absolute|delta} `rising-threshold high` *`value`* `low` *`value`* `status` {positive|negative} [*`rising-event-index`*] `falling- threshold high` *`value`* `low` *`value`* `status` {positive|negative} [*`falling-event-index`*] [`startup` {*`rising`*|*`falling`*|*`rising-falling`*}] [`owner` *`string`*]

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
High Capacity Alarm Index	Произвольное целочисленное значение, определяющее запись оповещения. Допустимые значения: от 1 до 65535.
High Capacity Alarm Variable	Идентификатор объекта переменной для выборки. Допускаются только переменные, которые имеют тип примитивного целого числа ASN.1.
High Capacity Alarm Interval	Интервал в секундах, по которому происходит выборка данных и их сравнение с нижним и верхним порогом. Допустимые значения: от 1 до 2147483647. Значение по умолчанию: 1.
High Capacity Alarm Sample Type	Метод выборки переменной и вычисления значения, которое будет сравниваться с порогами. Возможные типы: Absolute Value или Delta Value. По умолчанию: Absolute Value.
High Capacity Alarm Absolute Alarm Status	Знак значения для переменной большой разрядности (hcAlarmAbsValueobject).
High Capacity Alarm Startup Alarm	Возможные типы состояния: valueNotAvailable, valuePositive или valueNegative. По умолчанию: valueNotAvailable. Оповещение, которое должно быть отправлено. Предупреждение большой емкости запускает сигнал, который может быть отправлен. Возможные значения: rising, falling или rising-falling. По умолчанию: rising-falling.
High Capacity Alarm Rising- Threshold Absolute Value Low	Нижние 32 бит абсолютного значения верхнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 1.
High Capacity Alarm Rising- Threshold Absolute Value High	Верхние 32 бита абсолютного значения верхнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 0.
High Capacity Alarm Rising-Threshold Value Status	Знак числа верхнего порога, определенного объектами hcAlarmRisingThresAbsValueLow и hcAlarmRisingThresAbsValueHigh. Возможные значения: valueNotAvailable, valuePositive, или valueNegative. По умолчанию: valuePositive.
High Capacity Alarm Falling-Threshold Absolute Value Low	Нижние 32 бит абсолютного значения нижнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 1
High Capacity Alarm Falling-Threshold Absolute Value High	Верхние 32 бита абсолютного значения нижнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 0.

High Capacity Alarm Falling-Threshold Value Status	Знак числа нижнего порога, определенного объектами hcAlarmRisingThresAbsValueLow и hcAlarmRisingThresAbsValueHigh. Возможные значения: valueNotAvailable, valuePositive, или valueNegative. По умолчанию: valuePositive.
High Capacity Alarm Rising Event Index	Индекс объекта события eventEntry, использующегося при пересечении верхнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 1.
High Capacity Alarm Falling Event Index	Индекс объекта события eventEntry, использующегося при пересечении нижнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 2.
High Capacity Alarm Owner	Строка имени владельца, связанная с записью оповещения. Значение по умолчанию: monitorHCAlarm.

no rmon hcalarm

Удаляет запись RMON hcalarm.

Формат: `no rmon hcalarm` *`alarm number`*

Режим ввода команд: глобальная конфигурация

rmon event

Команда устанавливает запись объекта события RMON в таблице объектов событий RMON MIB.

Формат: `rmon event` *`event number`* `[description` *`string`*`|log|owner` *`string`*`|trap` *`community`*`]`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
Event Index	Индекс, который однозначно определяет запись в таблице событий. Каждая запись определяет одно событие, которое должно быть сгенерировано при определенных условиях. Допустимые значения: от 1 до 65535.
Event Description	Комментарий, описывающий объект события. Значение по умолчанию: alarmEvent
Event Type	Тип уведомления о событии. Возможные значения: None, Log, SNMP Trap, Log и SNMP Trap. Значение по умолчанию: None.
Event Owner	Строка имени владельца, связанная с записью. Значение по умолчанию: monitorEvent.
Event Community	Строка SNMP-сообщества, используемого для отправки SNMP-трапа. Значение по умолчанию: public

no rmon event

Удаляет запись объекта события RMON.

Формат: `no rmon event` *`event number`*

Режим ввода команд: глобальная конфигурация

rmon collection history

Устанавливает параметры контроля сбора истории RMON в соответствующей MIB-таблице.

Эта команда не поддерживается для диапазона интерфейсов. Каждая запись контроля сбора истории RMON может быть настроена только на одном интерфейсе. При попытке настройки на нескольких интерфейсах коммутатор выдает ошибку.

Формат: `rmon collection history` *`index number`* `[buckets` *`number`*`|interval` *`interval in sec`*`|owner` *`string`*`]`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
History Control Index	Индекс, который однозначно определяет запись в таблице historyControl. Каждая такая запись описывает ряд выборок по определенному интервалу для интерфейса на устройстве. Допустимые значения: от 1 до 65535.
History Control Data Source	Интерфейс источника, на котором собираются данные.
History Control Buckets Requested	Требуемое количество интервалов времени, для которых должны быть сохранены данные. Допустимые значения: от 1 до 65535. Значение по умолчанию: 50
History Control Interval	Интервал выборки данных в секундах. Допустимые значения: от 1 до 3600. Значение по умолчанию: 1800.
History Control Owner	Строка имени владельца, связанная с записью управления сбора истории. Значение по умолчанию: monitorHistoryControl.

no rmon collection history

Эта команда удаляет запись с указанным индексом в группе управления сбора истории.

Формат: `no rmon collection history` *`index number`*

Режим ввода команд: конфигурирование интерфейса

show rmon

Вывод записей таблицы оповещений RMON.

Формат: `show rmon {alarms | alarm` *`alarm-index`*`}`

Режим ввода команд: привилегированный

Параметр	*Описание*
Alarm Index	Индекс, который однозначно определяет запись в таблице оповещений. Каждая запись определяет диагностическую выборку по определенном интервалу времени для объекта на устройстве. Допустимые значения: от 1 до 65535.
Alarm Variable	Идентификатор объекта переменной для выборки. Допускаются только переменные, которые имеют тип примитивного целого числа ASN.1.
Alarm Interval	Интервал в секундах, по которому происходит выборка данных и их сравнение с нижним и верхним порогом. Допустимые значения: от 1 до 2147483647. Значение по умолчанию: 1.
Alarm Absolute Value	Значение измеряемой величины в прошлый период выборки. Объект — знаковое 32-разрядное значение, только для чтения.

Alarm Rising Threshold	Верхний порог для оповещения. Допустимые значения: от 2147483648 до 2147483647. Значение по умолчанию: 1.
Alarm Rising Event Index	Индекс объекта события eventEntry, использующегося при пересечении верхнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 1.
Alarm Falling Threshold	Нижний порог для оповещения. Допустимые значения: от 2147483648 до 2147483647. Значение по умолчанию: 1.
Alarm Falling Event Index	Индекс объекта события eventEntry, который используется при пересечении нижнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 2.
Alarm Startup Alarm	Оповещения, которые должны быть отправлены. Возможные значения: rising, falling или rising-falling. По умолчанию: rising-falling.
Alarm Owner	Строка имени владельца, связанная с записью оповещения. Значение по умолчанию: monitorAlarm.

show rmon collection history

Команда вывода записей таблицы управления сбора истории RMON.

Формат: `show rmon collection history [interfaces` *`unit/slot/port`*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
History Control Index	Индекс, который однозначно определяет запись в таблице historyControl. Каждая такая запись описывает ряд выборок по определенному интервалу для интерфейса на устройстве. Допустимые значения: от 1 до 65535.
History Control Data Source	Интерфейс источника, на котором собираются данные.
History Control Buckets Requested	Требуемое количество интервалов времени, для которых должны быть сохранены данные. Допустимые значения: от 1 до 65535. Значение по умолчанию: 50.
History Control Buckets Granted	Количество интервалов времени, для которых будут сохранены данные. Объект – только для чтения. Значение по умолчанию: 10.
History Control Interval	Интервал выборки данных в секундах. Допустимые значения: от 1 до 3600. Значение по умолчанию: 1800.
History Control Owner	Строка имени владельца, связанная с записью управления историей. Значение по умолчанию: monitorHistoryControl

show rmon events

Команда выводит записи таблицы событий RMON.

Формат: `show rmon events`

Режим ввода команд: привилегированный

Параметр	*Описание*
Event Index	Индекс, который однозначно определяет запись в таблице событий Каждая запись определяет одно событие, которое должно быть сгенерировано при определенных условиях. Допустимые значения: от 1 до 65535.
Event Description	Комментарий, описывающий объект события. Значение по умолчанию: alarmEvent.
Event Type	Тип уведомления о событии. Возможные значения: None, Log, SNMP Trap, Log и SNMP Trap. Значение по умолчанию: None.
Owner	Строка имени владельца, связанная с записью. Значение по умолчанию: monitorEvent.

Event Community	Строка SNMP-сообщества, используемая для отправки SNMP-трапа. По умолчанию: public.
Last time sent	Время последней записи в журнале или последнего отправленного SNMP-трапа.

show rmon history

Команда отображает указанную запись таблицы истории RMON.

Формат: `show rmon history` *`index`* `{errors [period` *`seconds`*`]|other [period` *`seconds`*`]|throughput [period` *`seconds`*`]}`

Режим ввода команд: привилегированный

Параметр	*Описание*
History Control Index	Индекс, который однозначно определяет запись в таблице historyControl. Каждая такая запись описывает ряд выборок по определенному интервалу для интерфейса на устройстве. Допустимые значения: от 1 до 65535.
History Control Data Source	Интерфейс источника, на котором собираются данные.
History Control Buckets Requested	Требуемое количество интервалов времени, для которых должны быть сохранены данные. Диапазон от 1 до 65535. Значение по умолчанию: 50.
History Control Buckets Granted	Количество интервалов дискретизации, для которых должны быть сохранены данные. Объект только для чтения. Значение по умолчанию: 10.
History Control Interval	Интервал выборки данных в секундах. Допустимые значения: от 1 до 3600. Значение по умолчанию: 1800.
History Control Owner	Строка имени владельца, связанная с записью управления сбора истории. Значение по умолчанию: monitorHistoryControl.
Maximum Table Size	Максимальное количество записей в таблице истории.
Time	Время, в которое сделана выборка, отображается в секундах.
CRC Align	Количество ошибок CRC align.
Undersize Packets	Общее количество неполных пакетов. Пакеты длиной менее 64 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета).
Oversize Packets	Общее количество пакетов избыточного размера. Пакеты длиной более, чем 1518 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета).
Fragments	Общее количество фрагментированных пакетов. Пакеты, количество октетов в которых не целое, и пакеты с ошибочной контрольной суммой длиной менее 64 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета).
Jabbers	Общее количество сбойных пакетов. Пакеты, количество октетов в которых не целое, и пакеты с ошибочной контрольной суммой длиной более 1518 октетов (без учёта межкадрового интервала, исключая кодирующие биты, но с учетом октетов контрольной суммы пакета).
Octets	Общее количество октетов, полученных на интерфейсе.
Packets	Общее количество полученных пакетов (включая ошибочные пакеты) на интерфейсе.
Broadcast	Общее количество широковещательных пакетов ошибок, принятых на интерфейсе.
Multicast	Общее количество многоадресных пакетов без ошибок, принятых на интерфейсе.
Util	Утилизация интерфейса, в определенный момент времени.
Dropped Collisions	Общее количество отброшенных коллизий.

show rmon log

Эта команда отображает записи таблицы журнала RMON.

Формат: `show rmon log [event-index]`

Режим ввода команд: привилегированный

Параметр	*Описание*
Maximum table size	Максимальное количество записей, которые может содержать таблица журнала.
Event	Индекс объекта события, для которого создана запись в журнале.
Description	Комментарий, описывающий объект события, для которого создана запись в журнале.
Time	Время создания события.

show rmon statistics interfaces

Вывод статистики RMON для заданного интерфейса.

Формат: `show rmon statistics interfaces unit/slot/port`

Режим ввода команд: привилегированный

Параметр	*Описание*
Port	Номер порта в формате unit/slot/port.
Dropped	Общее количество отброшенных пакетов на интерфейсе.
Octets	Общее количество октетов, полученных на интерфейсе.
Packets	Общее количество полученных пакетов (включая ошибочные пакеты) на интерфейсе.
Broadcast	Общее количество широковещательных пакетов без ошибок, принятых на интерфейсе.
Multicast	Общее количество многоадресных пакетов без ошибок, принятых на интерфейсе.
CRC Align Errors	Общее количество полученных пакетов длиной (без учёта межкадрового интервала, но с учетом октетов контрольной суммы) от 64 до 1518 октетов включительно.
Collisions	Общее количество коллизий на интерфейсе.
Undersize Pkts	Общее количество пакетов недостаточного размера. Пакеты длиной менее 64 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета).
Oversize Pkts	Общее количество пакетов избыточного размера. Пакеты более 1518 октетов длиной (без учёта межкадрового интервала, но с учетом октетов контрольной суммы).
Fragments	Общее количество фрагментированных пакетов. Пакеты, количество октетов в которых не целое, и пакеты с ошибочной контрольной суммой длиной менее 64 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы пакета).
Jabbers	Общее количество сбойных пакетов. Пакеты, количество октетов в которых не целое, и пакеты с ошибочной контрольной суммой длиной более 1518 октетов (без учёта межкадрового интервала, исключая кодирующие биты, но с учетом октетов контрольной суммы пакета).
64 Octets	Общее количество пакетов длиной 64 октета (без учёта межкадрового интервала, но с учетом октетов контрольной суммы).
65-127 Octets	Общее количество пакетов длиной 65–127 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы).

128-255 Octets	Общее количество пакетов длиной 128–255 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы).
256-511 Octets	Общее количество пакетов длиной 256–511 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы).
512-1023 Octets	Общее количество пакетов длиной 512–1023 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы).
1024-1518 Octets	Общее количество пакетов длиной 1024–1518 октетов (без учёта межкадрового интервала, но с учетом октетов контрольной суммы).
HC Overflow Pkts	Количество переполнений счётчика пакетов.
HC Overflow Octets	Количество переполнений счётчика октетов.
HC Overflow Pkts 64 Octets	Количество переполнений счётчика пакетов HC длиной 64 октета.
HC Overflow Pkts 65 - 127 Octets	Количество переполнений счётчика пакетов длиной 65–127 октетов.
HC Overflow Pkts 128 - 255 Octets	Количество переполнений счётчика пакетов длиной 128–255 октетов.
HC Overflow Pkts 256 - 511 Octets	Количество переполнений счётчика пакетов длиной 256–511 октетов.
HC Overflow Pkts 512 - 1023 Octets	Количество переполнений счётчика пакетов длиной 512–1023 октетов.
HC Overflow Pkts 1024 - 1518 Octets	Количество переполнений счётчика пакетов длиной 1024–1518 октетов.

show rmon hcalarms

Команда отображает записи таблицы оповещений RMON для объектов большой разрядности.

Формат: `show rmon {hcalarms|hcalarm` *`alarm index`*`}`

Режим ввода команд: привилегированный

Параметр	***Описание***
High Capacity Alarm Index	Индекс, который однозначно определяет запись оповещения. Допустимые значения: от 1 до 65535.
High Capacity Alarm Variable	Идентификатор объекта переменной для выборки. Допускаются только переменные, которые имеют тип примитивного целого числа ASN.1.
High Capacity Alarm Interval	Интервал в секундах, по которому происходит выборка данных и их сравнение с нижним и верхним порогом. Допустимые значения: от 1 до 2147483647. Значение по умолчанию: 1.
High Capacity Alarm Sample Type	Метод выборки переменной и вычисления значения, которое будет сравниваться с порогами. Возможные типы: Absolute Value или Delta Value. По умолчанию: Absolute Value.
High Capacity Alarm Absolute Value	Абсолютное значение (т.е. значение без знака) hcAlarmVariable переменной в прошлый период выборки. Значение не доступно, если период ещё не завершен. Объект — 64-разрядное значение без знака, только для чтения.
High Capacity Alarm Absolute Alarm Status	Объект указывает знак числа переменной большой емкости (hcAlarmAbsValueobject). Возможные типы состояния: valueNotAvailable, valuePositive или valueNegative. По умолчанию: valueNotAvailable.
High Capacity Alarm Startup Alarm	Оповещение, которое должно быть отправлено. Возможные значения: rising, falling или rising-falling. По умолчанию: rising-falling.
High Capacity Alarm Rising- Threshold Absolute Value Low	Нижние 32 бита абсолютного значения верхнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 1.

High Capacity Alarm Rising- Threshold Absolute Value High	Верхние 32 бита абсолютного значения верхнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 0.
High Capacity Alarm Rising- Threshold Value Status	Знак числа верхнего порога, определенного объектами hcAlarmRisingThresAbsValueLow и hcAlarmRisingThresAbsValueHigh. Возможные значения: valueNotAvailable, valuePositive, или valueNegative. По умолчанию: valuePositive.
High Capacity Alarm Falling- Threshold Absolute Value Low	Нижние 32 бит абсолютного значения нижнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 1.
High Capacity Alarm Falling- Threshold Absolute Value High	Верхние 32 бит абсолютного значения нижнего порога для оповещения. Допустимые значения: от 0 до 4294967295. Значение по умолчанию: 0.
High Capacity Alarm Falling- Threshold Value Status	Знак числа нижнего порога, определенного объектами hcAlarmRisingThresAbsValueLow и hcAlarmRisingThresAbsValueHigh. Возможные значения: valueNotAvailable, valuePositive, или valueNegative. По умолчанию: valuePositive.
High Capacity Alarm Rising Event Index	Индекс объекта события eventEntry, используемого при пересечении верхнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 1.
High Capacity Alarm Falling Event Index	Индекс объекта события eventEntry, используемого при пересечении нижнего порога. Допустимые значения: от 1 до 65535. Значение по умолчанию: 2.
High Capacity Alarm Failed Attempts	Сколько раз переменная hcAlarmVariable был опрошена, но значение было недоступно. 32-разрядный счетчик, только для чтения.
High Capacity Alarm Owner	Строка имени владельца, связанная с записью оповещения. Значение по умолчанию: monitorHCAlarm.
High Capacity Alarm Storage Type	Тип энергонезависимой памяти, настроенной для этой записи. Объект только для чтения. Значение по умолчанию: volatile.

6.20 Управление приложением статистики

Приложение статистики дает возможность запрашивать статистику утилизации порта, статистику на основе потока или статистику приема пакетов в программируемых временных интервалах. Приложение статистики собирает данные в настраиваемом диапазоне времени. Можно определить номер (номера) порта или диапазон портов для сбора статистики. Настроенный диапазон времени применяется ко всем портам. Подробная статистика собирается в диапазон времени, указанный в формате даты и времени. Вы можете определить диапазон времени как абсолютное время начала и конца или как повторяющийся период. Например, можно указать, чтобы статистика была собрана и отображена между 9:00 12 НОЯ 2011 (START) и 21:00 12 НОЯ 2012 (END) или запланировать сбор на каждые Пн, Ср, Пт 9:00 (START) до 21:00 (END).

Получить статистику можно одним из способов:

• Запросить в CLI набор счетчиков.

• Настроить устройство для отправки статистики, используя протокол syslog или электронную почту. Сообщения протокола syslog или электронной почты отправляются приложением статистики

в момент окончания заданного периода времени (END).

Можно настроить устройство для отображения статистики в консоли. Собранная статистика выводится в консоли в момент окончания заданного периода времени (END).

stats group

Команда создает новую группу для определенного идентификатора или имени и настраивает временной диапазон и механизм отчетности для данной группы.

Формат: `stats group group id|name timerange time range name reporting list of reporting methods`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
group ID, name	Имя группы статистических данных или ее идентификатор для применения на интерфейсе. Возможные варианты: • received • received-errors • transmitted • transmitted-errors • received-transmitted • port-utilization • congestion Значение по умолчанию: отсутствует
time range name	Имя интервала для группы или правила на основе потока. Диапазон: от 1 до 31 буквенно-цифровых символов. Значение по умолчанию: отсутствует
list of reporting methods	Метод отправки сообщений статистики. Возможные значения: • none • console • syslog • e-mail Значение по умолчанию: отсутствует.

stats flow-based

Эта команда настраивает правило сбора статистики на основе потока с указанными параметрами и временным диапазоном. В качестве IP-адреса источника и IP-адреса назначения можно указывать только адрес IPv4.

Формат: `stats flow-based` *`rule-id`* `timerange` *`time range name`* `[{srcip` *`ip-address`*`} {dstip` *`ip- address`*`} {srcmac` *`mac-address`*`} {dstmac` *`mac-address`*`} {srctcpport` *`portid`*`} {dsttcpport` *`portid`*`} {srcudpport` *`portid`*`} {dstudpport` *`portid`*`}]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
rule ID	Идентификатор правила сбора статистики на основе потока. Допустимые значения: от 1 до 16. Значение по умолчанию: отсутствует

time range name	Название временного интервала для группы или правила сбора статистики на основе потока. Диапазон: от 1 до 31 буквенно-цифровых символов. Значение по умолчанию: отсутствует.
srcip ip-address	IP-адрес источника.
dstip ip-address	IP-адрес назначения.
srcmac mac- address	MAC-адрес источника.
dstmac mac- address	MAC-адрес назначения.
srctcpport portid	Номер TCP-порта источника.
dsttcpport portid	Номер TCP-порта назначения.
srcudpport portid	Номер UDP-порта источника.
dstudpport portid	Номер UDP-порта назначения.

no stats flow-based

Команда удаляет правило сбора статистики на основе потока.

Формат: `stats flow-based` *`rule-id`*

Режим ввода команд: глобальная конфигурация

stats flow-based reporting

Команда настраивает механизм создания отчетов для всех правил сбора статистики на основе потока в системе. Отдельных механизмов создания отчетов для каждого правила не предусмотрено. Если метод установлен как ***none***, все методы отчета сбрасываются.

Формат: `stats flow-based reporting` *`list of reporting methods`*

Режим ввода команд: глобальная конфигурация

stats group

Эта команда применяет указанную группу к интерфейсу или диапазону интерфейсов.

Формат: `stats group <group id | name>`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
group id	Уникальный идентификатор группы.
name	Имя группы.

no stats group

Эта команда удаляет указанную группу на интерфейс или диапазон интерфейсов.

Формат: `no stats group <group id | name>`

Режим ввода команд: конфигурирование интерфейса

stats flow-based

Эта команда применяет указанное правило сбора статистики на основе потока с заданным идентификатором к интерфейсу или диапазону интерфейсов.

Формат: `stats flow-based <rule-id>`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*

rule-id	Уникальный идентификатор правила сбора статистики на основе потока.

no stats flow-based

Команда удаляет правило сбора статистики на основе потока с интерфейса или диапазона интерфейсов.

show stats group

Команда отображает настроенный диапазон времени и список интерфейсов для определенной группы, а также выводит собранную статистику для этого списка интерфейсов по истечении заданного времени.

Формат: `show stats group <group id | name>`

Режим ввода команд: привилегированный

Параметр	*Описание*
group id	Уникальный идентификатор группы.
name	Имя группы.

show stats flow-based

Данная команда отображает настроенный диапазон времени, параметры правила сбора статистики на основе потока и список интерфейсов для него.

Формат: `show stats flow-based` *`rule-id`*`|all`

Режим ввода команд: привилегированный

Параметр	*Описание*
rule-id	Уникальный идентификатор правила сбора статистики на основе потока.

6.21 Команды для резервирования конфигурации

В данном разделе описаны команды, предназначенные для настройки резервирования конфигурации по таймеру или при сохранении текущей конфигурации на flash-накопителе.

backup url <url>

С помощью этой команды задаются протокол, адрес сервера, путь на сервере и префикс файла для записи конфигурации на удаленном сервере.

Значение по умолчанию: выключено

Формат: `backup url <tftp://<ipaddr>/<filepath>/<filename>>`

Режим ввода команды: режим глобальной конфигурации

no backup url <url>

Отключить запись конфигурации на удаленном сервере.

Формат: `backup url <tftp://<ipaddr>/<filepath>/<filename>>`

Режим ввода команды: режим глобальной конфигурации

backup time-period

С помощью этой команды задается промежуток времени, по истечении которого будет осуществляться автоматическое резервирование конфигурации.

Значение по умолчанию: 720 min

Формат: `backup time-period` *`period`*

Режим ввода команды: Режим глобальной конфигурации

backup auto

Данная команда включает автоматическое резервирование конфигурации.

Значение по умолчанию: отключено

Формат: `backup auto`

Режим ввода команды: режим глобальной конфигурации

backup write-memory

Данная команда включает резервирование конфигурации при сохранении пользователем конфигурации на flash-накопитель.

Значение по умолчанию: отключено

Формат: `backup write-memory`

Режим ввода команды: режим глобальной конфигурации

7 КОМАНДЫ РЕЖИМА СТЕКИРОВАНИЯ

В этой главе описываются команды стекирования, доступные в CLI.

Команды этого раздела делятся на 2 функциональные группы:

- **Команды просмотра оперативного состояния (команды show) отображают настройки коммутации, статистику и другую информацию.**
- **Команды конфигурации настраивают функции и параметры коммутатора. Каждой команде конфигурации соответствует команда show, которая показывает настройки конфигурации.**

Главный юнит (мастер, ведущий юнит) – юнит, управляющий стеком.

7.1 Стекирование

В данном разделе описаны команды настройки стекирования через выделенные интерфейсы.

Для предотвращения разрыва L3-сессий и перестроения сети во время выхода из строя действующего Master-а стека, Master присваивает свой системный MAC-адрес портам всех юнитов стека (в том числе OOB-порт). После разрыва стека данные MAC-адреса не изменяются. Для возвращения заводских MAC-адресов требуется перезагрузка коммутатора.

stack

Эта команда осуществляет переход в режим настройки стека (Stack Global Config).

Формат: `stack`

Режим ввода команд: режим глобальной конфигурации

member

Эта команда настраивает коммутатор. Параметр `unit` – идентификатор коммутатора, который требуется добавить/удалить из стека. Параметр `Switchindex` – индекс в базе данных поддерживаемых типов устройств, указывающий тип предварительно сконфигурированного коммутатора. Индекс коммутатора – 32-битное целое число. Эта команда выполняется на ведущем юните.

Формат `member` *`unit switchindex`*

Режим ввода команд режим глобальной конфигурации стека

Индекс коммутатора может быть получен путем выполнения команды *show supported switchtype*. Он равен 1 (*member unit_id 1*).

no member

Эта команда удаляет коммутатор из стека. Параметр `unit` – идентификатор коммутатора, который надо удалить из стека. Эта команда выполняется на ведущем юните.

Формат: `no member` *`unit`*

Режим ввода команд: режим глобальной конфигурации

switch priority

Эта команда настраивает способность коммутатора работать в качестве мастер-юнита. Параметр `unit` – идентификатор коммутатора. *`Value`* – параметр предпочтения, который позволяет пользователю задать приоритет резервного коммутатора. Диапазон значений: 0–15. Если активный мастер-юнит перестает работать, то взамен выбирается коммутатор с самым высоким приоритетом. Приоритетом по умолчанию является аппаратный приоритет устройства со значением 1. Коммутаторы, у которых нет аппаратной возможности стать ведущим юнитом, не могут получить право на управление.

Unit-ы с приоритетом 0 не могут стать мастером стека. При сборке стека из устройств с одинаковым приоритетом мастером станет unit с самым большим MAC-адресом.

Значение по умолчанию: 1

Формат: `switch` *`unit`* `priority` *`value`*

Режим ввода команд: режим глобальной конфигурации

switch renumber

Эта команда изменяет идентификатор коммутатора в стеке. `Oldunit` – текущий идентификатор коммутатора, значение которого необходимо изменить. `Newunit` – обновленное значение идентификатора коммутатора. После выполнения коммутатор будет настроен в соответствии с конфигурационной информацией для нового коммутатора, если таковая имеется. Старая информация о конфигурации коммутатора будет сохранена, однако старый коммутатор будет отключен. Эта команда выполняется на ведущем юните.

Если юнит управления перенумерован, то текущая конфигурация становится недействительной (т. е. стек работает как при обнуленной конфигурации).

Формат: `switch` *`oldunit`* `renumber` *`newunit`*

Режим ввода команд: режим глобальной конфигурации

movemanagement

Эта команда передает функции главного юнита от одного коммутатора к другому. *`Fromunit`* – идентификатор текущего мастера. *`Tounit`* – идентификатор нового мастера. После выполнения команды происходит перенастройка конфигурацией с нового мастера. После завершения рестарта все управление стеком должно происходить через новый мастер-юнит. Чтобы сохранить текущую конфигурацию при перенастройке конфигурации стека, выполните команду `copy system:running-config nvram:startup-config` (в привилегированном режиме) прежде, чем выполнить смену мастера. При смена мастера все L3-маршруты и записи в MAC-таблице удаляются. Эта команда выполняется на главном юните. Система предложит подтвердить выполнение данной команды.

Формат: movemanagement *fromunit tounit*

Режим ввода команд: режим глобальной конфигурации стека

standby

Используйте эту команду, чтобы сконфигурировать устройство как резервный юнит (Standby Management Unit, STBY).

Резервный юнит не может быть обычным устройством. Резервный юнит должен поддерживать возможность управления стеком.

Формат: standby *unit number*

Режим ввода команд: режим глобальной конфигурации стека

Параметр	*Описание*
Standby Management Unit Number	Указывает номер юнита, который должен стать резервным юнитом. Параметр **Unit number** должен содержать допустимое значение номера юнита.

no standby

Отрицательная форма этой команды позволяет приложению запускать алгоритм автоматического назначения резервного юнита.

Формат: no standby

Режим ввода команд: режим глобальной конфигурации стека

slot

Эта команда конфигурирует слот в системе. *Unit/slot* – идентификатор слота. *Cardindex* – индекс в базе данных поддерживаемых типов карты, указывающий тип карты, предварительно сконфигурированной в указанном слоте. Индекс карты – 32-битное целое число. Если карта в настоящее время находится в не сконфигурированном слоте, её конфигурация будет удалена, и слот будет переконфигурирован с информацией для карты по умолчанию.

Формат: slot *unit/slot cardindex*

Режим ввода команд: режим глобальной конфигурации

Индекс карты может быть получен путем выполнения команды *show supported cardtype*.

no slot

Команда удаляет конфигурацию из существующего в системе слота.

Формат: no slot *unit/slot cardindex*

Режим ввода команд: режим глобальной конфигурации

Индекс карты может быть получен путем выполнения команды *show supported cardtype*.

set slot disable

Эта команда конфигурирует административный режим слота (слотов). При указании [all], команда применяется ко всем слотам, иначе команда применяется только к слоту, идентифицированному с помощью *unit/slot*.

Если карта или другой модуль находятся в слоте, то административный режим будет применен ко всему содержимому слота. Если слот пуст, административный режим будет применен к любому вставленному в слот модулю. Если карта отключена, все порты на устройстве оперативно отключаются и отображаются на экране как “unplugged”.

Формат: `set slot disable [`*`unit/slot`*`] | all]`

Режим ввода команд: режим глобальной конфигурации

no set slot disable

Эта команда реконфигурирует административный режим слота (слотов). При указании [all], команда применяется ко всем слотам, иначе команда применяется к слоту, идентифицированному с помощью *unit/slot*.

Если карта или другой модуль находятся в слоте, то административный режим реконфигурирует содержание слота. Если слот пуст, административный режим удалит конфигурацию из любого модуля в слоте. Если карта отключена, все порты на устройстве отключаются и отображаются на экране как “unplugged”.

Формат: `no set slot disable [`*`unit/slot`*`] | all]`

Режим ввода команд: режим глобальной конфигурации

set slot power

Эта команда конфигурирует режим питания слота (слотов) и разрешает подачу энергии на расположенную в слоте карту. Если Вы укажете `all`, команда будет выполнена для всех слотов, если нет, она будет применена к слоту, указанному *unit/slot*.

Используйте эту команду при установке или удалении карт. Если карта или другой модуль находятся в слоте, режим питания применяется к содержанию слота. Если слот пуст, режим питания применится к любой карте, вставленной в слот.

Формат: `set slot power [`*`unit/slot`*`] | all]`

Режим ввода команд: режим глобальной конфигурации

no set slot power

Эта команда возвращает на исходные значения режим питания слота (слотов) и запрещает подачу энергии на расположенную в слоте карту. Если Вы укажете `all`, команда отключит подачу

энергии для всех слотов. Если нет, то подача энергии будет отключена только для слота, указанного в формате *unit/slot*.

Используйте эту команду при установке или удалении карт. Если карта или другой модуль находятся в слоте, отключение питания применится ко всему содержимому слота. Если слот пуст, отключение питания применится к любой карте, вставленной в слот.

Формат: `no set slot power [unit/slot] | all]`

Режим ввода команд: режим глобальной конфигурации

reload (Stack)

Эта команда перезагружает весь стек или конкретный юнит с номером *unit*. *Unit*-идентификатор коммутатора. Система запросит подтверждение на перезагрузку коммутатора.

Формат: `reload [unit]`

Режим ввода команд: привилегированный режим

stack-status sample-mode

Эта команда используется для конфигурирования объема выборки режима управления глобальным состоянием. Параметры объема выборки режима применяются глобально ко всем модулям в стеке. Объем выборки данной операции по умолчанию – накопительное суммирование.

Эта команда конфигурации реализована как часть функциональности обслуживаемости и, следовательно, не рассчитана на постоянное использование при рестартах. Эта конфигурация никогда не отображается в текущей конфигурации. Пользователь должен самостоятельно переключать демонстрационный режим. Эта конфигурация применима ко всем устройствам, которые включены в стек при запуске команды. Эта конфигурация не воспроизводится на картах, которые присоединяются к стеку после выполнения команды.

Значение по умолчанию: Cumulative Summing

Формат: `stack-status sample-mode {cumulative | history} [max-samples 100 - 500]`

Режим ввода команд: Режим глобальной конфигурации стека

Ключевые слова	*Описание*
sample-mode	Режим выборки
cumulative	Отслеживает сумму накопления полученных смещений временной метки.
history	Отслеживает историю полученных смещений временной метки
max-samples	Максимальное количество выборок для сохранения

show slot

Эта команда отображает информацию по всем слотам, либо по отдельному слоту в системе.

Формат: `show slot [unit/slot]`

Режим ввода команд: пользовательский режим

привилегированный режим

Параметр	*Описание*
Slot	Идентификатор слота в формате *unit/slot*.
Slot Status	Слот пуст, занят или обнаружена ошибка
Admin State	Административный режим слота включен/выключен.
Power State	Режим питания слота включен /выключен.
Configured Card Model Identifier	Идентификатор модели карты предварительно сконфигурированной в слоте. Идентификатор модели – строка длиной в 32 символа, используемая для идентификации карты.
Pluggable	Карты в слоте подключаемые или нет.
Power Down	Указывает, может ли слот быть выключен.

Если вы укажете значение для *unit/slot*, появится следующая дополнительная информация:

Параметр	*Описание*
Inserted Card Model Identifier	Идентификатор модели карты, вставленной в слот. Идентификатор модели - строка длиной в 32 символа, используемая для идентификации карты. Поле выводится на экран, только если слот заполнен.
Inserted Card Description	Описание карты. Поле выводится на экран, только если слот заполнен.
Configured Card Description	Полудуплекс 10BASE-T

show stack-status

Используйте эту команду, чтобы вывести на экран таймеры полученных HB-сообщений и статистику сбросов/потерь для указанного юнита стека.

Формат: `show stack stack-status [1-n | all] [clear]`

Режим ввода команд: Привилегированный режим

Ключевые слова	*Описание*
Current	Текущее время приема сообщения heartbeat
Average	Среднее время приема сообщения heartbeat
Min	Минимальное время приема сообщения heartbeat
Max	Максимальное время приема сообщения heartbeat
Dropped	Счетчик удаления/потерь сообщений heartbeat

show supported cardtype

Эта команда выводит на экран информацию обо всех типах карт или определенных типах карт, поддерживаемых в системе.

Формат: `show supported cardtype [cardindex]`

Режим ввода команд: пользовательский режим

привилегированный режим

Если не указано значение для *cardindex*, то будет выведена следующая информация:

Параметр	*Описание*
Card Index (CID)	Индекс в базе данных поддерживаемых типов карт. Этот индекс используется при предварительном конфигурировании слота.
Card Model Identifier	Идентификатор модели для поддерживаемого типа карты.

Если Вы указываете значение для *cardindex*, будет выведена следующая информация:

Параметр	*Описание*
Card Type	32-разрядный числовой тип карты.
Model Identifier	Идентификатор модели для поддерживаемого типа карты.
Card Description	Описание для поддерживаемого типа карты.

show switch

Эта команда выводит информацию о состоянии всех юнитов в стеке или для одного заданного юнита.

Формат: `show switch [unit]`

Режим ввода команд: Привилегированный режим

Параметр	*Описание*
Switch	Идентификатор юнита, присвоенный данному коммутатору.

Если вы не указываете значение для *unit*, выводится следующая информация:

Параметр	*Описание*
Management Status	Указывает, является ли коммутатор главным юнитом, подчиненным, сконфигурированным резервным юнитом, оперативным резервным юнитом или состояние не определено.
Preconfigured Model Identifier	Идентификатор модели предварительно сконфигурированного коммутатора, готового присоединиться к стеку. Идентификатор модели – строка длиной 32 символа, присвоенная устройству производителем для идентификации.
Plugged-In Model Identifier	Идентификатор модели коммутатора в стеке. Идентификатор модели – строка длиной 32 символа, присвоенная устройству производителем для идентификации.
Switch Status	Состояние коммутатора. Возможные значения для этого состояния: **OK, Unsupported, Code Mismatch, SDM Mismatch, Config Mismatch,** или **Not Present**. Несоответствие (**Mismatch**) указывает, что на юните стека версия ПО, шаблон SDM или конфигурация отличаются от той/того, что на главном юните. **SDM Mismatch** указывает, что юнит присоединился к стеку, но на нем выполняется другой шаблон SDM, нежели на главном юните. Это состояние временное; юнит стека должен автоматически перезапуститься, используя шаблон SDM, выполняющийся на мастер-юните. Если в данный момент выполняется процедура синхронизации ПО в стеке (SFS), то состояние отображается как **Updating Code**.
Code Version	Версия ПО на данном коммутаторе.

При указании значения для *unit* появляется следующая информация.

Параметр	*Описание*
Management Status	Указывает, является ли коммутатор главным юнитом, подчиненным или состояние не присвоено.
Hardware Management Preference	Аппаратный приоритет устройства в стеке. Может быть отключено или не присвоено.
Admin Management Preference	Настраиваемый приоритет устройства в стеке. Указывает, с какой вероятностью коммутатор будет выбран в качестве главного юнита.
Switch Type	32-разрядный числовой тип коммутатора.
Model Identifier	Идентификатор модели для этого коммутатора. Идентификатор модели – поле с 32 символами, присвоенное устройству производителем для идентификации.
Switch Status	Состояние коммутатора. Возможные значения: OK, Unsupported, Code Mismatch, SDM Mismatch, Config Mismatch, или Not Present.
Switch Description	Описание коммутатора.
Expected Code Type	Ожидаемый тип ПО.
Expected Code Version	Ожидаемая версия ПО.
Detected Code Version	Текущая версия ПО на этом коммутаторе. Если юнита нет в системе и его предварительная конфигурация отсутствует, то версия кода отображается как “None”.
Detected Code in Flash	Версия ПО, которое в настоящее время хранится во flash-памяти коммутатора. Этот код выполняется после сброса коммутатора. Если юнита нет в системе и его предварительная конфигурация отсутствует, то версия отображается как “None”.
SFS Last Attempt Status	Состояние синхронизации ПО с момента последнего подключения юнита к стеку.
Serial Number	Порядковый номер для заданного юнита.
Up Time	Время работы системы.

show supported switchtype

Эта команда выводит информацию обо всех поддерживаемых типах коммутатора или определенном типе коммутатора.

Формат: `show supported switchtype [switchindex]`

Режим ввода команд: пользовательский режим

привилегированный режим

При указании значения для *switchindex* появляются следующие данные:

Параметр	*Описание*
Switch Index (SID)	Индекс в базе данных поддерживаемых типов коммутатора. Этот индекс используется при предварительном конфигурировании элемента для добавления в стек.
Model Identifier	Идентификатор модели для поддерживаемого типа коммутатора.
Management Preference	Значение предпочтения управления стеком для данного типа коммутатора.
Code Version	Идентификатор приемника загрузки кода данного типа коммутатора.

При указании значения для *switchindex* появляются следующие данные:

Параметр	*Описание*
Switch Type	32-разрядный числовой тип для поддерживаемого коммутатора.
Model Identifier	Идентификатор модели для поддерживаемого типа коммутатора.
Switch Description	Описание для поддерживаемого типа коммутатора

7.2 Команды настройки стек-портов

В этом разделе описаны команды просмотра и конфигурирования информации о стек-порте.

Стекирование осуществляется на максимальной скорости работы порта 40G.

stack-port

Эта команда переводит заданный порт/группу портов в стековый (*stack*) либо стандартный (*ethernet*) режим.

Значение по умолчанию: stack

Формат: `stack-port` *`unit/slot/port`* `[{ethernet | stack}]`

Режим ввода команд: режим глобальной конфигурации стека

show stack-port

Эта команда выводит на экран полную информацию о стек-порте для всех интерфейсов.

Формат: `show stack-port`

Режим ввода информации: привилегированный режим

Для каждого интерфейса:

Параметр	*Описание*
Unit	Номер юнита.
Interface	Номера слота и порта.
Configured Stack Mode	Сконфигурированный режим работы порта (стековый или стандартный).
Running Stack Mode	Текущий режим работы порта (стековый или стандартный).
Link Status	Состояние соединения.
Link Speed	Скорость (Гбит/с) соединения стек порта.

show stack-port counters

Эта команда выводит на экран полную информацию счетчика данных для всех интерфейсов.

Формат: `show stack-port counters [`*`1-n`*` | all]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Unit	Номер юнита.

Interface	Номера слота и порта.
Tx Data Rate	Скорость передачи данных (мегабит в секунду).
Tx Error Rate	Количество ошибок передачи в секунду (зависит от аппаратной платформы).
Tx Total Errors	Количество ошибок передачи (зависит от аппаратной платформы).
Rx Data Rate	Скорость приема данных (мегабит в секунду).
Rx Error Rate	Количество ошибок приёма в секунду (зависит от аппаратной платформы).
Rx Total Errors	Количество ошибок передачи (зависит от аппаратной платформы).
Link Flaps	Количество поднятий/падений для данного соединения с момента загрузки системы.

show stack-port diag

Команда отображает диагностику каждого стек порта и предназначена только для инженеров технической поддержки (FAE) и разработчиков. Инженер проконсультирует вас по вопросам необходимости выполнения этой команды и интерпретации отображаемой информации. В подробном режиме отображаются: статистика и счетчики для RPC, транспорта, CPU и модулей RX/TX.

Формат: `show stack-port diag [`*1-n* `|` `all] [verbose]`

Режим ввода команд: Привилегированный режим

Параметр	*Описание*
Unit	Номер юнита.
Interface	Номера слота и порта.
Diagnostic Entry1	Строка из 80 символов, используемая для диагностики.
Diagnostic Entry2	Строка из 80 символов, используемая для диагностики.
Diagnostic Entry3	Строка из 80 символов, используемая для диагностики.
TBYT	Переданные байты.
TPKT	Переданные пакеты.
TFCS	Счетчик переданных пакетов с ошибкой FCS.
TERR	Счетчик ошибок передачи данных (установленный системой).
RBYT	Принятые байты.
RPKT	Принятые пакеты.
RFCS	Счетчик принятых пакетов с ошибкой FCS (FCS Error Frame).
RFRG	Счетчик принятых фрагментов данных (Fragment).
RJBR	Счетчик принятых пакетов Jabber.
RUND	Счетчик принятых уменьшенных пакетов (Undersize).
ROVR	Счетчик принятых увеличенных пакетов (Oversized).
RUNT	Счетчик принятых RUNT-пакетов.

show stack-port stack-path

Показать маршрут, по которому пакет будет доставлен до адреса назначения.

Формат: `show stack-port stack-path {1-8 | all}`

Режим ввода команд: привилегированный режим

7.3 Команды синхронизации ПО в стеке

Команды синхронизации ПО в стеке (Stack Firmware Synchronization, SFS) позволяют автоматически синхронизировать ПО всех юнитов стека. Если присоединяющийся к стеку юнит имеет ПО иной версии, чем главный юнит, SFS обновляет или откатывает версию его ПО. Стек синхронизируется по главному юниту, а не по самой свежей версии в стеке.

boot auto-copy-sw

Используйте эту команду, чтобы включить опцию SFS в данном стеке.

Значение по умолчанию: отключено

Формат: `boot auto-copy-sw`

Режим ввода команды: привилегированный режим

no boot auto-copy-sw

Отключить опцию SFS в данном стеке**.**

Формат: `no boot auto-copy-sw`

Режим ввода команд: привилегированный режим

boot auto-copy-sw trap

Включить отправку SNMP-трапов при включенной опции SFS.

Значение по умолчанию: включено

Формат: `boot auto-copy-sw trap`

Режим ввода команд: привилегированный режим

no boot auto-copy-sw trap

Выключить отправку SNMP-трапов при включенной опции SFS.

Формат: `no boot auto-copy-sw trap`

Режим ввода команд: привилегированный режим

boot auto-copy-sw allow-downgrade

Разрешить главному юниту стека откатывать версию ПО другого юнита в данном стеке до версии, установленной на главном юните, если версия ПО главного юнита является более старой.

Формат: `boot auto-copy-sw allow-downgrade`

Режим ввода команд: привилегированный режим

no boot auto-copy-sw allow-downgrade

Запретить ведущему юниту стека откатывать версию ПО другого юнита.

Формат: `no boot auto-copy-sw allow-downgrade`

Режим ввода команд: привилегированный режим

show auto-copy-sw

Вывести информацию о конфигурации SFS.

Формат: `show auto-copy-sw`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Synchronization	Показывает, включена ли опция SFS.
SNMP Trap Status	Будет ли стек отправлять SNMP-трапы при включенной опции SFS.
Allow Downgrade	Разрешено ли главному юниту стека откатывать аппаратное ПО других членов стека.

Команды безостановочной обработки трафика (NSF)

Коммутатор может быть представлен тремя связанными уровнями: уровень пересылки, уровень контроля и уровень управления. На уровне пересылки происходит обработка и пересылка пакетов данных. Эта задача реализуется аппаратными средствами. Уровень контроля – это набор протоколов, определяющих, каким образом происходит пересылка пакетов, какие пакеты и куда разрешено отправлять. ПО на главном юните выполняет роль уровня контроля. Уровень управления – это ПО, работающее на главном юните и предоставляющее системному администратору средства для настройки и мониторинга состояния устройства.

Безостановочная пересылка (Nonstop Forwarding, NSF) позволяет уровню пересылки всех юнитов стека поддерживать передачу данных даже при сбоях на уровнях контроля и управления из-за отключения питания, отказа аппаратного или программного обеспечения юнита. Аварийное переключение при безостановочной пересылке также может быть настроено вручную с помощью команды *initiate failover*. Входящие и исходящие потоки трафика, передаваемые через физические порты подчинённых юнитов, будут восстановлены менее чем через секунду после сбоя на главном юните.

Для подготовки резервного юнита для обхода отказа, приложения на основном юните регулярно создают контрольные точки, сохраняя определенную информацию о состоянии основного юнита на резервный юнит. Изменения в конфигурации автоматически копируются на резервный юнит. При срабатывании механизма обхода отказа MAC-таблица не очищается, поэтому нет необходимости заново изучать их.

Когда срабатывает функция обхода отказа при NSF, уровень контроля на резервном юните начинает работу из частично инициализированного состояния и восстанавливает состояние, сохраненное в контрольных точках. В то время как происходит инициализация уровня контроля, стек не реагирует на внешние изменения, в том числе изменения топологии сети. Как только уровень контроля полностью вступает в работу на резервном юните, он выполняет проверку того, что состояние всех аппаратных таблиц обновилось как нужно. Время полного восстановления

функционала уровня контроля зависит от размера стека, сложности конфигурации и скорости центрального процессора.

При обходе отказа происходит перезапуск уровня управления. Сессии управления необходимо установить заново.

Для эффективной работы NSF смежные сетевые устройства не должны перенаправлять трафик в обход перезагружающегося устройства. ПО использует три алгоритма решения проблемы переадресации трафика:

1. Протокол может распределить часть своей работы по другим устройствам стека, таким образом, протокол будет действовать и во время перезапуска. Этот алгоритм используется протоколом STP и при агрегировании каналов.
2. Протокол может использовать соседние устройства посредством алгоритма мягкого перезапуска (сервис Graceful Restart). Протокол OSPF использует сервис Graceful Restart, если эта опция включена.
3. Протокол может просто запуститься заново после обхода отказа, если соседние устройства реагируют слишком медленно и есть вероятность, что они не зафиксируют сбой. В качестве примера можно привести IP-протоколы многоадресной маршрутизации.

Для наибольшей эффективности NSF соединения с соседями 2 уровня следует устанавливать через группы портов LAG, охватывающие два или более устройства стека, а соединения 3 уровня – через маршруты ECMP с близлежащими маршрутизаторами, подключенными через физические порты двух или более юнитов в стеке. В таком случае аппаратное обеспечение сможет быстро перенаправить потоки трафика с членов групп портов или маршрутов ECMP отказавшего юнита на другой работающий юнит.

nsf (Stack Global Config Mode)

Включить опцию безостановочной пересылки в данном стеке. Когда опция включена, при отказе главного юнита стека резервный юнит берет управление на себя, не очищая при этом таблицу аппаратных средств действующих юнитов. Трафик данных продолжает идти через аппаратное обеспечение, в это же время происходит инициализация функций управления на резервном юните.

Опция NSF включена по умолчанию на платформах, поддерживающих ее. Опция может быть выключена администратором для высвобождения ресурсов CPU, задействованных на создание контрольных точек.

Если к стеку подключен юнит, не поддерживающий NSF, то NSF выключается на всех юнитах стека. Когда юнит, не поддерживающий NSF, отсоединяется от стека, а все оставшиеся в стеке юниты поддерживают NSF, то NSF включается администратором и продолжает действовать.

Значение по умолчанию: включено

Формат: `nsf`

Режим ввода команд: режим глобальной конфигурации стека

no nsf

Выключить опцию NSF в данном стеке.

Формат: `no nsf`

Режим ввода команд: режим глобальной конфигурации стека

show nsf

Вывести информацию по глобальной конфигурации NSF и конфигурации NSF на каждом юните данного стека.

Формат: `show nsf`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
NSF Administrative Status	Включена или отключена администратором опция NSF. По умолчанию: enable
NSF Operational Status	Включена ли опция NSF для данного стека.
Last Startup Reason	Каким образом программное обеспечение было запущено в последний раз: • “Power-On” означает, что коммутатор был перезапущен. Это могло быть вызвано перезагрузкой по питанию или командой перезапуска (“Reload”), данной администратором системы. • “Administrative Move” означает, что администратор дал команду movemanagement для передачи управления на резервное устройство. • “Warm-Auto-Restart” означает, что первичная карта управления была перезапущена вследствие произошедшего сбоя и система выполнила обход отказа. • “Cold-Auto-Restart” означает, что система переключалась с главного юнита на резервный и не была способна поддерживать трафик пользователей. Как правило, это вызвано множественными сбоями, происходящими в непосредственной близости друг от друга
Time Since Last Restart	Время, прошедшее с тех пор, как текущий главный юнит принял на себя управление стеком.
Restart in progress	Выполняется ли перезапуск в текущий момент.
Warm Restart Ready	Готовность системы осуществить при отказе главного юнита передачу управления на резервный юнит.
Copy of Running Configuration to Backup Unit: Status	Включает ли конфигурация резервного юнита все изменения, внесенные в конфигурацию на главном юните. Может отображаться как «Текущая» (Current) или «Устаревшая» (Stale).
Time Since Last Copy	Когда в последний раз осуществлялось копирование текущей конфигурации главного юнита на резервный юнит.
Time Until Next Copy	Количество секунд до того, как текущая конфигурация будет скопирована на резервный юнит. Эта строка появляется лишь в том случае, если конфигурация резервного юнита распознана как «Устаревшая».
Параметры статуса отдельных юнитов стека	
NSF Support	Поддерживает ли юнит опцию NSF.

initiate failover

Вручную передать управление на резервный юнит и выполнить «горячий» перезапуск стека. При «горячем» перезапуске резервный юнит берет на себя функции главного юнита без очистки

аппаратных таблиц (при «холодном» перезапуске происходит очистка таблиц). Приложения восстанавливают свое состояние по сохраненным в контрольной точке на нынешнем главном юните. Бывший главный юнит перезагружается.

Если система не готова осуществить «горячий» перезапуск, к примеру, не был назначен резервный юнит либо одно или несколько юнитов стека не поддерживают NSF, команда не будет выполнена и будет выведено сообщение с предупреждением.

Команда movemanagement также передает управление с текущего главного юнита; однако, содержимое аппаратных таблиц при этом очищается, и все юниты проходят инициализацию заново.

Формат: `initiate failover`

Режим ввода команд: режим глобальной конфигурации стека

show checkpoint statistics

Показать общую информацию о действиях сервиса создания и управления контрольными точками.

Формат: `show checkpoint statistics`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Messages Check-pointed	Количество сообщений о контрольных точках, переданных на резервный юнит. Диапазон значений: целые числа. Значение по умолчанию: 0.
Bytes Checkpointed	Количество байтов, переданных на резервный юнит. Диапазон значений: целые числа. Значение по умолчанию: 0.
Time Since Counters Cleared	Количество дней, часов, минут и секунд, прошедших с момента сброса счетчиков на ноль. Счетчики обнуляются либо когда юнит принимает на себя управление стеком, либо отдельной командой. Значение по умолчанию: 0d00:00:00.
Checkpoint Message Rate	Среднее количество сообщений контрольных точек в секунду. Средний показатель подсчитывается за период с момента последнего обнуления счетчиков. Диапазон значений: целые числа. Значение по умолчанию: 0.
Last 10-second Message Rate	Среднее количество сообщений контрольных точек в секунду за последние 10 секунд. Средний показатель обновляется каждые 10 секунд. Диапазон значений: целые числа. Значение по умолчанию: 0.
Highest 10-second Message Rate	Наивысший зарегистрированный показатель за 10-секундный интервал с момента последнего обнуления счетчиков. Диапазон значений: целые числа. Значение по умолчанию: 0.

clear checkpoint statistics

Обнулить статистику контрольных точек и вернуться к исходным значениям.

Формат: `clear checkpoint statistics`

Режим ввода команд: привилегированный режим

7.4 Команды смешанного стекирования

Смешанное стекирование позволяет разнородным стекам формировать однородную систему количественных и качественных характеристик посредством использования шаблонов. Каждый шаблон определяет характеристики юнита в стеке. Эти характеристики включают в себя ёмкость различных таблиц, поддерживаемых в чипе (к примеру, размер L2-таблиц), а также набор функций и возможностей, предоставляемых этим чипом. Существует по одному шаблону для каждого из типов устройства, поддержанных в смешанном стеке. Существуют также дополнительные шаблоны, обеспечивающие размеры таблиц и набор возможностей по принципу «наименьшего общего знаменателя» (*least common denominator*), позволяя устройствам различных типов объединяться в единый стек.

При соединении устройств больших возможностей с устройствами меньших возможностей шаблоны обеспечивают функционирование всего стека в соответствии с возможностями наиболее «слабого» устройства. В некоторых случаях у одного устройства в стеке может быть какая-либо таблица большего размера, нежели у другого, но при этом оно обладает меньшим набором функций, нежели устройство с меньшим размером таблицы. В таком случае шаблоны обеспечивают функционирование стека как единого целого в режиме соответствия «наименьшему общему знаменателю» (*least common denominator*).

stack-template

Данная команда устанавливает идентификатор шаблона стека на отдельный юнит стека (если задан) или применительно ко всему стеку. Пользователь получает запрос на подтверждение того, что конфигурация запуска на задействованных юнитах будет обнулена и что обновляемое устройство (устройства) будет перезагружено.

Значение по умолчанию: задано платформой

Формат: `stack-template` *`templateId`* `[unit]`

Режим ввода команд: стековый режим

no stack-template

Эта команда возвращает идентификатор шаблона стека на заданном юните на значение по умолчанию (для данной платформы). Пользователю предлагается подтвердить действие, т.к. загрузочная конфигурация будет удалена, а изменяемый юнит – перезапущен.

Значение по умолчанию: задано платформой

Формат: `no stack-template` *`unit`*

Режим ввода команд: стековый режим

show stack-template list

Показать список идентификаторов шаблонов. Команда также использует опциональный параметр *switchindex*, соответствующий поддерживаемым моделям коммутаторов. Если задан индекс коммутатора, команда покажет шаблоны, которые могут быть сконфигурированы с данным типом коммутатора. Внимание: некоторые шаблоны не могут быть сконфигурированы с некоторыми типами коммутаторов.

Формат: `show stack-template list`

Режим ввода команд: привилегированный режим

show stack-template switch

Показать идентификаторы шаблонов, настроенных на каждом коммутаторе в стеке. Идентификатор шаблона юнита с предварительно заданной конфигурацией или юнита с несовпадением версии ПО будет представлен как «*unknown*».

Формат: `show stack-template switch`

Режим: привилегированный EXEC

7.5 Команды настройки протокола NETCONF

В данном разделе описаны команды конфигурации протокола NETCONF для доступа к коммутатору. Протокол NETCONF обеспечивает возможность добавлять, блокировать (для клиентов NETCONF) и удалять конфигурацию коммутатора посредством удаленного вызова процедур RPC.

NETCONF по умолчанию использует порт 830.

ip netconf server enable

Данная команда включает NETCONF-сервер.

Значение по умолчанию: отключено

Формат: `ip netconf server enable`

Режим ввода команд: привилегированный режим

no ip netconf server enable

Данная команда выключает NETCONF-сервер.

Формат: `no ip netconf server enable`

Режим ввода команд: привилегированный режим

8 КОМАНДЫ УПРАВЛЕНИЯ

В данном разделе описаны команды настройки управления, доступные в командном интерфейсе.

На коммутаторах IP-адрес по умолчанию отсутствует. DHCP Client на сервисном OOB-порту по умолчанию включен.

Все команды, приведенные в этом разделе, делятся на три функциональные группы:

- **Команды show выводят информацию о настройках коммутатора, статистику и прочую информацию.**
- **Команды конфигурации настраивают функции коммутатора. Каждой команде конфигурации соответствует команда show, выводящая на дисплей настройки.**
- **Команды очистки (clear) откатывают некоторые или все настройки до заводского состояния.**

8.1 Команды настройки интерфейса удалённого управления

В этом разделе описаны команды настройки логического интерфейса для доступа к устройству с целью управления им.

enable (доступ в привилегированный режим)

Данная команда открывает доступ к привилегированному режиму. Привилегированный режим позволяет конфигурировать интерфейс удалённого управления.

Формат: `enable`

Режим ввода команд: пользовательский режим

do (выполнить команду в привилегированном режиме)

Эта команда позволяет выполнить команду привилегированного режима из любого режима конфигурации.

Формат: `do` *`Priv Exec Mode Command`*

Режим ввода команд: Режим глобальной конфигурации
Режим конфигурирования интерфейса
Режим конфигурации VLAN
Режим конфигурации маршрутизации

serviceport ip

Команда устанавливает IP-адрес, маску сети и шлюз для сервисного порта. Параметр none позволяет сбросить адрес сети IPv4, маску и шлюз по умолчанию (при сбросе все эти значения устанавливаются на 0.0.0.0).

Формат: `serviceport ip {ipaddr netmask [gateway] | none}`

Режим ввода команд: привилегированный режим

serviceport protocol

Эта команда задает протокол конфигурации сервисного порта. Изменение этого параметра вступает в силу незамедлительно. При использовании параметра *bootp* коммутатор будет регулярно отправлять запросы на BootP-сервер до получения ответа. При использовании параметра *dhcp* коммутатор будет регулярно отправлять запросы на DHCP-сервер до получения ответа. При использовании параметра none необходимо сконфигурировать сетевой адрес коммутатора вручную.

Формат: `serviceport protocol {none | bootp | dhcp}`

Режим ввода команд: привилегированный режим

serviceport protocol dhcp

Включить DHCPv4-клиент на сервисном порте. Если задан параметр *client-id*, сообщения DHCP-клиента отправляются с опцией client-id (61)идентификатора клиента.

Значение по умолчанию: не задано

Формат: `serviceport protocol dhcp [client-id]`

Режим ввода команд: привилегированный режим

Использование отрицательной формы команды *serviceport protocol dhcp client-id* не поддерживается. Чтобы выключить добавление опции client-id к сообщениям клиента DHCP, необходимо ввести команду serviceport protocol dhcp без параметра client-id. Команда интерфейса serviceport protocol none используется для одновременного отключения клиента DHCP идобавления опции client-id.

network parms

Команда устанавливает IP-адрес, маску подсети и шлюз для mgmt_vlan. Опция none сбрасывает IP-адрес, маску подсети и шлюз до значений заводской конфигурации.

Формат: `network parms {ipaddr netmask [gateway]| none}`

Режим ввода команд: привилегированный режим

network mgmt_vlan

Команда настраивает идентификатор управляющей VLAN. По умолчанию управляющим является VLAN 1, он назначен на всех физических интерфейсах (кроме OOB). Если идентификатор управляющей VLAN был изменен, то данный VLAN необходимо назначить на используемые физические интерфейсы.

Значение по умолчанию: 1

Формат: `network mgmt_vlan` *1-4093*

Режим ввода команд: привилегированный

no network mgmt_vlan

Данная команда устанавливает идентификатор управляющей VLAN в значение по умолчанию.

Формат: `no network mgmt_vlan`

Режим ввода команд: привилегированный

network protocol

Задать протокол сетевой конфигурации. Изменение этого параметра вступает в силу незамедлительно. При использовании параметра *bootp* коммутатор будет регулярно отправлять запросы на BootP-сервер до получения ответа. При использовании параметра *dhcp* коммутатор будет регулярно отправлять запросы на DHCP-сервер до получения ответа. При использовании параметра *none* необходимо конфигурировать сетевую информацию коммутатора вручную.

Значение по умолчанию: none

Формат: `network protocol {none | bootp | dhcp}`

Режим ввода команд: привилегированный режим

network protocol dhcp

Данная команда включает DHCPv4-клиент на сервисному порту. Если задан параметр `client-id`, сообщения DHCP-клиента отправляются с опцией client-id (61)идентификатора клиента

Значение по умолчанию: none

Формат: `network protocol dhcp [client-id]`

Режим ввода команд: режим глобальной конфигурации

Использование no-формы команды **network protocol dhcp client-id** не поддерживается. Чтобы отключить добавление опции client-id к сообщениям клиента DHCP, необходимо ввести команду **network protocol dhcp** без параметра client-id. Команда интерфейса **network protocol none** используется для одновременного отключения клиента DHCP и добавления опции client-id.

network mac-address

Команда задает локально администрируемые MAC-адреса. Действуют следующие правила:

- Бит 6 байта 0 (так называемый «бит U/L» - Универсальный/Локальный) указывает, является ли адрес администрируемым универсально (b'0') или локально (b'1').
- Бит 7 байта 0 (так называемый «бит I/G» - Индивидуальный/Групповой) указывает, является ли адрес назначения индивидуальным (b'0') или групповым (b'1').
- Второй символ двенадцатизначного MAC-адреса должен быть: 2, 6, A или E.

В локально администрируемом адресе бит 6 должен иметь значение 1 (b'1') , а бит 7 – 0 (b'0').

Формат: `network mac-address` *`macaddr`*

Режим ввода команд: привилегированный режим

network mac-type

Задать использование коммутатором заводского либо локально администрируемого MAC-адреса.

Значение по умолчанию: заводской

Формат: `network mac-type {local | burnedin}`

Режим ввода команд: привилегированный режим

no network mac-type

Установить значение MAC-адреса на заданное по умолчанию.

Формат: `no network mac-type`

Режим ввода команд: привилегированный режим

network javamode

Задать коммутатору режим доступа к Java-апплету в верхней части web-интерфейса. Если доступ разрешен, пользователь может просматривать Java-апплет через web-интерфейс. Когда доступ запрещен, пользователь не может просматривать Java-апплет.

Значение по умолчанию: включено

Формат: `network javamode`

Режим ввода команд: привилегированный режим

no network javamode

Запретить доступ к Java-апплету в верхней части web-интерфейса. Когда доступ запрещен, пользователь не может просматривать Java-апплет.

Формат: `no network javamode`

Режим ввода команд: привилегированный режим

show network

Показать настройки конфигурации сетевого интерфейса коммутатора. Сетевой интерфейс – логический интерфейс, используемый для поддерживания связности с коммутатором через любой порт лицевой панели коммутатора. Параметры конфигурации сетевого интерфейса коммутатора не влияют на конфигурацию портов лицевой панели, через которые происходит коммутация или маршрутизация трафика. Сетевой интерфейс всегда активен вне зависимости от того, активны ли порты устройства. Таким образом, команда *show network* всегда будет показывать значение графы **Interface Status (Состояние интерфейса)** как **Up** (**Активно)**.

Формат: `show network`

Режимы ввода команды: привилегированный режим

пользовательский режим

Параметр	*Описание*
Interface Status	Состояние сетевого интерфейса.
IP Address	IP-адрес интерфейса. Значение, заданное заводской конфигурацией: 0.0.0.0.
Subnet Mask	IP-маска подсети интерфейса. Значение, заданное заводской конфигурацией: 0.0.0.0.
Default Gateway	Шлюз по умолчанию для интерфейса данного IP. Значение по умолчанию: 0.0.0.0.
IPv6 Administrative Mode	Включен или выключен.
IPv6 Address/Length	IPv6-адрес и длина маски.
IPv6 Default Router	IPv6 -адрес маршрутизатора по умолчанию.
Burned In MAC Address	Заводской MAC-адрес.
Locally Administered MAC Address	По желанию пользователя локально администрируемый MAC-адрес может быть сконфигурирован для поддержания связности сети. Для этого в графе «Тип MAC-адреса» должно быть выбрано значение «Локально администрируемый». Адрес вводится как 12 шестнадцатеричных чисел (6 байт) с двоеточием между байтами. Бит 1 байта 0 должен быть 1, а бит 0 байта 0 – 0, то есть байт 0 должен иметь маску следующего вида: 'xxxx xx10'. MAC-адрес, используемый этим сетевым мостом (bridge), должен быть уникальным. Рекомендуется использовать численно наименьший MAC-адрес на всех портах этого моста, но обязательным требованием это не является. При соединении с dot1dStpPriority мосту присваивается уникальный идентификатор (Bridge Identifier), который используется протоколом STP (Spanning Tree Protocol).
MAC Address Type	MAC-адрес, используемый для поддержаний внутренней связности сети. Может быть заводским или локально администрируемым. При заводской конфигурации используется заводской MAC-адрес.
Configured IPv4 Protocol	Используемый сетевой протокол IPv4. Возможные значения: bootp | dhcp | none (не используется).
Configured IPv6 Protocol	Используемый сетевой протокол IPv6. Возможные значения: dhcp | none (не используется).
DHCPv6 Client DUID	Уникальный идентификатор (DHCP Unique Identifier) клиента DHCPv6. Эта графа выводится на дисплей, если в качестве сконфигурированного протокола IPv6 выбран dhcp.
IPv6 Autoconfig Mode	Включена или выключена для сети IPv6 stateless автоконфигурация адреса.
DHCP Client Identifier	Идентификатор клиента выводится на дисплей, только если на сетевой порт открыт доступ протоколу DHCP с включенным параметром **client-id**. См. network protocol dhcp.

show serviceport

Показать конфигурацию сервисного порта.

Формат: `show serviceport`

Режим ввода команд: привилегированный режим

пользовательский режим

Параметр	*Описание*
Interface Status	Состояние сетевого интерфейса. Всегда отображается как Up «Активно».
IP Address	IP-адрес интерфейса. Значение, заданное заводской конфигурацией: 0.0.0.0.
Subnet Mask	IP-маска подсети интерфейса. Значение, заданное заводской конфигурацией: 0.0.0.0.
Default Gateway	Шлюз по умолчанию для интерфейса данного IP. Значение, заданное заводской конфигурацией: 0.0.0.0.
IPv6 Administrative Mode	Включен или выключен. По умолчанию: Enabled (включен).
IPv6 Address/Length	Адрес и длина маски IPv6. По умолчанию: Местная сеть (Link Local).
IPv6 Default Router	Адрес маршрутизатора IPv6 по умолчанию. По умолчанию: Не задан.
Configured IPv4 Protocol	Используемый сетевой протокол IPv4. Возможные значения: bootp | dhcp | none (не используется).
Configured IPv6 Protocol	Используемый сетевой протокол IPv6. Возможные значения: dhcp | none (не используется).
DHCPv6 Client DUID	Уникальный идентификатор (DHCP Unique Identifier) клиента DHCPv6. Эта графа выводится на дисплей, если в качестве сконфигурированного протокола IPv6 выбран dhcp.
IPv6 Autoconfig Mode	Включена или выключена для сети IPv6 автоконфигурация адреса без сохранения состояния.
Burned in MAC Address	Заводской MAC-адрес.
DHCP Client Identifier	Идентификатор клиента выводится на дисплей, только если на сервисном порту включен DHCP-клиент с параметром client-id.

8.2 Команды для настройки доступа с помощью консольного порта

В данном разделе описаны команды конфигурации консольного порта. Для соединения компьютера напрямую с портом консоли коммутатора используется консольный кабель.

configure

Данная команда открывает доступ к режиму глобальной конфигурации. Этот режим позволяет конфигурировать различные системные настройки, в том числе учетные записи пользователей, а также использовать иные режимы ввода команд, в том числе режим конфигурирования командной строки (Line Config).

Формат: `configure`

Режим ввода команд: привилегированный режим

line

Эта команда открывает доступ к режиму Line Console, позволяющему конфигурировать настройки Telnet и порт консоли, а также аутентификацию при запуске консоли.

Формат: `line {console | telnet | ssh}`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
console	Настройка параметров последовательного порта
telnet	Настройка параметров удалённого подключения с помощью протокола Telnet.
ssh	Настройка параметров удалённого подключения с помощью протокола SSH.

serial baudrate

Эта команда задает скорость передачи информации интерфейса консоли. Поддерживаемые скоростные режимы: 1200, 2400, 4800, 9600, 19200, 38400, 57600 и 115200.

Значение по умолчанию: 115200

Формат: `serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`

Режим ввода команд: режим конфигурирования командной строки

no serial baudrate

Задать скорость передачи информации интерфейса консоли.

Формат: `no serial baudrate`

Режим ввода команд: режим конфигурирования командной строки

serial timeout

Задать максимальное время жизни соединения (в минутах) при бездействии консоли. Диапазон значений: десятичное число от 0 до 65535. Значение 0 указывает, что установлено бесконечное время жизни консольной сессии.

Значение по умолчанию: 5

Формат: `serial timeout` *`0-65535`*

Режим ввода команд: режим конфигурирования командной строки

no serial timeout

Задать максимальное время соединения (в минутах) при бездействии консоли.

Формат: `no serial timeout`

Режим ввода команд: режим конфигурирования командной строки

show serial

Эта команда показывает настройки консольного порта коммутатора.

Формат: `show serial`

Режим ввода команд: привилегированный режим

пользовательский режим

Параметр	*Описание*
Serial Port Login Timeout (minutes)	Время (в минутах) бездействия соединения с последовательным портом, по истечении которого соединение будет разорвано коммутатором. Значение 0 соответствует бесконечному времени.
Baud Rate (bps)	Установленная по умолчанию скорость передачи данных в бодах, на которой последовательный порт будет работать.
Character Size (bits)	Количество битов в символе. Всегда равно 8.
Flow Control	Включена или выключена опция управления потоком данных аппаратных средств (Hardware Flow-Control). Всегда выключена.
Stop Bits	Количество стоповых битов на символ. Всегда равно 1.
Parity	Контроль четности, используемый последовательным портом. Всегда None («Не используется»).

session-limit

Установить максимальное количество одновременных исходящих сессий Telnet/SSH. Значение 0 означает невозможность установления исходящих сессий Telnet/SSH.

Значение по умолчанию: 5

Формат: `session-limit` *`0-5`*

Режим ввода данных: режим конфигурирования командной строки

no session-limit

Отрицательная форма данной команды сбрасывает максимальное количество одновременных исходящих сессий к заводскому значению.

Формат: `no session-limit`

Режим ввода команд: режим конфигурирования командной строки

session-timeout

Установить максимальное время жизни сессии Telnet/SSH. Значение выставляется в минутах.

Значение по умолчанию 5

Формат `session-timeout` *`1-160`*

Режим ввода данных Режим конфигурирования командной строки

no session-timeout

Сбросить лимит превышения времени сессии Telnet/SSH к значению по умолчанию. Значение выставляется в минутах.

8.3 Команды настройки протокола Telnet

В данном разделе описаны команды конфигурации и просмотра настроек Telnet. Telnet используется для управления устройством с удалённого устройства.

ip telnet server enable

Данная команда разрешает устанавливать соединения с системой по протоколу Telnet и включает режим управления сервером Telnet, а также открывает порт Telnet для входящих подключений.

Значение по умолчанию: отключено

Формат: `ip telnet server enable`

Режим ввода команд: привилегированный режим

no ip telnet server enable

Данная команда запрещает доступ к системе по протоколу Telnet и отключает режим управления сервером Telnet. Закрывает порт Telnet для входящих подключений и разрывает все открытые сессии Telnet.

Формат: `no ip telnet server enable`

Режим ввода команд: привилегированный режим

ip telnet port

Сконфигурировать номер порта TCP, через который Telnet получает входящие запросы.

Значение по умолчанию: 23

Формат: `ip telnet port` *`1-65535`*

Режим ввода команд: привилегированный режим

no ip telnet port

Вернуть настройки порта Telnet-сервера для входящих подключений к заводским значениям.

Формат: `no ip telnet port`

Режим ввода команд: привилегированный режим

telnet

Установить новое исходящее соединение Telnet с удаленным хостом. В поле *host* должен быть указан либо действительный IP-адрес, либо имя хоста. В поле *port* следует указать целое число десятичной системы счисления в диапазоне от 0 до 65535, значение по умолчанию – 23. Команда *[debug]* выводит список опций Telnet, включенных в данный момент. Опциональный параметр *line* устанавливает в качестве операционного режима исходящих сессий Telnet строчный режим, в то время как по умолчанию используется текстовый (символьный) режим. Опция *localecho* включает режим локального отображения.

Формат: `telnet` *`ip-address|hostname port`* `[debug] [line] [localecho]`

Режим ввода команд: привилегированный режим

пользовательский режим

transport input telnet

Данная команда регулирует новые входящие сессии Telnet. Если данная опция включена, новые сессии Telnet будут открываться до тех пор, пока не будет исчерпан лимит их количества. Открытая сессия остается активной до ее закрытия или до непредвиденной ошибки сети.

Если режим администрирования сервера Telnet (Telnet Server Admin Mode) отключен, сессии Telnet не будут открываться. Для запуска режима администрирования сервера Telnet используется команда `ip telnet server enable`.

Значение по умолчанию: включено

Формат: `transport input telnet`

Режим ввода данных: режим конфигурирования командной строки

no transport input telnet

Запретить открывать новые входящие сессии Telnet.

Формат: `no transport input telnet`

Режим ввода данных: режим конфигурирования командной строки

transport output telnet

Данная команда регулирует новые исходящие сессии Telnet. Если данная опция включена, пользователь может устанавливать новые исходящие соединения Telnet до достижения системного лимита количества одновременно открытых сессий Telnet. Открытая сессия остается активной до ее закрытия или до непредвиденной ошибки сети.

Значение по умолчанию: включено

Формат: `transport output telnet`

Режим ввода команд: режим конфигурирования командной строки

no transport output telnet

Запретить устанавливать новые исходящие сессии Telnet.

Формат: `no transport output telnet`

Режим ввода команд: режим конфигурирования командной строки

telnetcon maxsessions

Установить максимальное количество доступных входящих сессий Telnet. 0 означает невозможность установления соединений Telnet. Диапазон значений: 0-5.

Значение по умолчанию: 5

Формат: `telnetcon maxsessions` *`0-5`*

Режим ввода команд: привилегированный режим

no telnetcon maxsessions

Установить максимальное количество доступных входящих сессий Telnet на значение по умолчанию.

Формат: `no telnetcon maxsessions`

Режим ввода команд: привилегированный режим

telnetcon timeout

Установить максимальное время жизни (в минутах) для входящих сессий Telnet. Диапазон значений: десятичное число от 0 до 65535. Значение 0 указывает, что установлено бесконечное время жизни входящих сессий Telnet.

При изменении лимита времени новое значение применяется ко всем активным и неактивным сессиям немедленно. Сессия, превысившая новый лимит времени бездействия, разрывается немедленно.

Значение по умолчанию: 5

Формат: `telnetcon timeout` *`1-160`*

Режим ввода данных: привилегированный режим

no telnetcon timeout

Сбросить лимит превышения времени входящих сессий Telnet к значению по умолчанию.

Для вступления в силу изменений лимита времени для активных сессий следует перезапустить сессию. Нажатие любой клавиши перезапускает отсчет времени.

Формат: `no telnetcon timeout`

Режим ввода данных: привилегированный режим

show telnet

Показать текущие настройки исходящих сессий Telnet. Исходящие сессии – соединения Telnet, которые коммутатор устанавливает с удалённой системой.

Формат: `show telnet`

Режимы ввода команд: привилегированный режим

пользовательский режим

Параметр	*Описание*
Outbound Telnet Login Timeout	Количество минут бездействия до разрыва сессии Telnet.
Maximum Number of Outbound Telnet Sessions	Количество одновременно доступных исходящих сессий Telnet.

Allow New Outbound Telnet Sessions	Доступность открытия новых исходящих сессий Telnet.

show telnetcon

Показать текущие настройки входящих сессий Telnet. Входящие сессии – соединения Telnet, которые удаленная система устанавливает с коммутатором.

Формат: `show telnetcon`

Режимы ввода команд: привилегированный режим
пользовательский режим

Параметр	*Описание*
Remote Connection Login Timeout (minutes)	Количество минут бездействия до разрыва удаленной сессии Telnet. Значение: десятичное число от 0 до 65535. Значение по умолчанию: 5.
Maximum Number of Remote Connection Sessions	Количество доступных одновременных удаленных соединений. Значение по умолчанию: 5
Allow New Telnet Sessions	Если значение установлено на No («Нет»), то устанавливать новые сессии Telnet запрещено. Значение по умолчанию: Yes («Да»).
Telnet Server Admin Mode	Включен ли режим управления Telnet (Telnet Admin mode).
Telnet Server Port	Сконфигурированный номер порта TCP, через который сервер Telnet получает запросы на входящие подключения (значение по умолчанию: 23).

8.4 Команды настройки протокола SSH

В данном разделе описаны команды конфигурации протокола SSH для доступа к коммутатору. Протокол SSH используется для доступа к коммутатору с удаленного хоста управления.

Максимальное количество сессий SSH – 5.

ssh

Установить новое исходящее соединение SSH с удаленным хостом. В поле *host* должен быть указан либо действительный IP-адрес, либо имя хоста. В поле *port* следует указать целое число десятичной системы счисления в диапазоне от 0 до 65535, значение по умолчанию – 22.

Формат: `ssh` *`ip-address|hostname port`*

Режим ввода команд: привилегированный режим
пользовательский режим

transport output ssh

Данная команда регулирует новые исходящие сессии SSH. Если данная опция включена, пользователь может устанавливать новые исходящие соединения SSH до достижения системного

лимита количества одновременно открытых сессий SSH. Открытая сессия остается активной до ее закрытия или до непредвиденной ошибки сети.

Значение по умолчанию: включено

Формат: `transport output ssh`

Режим ввода команд: режим конфигурирования командной строки

no transport output ssh

Запретить устанавливать новые исходящие сессии SSH.

Формат: `no transport output ssh`

Режим ввода команд: режим конфигурирования командной строки

show ssh

Показать текущие настройки исходящих сессий SSH. Исходящие сессии – соединения ssh, которые коммутатор устанавливает с удалённой системой.

Формат: `show ssh`

Режимы ввода команд: привилегированный режим

пользовательский режим

Параметр	*Определение*
Outbound Telnet Login Timeout	Количество минут бездействия до разрыва сессии SSH.
Maximum Number of Outbound SSH Sessions	Количество одновременно доступных исходящих сессий SSH.
Allow New Outbound Telnet Sessions	Доступность открытия новых исходящих сессий SSH.

clear ssh-client-knownhost

Очистить файл публичных ssh-ключей.

Формат: `clear ssh-client-knownhost`

Режим ввода команд: привилегированный режим

ip ssh

Разрешить доступ к данной системе через протокол SSH (эта команда – сокращенная форма от ip ssh server enable).

Значение по умолчанию: отключено

Формат: `ip ssh`

Режим ввода команд: привилегированный режим

ip ssh port

Сконфигурировать номер порта TCP, через который сервер SSH получает запросы на входящие подключения. Действительные номера портов: от 1 до 65535.

Значение по умолчанию: 22

Формат: `ip ssh port 1-65535`

Режим ввода команд: привилегированный режим

no ip ssh port

Сбросить порт входящих подключений сервера SSH к значению по умолчанию.

Формат: `no ip ssh port`

Режим ввода команд: привилегированный режим

ip ssh protocol

Установить или удалить уровни (или версии) протокола SSH. Возможные значения: SSH1 (1), SSH2 (2) или одновременно SSH 1 и SSH 2 (1 и 2).

Значение по умолчанию: 2

Формат: `ip ssh protocol [1] [2]`

Режим ввода команд: привилегированный режим

ip ssh server enable

Данная команда включает IP-сервер SSH.

Значение по умолчанию: выключено

Формат: `ip ssh server enable`

Режим ввода команд: привилегированный режим

no ip ssh server enable

Выключить IP-сервер SSH.

Формат: `no ip ssh server enable`

Режим ввода команд: привилегированный режим

sshcon maxsessions

Эта команда определяет максимальное количество сессий соединений SSH, которые могут быть установлены. Значение 0 указывает, что ssh-соединение не может быть установлено. Диапазон значений: 0-5.

Значение по умолчанию: 5

Формат: `sshcon maxsessions 0-5`

Режим ввода команды: привилегированный режим

no sshcon maxsessions

Сбросить максимальное количество сессий через SSH-соединения к значению по умолчанию.

Формат: `no sshcon maxsessions`

Режим ввода команд: привилегированный режим

sshcon timeout

Установить время жизни (в минутах) SSH-соединения. Сессия активна, пока не превышен заданный лимит времени бездействия. Время задается десятичным числом от 0 до 65535. Значение 0 указывает, что установлено бесконечное время жизни сессий SSH.

Для вступления в силу изменений лимита времени для активных сессий следует перезапустить сессию. Нажатие любой клавиши перезапускает отсчет времени.

По умолчанию: 5

Формат: `sshcon timeout` *`0-65535`*

Режим ввода команд: привилегированный режим

no sshcon timeout

Сбросить время жизни SSH-соединения к значению по умолчанию.

Для вступления в силу изменений лимита времени для активных сессий следует перезапустить сессию. Нажатие любой клавиши перезапускает отсчет времени.

Формат: `no sshcon timeout`

Режим ввода команд: привилегированный режим

show ip ssh

Показать настройки SSH.

Формат: `show ip ssh`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Administrative Mode	Включен или выключен сервер SSH
SSH Port	Порт SSH
Protocol Level	Уровень протокола может содержать версию 1, версию 2 или версию 1 и версию 2 одновременно.
SSH Sessions Currently Active	Количество сессий SSH, активных в текущий момент
Max SSH Sessions Allowed	Максимальное количество разрешенных сессий SSH
SSH Timeout	Таймаут SSH сессии (в минутах)
Keys Present	Наличие файлов ключей RSA и DSA для SSH
Key Generation in Progress	Происходит ли генерация файлов ключей RSA или DSA в текущий момент.

8.5 Команды управления ключами безопасности

В данном разделе описаны команды генерации ключей и сертификатов. Доступна возможность их загружать.

crypto certificate generate

Эта команда генерирует самоподписанный сертификат протокола HTTPS. Генерируемый ключ RSA для SSL имеет длину в 1024 бита. Результирующий сертификат генерируется с общим именем, соответствующим наименьшему IP-адресу данного устройства, и действует 365 дней.

Формат: `crypto certificate generate`

Режим ввода команд: режим глобальной конфигурации

no crypto certificate generate

Удалить файлы сертификата HTTPS с данного устройства, вне зависимости от того, самоподписанный это сертификат или загруженный из внешнего источника.

Формат: `no crypto certificate generate`

Режим ввода команд: режим глобальной конфигурации

crypto key generate rsa

Сгенерировать пару ключей RSA для SSH размером 1024 или 2048 бит. Новые файлы ключей будут записаны поверх существующих (сгенерированных или загруженных) файлов ключей RSA.

Значение по умолчанию: 1024

Формат: `crypto key generate rsa`

Режим ввода команд: режим глобальной конфигурации

no crypto key generate rsa

Удалить файлы ключей RSA с данного устройства.

Формат: `no crypto key generate rsa`

Режим ввода команд: режим глобальной конфигурации

crypto key generate dsa

Сгенерировать пару ключей DSA для SSH. Новые файлы ключей будут записаны поверх существующих (сгенерированных или загруженных) файлов ключей DSA.

Формат: `crypto key generate dsa`

Режим ввода команд: режим глобальной конфигурации

no crypto key generate dsa

Удалить файлы ключей DSA с данного устройства.

Формат: `no crypto key generate dsa`

Режим ввода команд: режим глобальной конфигурации

8.6 Команды настройки протоколов HTTP/HTTPS

В данном разделе описаны команды конфигурации протокола передачи гипертекста (HTTP) и безопасный доступ к коммутатору через протокол HTTP. Доступ к коммутатору через web-браузер разрешен по умолчанию. Все, что можно просматривать и конфигурировать через CLI, также доступно через web.

ip http accounting exec, ip https accounting exec

Применить учетный список пользовательского режима (start-stop/stop-only) к методам доступа HTTP и HTTPS.

Для создания списка методов учёта пользователей используется команда `aaa accounting`.

Формат: `ip {http|https} accounting exec {default|`*`listname`*`}`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
http/https	Метод доступа, к которому применяется список
default	Список методов, используемых сервисами авторизации по умолчанию
listname	Имя списка учетных методов (формат: буквенно-цифровая строка символов).

no ip http/https accounting exec

Удалить список методов учёта.

Формат: `no ip {http|https} accounting exec {default|`*`listname`*`}`

Режим ввода команд: режим глобальной конфигурации

ip http authentication

Данная команда позволяет установить методы аутентификации для пользователей сервера HTTP. При конфигурации по умолчанию используется локальная база данных пользователей. Действие данной команды аналогично команде ip http authentication local. Дополнительные методы аутентификации используются только в случае, если предыдущий метод выдает ошибку, но не в случае сбоя. Для успешной аутентификации в случае, если все методы выдают ошибку, необходимо через командную строку задать none в качестве заключительного метода. К примеру, если в качестве метода аутентификации после параметра radius задан параметр none, то аутентификация не используется, если сервер RADIUS недоступен.

Значение по умолчанию: локальная база данных

Формат: `ip http authentication method1 [method2...]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
local	Использовать для аутентификации локальную базу данных с именами пользователей
none	Не использовать аутентификацию
radius	Использовать для аутентификации список всех серверов RADIUS
tacacs	Использовать для аутентификации список всех серверов TACACS+.

no ip http authentication

Вернуться к значению по умолчанию.

Формат: `no ip http authentication`

Режим ввода команд: режим глобальной конфигурации

ip https authentication

Установить методы аутентификация для пользователей HTTPS-сервера. При конфигурации по умолчанию используется локальная база данных пользователей. Действие данной команды аналогично таковому команды ip https authentication local. Дополнительные методы аутентификации используются только в случае, если предыдущий метод выдает ошибку, но не в случае сбоя. Для успешной аутентификации в случае, если все методы выдают ошибку, необходимо через командную строку задать none в качестве заключительного метода. К примеру, если в качестве метода аутентификации после параметра radius задан параметр none, то аутентификация не используется, если сервер RADIUS недоступен.

Значение по умолчанию: `local`

Формат: `ip https authentication method1 [method2...]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
local	Использовать для аутентификации локальную базу данных с именами пользователей.
none	Не использовать аутентификацию.
radius	Использовать для аутентификации список всех серверов RADIUS.
tacacs	Использовать для аутентификации список всех серверов TACACS+.

no ip https authentication

Вернуться к значению по умолчанию.

Формат: `no ip https authentication`

Режим ввода команд: режим глобальной конфигурации

ip http server

Включить доступ к коммутатору через web-интерфейс. Если опция включена, пользователь может авторизоваться на коммутаторе через web-интерфейс. Если выключена, пользователь не может авторизоваться на web-сервере коммутатора. Выключение web-интерфейса вступает в силу немедленно. Действие распространяется на все интерфейсы.

Значение по молчанию: включено

Формат: `ip http server`

Режим ввода команд: привилегированный режим

no ip http server

Отключить доступ к коммутатору через web-интерфейс. При этом пользователь не может авторизоваться на web-сервере коммутатора.

Формат: `no ip http server`

Режим ввода команд: привилегированный режим

ip http secure-server

Включить протокол SSL (уровень защищенных сокетов) для безопасного режима HTTP.

Значение по умолчанию: выключено

Формат: `ip http secure-server`

Режим ввода команд: привилегированный режим

no ip http secure-server

Отключить протокол SSL (уровень защищенных сокетов) для безопасного режима HTTP.

Формат: `no ip http secure-server`

Режим ввода команд: привилегированный режим

ip http java

Включить режим Web Java. Режим Java может использоваться как при защищенном, так и при незащищенном интернет соединениях.

Значение по умолчанию: включено

Формат: `ip http java`

Режим ввода команд: привилегированный режим

no ip http java

Выключить режим Web Java. Режим Java может использоваться как при защищенном, так и при незащищенном интернет соединениях.

Формат: `no ip http java`

Режим ввода команд: привилегированный режим

ip http port

Сконфигурировать номер TCP-порта, через который HTP-сервер получает запросы.

Значение по умолчанию: 80

Формат: `ip http port 1-65535`

Режим ввода команд: привилегированный режим

no ip http port

Сбросить настройки порта, через который HTTP-сервер получает запросы, к значениям по умолчанию.

Формат: `no ip http port`

Режим ввода команд: привилегированный режим

ip http rest-api port

Сконфигурировать номер TCP-порта HTTP-сервера, REST-запросы которого слушает сервер с открытым RESTful API.

Значение по умолчанию: 8080

Формат: `ip http rest-api port 1025-65535`

Режим ввода команд: привилегированный режим

no ip http rest-api port

Сбросить настройки прослушиваемого порта HTTP-сервера с открытым RESTful API к значению по умолчанию.

Формат: `no ip http rest-api port`

Режим ввода команд: привилегированный режим

ip http rest-api secure-port

Сконфигурировать номер TCP-порта HTTPS-сервера, который получает защищенные REST-запросы с сервера с открытым RESTful API.

Значение по умолчанию: 8443

Формат: `ip http rest-api secure-port 1025-65535`

Режим ввода команд: привилегированный режим

no ip http rest-api secure-port

Сбросить настройки слушающего HTTP-сервера с открытым RESTful API к значению по умолчанию.

Формат: `no ip http rest-api secure-port`

Режим ввода команд: привилегированный режим

ip http session hard-timeout

Настроить таймаут в часах, после истечения которого неактивный клиент будет отключен от незащищенной HTTP-сессии. Установление данного параметра на 0 (ноль) задает неограниченное по

времени пользование. Когда установленное время истекает, пользователю необходимо пройти повторную аутентификацию. Отсчет времени ведется с начала сессии и не зависит от уровня активности соединения.

Значение по умолчанию: 24

Формат: `ip http session hard-timeout` *`1-168`*

Режим ввода команд: привилегированный режим

no ip http session hard-timeout

Сбросить настройки таймаута, при достижении которого клиент будет отключен от незащищенной HTTP-сессии, к значению по умолчанию.

Формат: `no ip http session hard-timeout`

Режим ввода команд: привилегированный режим

ip http session maxsessions

Настроить количество возможных незащищенных HTTP-сессий. Минимальное значение: 0 (ноль).

Значение по умолчанию: 16

Формат: `ip http session maxsessions` *`0-16`*

Режим ввода команд: привилегированный режим

no ip http session maxsessions

Сбросить настройки количества возможных незащищенных HTTP-сессий к значению по умолчанию.

Формат: `no ip http session maxsessions`

Режим ввода команд: привилегированный режим

ip http session soft-timeout

Настроить лимит времени подключения к незащищенной HTTP-сессии в минутах. Установление данного параметра на 0 (ноль) задает неограниченное по времени пользование. Когда установленное время истекает, пользователю необходимо пройти повторную аутентификацию. Отсчет времени ведется с начала сессии и перезапускается с каждым новым подключением.

Значение по умолчанию: 5

Формат: `ip http session soft-timeout` *`1-60`*

Режим ввода команд: привилегированный режим

no ip http session soft-timeout

Сбросить настройки времени отключения неактивного клиента от незащищенной HTTP-сессии к значению по умолчанию.

Формат: `no ip http session soft-timeout`

Режим ввода команд: привилегированный режим

Настроить время в часах, после которого неактивный клиент будет отключен от защищенной HTTP-сессии. Когда установленное время истекает, пользователю необходимо пройти повторную аутентификацию. Отсчет времени ведется с начала сессии и не зависит от уровня активности соединения. Данный параметр не может быть равен нулю (бесконечности).

Значение по умолчанию: 24

Формат: `ip http secure-session hard-timeout` *`1-168`*

Режим ввода команд: привилегированный режим

no ip http secure-session hard-timeout

Сбросить настройки лимита времени для защищенной HTTP-сессии к значению по умолчанию.

Формат: `no ip http secure-session hard-timeout`

Режим ввода команд: привилегированный режим

ip http secure-session maxsessions

Настроить количество возможных защищенных HTTP-сессий. Минимальное значение: 0 (ноль).

По умолчанию: 16

Формат: `ip http secure-session maxsessions` *`0-16`*

Режим ввода команд: привилегированный режим

no ip http secure-session maxsessions

Сбросить настройки количества возможных защищенных HTTP-сессий к значению по умолчанию.

Формат: `no ip http secure-session maxsessions`

Режим ввода команд: привилегированный режим

ip http secure-session soft-timeout

Настроить лимит времени подключения к защищенной HTTP-сессии в минутах. Установление данного параметра на ноль создаст неограниченное по времени пользование. Когда установленное время истекает, пользователю необходимо пройти повторную аутентификацию. Отсчет времени ведется с начала сессии и перезапускается с каждым новым подключением. Данный параметр не может быть равен нулю (бесконечности).

Значение по умолчанию: 5

Формат: `ip http secure-session soft-timeout` *`1-60`*

Режим ввода команд: привилегированный режим

no ip http secure-session soft-timeout

Сбросить настройки времени отключения клиента от защищенной HTTP-сессии к значению по умолчанию.

Формат: `no ip http secure-session soft-timeout`

Режим ввода команд: привилегированный режим

ip http secure-port

Сконфигурировать порт SSL, может принимать значения 1025-65535, по умолчанию 443.

По умолчанию: 443

Формат: `ip http secure-port` *`portid`*

Режим ввода команд: привилегированный режим

no ip http secure-port

Сбросить настройки порта SSL к значению по умолчанию.

Формат: `no ip http secure-port`

Режим ввода команд: привилегированный режим

ip http secure-protocol

Настроить уровни протокола (версии). Уровень протокола может быть установлен как TLS1, SSL3 или оба TLS1 и SSL3.

Значение по умолчанию: SSL3 и TLS1

Формат: `ip http secure-protocol` *`[SSL3] [TLS1]`*

Режим ввода команд: привилегированный режим

show ip http

Отобразить настройки протокола HTTP.

Формат: `show ip http`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
HTTP Mode (Unsecure)	Незащищенный режим HTTP-сервера.
Java Mode	Административный режим Java-апплета, который используется для работы как с защищенным, так и с незащищенным соединениями.
HTTP Port	Конфигурируемый слушающий TCP-порт HTTP-сервера (значение 80).
RESTful API HTTP Port	Номер HTTP TCP-порта, REST-запросы которого слушает сервер с OpEN RESTful API.
RESTful API HTTPS Port	Номер HTTPS-порта, REST-запросы которого слушает сервер с OpEN RESTful API.

Maximum Allowable HTTP Sessions	Число возможных незащищенных HTTP-сессий.
HTTP Session Hard Timeout	Время отключения клиента от незащищенной HTTP-сессии в часах.
HTTP Session Soft Timeout	Время отключения неактивного клиента от незащищенной HTTP-сессии в минутах.
HTTP Mode (Secure)	Административный режим защищенного HTTP-сервера.
Secure Port	Номер порта защищенного HTTP-сервера.
Secure Protocol Level(s)	Уровень протокола может иметь значения SSL3, TSL1 или оба – SSL3 и TSL1.
Maximum Allowable HTTPS Sessions	Число возможных защищенных HTTP-сессий.
HTTPS Session Hard Timeout	Время отключения клиента от защищенной HTTP-сессии в часах.
HTTPS Session Soft Timeout	Время отключения неактивного клиента от защищенной HTTP-сессии в минутах.
Certificate Present	Присутствуют ли на устройстве файлы сертификата защищенного сервера.
Certificate Generation in Progress	Осуществляется ли процесс генерации сертификата.

8.7 Команды доступа

Используйте команды данного подраздела для отключения удаленного подключения и просмотра информации о состоянии подключений к системе.

disconnect

Закрыть сессию HTTP, HTTPS, Telnet или SSH. Используйте параметр all для закрытия всех активных сессий или session-id, чтобы задать конкретную сессию. Чтобы просмотреть возможные значения session-id, используйте команду `show loginsession`.

Формат: `disconnect {`*`session_id`*` | all}`

Режим ввода команд: привилегированный режим

linuxsh

Команда используется для получения доступа к командной строке Linux. Используйте команду exit, чтобы выйти из командной оболочки Linux и вернуться в CLI. Сессия командной оболочки будет завершена после пяти минут бездействия. Лимит времени бездействия может быть изменен командой `session-timeout` в режиме командной строки консоли.

Доступ в linuxsh доступен при наличии специально сгенерированного debug-ключа. При необходимости получения ключа, обратитесь в техподдержку.

Значение по умолчанию: ip-port:2324

Формат: `linuxsh [`*`ip-port`*`]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
ip-port	Номер слушающего IP-порта демона telnet. Параметр ip-port может иметь значения от 1 до 65535. Значение по умолчанию: 2324.

show loginsession

Отобразить текущие соединения с коммутатором, установленные посредством Telnet, SSH и консольного порта, и сокращенные имена пользователей. Для отражения полных имен пользователей используйте команду `show loginsession long`.

Формат: `show loginsession`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
ID	Идентификатор сессии.
User Name	Имя пользователя, вводимое для входа в систему.
Connection From	IP-адрес устройства удаленного клиента или EIA-232 для консольного порта.
Idle Time	Время бездействия.
Session Time	Общее время сессии.
Session Type	Отображает тип сессии, может быть: HTTP, HTTPS, telnet, serial (консольный порт) или SSH.

show loginsession long

Данная команда отображает полные имена пользователей, подключенных к коммутатору.

Формат: `show loginsession long`

Режим ввода команд: привилегированный режим

8.8 Команды настройки контроля учетных записей пользователя

Данный подраздел содержит команды, используемые для управления пользователями системы, их добавления и удаления. В системе по умолчанию есть один пользователь — Администратор. Администратор может просматривать и конфигурировать системные настройки.

Нельзя удалить пользователя «Администратор». Вы можете сконфигурировать до 5 локальных пользователей.

aaa authentication login

Настроить аутентификацию при входе на устройство. Произвольный список имен или список имен по умолчанию, созданный при помощи данной команды, используется с командой `aaa authentication login`. Для создания списка введите команду `aaa authentication login list-name method`, где `list-name` представляет собой любую последовательность знаков, используемую

для наименования списка. Method означает методы, применяемые алгоритмом аутентификации в заданной последовательности.

Дополнительные методы аутентификации используются только в случае получения сообщения об ошибке в вышеуказанном методе, но не в случае ошибки аутентификации. Чтобы убедиться, что аутентификация прошла успешно, даже в случае ошибки всех методов аутентификации, укажите в командной строке none, как последний метод аутентификации. Например, если в качестве метода аутентификации после метода radius указано none, то аутентификация не потребуется, если RADIUS-сервер перестал отвечать.

Значение по умолчанию: defaultList. Используется в консоли и включает только метод none.
networkList. Используется telnet и SSH, содержит только метод local.

Формат: aaa authentication login {default | *list-name*} *method1 [method2...]*

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
default	При регистрации пользователя методы аутентификации, следующие за данным параметром, используются в качестве методов по умолчанию.
list-name	Последовательность символов (не более 15 символов), которая используется для наименования списка методов аутентификации, активирующихся при регистрации пользователя.
method1... ***[*method2...*]***	Один из следующих: • *deny*. Используется для отказа в доступе; • *enable*. Использует для аутентификации пароль enable; • *line*. Использует для аутентификации пароль line; • *none*. Аутентификация не используется; • *radius*. Использует для аутентификации все RADIUS-сервера; • *tacacs*. Использует для аутентификации все сервера TACACS+.

no aaa authentication login

Сбросить настройки к значениям по умолчанию.

Формат: aaa authentication login {default | *list-name*}

Режим ввода команд: режим глобальной конфигурации

aaa authentication enable

Настроить аутентификацию для доступа к более высоким уровням привилегий. Список enable по умолчанию – enableList. Он используется только при работе с консолью и включает такие методы как enable, за которым следует none.

Отдельный enable-список, enableNetList, по умолчанию используется для Telnet и SSH совместно enableList. Этот список по умолчанию подходит для протоколов Telnet и SSH и включает в себя enable, за которым следуют методы deny. В соответствии с исходными настройками ПО, пароль enable не подлежит конфигурированию. Это означает, что в соответствии с исходными настройками, пользователи протоколов Telnet и SSH не имеют доступа к режиму высоких привилегий EXEC. С

другой стороны, исходные настройки всегда позволяют пользователю консоли входить в режим высоких привилегий без ввода пароля enable.

Названия списка по умолчанию и опционального списка задаются командой aaa authentication enable и используются вместе с командой enable authentication. Создать список можно при помощи команды aaa authentication enable list-name method, где параметр list-name представляет собой последовательность символов, используемую для наименования списка. Параметр method определяет список методов, которые, в соответствии с заданной последовательностью, применяет алгоритм аутентификации.

Диспетчер пользователей присылает сообщение об ошибке ERROR (не «PASS» или «FAIL») при использовании методов enable и line, если пароль не был сконфигурирован, и затем запускает следующий метод из списка аутентификации. Метод none означает, что аутентификация не требуется.

Пароль enable будет подсказываться только в том случае, если он требуется. Следующие методы аутентификации пароля не требуют:

- none (не указано);
- deny (отклонено);
- enable (если пароль enable не сконфигурирован);
- line (если пароль line не сконфигурирован).

В примерах a и b запрос пароля не выводится, однако, поскольку в примерах c и d содержатся методы radius и tacacs, запрос о вводе пароля выведется на экран.

Если методы входа в систему включают только enable, но пароль enable не сконфигурирован, то в таком случае система не запрашивает имя пользователя, а только пароль. ПО поддерживает введение дополнительных методов после метода local в списке аутентификации и авторизации. Если пользователь отсутствует в локальной базе данных, то применяется следующий по списку сконфигурированный метод.

Дополнительные методы аутентификации используются, только если при использовании других методов поступило сообщение об ошибке, но не в случае неудачи аутентификации. Чтобы убедиться, что аутентификация прошла успешно, даже если сообщение об ошибке поступило при использовании всех методов аутентификации, укажите в командной строке метод none в качестве последнего метода аутентификации.

Используйте команду `show authorization methods`, чтобы просмотреть информацию о методах аутентификации.

Запросы, которые маршрутизатор посылает серверу RADIUS, включают имя пользователя $enabx$, где x означает запрашиваемый уровень привилегий. Для аутентификации на сервере Radius, добавьте к ним пользователей $enabx$. Тогда регистрационный ID будет направляться серверам TACACS+ для аутентификации.

Значение по умолчанию: значение по умолчанию

Формат: `aaa authentication enable {default | list-name} method1 [method2...]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
default	Использует список методов аутентификации, следующих за данным параметром, в качестве методов по умолчанию на высоких уровнях привилегий.
list-name	Последовательность символов, используемая для наименования активированных методов аутентификации при использовании доступа к высоким уровням привилегий. Не более 15 символов.
Method1 *[***method2...***]*	Выберите один (или более) из указанных ниже: • *deny*. Используется для отказа в доступе; • *enable*. Использует для аутентификации пароль enable; • *line*. Использует для аутентификации пароль line; • *none*. Аутентификация не используется; • *radius*. Использует для аутентификации все RADIUS-сервера; • *tacacs*. Использует для аутентификации все сервера TACACS+.

Пример: Данный пример показывает запуск аутентификации на высоких уровнях.

```
(switch)(config)# aaa authentication enable default enable
```

no aaa authentication enable

Сбросить настройки конфигурации к значениям по умолчанию.

Формат: `no aaa authentication enable {default | list-name}`

Режим ввода команд: режим глобальной конфигурации

aaa authorization

Данная команда используется для конфигурирования списков методов авторизации для ввода команд и режимов конфигурирования командной строки. Список определяется параметром "default" (по умолчанию) или заданным пользователем параметром "list_name" (имя списка). Может быть указано не более пяти методов авторизации.

Метод local не поддерживает авторизацию ввода команд.

Авторизация ввода команд

Когда сконфигурирована авторизация для режима line, диспетчер пользователей (User Manager) отправляет информацию о введенных командах на сервер AAA. Сервер AAA подтверждает получение команды и отправляет ответ PASS (разрешена) или FAIL (разрешена). Если команда разрешена, она выполняется. В противном случае, если команда отклонена, пользователь получает сообщение об ошибке. Различные служебные команды, такие как tftp, а также ping и исходящие сессии протокола telnet также должны проходить авторизацию. Применение сценариев script рассматривается как выполнение отдельной команды и тоже проходит авторизацию. Команды конфигурации начальной загрузки, используемые при запуске устройства, не подвержены процедуре авторизации.

Порядок авторизации ввода команд:

1 Конфигурирование списка методов авторизации.

```
aaa authorization commands listname tacacs radius none
```

2 Применение списка методов авторизации для line режима (консоль, telnet, SSH).

```
authorization commands listname
```

3 Команды, вводимые пользователем, пройдут авторизацию через серверы TACACS+ или RADIUS и будут приняты или отклонены.

Авторизация режима конфигурирования командной строки

Когда параметры авторизации режима конфигурирования командной строки применяются для line, команда enable для входа в привилегированный режим может не требоваться. Если ответ авторизации показывает, что уровень пользователя достаточно высок для входа в привилегированный режим, пользователь получает к нему полный доступ.

Порядок авторизации пользовательского режима (exec):

1 Конфигурирование списка методов авторизации.

```
aaa authorization exec listname method1 [method2....]
```

2 Применение списка методов авторизации в режиме line (консоль, telnet, SSH).

```
authorization exec listname
```

3 При входе пользователя в систему, в дополнение к аутентификации (log in) проводится авторизация, чтобы определить, обладает ли пользователь правом на прямой доступ к привилегированному режиму.

Формат: `aaa authorization {commands|exec} {default|list-name} method1[method2]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
commands	Проверяет авторизацию всех команд пользователя.
exec	Проверяет авторизацию пользовательского режима.
default	Список методов авторизации сервисов по умолчанию.
list-name	Буквенно-цифровая последовательность символов, используемая в качестве имени списка методов авторизации.
method	Допустимые значения: TACACS+/RADIUS/Local и none.

no aaa authorization

Удалить список методов авторизации.

Формат: `no aaa authorization {commands|exec} {default|list-name}`

Режим ввода команд: режим глобальной конфигурации

authorization commands

Данная команда применяет список методов авторизации ввода команд для режима доступа. Порядок конфигурирования авторизации ввода команд см. в разделе aaa authorization.

Формат: `authorization commands [default|list-name]`

Режим ввода команд: Line console, Line telnet, Line SSH

Параметр	*Описание*
commands	Запускает авторизацию для каждого исполнения команды.

no authorization commands

Убрать авторизацию ввода команд для режима доступа.

Формат: `no authorization {commands|exec}`

Режим ввода команд: Line console, Line telnet, Line SSH

authorization exec

Данная команда применяет список методов авторизации режима конфигурирования командной строки для метода доступа так, что пользователь может не использовать команду enable для входа в привилегированный режим. Порядок конфигурирования авторизации см. в разделе aaa authorization.

Формат `authorization exec list-name`

Режим ввода команд Line console, Line telnet, Line SSH

Параметр	*Описание*
list-name	Список методов авторизации пользовательского режима.

no authorization exec

Убрать авторизацию команд для режима конфигурирования командной строки.

Формат: `no authorization exec`

Режим ввода команд: Line console, Line telnet, Line SSH

authorization exec default

Данная команда применяет заданный по умолчанию список методов авторизации режима конфигурирования командной строки для метода доступа так, что пользователь может не использовать команду enable для входа в привилегированный режим. Порядок конфигурирования авторизации см. в разделе aaa authorization.

Формат: `authorization exec default`

Режим ввода команд: Line console, Line telnet, Line SSH

no authorization exec default

Убрать авторизацию режима конфигурирования командной строки.

Формат: `no authorization exec default`

Режим ввода команд: Line console, Line telnet, Line SSH

show authorization methods

Показать сконфигурированные списки методов авторизации.

Формат: `show authorization methods`

Режим ввода команд: привилегированный режим

enable authentication

Задать список методов аутентификации при доступе к уровню высоких привилегий через удаленное соединение telnet или консоль.

Формат: `enable authentication {default | list-name}`

Режим ввода команд: режим конфигурирования командной строки

Параметр	*Описание*
default	Используется список по умолчанию, созданный при помощи команды `aaa authentication`.
list-name	Используется указанный список, созданный при помощи команды `aaa authentication enable`.

no enable authentication

Сбросить настройки к значениям по умолчанию, заданным командой `enable authentication`.

Формат: `no enable authentication`

Режим ввода команд: режим конфигурирования командной строки

username (режим глобальной конфигурации)

Используйте команду `username` в режиме глобальной конфигурации для добавления нового пользователя в базу данных локальных пользователей. Уровень привилегий по умолчанию 1. Использование ключевого слова `encrypted` позволяет администратору переносить пароли локальных пользователей между устройствами, не зная самих паролей. Когда параметр `password` используется вместе с параметром `encrypted`, длина пароля должна равняться 128 шестнадцатеричным символам. Если активирована проверка пароля на надежность, данная команда проверяет надежность пароля и присылает сообщение о соответствующей ошибке, если пароль не отвечает критериям безопасности. Опциональный параметр `override-complexity-check` активирует проверку надежности пароля.

Формат: `username` *`name`* `{password` *`password`* `[encrypted [override-complexity-check] | level` *`level`* `[encrypted [override-complexity-check]] | override-complexity-check]} | {level` *`level`* `[override-complexity-check] password}`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
name	Имя пользователя. Длина: 1-64 символов.

password	Аутентификационный пароль пользователя. Длина 8-64 символов. Данное значение может быть 0, если не была использована команда passwords min-length. В пароле допустимы специальные символы, в том числе ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
level	Уровень пользователя. Пользователь уровня 15 может назначить другому пользователю уровень 0 для запрета доступа этому пользователю. Значения: 0, 1, 15. Укажите уровень доступа 1 для непривилегированного режима (switch> prompt) или 15 для доступа к высшему уровню привилегий (switch# prompt). Если данный опциональный параметр не задан, уровень привилегий будет 1.
encrypted	Пароль, который вводится путем копирования из другой конфигурации коммутатора.
override-complexity-check	Отменяет проверку надежности пароля.

no username

Удалить пользователя.

Формат: `no username` *name*

Режим ввода команд: режим глобальной конфигурации

username nopassword

Удалить существующий пользовательский пароль (NULL password).

Формат: `username` *name* `nopassword` *[level level]*

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
name	Имя пользователя. Длина: 1-32 символа.
password	Аутентификационный пароль пользователя. Длина 8-64 символа.
level	Уровень пользователя. Уровень 0 может быть назначен пользователем уровня 15 другому пользователю для запрета доступа этому пользователю. Значения: 0, 1, 15.

username unlock

Разблокировать заблокированный аккаунт пользователя. Только пользователь с уровнем доступа 15 может снова открыть доступ к заблокированному аккаунту пользователя.

Формат: `username` *name* `unlock`

Режим ввода команд: режим глобальной конфигурации

username snmpv3 accessmode

Данная команда задает привилегии доступа snmpv3 для зарегистрированных пользователей. Действующие параметры режима доступа – `readonly` (только чтение) или `readwrite` (чтение и запись). Параметр `username` представляет собой зарегистрированное имя пользователя, за которым закреплен определенный режим доступа. Для пользователя “admin” (Администратор) значением по умолчанию является `readwrite`, а для всех остальных пользователей – `readonly`. Параметр `username` должен вводиться в том же регистре, что использовался при добавлении имени пользователя. Для просмотра регистра `username` введите команду `show users`.

Значение по умолчанию: администратор – readwrite (чтение и запись)
прочие – readonly (только чтение)

Формат: `username snmpv3 accessmode` *`username`* {*`readonly`* | *`readwrite`*}

Режим ввода команд: режим глобальной конфигурации

no username snmpv3 accessmode

Данная команда устанавливает привилегии доступа snmpv3 для определенных пользователей, для пользователя “admin” (Администратор) это **readwrite,** для всех остальных – **readonly**. Параметр `username` – имя пользователя, за которым закреплен определенный режим доступа.

Формат: `no username snmpv3 accessmode` *`username`*

Режим ввода команд: режим глобальной конфигурации

username snmpv3 authentication

Задать протокол аутентификации, который будет использоваться для определенного пользователя. Допустимые значения протоколов: none, `md5` или `sha`. Если вы указываете `md5` или `sha`, пароль для входа в систему также используется, как пароль аутентификации snmpv3, и, таким образом, должен состоять не менее чем из восьми символов. Параметр `username` представляет собой имя пользователя, за которым закреплен определенный протокол аутентификации. Параметр `username` должен быть введен в том же регистре, что использовался при добавлении пользователя. Для просмотра регистра `username` введите команду `show users`.

Значение по умолчанию: аутентификация не используется

Формат: `username snmpv3 authentication` *`username`* {`none` | `md5` | `sha`}

Режим ввода команд: режим глобальной конфигурации

no username snmpv3 authentication

Задать параметр none (не используется) в качестве протокола аутентификации, закрепленного за определенным пользователем. Параметр `username` представляет собой имя пользователя, за которым закреплен определенный протокол аутентификации.

Формат: `no username snmpv3 authentication` *`username`*

Режим ввода команд: режим глобальной конфигурации

username snmpv3 encryption

Данная команда определяет протокол шифрования, закрепленный за определенным пользователем. Допустимые значения параметра: `des` или none.

Если выбран параметр `des`, вы можете указать ключ в командной строке. Длина ключа шифрования должна быть от 8 до 64 символов. Если выбран параметр `des`, но ключ не указан, пользователю будет выведен запрос ключа. При использовании протокола `des` пароль для входа в систему также используется, как пароль шифрования snmpv3, таким образом, он должен состоять не менее чем из восьми символов. Если выбрано none, ключ шифрования не требуется.

Параметр `username` представляет собой регистрационное имя пользователя, за которым закреплен определенный протокол шифрования. Параметр `username` должен быть введен в том же

регистре, что использовался при добавлении пользователя. Для просмотра регистра username введите команду show users.

Значение по умолчанию: шифрование не используется

Формат: username snmpv3 encryption *username* {none | des*[key]*}

Режим ввода команд: режим глобальной конфигурации

no username snmpv3 encryption

Настроить протокол шифрования как **none**. Параметр username представляет собой регистрационное имя пользователя, за которым закреплен определенный протокол шифрования.

Формат: no username snmpv3 encryption *username*

Режим ввода команд: режим глобальной конфигурации

username snmpv3 encryption encrypted

Задать протокол шифрования des и ключ шифрования для определенного пользователя. Длина ключа шифрования должна быть от 8 до 64 символов.

Значение по умолчанию: шифрование не используется

Формат: username snmpv3 encryption encrypted *username* des *key*

Режим ввода команд: режим глобальной конфигурации

show users

Отобразить сокращенные имена сконфигурированных пользователей и их настройки. Для отображения полных имен пользователей используйте команду users long. Команда show users доступна только на 15 уровне привилегий. Поля SNMPv3 будут отображены, только в случае если SNMP доступен для данной системы.

Формат: show users

Режим ввода команд: привилегированный режим

Параметр	*Описание*
User Name	Имя пользователя, которое вводится для регистрации при использовании порта с последовательным выводом данных, Telnet или Web.
Access Mode	Показывает, может ли пользователь менять параметры коммутатора (уровень 15) или только просматривать их (уровень 1). Согласно настройкам по умолчанию, пользователю “admin” (Администратор) присвоен уровень доступа 15, а пользователю “guest” (Гость) – уровень доступа 1.
SNMPv3 Access Mode	Режим доступа SNMPv3. Если значение установлено на ReadWrite, пользователь SNMPv3 может просматривать параметры системы и изменять их. Если значение установлено на ReadOnly, пользователь SNMPv3 может только просматривать информацию о параметрах. Режим доступа SNMPv3 может отличаться от режимов доступа CLI и Web.
SNMPv3 Authentication	Протокол аутентификации, закрепленный за определенным зарегистрированным пользователем.
SNMPv3 Encryption	Протокол шифрования, закрепленный за определенным зарегистрированным пользователем.

show users long

Отобразить полные имена сконфигурированных пользователей коммутатора.

Формат: `show users long`

Режим ввода команд: привилегированный режим

show users accounts

Отобразить статус локального пользователя с учетом блокировки учетных записей и устаревания пароля. Выводятся сокращенные имена пользователей. Используйте команду `show users long` для отображения полных имен пользователей.

Формат: `show users accounts [detail]`
Режим ввода команд: привилегированный режим

Параметр	*Описание*
User Name	Имя пользователя локального пользовательского аккаунта.
Access Level	Уровень доступа пользователя. 1 для непривилегированного доступа (switch>prompt) или 15 для доступа к высшему уровню привилегий (switch# prompt).
Password Aging	Количество дней с момента последней конфигурации пароля, по прошествии которых срок действия пароля истекает.
Password Expiry Date	Время устаревания пароля в формате даты.
Lockout	Показывает, заблокирован ли пользовательский аккаунт (true или false).

Если указан конкретный ключ шифрования, отображается следующее дополнительное поле.

Параметр	*Описание*
Password Override Complexity Check	Отображает статус проверки безопасности пароля пользователя. По умолчанию выключен.
Password Strength	Отображает безопасность пользовательского пароля (Strong или Weak). Данное поле отображается только в том случае, если параметр безопасности пароля включен.

show users login-history [long]

Показать информацию об истории подключений пользователей.

Формат: `show users login-history [long]`

Режим ввода команд: привилегированный режим

show users login-history [username]

Показать информацию об истории подключений пользователей.

Формат: `show users login-history [username` *`name`*`]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
name	Имя пользователя. Длина: 1-20 символов.

login authentication

Задать список методов аутентификации регистрационного имени для способа подключения (консоль, TELNET или SSH). Конфигурация по умолчанию использует набор методов по умолчанию с командой `aaa authentication login`.

Формат: `login authentication {default | list-name}`

Режим ввода команд: режим конфигурирования командной строки

Параметр	*Описание*
default	Использует список по умолчанию, создаваемый с командой `aaa authentication login`.
list-name	Использует указанный список, создаваемый с командой `aaa authentication login`.

no login authentication

Сбросить настройки к значениям по умолчанию, определяемым командой `authentication login`.

password

Данная команда позволяет авторизованным пользователям менять свои пароли, не имея 15 уровень привилегий.

Формат: `password cr`

Режим ввода команд: пользовательский режим

password (режим конфигурирования командной строки)

Используйте команду `password` в режиме конфигурирования командной строки для ввода пароля. Согласно настройкам конфигурации по умолчанию, пароль не требуется.

Формат: `password [password [encrypted]]`

Режим ввода команд: режим конфигурирования командной строки

Параметр	*Описание*
password	Пароль для данного уровня. Длина: 8-64 символа.
encrypted	Зашифрованный пароль для ввода, который копируется из другой конфигурации коммутатора. Длина зашифрованного пароля должна быть 128 символов, предполагается, что данный пароль уже зашифрован AES.

no password (режим конфигурирования командной строки)

Удалить пароль.

Формат `no password`

Режим ввода команд режим конфигурирования командной строки

password (пользовательский режим)

Данная команда используется для предоставления возможности пользователю менять только свой пароль. Данная команда используется после истечения срока действия пароля. Пользователю потребуется ввести старый и новый пароли.

Формат: `password`

Режим ввода команд: пользовательский режим

password (режим конфигурации пользователя IAS aaa)

Сконфигурировать пароль для пользователя. Опциональный параметр [encrypted] указывает, что пароль, заданный в команде, уже был предварительно зашифрован.

Формат: `password` *`password`* `[encrypted]`

Режим ввода команд: режим конфигурации пользователя IAS aaa

no password (режим конфигурации пользователя IAS aaa)

Отменить пароль для пользователя.

Формат: `no password`

Режим ввода команд: режим конфигурации пользователя IAS aaa

enable password (привилегированный режим)

Установить локальный пароль контроля доступа к привилегированному режиму.

Формат: `enable password [`*`password`* `[encrypted]]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
password	Строка пароля. Длина: 8-64 символов.
encrypted	Вводимый зашифрованный пароль, который копируется с другой конфигурации коммутатора. Зашифрованный пароль должен состоять из 128 символов, поскольку предполагается, что данный пароль уже зашифрован AES.

no enable password (привилегированный режим)

Отменить запрос пароля.

Формат: `no enable password`

Режим ввода команд: привилегированный режим

passwords min-length

Задать минимальную длину пароля для локального пользователя. Значение также подходит для пароля enable. Допустимы значения 8-64.

По умолчанию: 8

Формат: `passwords min-length` *`8-64`*

Режим ввода команд: режим глобальной конфигурации

no passwords min-length

Сбросить настройки минимальной длины пароля к значению по умолчанию.

Формат: `no passwords min-length`

Режим ввода команд: режим глобальной конфигурации

passwords history

Задать количество предыдущих паролей, сохраняющихся для каждого пользовательского аккаунта. Когда локальный пользователь меняет пароль, он не сможет повторно использовать пароль, который хранится в истории паролей. Таким образом, можно удостовериться, что пользователь не использует часто один и тот же пароль. Допустимые значения: 0-10.

Количество по умолчанию: 0

Формат: `passwords history` *`0-10`*

Режим ввода команд: режим глобальной конфигурации

no passwords history

Сбросить настройки истории паролей к значению по умолчанию.

Формат: `no passwords history`

Режим ввода команд: режим глобальной конфигурации

passwords aging

Настроить срок действия паролей локальных пользователей. Когда время действия пользовательского пароля истекает, пользователю потребуется сменить пароль перед повторным входом в систему. Допустимые значения 1-365. Значение по умолчанию – 0 (пароли не устаревают).

Значение по умолчанию: 0

Формат: `passwords aging` *`1-365`*

Режим ввода команд: режим глобальной конфигурации

no passwords aging

Сбросить настройки устаревания паролей к значению по умолчанию.

Формат: `no passwords aging`

Режим ввода команд: режим глобальной конфигурации

passwords lock-out

Данная команда используется для повышения безопасности коммутатора путем блокировки аккаунтов пользователей в случае неправильного ввода пароля. Когда устанавливается отсчет

блокировки, для входа в систему пользователю необходимо правильно ввести пароль за определенное число попыток. В противном случае, дальнейший доступ пользователя к коммутатору будет заблокирован. Только пользователь 15 уровня доступа может разблокировать заблокированный пользовательский аккаунт. Блокировка не применяется при авторизации с последовательной консоли. Допустимые значения: 1-5. Значение по умолчанию – 0 (блокировка не предусмотрена).

Значение по умолчанию: 0

Формат: `passwords lock-out` *`1-5`*

Режим ввода команд: режим глобальной конфигурации

no passwords lock-out

Сбросить настройки количества неверных попыток при вводе пароля к значению по умолчанию.

Формат: `no passwords lock-out`

Режим ввода команд: режим глобальной конфигурации

passwords strength-check

Включить проверку безопасности пароля. Она используется для подтверждения безопасности пароля в процессе его конфигурирования.

Значение по умолчанию: отключено

Формат: `passwords strength-check`

Режим ввода команд: режим глобальной конфигурации

no passwords strength-check

Сбросить настройки проверки надежности пароля к значению по умолчанию.

Формат: `no passwords strength-check`

Режим ввода команд: режим глобальной конфигурации

passwords strength maximum consecutive-characters

Настроить максимальное количество последовательных символов, которые используются для обеспечения безопасности пароля. Допустимые значения: 0-15. Значение по умолчанию – 0. Минимальное значение 0 означает отсутствие ограничений.

Значение по умолчанию: 0

Формат: `passwords strength maximum consecutive-characters` *`0-15`*

Режим ввода команд: режим глобальной конфигурации

passwords strength maximum repeated-characters

Настроить максимальное количество повторяющихся символов, допустимых к использованию, для обеспечения безопасности пароля. Допустимые значения: 0-15. Значение по умолчанию 0. Минимальное значение 0 означает отсутствие ограничений.

Значение по умолчанию: 0

Формат: `passwords strength maximum consecutive-characters` *`0-15`*

Режим ввода команд: режим глобальной конфигурации

passwords strength minimum uppercase-letters

Настроить минимальное количество символов верхнего регистра, которое должен содержать пароль. Допустимые значения: 0-16. Значение по умолчанию – 2. Минимальное значение 0 означает отсутствие ограничений.

Значение по умолчанию: 2

Формат: `passwords strength minimum uppercase-letters`

Режим ввода команд: режим глобальной конфигурации

no passwords strength minimum uppercase-letters

Сбросить минимально требуемое количество букв верхнего регистра в пароле к значению по умолчанию.

Формат: `no passwords minimum uppercase-letter`

Режим ввода команд: режим глобальной конфигурации

passwords strength minimum lowercase-letters

Настроить минимальное количество символов нижнего регистра, которое должен содержать пароль. Допустимые значения: 0-16. Значение по умолчанию – 2. Минимальное значение 0 означает отсутствие ограничений.

Значение по умолчанию: 2

Формат: `passwords strength minimum lowercase-letters`

Режим ввода команд: режим глобальной конфигурации

no passwords strength minimum lowercase-letters

Сбросить минимально требуемое количество букв нижнего регистра в пароле к значению по умолчанию.

Формат: `no passwords minimum lowercase-letter`

Режим ввода команд: режим глобальной конфигурации

passwords strength minimum numeric-characters

Настроить минимальное количество цифровых символов, которое должен содержать пароль. Допустимые значения: 0-16. Значение по умолчанию – 2. Минимальное значение 0 означает отсутствие ограничений.

Значение по умолчанию: 2

Формат: `passwords strength minimum numeric-characters`

Режим ввода команд: режим глобальной конфигурации

no passwords strength minimum numeric-characters

Сбросить минимально требуемое количество цифровых символов в пароле к значению по умолчанию.

Формат: `no passwords minimum numeric-characters`

Режим ввода команд: режим глобальной конфигурации

passwords strength minimum special-characters

Настроить минимальное количество специальных символов, которое должен содержать пароль. Допустимые значения: 0-16. Значение по умолчанию – 2. Минимальное значение 0 означает отсутствие ограничений.

Значение по умолчанию: 2

Формат: `passwords strength minimum special-characters`

Режим ввода команд: режим глобальной конфигурации

no passwords strength minimum special-characters

Сбросить минимально требуемое количество специальных символов в пароле к значению по умолчанию.

Формат: `no passwords minimum special-characters`

Режим ввода команд: режим глобальной конфигурации

passwords strength minimum character-classes

Настроить минимальное количество классов символов, которое должен содержать пароль. Класс символов включает в себя буквы верхнего регистра, буквы нижнего регистра, цифры и специальные символы. Допустимые значения: 0-4. Значение по умолчанию – 4.

Значение по умолчанию: 4

Формат: `passwords strength minimum character-classes`

Режим ввода команд: режим глобальной конфигурации

no passwords strength minimum character-classes

Сбросить минимально требуемое количество классов символов в пароле к значению по умолчанию.

Формат: `no passwords minimum character-classes`

Режим ввода команд: режим глобальной конфигурации

passwords strength exclude-keyword

Данная команда используется для исключения ключевого слова при конфигурировании пароля. Пароль не принимает ключевое слово в любой форме (внутри строки, не чувствительно к регистру и в обратной последовательности) как подстроку. Пользователь может сконфигурировать не более 3 ключевых слов.

Формат: `passwords strength exclude-keyword keyword`

Режим ввода команд: режим глобальной конфигурации

no passwords strength exclude-keyword

Сбросить ограничение для определенного конфигурируемого ключевого слова или всех конфигурируемых ключевых слов к значению по умолчанию.

Формат: `no passwords exclude-keyword [keyword]`

Режим ввода команд: режим глобальной конфигурации

show passwords configuration

Данная команда отображает настройки управления конфигурируемого пароля.

Формат: `show passwords configuration`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Minimum Password Length	Минимальное число символов, требуемое при смене паролей.
Password History	Число паролей, которые хранятся для предотвращения их повторного использования.
Password Aging	Временной промежуток в днях, в течение которого пароль является действительным.
Lockout Attempts	Число неудавшихся попыток авторизации, предпринятых перед блокировкой.
Minimum Password Uppercase Letters	Минимальное требуемое число символов верхнего регистра при конфигурации пароля.
Minimum Password Lowercase Letters	Минимальное требуемое число символов нижнего регистра при конфигурации пароля.
Minimum Password Numeric Characters	Минимальное требуемое число цифр при конфигурации пароля.
Maximum Password Consecutive Characters	Максимальная длина последовательности символов, которые допустима при конфигурации пароля.
Maximum Password Repeated Characters	Максимальное допустимое число повторяющихся символов при конфигурации пароля.
Minimum Password Character Classes	Минимальное допустимое число классов символов (верхнего регистра, нижнего регистра, цифр и специальных символов) при конфигурации пароля.
Password Exclude-Keywords	Набор ключевых слов, исключаемых из конфигурируемого пароля при активной опции проверки надежности пароля.

show passwords result

Отобразить последнюю информацию о состоянии паролей.

Формат: `show passwords result`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Last User Whose Password Is Set	Отображает имя последнего пользователя, который вводил пароль.
Password Strength Check	Показывает, активна ли проверка безопасности пароля.
Last Password Set Result	Показывает, была ли успешной попытка ввода пароля. Если попытка провалилась, будет указана причина.

aaa accounting

Используйте эту команду в режиме глобальной конфигурации, чтобы создать список методов учета для сессий пользовательского режима, пользовательских команд или DOT1X. Этот список определяется параметром "**default**" (по умолчанию) или заданным пользователем параметром "**list_name**" (имя списка). Запись учета может быть отправлена в начале и в конце (**start-stop**) или только в конце (**stop-only**). Если ни один не определен, то учет отключен для указанного списка. Если **tacacs** определен как метод учета, записи учёта регистрируются на **TACACS+** сервере. Если **radius** – указанный метод учета, записи учета регистрируются на сервере **RADIUS**.

- **Может быть создано до 5 списков методов учёта для каждого режима выполнения и типа команд.**
- **Для DOT1X может быть создан только один список метода учёта по умолчанию. Более одного списка создать невозможно.**
- **Один и тот же список имен может быть использован для учета пользовательского режима и команд**
- **AAA-учёт команд не поддерживает RADIUS в качестве метода учёта.**
- **Start-stop или None – единственные режимы, поддерживающие типы записи для учёта DOT1X. Start-stop активирует учёт, а None – отключает.**
- **RADIUS – единственный тип метода учёта, поддерживаемый для учета DOT1X.**

Формат: `aaa accounting {exec | commands | dot1x} {default | list_name} {start-stop | stop- only |none}` *`method1`* `[`*`method2`*`…]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
exec	Предоставляет учет для терминальных сессий пользовательского режима.
commands	Обеспечивает учет всех выполненных команд пользователя.
dot1x	Обеспечивает учет DOT1X.
default	Список методов учета по умолчанию.
list-name	Символьная строка – имя списка методов учета.
start-stop	Отправляет уведомление о начале учета в начале процесса и уведомление об остановке учета при завершении процесса.
stop-only	Отправляет уведомление об остановке учета при завершении пользовательского процесса.
none	Отключает учетный сервис.
method	Используйте сервер TACACS или RADIUS в целях учета.

Администратор может изменить тип записи или список методов для существующего набора типов учёта и имени списка, удаление предыдущей конфигурации при этом не требуется.

```
(Routing) #
(Routing) #configure
(Routing) #aaa accounting exec ExecList stop-only tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs
(Routing) #aaa accounting exec ExecList start-stop tacacs radius
```

Первая **aaa** команда создает список методов для сессий пользовательского режима с именем ExecList, типом записи **record-type**, указанным как `stop-only`, и методом **method** – как TACACS+. Вторая команда изменяет **record type** на `start-stop` со `stop-only` для того же списка методов. Третья команда для того же списка изменяет список методов с {*tacacs*} на {*tacacs, radius*}.

no aaa accounting

Удалить список методов учёта.

Формат: `no aaa accounting {exec | commands | dot1x} {default | list_name default}`

Режим ввода команд: режим глобальной конфигурации

aaa accounting update

Используйте эту команду для настройки промежуточных записей журнала учета.

Значение по умолчанию: newinfo: Выключено

Periodic: 5 минут

Формат: `aaa accounting update [newinfo [periodic 1-200] | periodic 1-200]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
newinfo	Указывает, что обновления должны отправляться на RADIUS-сервер каждый раз, когда появляется новая информация, например «Повторная аутентификация клиента».
periodic	Интервал отправки промежуточных записей журнала учета в минутах.

no aaa accounting update

Эта команда сбрасывает настройки отправки промежуточных записей журнала учета.

Формат: `no aaa accounting update`

Режим ввода команд: глобальная конфигурация

Пример:

```
(Routing) #configure
(Routing) (Config)#aaa accounting update newinfo periodic 20
```

accounting

Используйте эту команду в режиме конфигурирования командной строки, чтобы применить список методов учета к способам доступа (консоль / telnet / ssh).

Формат: `accounting {exec | commands } {default | listname}`

Режим ввода команд: режим конфигурирования командной строки

Параметр	*Описание*
exec	Только для начала/завершения сессии.
commands	Для каждой введённой команды. Если пользователь включит режим учета пользовательского режима для текущего типа конфигурации командной строки, он выйдет из системы.
default	Список учёта по умолчанию.
listname	Название списка. Строка не длиннее 15 символов.

no accounting

Прекратить учет в режиме конфигурирования командной строки.

Формат: `no accounting {exec|commands]`

Режим ввода команд: Line Config

show accounting

Вывести на экран перечень методов для списков учета.

Формат: `show accounting`

Режим ввода команд: привилегированный режим

show accounting methods

Вывести на экран сконфигурированные списки методов учета.

Формат: `show accounting methods`

Режим ввода команд: привилегированный режим

clear accounting statistics

Очистить статистику учёта.

Формат: `clear accounting statistics`

Режим ввода команд: привилегированный режим

show domain-name

Показать сконфигурированное имя домена.

Формат: `show domain-name`

Режим ввода команд: привилегированный режим

aaa ias-user username

База данных IAS является особой внутренней базой, используемой для локальной идентификации пользователей для доступа к сети через функцию IEEE 802.1X.

Используйте команду `aaa ias-user username` в режиме глобальной конфигурации, чтобы добавить определенного пользователя в базу данных. Данная команда также производит переключение на режим конфигурации пользователя AAA.

Формат: `aaa ias-user username` *`user`*

Режим ввода команд: режим глобальной конфигурации

no aaa ias-user username

Убрать определённого пользователя из базы данных.

Формат: `no aaa ias-user username` *`user`*

Режим ввода команд: режим глобальной конфигурации

aaa session-id

Используйте команду в режиме глобальной конфигурации, чтобы определить, какой идентификатор используется для сессии AAA.

По умолчанию: `common`

Формат: `aaa session-id [common | unique]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
common	Использовать единый идентификатор сессии для всех типов обслуживания AAA.
unique	Использовать отдельный идентификатор сессии для каждого типа обслуживания AAA.

no aaa session-id

Используйте команду в режиме глобальной конфигурации для сброса идентификатор сессии aaa к значению по умолчанию.

Формат: `no aaa session-id [unique]`

Режим ввода команд: режим глобальной конфигурации

password (режим конфигурации пользователя IAS aaa)

Сконфигурировать пароль для пользователя в базе данных IAS. Дополнительный параметр `encrypted` указывает, что пароль уже предварительно зашифрован.

Формат: `password` *`password`* `[encrypted]`

Режим ввода команд: AAA IAS User Config

Параметр	*Описание*
password	Пароль для этого уровня: 8-64 знака.

encrypted	Зашифрованный пароль, который может быть введён или скопирован с конфигурации другого коммутатора.

no password (режим конфигурации пользователя IAS aaa)

Убрать пароль для пользователя.

Формат: `no password`

Режим ввода команд: режим конфигурации пользователя IAS AAA

clear aaa ias-users

Удалить всех пользователей из базы данных IAS.

Формат: `clear aaa ias-users`

Режим ввода команд: привилегированный режим

Параметр	*Определение*
password	Пароль для этого уровня: 8-64 знака.
encrypted	Зашифрованный пароль, который может быть введён или скопирован с конфигурации другого коммутатора.

show aaa ias-users

Показать сконфигурированных пользователей IAS и их атрибуты. Данная show-команда не показывает сконфигурированные пароли.

Формат: `show aaa ias-users [username]`

Режим ввода команд: привилегированный режим

8.9 Команды настройки протокола SNMP

Данный подраздел содержит описание команд конфигурирования протокола SNMP. Вы можете сконфигурировать коммутатор как агент SNMP, чтобы он мог связаться с SNMP-менеджерами вашей сети.

snmp-server

Настроить имя и физическое расположение коммутатора и организации, ответственной за сеть. Параметры `name`, `loc` и `con` могут включать в себя до 255 символов каждый.

Значение по умолчанию: нет

Формат: `snmp-server {sysname` *`name`* `|` `location` *`loc`* `|` `contact` *`con`*`}`

Режим ввода команд: режим глобальной конфигурации

Чтобы очистить snmp-сервер, введите пустую строку в кавычках. Например, команда `snmp-server {sysname “ “}` очищает имя системы.

snmp-server community

Эта команда добавляет (и именует) новое SNMP-сообщество; опциональные параметры устанавливают режим доступа, допустимый IP-адрес и представление для сообщества.

Имена сообщества в таблице SNMP-сообщества (SNMP Community Table) должны быть уникальными. При создании нескольких записей под одним и тем же именем сообщества первая запись сохраняется и обрабатывается, все дублирующие записи игнорируются.

Значение по умолчанию: Два вида сообщества могут быть созданы по умолчанию:

- публичное (public), с полномочиями «только для чтения», именем представления по умолчанию и предоставлением доступа со всех IP-адресов
- приватное (private), с полномочиями «чтения-записи», именем представления по умолчанию и предоставлением доступа со всех IP-адресов.

Формат: `snmp-server community` *`community-string`* `[{ro | rw |su }] [ipaddress` *`ip-address`*`] [view` *`view-name`*`]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
community-name	Имя, связанное с коммутатором и с рядом SNMP-менеджеров, которые управляют им в привилегированном режиме. Длина имени сообщества – до 16 символов (чувствительно к регистру).
ro | rw | su	Режим доступа SNMP-сообщества: может быть публичным (Read-Only/RO), приватным (Read-Write/RW) или Super User (SU).
ip-address	Адрес отправки пакета SNMP-сообщества, используемый вместе с клиентским значением маски IP, чтобы обозначить диапазон IP-адресов, от которых SNMP-клиенты могут получать доступ к устройству через данное сообщество. Значение 0.0.0.0 предоставляет доступ с любого IP-адреса. Для того, чтобы задать диапазон IP-адресов допустимых клиентов, объедините это значение с маской, используя операцию И (AND).
view-name	Имя представления для создания и обновления.

no snmp-server community

Удалить SNMP-сообщество из таблицы. *Name* – имя сообщества, которое будет удалено.

Формат: `no snmp-server community` *`community-name`*

Режим ввода команд: режим глобальной конфигурации

snmp-server community-group

Сконфигурировать сообщество, связанное с группой, чтобы разрешить доступ через протоколы SNMPv1 и SNMPv2c.

Формат: `snmp-server community-group` *`community-string group-name`* `[ipaddress` *`ipaddress`*`]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
community- string	Сообщество, которое создано и затем связано с группой. Диапазон: 1-20 символов.
group-name	Имя группы, с которой связано сообщество. Диапазон: 1-30 символов.
ipaddress	Опциональный параметр. IPv4-адрес, с которого может быть осуществлен доступ к сообществу.

snmp-server enable traps violation

Компонент привязки MAC к порту настраивает отправку SNMP-трапа при обнаружении нарушения, с частотой по умолчанию – 30 секунд. При выполнении в глобальном режиме данная команда конфигурирует режим отсылки трапов при нарушениях на всех интерфейсах с поддержкой защищенных портов. Глобальный режим конфигурирования трапа не существует как таковой.

Значение по умолчанию: отключено

Формат: `snmp-server enable traps violation`

Режим ввода команд: режим глобальной конфигурации

режим конфигурирования интерфейса

no snmp-server enable traps violation

Отключить отправку новых трапов о нарушениях.

Формат: `no snmp-server enable traps violation`

Режим ввода команд: режим конфигурирования интерфейса

snmp-server enable traps

Включить флаг аутентификации.

Значение по умолчанию: включено

Формат: `snmp-server enable traps`

Режим ввода команд: режим глобальной конфигурации

no snmp-server enable traps

Выключить флаг аутентификации.

Формат: `no snmp-server enable traps`

Режим ввода команд: режим глобальной конфигурации

snmp-server enable traps bgp

Опция bgp в вышеприведенной команде `snmp-server enable traps` включает два трапа, определённых в стандарте BGP MIB, RFC 4273. Трап отправляется, когда соседство достигает состояния УСТАНОВЛЕНО (ESTABLISHED) и когда происходит обратное изменение состояния соседства.

Значение по умолчанию: BGP-трапы по умолчанию выключены.

Формат: `snmp-server enable traps bgp state-changes limited`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
state-changes limited	Включает стандартные трапы, определённые в RFC 4273

no snmp-server enable traps bgp state-changes limited

Выключить два трапа, определенных в стандарте BGP MIB, RFC 4273.

Формат: `no snmp-server enable traps bgp state-changes limited`

Режим ввода команд: режим глобальной конфигурации

snmp-server enable traps fip-snooping

Включить трапы отслеживания протокола FIP (FCoE Initialization Protocol) для всего коммутатора. Когда данная опция включена, трапы соединений отправляются, только если в настройках порта включен флаг Link Trap. См. раздел `show snmp`.

Значение по умолчанию: включено

Формат: `snmp-server enable traps fip-snooping`

Режим ввода команд: режим глобальной конфигурации

no snmp-server enable traps fip-snooping

Выключить трапы отслеживания протокола FIP (FCoE Initialization Protocol) на всем коммутаторе.

Значение по умолчанию: включено

Формат: `no snmp-server enable traps fip-snooping`

Режим ввода команд: режим глобальной конфигурации

snmp-server port

Настроить номер слушающего UDP-порта SNMP-сервера.

Значение по умолчанию: 161

Формат: `snmp-server port` *`1025-65535`*

Режим ввода команд: привилегированный режим

no snmp-server port

Сбросить настройки слушающего порта SNMP-сервера к значению по умолчанию.

Формат: `no snmp-server port`

Режим ввода команд: привилегированный режим

snmp trap link-status

Включить трапы статуса соединения на интерфейсе или диапазоне интерфейсов.

Команда доступна только при включенном флаге Link Up/Down Flag.

Формат: `snmp trap link-status`

Режим ввода команд: режим конфигурирования интерфейса

no snmp trap link-status

Выключить трапы статуса соединения, отправляемые интерфейсом.

Команда доступна только при включенном флаге Link Up/Down Flag.

Формат: `no snmp trap link-status`

Режим ввода команд: режим конфигурирования интерфейса

snmp trap link-status all

Включить трапы статуса соединения для всех интерфейсов.

Команда доступна только при включенном флаге Link Up/Down Flag.

Формат: `snmp trap link-status all`

Режим ввода команд: режим глобальной конфигурации

no snmp trap link-status all

Выключить трапы статуса соединения для всех интерфейсов.

Команда доступна только при включенном флаге Link Up/Down Flag.

Формат: `no snmp trap link-status all`

Режим ввода команд: режим глобальной конфигурации

snmp-server enable traps linkmode

Команда доступна только при включенном флаге Link Up/Down Flag.

Включить трапы с флагами Link Up/Down для всего коммутатора. Когда команда включена, трапы соединения отправляются только при установке флага Link Trap, связанного с портом.

Значение по умолчанию: включено

Формат: `snmp-server enable traps linkmode`

Режим ввода команд: режим глобальной конфигурации

no snmp-server enable traps linkmode

Выключить трапы с флагами Link Up/Down для всего коммутатора.

Формат: `no snmp-server enable traps linkmode`

Режим ввода команд: режим глобальной конфигурации

snmp-server enable traps multiusers

Включить многопользовательские трапы (Multiple User Trap). Если опция включена, то многопользовательский трап отправляется, когда пользователь входит в систему терминального интерфейса (EIA 232 или Telnet) при уже открытой сессии терминального интерфейса.

Значение по умолчанию: включено

Формат: `snmp-server enable traps multiusers`

Режим ввода команд: режим глобальной конфигурации

no snmp-server enable traps multiusers

Выключить многопользовательские трапы.

Формат: `no snmp-server enable traps multiusers`

Режим ввода команд: режим глобальной конфигурации

snmp-server enable traps stpmode

Включить отправку трапов об изучении новых путей (new root) и трапов уведомления об изменении топологии.

Значение по умолчанию: включено

Формат: `snmp-server enable traps stpmode`

Режим ввода команд: режим глобальной конфигурации

no snmp-server enable traps stpmode

Выключить отправку трапов об изучении новых путей (new root) и трапов уведомления об изменении топологии.

Формат: `no snmp-server enable traps stpmode`

Режим ввода команд: режим глобальной конфигурации

snmp-server engineID local

Сконфигурировать engine ID протокола SNMP на локальном устройстве.

Значение по умолчанию: engineID конфигурируется автоматически, основываясь на MAC-адресе устройства.

Формат: `snmp-server engineID local {engineid-string|default}`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
engineid-string	Шестнадцатеричная строка, идентифицирующая engine-id, используемая для локализации конфигурации. Длина engine-id должна составлять 6-32 шестнадцатеричных символов.
Default	Сбрасывает параметр engine-id к значению по умолчанию, получаемому на основе MAC-адреса устройства.

Изменение engine-id аннулирует всю конфигурацию SNMP.

no snmp-server engineID local

Удалить заданный engine ID.

Значение по умолчанию: engineID конфигурируется автоматически, основываясь на MAC адресе устройства.

Формат: `no snmp-server engineID local`

Режим ввода команд: режим глобальной конфигурации

snmp-server filter

Создать фильтрующую запись для ограничения трапов, определенных OID-Tree, отправляемых на главный интерфейс.

Значение по умолчанию: нет фильтров по умолчанию.

Формат: `snmp-server filter filtername oid-tree {included|excluded}`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
filtername	Метка создаваемого фильтра. Диапазон: 1-30 символов.
oid-tree	Поддерево OID для включения или исключения из фильтра. Поддеревья могут быть определены числительными (1.3.6.2.4) или ключевыми словами (system), также могут использоваться звездочки (символ *), чтобы определить семью поддерева (1.3. *.4).
included	Дерево добавлено в фильтр.
excluded	Дерево исключено из фильтра.

no snmp-server filter

Удалить заданный фильтр.

Значение по умолчанию: нет фильтров по умолчанию.

Формат: `snmp-server filter filtername [oid-tree]`

Режим ввода команд: режим глобальной конфигурации

snmp-server group

Создать группу доступа SNMP.

Значение по умолчанию: универсальные группы создаются для всех версий и полномочий. Используется представление по умолчанию.

Формат: `snmp-server group` *`group-name`* `{v1 | v2c | v3 {noauth | auth | priv}} [context` *`context- name`*`] [read` *`read-view`*`] [write` *`write-view`*`] [notify` *`notify-view`*`]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
group-name	Название группы, которое будет использоваться при конфигурировании сообществ или пользователей. Диапазон: 1-30 символов.
v1	Доступ к группе возможен только через SNMPv1.
v2	Доступ к группе возможен только через SNMPv2c
v3	Доступ к группе возможен только через SNMPv3.
noauth	К этой группе можно получить доступ только при выключенных опциях аутентификации или шифрования. Применимо, только если выбран SNMPv3 протокол.
auth	К этой группе можно получить доступ, только если опция аутентификации включена, а опция шифрования – выключена. Применимо, только если выбран SNMPv3-протокол.
priv	К этой группе можно получить доступ, только если одновременно включены опции аутентификации и шифрования. Применимо, только если выбран SNMPv3-протокол.
context-name	Контекст SNMPv3, используемый во время доступа. Применимо, только если выбран SNMPv3-протокол.
read-view	Представление группы при GET-запросах. Диапазон: 1-30 символов.
write-view	Представление группы при SET-запросах. Диапазон: 1-30 символов.
notify-view	Представление группы при отсылке трапов. Диапазон: 1-30 символов.

no snmp-server group

Удалить указанную группу.

Формат: `no snmp-server group` *`group-name`* `{v1|v2c| 3 {no-auth|auth|priv}} [context context-name]`

Режим ввода команд: режим глобальной конфигурации

snmp-server host

Сконфигурировать запись узла для отправки трапов.

Значение по умолчанию: нет сконфигурированных по умолчанию узлов.

Формат: `snmp-server host host-addr {informs [timeout seconds] [retries retries]|traps version {1 | 2c }} community-string [udp-port port] [filter filter-name]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
host-addr	IPv4- или IPv6-адрес узла для отправки трапа или сообщения.
traps	Отправляет узлу SNMP-трапы. Опция выбрана по умолчанию.
version 1	Отправляет SNMPv1-трапы. Опция не доступна, если выбрана опция "informs".
version 2	Отправляет SNMPv2c-трапы. Опция не доступна, если выбрана опция "informs". Опция по умолчанию.
informs	Отправить узлу SNMPv2-inform.
seconds	Количество секунд ожидания перед повторной отправкой сообщения. Значение по умолчанию составляет 15 секунд. Диапазон: 1-300 секунд.
retries	Число повторных отправок сообщения. Значение по умолчанию: 3 попытки. Диапазон: 0-255 (попыток).
community- string	Строка сообщества отправлена как часть уведомления. Диапазон: 1-20 символов.
port	Порт получателя SNMP-трапа. Значение по умолчанию: порт 162.
filter-name	Имя фильтра для связи с узлом. Фильтры могут использоваться, чтобы определить, какие трапы отправлены на этот узел. Диапазон: 1-30 символов.

no snmp-server host

Удалить запись указанного узла.

Формат: `no snmp-server host host-addr [traps|informs]`

Режим ввода команд: режим глобальной конфигурации

snmp-server user

Создать SNMPv3-пользователя для доступа к системе.

Значение по умолчанию: нет пользователей по умолчанию.

Формат: `snmp-server user username groupname [remote engineid-string] [ {auth-md5 password | auth-sha password | auth-md5-key md5-key | auth-sha-key sha-key} [priv-des password | priv-des-key des-key]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
username	Имя SNMPv3-пользователя для соединения с коммутатором. Диапазон: 1-30 символов.
group-name	Имя группы, к которой принадлежит пользователь. Диапазон: 1-30 символов.

Engineid-string	Идентификатор удаленной станции управления, с которой пользователь производит запрос. Диапазон: 5-32 символа.
password	Пароль, который пользователь будет использовать для шифрования или аутентификации. Диапазон:1-32 символа.
md5-key	Предварительно сгенерированный ключ аутентификации MD5. Длина – 32 символа.
sha-key	Предварительно сгенерированный ключ аутентификации SHA. Длина – 48 символов.
des-key	Предварительно сгенерированный ключ шифрования DES. Длина – 32 символа, если выбран MD5, и 48 символов, если выбран SHA.

no snmp-server user

Удалить указанного SNMPv3-пользователя.

Формат: `no snmp-server user` *`username`*

Режим ввода команд: режим глобальной конфигурации

snmp-server view

Создать или изменить запись представления, которая используется группами для определения, к каким объектам может получить доступ сообщество или пользователь.

Значение по умолчанию: представление создается по умолчанию для обеспечения доступа к группам по умолчанию.

Формат: `snmp-server` *`viewname oid-tree`* `{included|excluded}`

Режим ввода команд: режим глобальной конфигурации

Параметр	Описание
viewname	Метка для создаваемого представления. Диапазон: 1-30 символов.
oid-tree	Поддерево OID для включения или исключения из просмотра. Поддеревья могут быть определены числительными (1.3.6.2.4) или ключевыми словами (system), также могут использоваться звездочки (символ *), чтобы определить семейство поддерева (1.3.*.4).
included	Дерево добавлено в режим просмотра.
excluded	Дерево исключено из режима просмотра.

no snmp-server view

Удалить заданное представление.

Формат: `no snmp-server view` *`viewname`* [*`oid-tree`*]

Режим ввода команд: режим глобальной конфигурации

snmp-server v3-host

Сконфигурировать запись узла для отправки трапов.

Значение по умолчанию: нет узлов по умолчанию.

Формат: `snmp-server v3-host host-addr username [traps | informs [timeout seconds] [retries retries]] [auth | noauth | priv] [udpport port] [filter filtername]`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
host-addr	IPv4- или IPv6-адрес узла назначения отправления трапа или сообщения.
user-name	Пользователь, ранее отправлявший трап или сообщение. Этот пользователь должен принадлежать к группе, которая поддерживает версию и метод доступа. Диапазон: 1-30 символов.
traps	SNMP-трапы, отправленные на узел. Опция по умолчанию.
informs	SNMP-сообщения, отправленные на узел.
seconds	Число секунд ожидания подтверждения перед повторной отправкой сообщения. По умолчанию – 15 секунд. Диапазон составляет 1-300 секунд.
retries	Число попыток повторной отправки сообщения. По умолчанию: 3 попытки. Диапазон: 0-255 (повторов).
auth	Включает аутентификацию, но не шифрование.
noauth	Без аутентификации и шифрования. Значение по умолчанию.
priv	Включает аутентификацию и шифрование.
port	Порт получателя SNMP-трапа. Значение по умолчанию: порт 162.
filter-name	Имя фильтра, чтобы связаться с этим узлом. Фильтры могут использоваться, чтобы определить, какие трапы отправлены на этот узел. Диапазон: 1-30 символов.

snmptrap source-interface

Используйте эту команду в режиме глобальной конфигурации, чтобы сконфигурировать глобальный исходящий интерфейс (IP-адрес источника) для SNMP-соединений между клиентом SNMP и сервером.

Формат: `snmptrap source-interface {unit/slot/port | loopback loopback-id | tunnel tunnel- id|vlan vlan-id | serviceport | network}`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
unit/slot/port	Использовать IP-адрес физического интерфейса в качестве IP-адреса источника SNMP-сообщений.
loopback-id	Использовать IP-адрес loopback-интерфейса в качестве IP-адреса источника SNMP-сообщений. Диапазон идентификатора loopback от 0 до 7.
tunnel-id	Использовать IP-адрес физического интерфейса в качестве IP-адреса источника SNMP-сообщений. Диапазон туннельного ID от 0 до 7.
vlan-id	Использовать IP-адрес VLAN-интерфейса в качестве IP-адреса источника SNMP-сообщений. Диапазон ID VLAN: 1-4093.

serviceport	Использовать IP-адрес OOB-интерфейса в качестве IP-адреса источника SNMP-сообщений.
network	Использовать IP-адрес интерфейса управления в качестве IP-адреса источника SNMP-сообщений.

no snmptrap source-interface

Используйте эту команду в режиме глобальной конфигурации, чтобы удалить глобальный исходный интерфейс (IP источника) для всех SNMP-соединений между SNMP-клиентом и сервером.

Формат: `no snmptrap source-interface`

Режим ввода команд: режим глобальной конфигурации

snmptrap ipaddr snmpversion[1]

Изменить SNMP-версию трапа. Максимальная длина имени – 16 чувствительных к регистру алфавитно-цифровых символов. Возможные значения параметра *snmpversion*: snmpv1 или snmpv2.

У данной команды нет отрицательной формы.

Формат: `snmptrap ipaddr snmpversion` *`name snmpversion`*

Режим ввода команд: режим глобальной конфигурации

snmptrap ip6addr snmpversion[1]

Изменить SNMP-версию трапа. Максимальная длина параметра *name* – 16 чувствительных к регистру алфавитно-цифровых символов. Допустимые значения параметра *snmpversion*: snmpv1 или snmpv2.

У данной команды нет отрицательной формы.

Формат: `snmptrap ip6addr snmpversion` *`name snmpversion`*

Режим ввода команд: режим глобальной конфигурации

show snmp

Вывести на экран текущую конфигурацию SNMP.

Формат: `show snmp`

Режим ввода команд: привилегированный режим

[1] Не поддерживается в текущей версии ПО.

Параметр		*Описание*
Community Table	**Community- String**	Название сообщества для записи. Используется протоколами SNMPv1 и SNMPv2 для получения доступа к коммутатору.
	Community- Access	Типы доступа: • Только для чтения (ro/Read only); • Чтение и запись (rw/Read write); • Супер пользователь (su/Super User).
	View Name	Представление, к которому имеет доступ сообщество.
	IP Address	Доступ к сообществу ограничен этим IP-адресом.
Community Group Table	**Community-String**	Сообщество, конфигурируемое маппингом.
	Group Name	Группа, к которой относится сообщество.
	IP Address	IP-адрес, которым ограничено сообществом.
Host Table	**Target Address**	Адрес узла, куда должны быть отправлены трапы.
	Type	Тип сообщения для отправки (трапы или информация).
	Community	Сообщество, которому будут отправлены трапы.
	Version	SNMP-версия трапа.
	UDP Port	UDP-порт, которому будет отправлен трап или информация.
	Filter name	Фильтр, ограничивающий трапы для этого узла.
	TO Sec	Количество секунд до истечения времени жизни информационного сообщения, отправленного на этот узел.
	Retries	Количество отправлений информационных сообщений после истечения времени жизни.

show snmp engineID

Отобразить текущую конфигурацию engineID протокола SNMP.

Формат: `show snmp engineID`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Local SNMP EnginID	Текущая конфигурация отображенного SNMP engineID.

show snmp filters

Отобразить сконфигурированные фильтры, используемые при отправке трапов.

Формат: `show snmp filters [`*`filtername`*`]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Name	Имя фильтра для данной записи.
OID Tree	OID-дерево будет включено или исключено для данной точки входа.

Type	Определяет, включает ли эта запись OID-дерево.

show snmp group

Отобразить сконфигурированные группы.

Формат: `show snmp group [`*`groupname`*`]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Name	Имя группы.
Security Model	Указывает, какой протокол может получить доступ к системе через эту группу.
Security Level	Указывает степень защиты, допустимой для этой группы.
Read View	Представление, обладающее правом чтения.
Write View	Представление, обладающее правом записи.
Notify View	Представление, обладающее правом доступа к трапам.

show snmp-server

Отобразить текущую пользовательскую конфигурацию SNMP-сервера.

Формат: `show snmp-server`

Режим ввода команд: привилегированный режим

show snmp source-interface

Используйте данную команду в привилегированном режиме для отображения деталей глобального исходящего интерфейса (IP-адрес источника), сконфигурированного для SNMP-клиента.

Формат: `show snmp source-interface`

Режим ввода команд: привилегированный режим

show snmp user

Отобразить SNMPv3-пользователей, сконфигурированных в текущий момент.

Формат: `show snmp user [`*`username`*`]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Name	Имя пользователя.
Group Name	Имя группы, определяющей параметры SNMPv3-доступа.
Auth Method	Аутентификационный алгоритм, сконфигурированный для этого пользователя.
Privilege Method	Алгоритм шифрования, сконфигурированный для этого пользователя.
Remote Engine ID	engineID для пользователя, определяемого на машине клиента.

show snmp views

Вывести на экран сконфигурированные в текущий момент представления.

Формат: `show snmp views [viewname]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Name	Имя представления для данной записи.
OID Tree	Дерево OID, которое эта запись будет включать или исключать.
Type	Указывает, включает или исключает эта запись дерево OID.

show trapflags

Команда выводит на экран условия генерации трапов. Показывает все включенные флаги OSPFv2 и OSPFv3. Генерация трапов настраивается с помощью включения/отключения тех или иных условий. Если включено условие отправки трапа и обнаружено соответствие этому условию, SNMP-агент на коммутаторе отправляет трап на все разрешенные серверы. Для активации изменений рестарт коммутатора не требуется. Трапы "холодного" и "теплого" запуска всегда генерируются и не могут быть отключены.

Формат: `show trapflags`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Authentication Flag	Может быть enabled (включено) или disabled (отключено). По умолчанию: enabled (включено). Определяет, отправляются ли трапы ошибки аутентификации.
Link Up/Down Flag	Может быть включено/отключено. По умолчанию: enabled (включено). Определяет, отправляются ли трапы состояния соединения.
Multiple Users Flag	Может быть включено/отключено. По умолчанию: enabled (включено). Определяет, отправляются ли трапы, когда тот же ID пользователя регистрируется на коммутаторе несколько раз одновременно (через Telnet или последовательный порт).
Spanning Tree Flag	Может быть включено/отключено. По умолчанию: enabled (включено). Определяет, отправляются ли STP-трапы.
ACL Traps	Может быть включено/отключено. По умолчанию: disabled (отключено). Определяет, отправляются ли ACL-трапы.
BGP4 Traps	Может быть включено/отключено. По умолчанию: disabled (отключено). Определяет, отправляются ли BGP4-трапы. (Это поле появляется только на системах с установленным BGPv4-пакетом ПО.)
OSPFv2 Traps	Может быть включено/отключено. По умолчанию: disabled (отключено). Определяет, отправляются ли OSPF-трапы. Если какой-либо из флагов OSPF-трапов не включен, команда отображает disabled. В ином случае, команда показывает всю разрешенную информацию о OSPF-трапах.
OSPFv3 Traps	Может быть включено/отключено. По умолчанию: disabled (отключено). Определяет, отправляются ли OSPF-трапы. Если какой-либо из флагов OSPFv3-трапов не включен, команда отображает disabled. В ином случае, команда показывает всю разрешенную информацию о OSPFv3-трапах.

8.10 Команды настройки протокола RADIUS

В данном подразделе описываются команды конфигурации коммутатора для использования RADIUS-сервера для процедур аутентификации и учёта в вашей сети.

aaa server radius dynamic-author

Данная команда включает CoA и запускает режим конфигурирования локального сервера динамической авторизации.

Значение по умолчанию: нет

Формат: `aaa server radius dynamic-author`

Режим ввода команд: режим глобальной конфигурации

no aaa server radius dynamic-author

Выключить CoA.

Значение по умолчанию: нет

Формат: `no aaa server radius dynamic-author`

Режим ввода команд: режим глобальной конфигурации

authentication command bounce-port ignore

Данная команда запрещает обработку системой команд bounce-host-port от RADIUS-сервера. Команда bounce-host-port заставляет устройство сбрасывать соединение на аутентифицированном порте.

Значение по умолчанию: выключен

Формат: `authentication command bounce-port ignore`

Режим ввода команд: режим глобальной конфигурации

no authentication command bounce-port ignore

Данная команда отменяет запрет на обработку системой команд bounce-host-port от RADIUS-сервера.

Формат: `no authentication command bounce-port ignore`

Режим ввода команд: режим глобальной конфигурации

auth-type

Задать тип авторизации, используемый устройством для RADIUS-клиентов. Для успешной авторизации клиент должен соответствовать сконфигурированным атрибутам.

Значение по умолчанию: All

Формат: `auth-type { any | all | session-key }`

Режим ввода команд: режим динамической авторизации

no auth-type

Сбросить тип авторизации, используемый устройством для RADIUS-клиентов.

Значение по умолчанию: нет

Формат: `no auth-type`

Режим ввода команд: режим динамической авторизации

authorization network radius

Разрешить коммутатору принимать назначение VLAN от RADIUS-сервера.

Значение по умолчанию: выключено

Формат: `authorization network radius`

Режим ввода команд: режим глобальной конфигурации

no authorization network radius

Запретить коммутатору принимать назначение VLAN от RADIUS-сервера.

Формат: `no authorization network radius`

Режим ввода команд: режим глобальной конфигурации

clear radius dynamic-author statistics

Очистить статистику счетчиков динамической авторизации RADIUS.

Значение по умолчанию: none

Формат: `clear radius dynamic-author statistics`

Режим ввода команд: привилегированный режим

client

Сконфигурировать IP-адрес или имя узла клиента сервера AAA. Используйте опциональное ключевое слово server-key и параметр key-string, чтобы сконфигурировать ключ сервера на уровне клиента.

Значение по умолчанию: нет

Формат: `client { ip-address | hostname } [server-key [0|7] key-string]`

Режим ввода команд: режим динамической авторизации

no client

Удалить сконфигурированный клиент динамической авторизации и ключ, связанный с этим клиентом на данном устройстве.

Значение по умолчанию: нет

Формат: `no client { ip-address | hostname }`

Режим ввода команд: режим динамической авторизации

debug aaa coa

Отобразить информацию по отладке работы сервера динамической авторизации.

Значение по умолчанию: нет

Формат: `debug aaa coa`

Режим ввода команд: режим динамической авторизации

debug aaa pod

Просмотреть пакеты сообщений о разъединении (Disconnect Message).

Значение по умолчанию: нет

Формат: `debug aaa pod`

Режим ввода команд: режим динамической авторизации

ignore server-key

Опциональная команда, задающая игнорирование ключа сервера устройством.

Значение по умолчанию: отключено

Формат: `ignore server-key`

Режим ввода команды: режим динамической авторизации

no ignore server-key

Прекратить игнорирование ключа сервера на данном устройстве. Опциональная команда.

Значение по умолчанию: выключено

Формат: `no ignore server-key`

Режим ввода команды: режим динамической авторизации

ignore session-key

Игнорировать ключ сессии. Опциональная команда.

Значение по умолчанию: выключено

Формат: `ignore session-key`

Режим ввода команды: режим динамической авторизации

no ignore session-key

Прекратить игнорирование ключа сессии на данном устройстве. Опциональная команда.

Значение по умолчанию: включено

Формат: `no ignore session-key`

Режим ввода команды: режим динамической авторизации

port

Задать UDP-порт, через который устройство получает RADIUS-запросы от сконфигурированных клиентов динамической авторизации. Диапазон номера порта: 1025-65535.

Значение по умолчанию: 3799

Формат: `port port-number`

Режим ввода команды: режим динамической авторизации

no port

Сбросить настройки UDP-порта, через который устройство получает RADIUS-запросы от сконфигурированных клиентов динамической авторизации, к значению по умолчанию.

Значение по умолчанию: 3799

Формат: `no port`

Режим ввода команды: режим динамической авторизации

radius accounting mode

Активировать функцию учёта RADIUS.

Значение по умолчанию: отключено

Формат: `radius accounting mode`

Режим ввода команды: режим глобальной конфигурации

no radius accounting mode

Сбросить настройки учётной функции RADIUS к значению по умолчанию (отключить функцию учёта RADIUS).

Формат: `no radius accounting mode`

Режим ввода команды: режим глобальной конфигурации

radius server attribute 4

Задать использование IP-адреса в атрибуте IP-адреса NAS клиентом RADIUS в RADIUS-запросах. Если определённый IP-адрес сконфигурирован при разрешенном атрибуте, то RADIUS-клиент использует этот IP-адрес при отправке атрибута IP-адреса NAS на RADIUS-сервер.

Формат: `radius server attribute 4 [ipaddr]`

Режим ввода команды: режим глобальной конфигурации

Параметр	***Описание***
4	Атрибут IP-адреса NAS, используемый для RADIUS-запросов.
ipaddr	IP-адрес сервера.

no radius server attribute 4

Отрицательная форма команды выключает глобальный параметр атрибута IP-адреса NAS для RADIUS-клиента. Если параметр выключен, RADIUS-клиент не отправляет атрибут IP-адреса NAS в RADIUS-запросах.

Формат: `no radius server attribute 4 [ipaddr]`

Режим ввода команды: режим глобальной конфигурации

radius server attribute 95

Задать использование IPv6-адреса в атрибуте IPv6-адреса NAS клиентом RADIUS в RADIUS-запросах. Если определённый IPv6-адрес сконфигурирован при разрешенном атрибуте, то RADIUS-клиент использует этот IP-адрес при отправке атрибута IP-адреса NAS на RADIUS-сервер.

Формат: `radius server attribute 95 [ipv6addr]`

Режим ввода команды: режим глобальной конфигурации

Параметр	*Описание*
95	Атрибут IPv6-адреса NAS, используемый для RADIUS-запросов
Ipv6addr	IPv6-адрес сервера

no radius server attribute 95

Отрицательная форма команды выключает глобальный параметр атрибута IPv6-адреса NAS для RADIUS-клиента. Если параметр выключен, RADIUS-клиент не отправляет атрибут IPv6-адреса NAS в RADIUS-запросах.

Формат: `no radius server attribute 95 [ipv6addr]`

Режим ввода команды: режим глобальной конфигурации

radius server attribute 31

Задать использование calling station id станции NAS в заданном MAC-формате в RADIUS-запросах.

Формат: `radius server attribute 31 mac-format [ietf | legacy | unformatted] [lower-case | upper-case]`

Режим ввода команды: режим глобальной конфигурации

Формат calling station id	**Описание**
ietf	aa-bb-cc-dd-ee-ff
legacy	aa:bb:cc:dd:ee:ff
unformated	aaaabbbbcccc

no radius server attribute 31 mac-formate

Отрицательная форма команды выключает глобальный параметр атрибута 31 NAS для RADIUS-клиента. Если параметр выключен, RADIUS-клиент не отправляет атрибут calling station id NAS в RADIUS-запросах.

Формат: `radius server attribute 31 mac-format`

Режим ввода команды: Режим глобальной конфигурации

radius server host

Команда конфигурирует IP-адрес или DNS-имя для связи с выбранным типом RADIUS-сервера. Вы можете настроить IP-адрес или DNS-имя для серверов аутентификации или учёта, а также номер порта и имя сервера. Если аутентификационные или учётные сервера сконфигурированы без имени, команда использует Default_RADIUS_Auth_Server и Default_RADIUS_Acct_Server в качестве имени по умолчанию. Одно и то же имя может быть задано для нескольких аутентификационных серверов, но имя каждого учетного сервера должно быть уникальным. RADIUS-клиент позволяет сконфигурировать до 32 аутентификационных и учётных серверов (включительно).

При использовании параметра auth команда конфигурирует IP-адрес или имя устройства, чтобы подключиться к аутентификационному RADIUS-серверу. Можно сконфигурировать не более 3 серверов для одного RADIUS-клиента. Если достигнуто максимальное количество сконфигурированных серверов, то возможны сбои команды, пока один из серверов не будет удален с помощью отрицательной формы данной команды. При использовании опционального параметра port команда конфигурирует номер UDP-порта для соединения со сконфигурированным RADIUS-сервером. Диапазон номеров порта: 1-65535, значение по умолчанию: 1812.

Чтобы переконфигурировать сервер аутентификации RADIUS на использование порта UDP по умолчанию, установите параметр порта на 1812.

Если вы используете параметр acct, команда конфигурирует IP-адрес или имя узла, чтобы использовать его для учётного RADIUS-сервера. Можно сконфигурировать только один учётный сервер. Если сервер находится в процессе конфигурирования, отрицательная форма данной команды удаляет его из конфигурации. Заданные IP-адрес или имя устройства должны соответствовать IP-адресу сконфигурированного ранее сервера учёта. При использовании опционального параметра port команда конфигурирует UDP-порт для соединения с учётным сервером RADIUS. Если порт для учётного сервера уже сконфигурирован, новый порт заменяет его. Значение параметра port должно быть в пределах 0-65535, значение по умолчанию: 1813.

Для перенастройки учётного RADIUS-сервера и возвращения к использованию UDP-порта по умолчанию, установите значение параметра port на 1813.

Формат: `radius server host {auth | acct} {`*`ipaddr`*`|`*`dnsname`*`} [name `*`servername`*`] transport {tls | udp} [0-8] [port `*`0-65535`*`]`

Режим ввода команды: режим глобальной конфигурации

Поле	*Описание*
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.
0-65535	Номер порта, используемого для соединения с указанным сервером RADIUS.
0-8	Номер ячейки памяти в которой хранятся загруженные ключи и сертификаты для TLS-соединения.
servername	Альтернативное имя для идентификации сервера.
tls	Использовать tls соединение для общения с сервером RADIUS.

udp	Использовать udp протокол для общения с сервером RADIUS.

no radius server host

Отрицательная форма команды удаляет сконфигурированную запись сервера из списка сконфигурированных RADIUS-серверов. Если удаляемый аутентификационный RADIUS-сервер активен, и есть другие серверы с тем же именем, то RADIUS-клиент выбирает другой сервер для операций RADIUS. Если используется параметр "auth", ранее сконфигурированный сервер аутентификации RADIUS удаляется из конфигурации.

То же самое производится в случае, если используется параметр “acct”. Параметр ipaddr|dnsname должен соответствовать IP-адресу или DNS-имени ранее сконфигурированного аутентификационного/учетного RADIUS-сервера.

Формат: `no radius server host {auth | acct} {`*`ipaddr|dnsname`*`}`

Режим ввода команды: режим глобальной конфигурации

radius server key

Данная команда конфигурирует ключ, используемый при соединении RADIUS-клиента с выбранным сервером. При выставленном параметре 'auth' общий ключ конфигурируется для соединения с сервером аутентификации RADIUS, при параметре 'acct' ключ конфигурируется для соединения с сервером учета RADIUS. IP-адрес или имя устройства должны соответствовать ранее сконфигурированному серверу. При выполнении данной команды ключ вводится пользователем.

Конфигурации с текстовым интерфейсом поддерживают ключи RADIUS-сервера в зашифрованном и незашифрованном виде. При сохранении конфигурации ключи хранятся только в зашифрованном виде. Для того чтобы ввести ключ в зашифрованном виде, следует вводить ключ вместе с параметром `encrypted`. При выполнении команды `show running-config` секретные ключи отображаются в зашифрованном виде. В виде открытой информации секретные ключи не отображаются.

Ключ вводится в алфавитно-цифровом формате и должен содержать не более 16 символов.

Формат: `radius server key {auth | acct} {`*`ipaddr|dnsname`*`}` *`encrypted password`*

Режим ввода команды: режим глобальной конфигурации

Поле	*Описание*
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.
password	Пароль в зашифрованном виде.

radius server msgauth

Включить использование проверки подлинности сообщений при соединении с выбранным RADIUS-сервером аутентификации.

Формат: `radius server msgauth ipaddr|dnsname`

Режим ввода команды: режим глобальной конфигурации

Поле	*Описание*
ipaddr	IP-адрес сервера/
dnsname	DNS-имя сервера.

no radius server msgauth

Отключить использование проверки подлинности сообщений при соединении с выбранным сервером аутентификации RADIUS.

Формат: `no radius server msgauth ipaddr|dnsname`

Режим ввода команды: режим глобальной конфигурации

radius server primary

Задать сконфигурированный сервер в качестве сервера-источника для группы серверов с единым именем сервера. Для каждой группы серверов с единым именем сервера может быть сконфигурировано несколько серверов-источников. При обмене данными с сервером аутентификации RADIUS клиент по умолчанию подключается к серверу-источнику с заданным именем. При невозможности соединения с сервером-источником происходит попытка соединения с резервными серверами, сконфигурированными с тем же именем сервера. Резервные серверы расцениваются как дополнительные.

Формат: `radius server primary {ipaddr|dnsname}`

Режим ввода команды: режим глобальной конфигурации

Поле	*Описание*
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.

radius server retransmit

Сконфигурировать глобальный параметр RADIUS-клиента, задающий количество попыток передачи сообщения до установления невозможности соединения с заданным аутентификационным RADIUS-сервером и перехода на соединение с сервером с меньшей скоростью передачи данных. При превышении лимита безответных попыток соединения с сервером учета RADIUS-клиент не подключается к другим серверам.

Значение по умолчанию: 4

Формат: `radius server retransmit retries`

Режим ввода команды: режим глобальной конфигурации

Поле	*Описание*
retries	Максимальное количество попыток передачи. Диапазон значений: 1-15.

no radius server retransmit

Отрицательная форма команды сбрасывает данный параметр к значению по умолчанию.

Формат: `no radius server retransmit`

Режим ввода команды: режим глобальной конфигурации

radius source-interface

Задать физический или логический интерфейс в качестве исходного интерфейса RADIUS-клиента (исходный IP-адрес). Сконфигурированный адрес исходного интерфейса используется для всех соединений между RADIUS-сервером и RADIUS-клиентом. IP-адрес выбранного исходного интерфейса используется в IP-заголовках пакетов протокола системы управления RADIUS. Это позволяет средствам межсетевой защиты (брандмауэрам) опознавать исходные пакеты, получаемые от того или иного коммутатора.

Если исходный интерфейс не задан, в качестве исходного IP-адреса используется главный адрес интерфейса инициирующего соединение удаленного устройства. При сбое сконфигурированного интерфейса RADIUS-клиент возвращается к алгоритму действий по умолчанию.

Формат: `radius source-interface {`*`unit/slot/port`* `|` `loopback` *`loopback-id`* `|` `vlan` *`vlan-id`* `|` *`serviseport`* `|` *`network`*`}`

Режим ввода команды: режим глобальной конфигурации

Поле	*Описание*
unit/slot/port	Идентификатор устройства, присвоенный коммутатору.
loopback-id	Конфигурирует loopback-интерфейс. Диапазон значений идентификатора: 0-63.
vlan-id	Конфигурирует интерфейс VLAN, используемый в качестве исходного IP-адреса. Диапазон идентификаторов VLAN: 1-4094.

no radius source-interface

Сбросить исходный интерфейс RADIUS к настройкам по умолчанию.

Формат: `no radius source-interface`

Режим ввода команды: режим глобальной конфигурации

radius server timeout

Сконфигурировать глобальный параметр RADIUS-клиента, задающий интервал времени (в секундах) на получение ответа от RADIUS-сервера, по истечении которого происходит повторная передача запроса. Диапазон значений: целое число от 1 до 30.

Значение по умолчанию: 5

Формат: `radius server timeout` *`seconds`*

Режим ввода команды: режим глобальной конфигурации

Поле	*Описание*
retries	Максимальное число попыток передачи, диапазон значений 1-30.

no radius server timeout

Установить глобальный параметр интервала времени на значение по умолчанию.

Формат: `no radius server timeout`

Режим ввода команды: режим глобальной конфигурации

server-key

Сконфигурировать глобальный общий секретный ключ, используемый для динамической авторизации всеми клиентами без сконфигурированного индивидуального общего секретного ключа.

Значение по умолчанию: нет

Формат: `server-key [7] key-string`

Режим ввода команд: режим динамической авторизации

Поле	*Описание*
0	Требуется ввести незашифрованный ключ.
7	Требуется ввести зашифрованный ключ.
string	Общая секретная строка. Количество символов не должно превышать 128 для незашифрованного ключа и 256 для зашифрованного ключа. Превалирует над глобальными настройками только для данного клиента. Специальные символы или внутренние пробелы вводятся в кавычках.

no server-key

Удалить настройку глобального общего секретного ключа.

Значение по умолчанию: нет

Формат: `no server-key`

Режим: режим динамической авторизации

show radius servers

Показать параметры аутентификации.

Формат: `show radius servers { serverIP | name serverName }`

Режим ввода команд: пользовательский режим

show radius

Показать сконфигурированные значения глобальных параметров RADIUS-клиента.

Формат: `show radius`

Режим ввода команды: привилегированный режим

Параметр	*Определение*
Number of Configured Authentication Servers	Количество сконфигурированных серверов аутентификации RADIUS.

Number of Configured Accounting Servers	Количество сконфигурированных серверов учета RADIUS.
Number of Named Authentication Server Groups	Количество сконфигурированных групп серверов аутентификации RADIUS с общим именем.
Number of Named Accounting Server Groups	Количество сконфигурированных групп серверов учета RADIUS с общим именем.
Number of Retransmits	Сконфигурированное значение максимального количества повторных передач пакета запроса.
Time Duration	Интервал времени (в секундах) между повторными передачами запросов.
RADIUS Accounting Mode	Глобальный параметр. Включен или выключен режим учета для всех серверов.
RADIUS Attribute 4 Mode	Глобальный параметр. Разрешено ли использование атрибута NAS-IP-адреса (IP-адрес системы сетевого администрирования) при RADIUS запросах.
RADIUS Attribute 4 Value	Глобальный параметр. IP-адрес, используемый в атрибуте NAS-IP-адреса в RADIUS-запросах.

show radius servers

Показать информацию по серверам аутентификации RADIUS, сконфигурированным для RADIUS-клиента.

Формат: `show radius servers [{`*`ipaddr`*`|`*`dnsname`*` | name [servername]}]`

Режим ввода команд: привилегированный режим

Поле	*Описание*
ipaddr	IP-адрес сервера аутентификации.
dnsname	DNS-имя сервера аутентификации.
servername	Дополнительное имя для идентификации сервера.
Current	Символ * перед адресом хоста сервера обозначает, что сервер активен в текущий момент.
Host Address	IP-адрес хоста.
Server Name	Имя сервера аутентификации.
Port	Порт, используемый для соединения с сервером аутентификации.
Type	Относится сервер к первичному (источник) или вторичному (дополнительный) типу.
Current Host Address	IP-адрес сервера аутентификации, активного в текущий момент.
Secret Configured	Сконфигурирована ли защита от несанкционированного доступа к серверу. Булево значение: Yes (Да) или No (Нет).
Number of Retransmits	Заданное максимальное количество попыток повторной передачи пакета запроса.

Message Authenticator	Глобальный параметр. Разрешен или запрещен атрибут удостоверения сообщения.
Time Duration	Интервал времени (в секундах) между повторными передачами запроса.
RADIUS Accounting Mode	Глобальный параметр. Включен ли режим учета для всех серверов или нет.
RADIUS Attribute 4 Mode	Глобальный параметр. Разрешено ли использование атрибута IP-адреса NAS при RADIUS-запросах.
RADIUS Attribute 4 Value	Глобальный параметр. IP-адрес, используемый в атрибуте IP-адреса NAS в RADIUS-запросах.

show radius accounting

Показать общую информацию по сконфигурированным RADIUS-серверам учета.

Формат: `show radius accounting name [`*`servername`*`]`

Режим ввода команд: привилегированный режим

Поле	*Описание*
servername	Дополнительное имя для идентификации сервера.
RADIUS Accounting Mode	Глобальный параметр. Включен ли режим учета для всех серверов или нет.

Если параметры не заданы администратором, то отображаются только характеристики режима учета и сервера учета RADIUS.

Поле	*Описание*
Host Address	IP-адрес хоста.
Server Name	Имя сервера учета.
Port	Порт, используемый для соединения с сервером учета.
Secret Configured	Сконфигурирована ли защита от несанкционированного доступа к серверу. Булево значение: Yes (Да) или No (Нет).

show radius accounting statistics

Показать общую статистическую информацию по сконфигурированным серверам учета RADIUS.

Формат: `show radius accounting statistics {`*`ipaddr`*`|`*`dnsname`*` | name `*`servername`*`}`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
ipaddr.	IP-адрес сервера.
dnsname	DNS-имя сервера.
servername	Дополнительное имя для идентификации сервера.

RADIUS Accounting Server Name	Имя сервера учета.
Server Host Address	IP-адрес хоста.
Round Trip Time	Временной интервал (в сотых долях секунды) между последним ответом на соответствующий учетный запрос, полученный от сервера учета RADIUS.
Requests	Количество пакетов учетных RADIUS-запросов, отправленных на сервер. Количество повторных передач не входит в данный показатель.
Retransmission	Количество пакетов учетных RADIUS-запросов, повторно переданных на сервер учета RADIUS.
Responses	Количество RADIUS-пакетов, принятых учетным портом сервера.
Malformed Responses	Количество искаженных пакетов учетных RADIUS-ответов, полученных от сервера. Этот показатель включает в себя пакеты неверной длины, но не учитывает неверные удостоверения, атрибуты сигнатуры и неизвестные типы данных.
Bad Authenticators	Количество пакетов учетных RADIUS-ответов с недопустимыми удостоверениями, полученных от сервера учета.
Pending Requests	Количество отправленных на сервер пакетов учетных RADIUS-запросов, не получивших ответа от сервера, но еще не превысивших интервал ожидания ответа.
Timeouts	Количество превышений временного интервала при обмене учетными данными с сервером.
Unknown Types	Количество RADIUS-пакетов неизвестного типа, принятых от сервера через учетный порт.
Packets Dropped	Количество RADIUS-пакетов, принятых от сервера через учетный порт, но пропавших по другой причине.

show radius source-interface

Показать информацию о конфигурации исходного интерфейса (IP-адрес источника) RADIUS-клиента. Команда действует только в привилегированном режиме.

Формат: `show radius source-interface`

Режим ввода команд: привилегированный режим

show radius statistics

Показать общую статистику сконфигурированных серверов RADIUS.

Формат: `show radius statistics {`*`ipaddr`*`|`*`dnsname`*` | name `*`servername`*`}`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
ipaddr	IP-адрес сервера.
dnsname	DNS-имя сервера.
servername	Дополнительное имя для идентификации сервера.
RADIUS Server Name	Имя сервера аутентификации.

Server Host Address	IP-адрес хоста.
Access Requests	Количество пакетов RADIUS запросов на доступ, отправленных на сервер. Повторные передачи не учитываются.
Access Retransmissions	Количество пакетов RADIUS запросов на доступ, повторно переданных на сервер аутентификации RADIUS.
Access Accepts	Количество допустимых и недопустимых RADIUS-пакетов, полученных от сервера, которым был разрешен доступ.
Access Rejects	Количество допустимых и недопустимых RADIUS-пакетов, полученных от сервера, которым не был разрешен доступ.
Access Challenges	Количество допустимых и недопустимых RADIUS-пакетов вызовов доступа, полученных от сервера.
Malformed Access Responses	Количество искаженных RADIUS-пакетов ответов на запросы на доступ, полученных от сервера. Этот показатель включает в себя пакеты неверной длины, но не учитывает неверные удостоверения, атрибуты сигнатуры и неизвестные типы данных.
Bad Authenticators	Количество RADIUS-пакетов ответов на запросы на доступ с недопустимыми удостоверениями или атрибутами сигнатуры, полученных от сервера.
Pending Requests	Количество отправленных на сервер RADIUS-пакетов запросов на доступ, не получивших ответа от сервера, но еще не превысивших интервал ожидания ответа.
Timeouts	Количество превышений временного интервала при аутентификации.
Unknown Types	Количество пакетов неизвестного типа, принятых от сервера через порт аутентификации.
Packets Dropped	Количество RADIUS-пакетов, принятых от сервера через порт аутентификации, но пропавших по другой причине.

8.11 Команды настройки протокола TACACS+

TACACS+ обеспечивает контроль доступа к объединенным в сеть устройствам через один или несколько централизованных серверов. Аналогично системе RADIUS, данный протокол упрощает аутентификацию посредством использования единой базы данных, к которой могут одновременно обращаться все клиенты обширной сети. Протокол TACACS+ основан на протоколе TACACS (описан в RFC1492), но дополнительно обеспечивает поддержку отдельных аутентификации, авторизации и учета. TACACS основывался на протоколе UDP (User Datagram Protocol), передача текстовых сообщений по сети проводилась в открытой форме; TACACS+ использует протокол TCP, что обеспечивает надежность доставки, и единый ключ для шифрования всех сообщений между клиентом и сервером.

tacacs-server host

Сконфигурировать сервер TACACS+. Команда используется в режиме глобальной конфигурации и включает режим конфигурации TACACS+. Параметр *ip-address|hostname* задает IP-адрес или имя хоста сервера TACACS+. Команда может использоваться неоднократно при необходимости задать несколько хостов.

Формат: `tacacs-server host {ip-address | ipv6-address | hostname}`

Режим ввода команд: режим глобальной конфигурации

no tacacs-server host

Удалить заданное имя хоста или IP-адрес. Параметр ipaddress| hostname задает IP-адрес сервера TACACS+.

Формат: `no tacacs-server host {ip-address | ipv6-address | hostname}`

Режим ввода команд: режим глобальной конфигурации

tacacs-server key

Сгенерировать ключ аутентификации и шифрования для всех соединений TACACS+ между коммутатором и TACACS+. Параметр key-string может содержать от 0 до 128 символов и задает ключ аутентификации и шифрования для всех соединений TACACS+ между коммутатором и сервером TACACS+. Данный ключ должен соответствовать ключу, используемому TACACS+.

Конфигурации с текстовым интерфейсом поддерживают секретные ключи сервера TACACS в зашифрованном и незашифрованном виде. При сохранении конфигурации секретные ключи хранятся только в зашифрованном виде. Для того чтобы ввести ключ в зашифрованном виде, следует вводить ключ вместе с ключевым словом encrypted. При выполнении команды show running-config секретные ключи отображаются в зашифрованном виде. В виде открытой информации данные ключи не отображаются.

Формат: `tacacs-server key [key-string | encrypted key-string]`

Режим ввода команд: режим глобальной конфигурации

no tacacs-server key

Отключить использование ключа аутентификации и шифрования для всех соединений TACACS+ между коммутатором и TACACS+. Параметр key-string может содержать от 0 до 128 символов. Данный ключ должен соответствовать ключу, используемому TACACS+.

Формат: `no tacacs-server key key-string`

Режим ввода команд: режим глобальной конфигурации

tacacs-server keystring

Задать глобальный ключ аутентификации и шифрования для всех TACACS+ соединений между сервером TACACS+ и клиентом.

Формат: `tacacs-server keystring`

Режим ввода команд: режим глобальной конфигурации

tacacs-server source-interface

Задать исходный интерфейс (IP-адрес источника) для конфигурации сервера TACACS+. Команда используется в режиме глобальной конфигурации. Выбранный IP-адрес исходного интерфейса используется в IP-заголовках пакетов протокола системы управления. Это позволяет средствам межсетевой защиты (брандмауэрам) опознавать исходные пакеты, получаемые от того или иного коммутатора.

Если исходный интерфейс не задан, в качестве исходного IP-адреса используется главный адрес интерфейса, инициирующего соединение удаленного устройства.

Формат: `tacacs-server source-interface {`*`unit/slot/port`*`|loopback `*`loop-back-id`*`|vlan `*`vlan-id`*`|`*`serviseport`*`|`*`network`*`}`

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
unit/slot/port	Идентификатор устройства, присвоенный коммутатору, в виде unit/slot/port.
loopback-id	Конфигурация loopback-интерфейса. Диапазон идентификаторов: 0-63.
vlan-id	Конфигурация интерфейса VLAN, используемого в качестве исходного IP-адреса. Диапазон VLAN-идентификаторов: 1-4093.

no tacacs-server source-interface

Удалить глобальный исходный интерфейс (выбор IP источника) для всех соединений TACACS+ между клиентом TACACS+ и сервером. Команда используется в режиме глобальной конфигурации.

Формат: `no tacacs-server source-interface`

Режим ввода команд: режим глобальной конфигурации

tacacs-server timeout

Задать временной интервал ожидания ответа при соединении с серверами TACACS+. Параметр *timeout* задает время ожидания в секундах, диапазон значений: 1-30. Если интервал не задан администратором, команда устанавливает глобальный интервал на значение по умолчанию. Серверы TACACS+, не использующие глобальный интервал, сохранят заданные значения данного параметра.

По умолчанию: 5

Формат: `tacacs-server timeout `*`timeout`*

Режим ввода команд: режим глобальной конфигурации

no tacacs-server timeout

Установить параметр ожидания ответа для всех серверов TACACS на значение по умолчанию.

Формат: `no tacacs-server timeout`

Режим ввода команд: режим глобальной конфигурации

key

Задать глобальный ключ аутентификации и шифрования для всех TACACS+ соединений между устройством и сервером TACACS. Команда используется в режиме конфигурации TACACS. Данный ключ должен соответствовать ключу, используемому TACACS+. Параметр key-string задает имя ключа и может содержать от 0 до 128 символов. Пустая строка вводится как пробел в кавычках « ».

Конфигурации с текстовым интерфейсом поддерживают секретные ключи сервера TACACS в зашифрованном и незашифрованном виде. При сохранении конфигурации секретные ключи хранятся только в зашифрованном виде. Для того чтобы ввести ключ в зашифрованном виде, следует

вводить ключ вместе с ключевым словом encrypted. При выполнении команды show running-config секретные ключи отображаются в зашифрованном виде. В виде открытой информации данные ключи не отображаются.

Формат: `key [key-string | encrypted key-string]`

Режим ввода команд: режим конфигурирования TACACS

keystring

Задать ключ аутентификации и шифрования данного сервера TACACS+ для всех TACACS+ соединений между сервером TACACS+ и клиентом

Формат: `keystring`

Режим ввода команд: режим конфигурирования TACACS-сервера

port

Задать номер порта сервера. Диапазон значений параметра *port-number*: 0-65535.

Значение по умолчанию: 49

Формат: `port port-number`

Режим ввода команд: режим конфигурирования TACACS

priority (режим конфигурации TACACS)

Задать порядок обращения к серверам. Команда выполняется в режиме конфигурации TACACS. Параметр priority задает приоритет серверов. Высший приоритет – 0 (ноль), диапазон значений: 0-65535.

Значение по умолчанию: 0

Формат: `priority priority`

Режим ввода команд: режим конфигурирования TACACS

timeout

Задать интервал ожидания ответа (в секундах). Команда используется в режиме конфигурации TACACS. Если интервал не задан администратором, используется глобальное значение. Параметр timeout задает интервал ожидания (в секундах), диапазон значений: 1-30.

Формат: `timeout timeout`

Режим ввода команд: режим конфигурирования TACACS

show tacacs

Показать информацию о конфигурации, статистике и исходящем интерфейсе клиента TACACS+.

Формат: `show tacacs [ip-address|hostname|client|server]`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Host address	IP-адрес или имя хоста сконфигурированного сервера TACACS+.

Port	Номер порта сконфигурированного сервера TACACS+.
TimeOut	Интервал ожидания (в секундах) установления соединения TCP.
Priority	Порядок обращения к серверам TACACS+. В случае сбоя соединения с сервером следует попытка соединения со следующим по порядку сервером.

show tacacs source-interface

Показать информацию о сконфигурированном глобальном исходящем интерфейсе клиента TACACS+. Команда используется в режиме глобальной конфигурации. IP-адрес выбранного интерфейса используется как IP-источника для всех соединений с сервером.

Формат: `show tacacs source-interface`

Режим ввода команд: привилегированный режим

8.12 Команды сценариев конфигурации

Команды сценариев используются для генерирования в текстовом формате файлов сценариев, отображающих текущую конфигурацию системы. Файлы сценариев конфигурации могут быть загружены на PC или систему UNIX и изменены. Измененные файлы могут быть впоследствии выгружены в другую систему для запуска новой конфигурации. Сценарии конфигурации могут выполняться на одном или нескольких коммутаторах с незначительными изменениями или без таковых.

Команда `show running-config` сохраняет текущую конфигурацию в виде сценария. Команда copy переносит сценарий конфигурации на коммутатор или с коммутатора.

Команда show показывает настройки конфигурации, хранящиеся в файле конфигурации при запуске (startup-config), резервной конфигурации (backup-config) или заводской конфигурации (factorydefaults).

Сценарии следует запускать на системах с конфигурациями по умолчанию; однако, возможен запуск и на системах с измененными конфигурациями.

Сценарии должны соответствовать следующим правилам:

- Файлы сценариев не распределяются по стеку, а хранятся в устройстве, которое являлось главным в стеке на момент загрузки файла;
- Необходимое разрешение файла: “.scr”;
- Находиться на коммутаторе могут не более 10 сценариев;
- Совокупный размер всех файлов сценариев на коммутаторе не должен превышать 2048 KB;
- Количество команд в файле конфигурации не должно превышать 2000.

Допускаются однострочные комментарии при написании тестовых сценариев или сценариев конфигурации для пояснения. Начало комментария отмечается восклицательным знаком (!). Символ, отмечающий начало комментария, может использоваться перед любым словом в команде, любая информация после этого символа не будет учитываться как часть команды. Любая команда, в начале которой стоит символ «!», распознается как комментарий и не учитывается анализатором.

Примеры строк в сценарии:

```
! Script file for displaying management access

show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

Для обозначения пустого пользовательского пароля необходимо в сценарии конфигурации указать пароль как пробел в кавычках (« »). Так, команда изменения пароля для пользователя jane на пароль *hello* выглядит следующим образом:

```
users passwd jane
" "
hello
hello
```

script apply

Применить команды сценария на коммутаторе. Параметр *scriptname* соответствует имени сценария, который следует выполнить.

Формат: `script apply` *`scriptname`*

Режим ввода команд: привилегированный режим

script delete

Удалить сценарий. Параметр `scriptname` соответствует имени сценария, который следует удалить. Опция `all` удаляет все сценарии, присутствующие на устройстве.

Формат: `script delete {`*`scriptname`* `| all}`

Режим ввода команд: привилегированный режим

script list

Вывести список всех сценариев, присутствующих на устройстве, и оставшееся свободное место.

Формат: `script list`

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Configuration Script	Имя сценария.
Size	Размер файла сценария.

script show

Отобразить содержание файла сценария под именем *scriptname*.

Формат: `script show` *`scriptname`*

Режим ввода команд: привилегированный режим

Параметр	*Описание*
Output Format	Номер строки: содержание строки.

script validate

Проверить правильность файла сценария путем анализа каждой строки в файле. Параметр `scriptname` – имя проверяемого сценария. Данная опция выявляет потенциальные источники проблем и используется для отладки сценария. Проблемы, порождаемые применением данного сценария на данном устройстве, могут остаться не выявленными.

Формат: `script validate` *`scriptname`*

Режим ввода команд: привилегированный режим

8.13 Команды настройки баннера, подсказки командной строки и имени устройства

В данном разделе описаны команды настройки баннера и подсказки командной строки. Баннер представляет собой текст, выводимый перед авторизацией пользователя на подсказке User: prompt.

copy (pre-login banner)

Загрузить баннер CLI на коммутатор или с коммутатора. Команда `copy` позволяет задать локальные URL-адреса через протоколы FTP, TFTP, SFTP, SCP и Xmodem.

Параметр `ip6address` также допустим.

Значение по умолчанию: нет

Формат:
```
copy <tftp://<ipaddr>/<filepath>/<filename>> nvram:cliban-
ner
copy nvram:clibanner <tftp://<ipaddr>/<filepath>/<file-
name>>
```

Режим ввода команд: привилегированный режим

set prompt

Изменить имя подсказки. Имя вводится в буквенно-цифровом формате, длина имени не должна превышать 64 символа.

Формат: `set prompt` *`prompt_string`*

Режим ввода команд: привилегированный режим

hostname

Задать имя хоста системы. Данная команда также меняет подсказку. Имя вводится в буквенно-цифровом виде с учетом регистра, длина имени не должна превышать 64 символа.

Формат: `hostname` *`hostname`*

Режим ввода команд: привилегированный режим

show clibanner

Показать сконфигурированный баннер CLI перед входом в систему. Баннер перед входом в систему представляет собой текст, выводимый перед отображением подсказки CLI.

Значение по умолчанию: не показывать ничего перед подсказкой авторизации

Формат: `show clibanner`

Режим ввода команд: привилегированный режим

set clibanner

Настроить баннер CLI, отображающийся перед выведением подсказки авторизации.

Формат: `set clibanner` *`line`*

Режим ввода команд: режим глобальной конфигурации

Параметр	*Описание*
line	Текст баннера. Разграничивающий символ – “” (двойные кавычки подряд). Сообщение баннера должно содержать не более 2000 символов.

no set clibanner

Убрать настроенный баннер CLI.

Формат: `no set clibanner`

Режим ввода команд: режим глобальной конфигурации

9 КОМАНДЫ НАСТРОЙКИ КОММУТАЦИИ

Этот раздел описывает команды коммутации, доступные в интерфейсе командной строки.

Все команды, приведенные в этом разделе, делятся на три функциональные группы:

- **Команды show выводят информацию о настройках коммутатора, статистику и прочую информацию.**
- **Команды конфигурации настраивают функции коммутатора. Каждой команде конфигурации соответствует команда show, выводящая на дисплей настройки.**
- **Команды очистки, которые возвращают отдельные параметры или все настройки к заводским.**

9.1 Команды настройки порта

В этой части описаны команды, которые используются для просмотра и изменения настроек порта.

interface

Данная команда предоставляет доступ к режиму конфигурации интерфейса, в котором можно выполнять включение или изменение операций определенного интерфейса (порта). Для одновременной настройки можно определить и диапазон портов, указав начальное значение unit/slot/port, конечное значение unit/slot/port и разделив их с помощью дефиса.

Формат: `interface {unit/slot/port | unit/slot/port(начало диапазона)-unit/slot/port(конец диапазона)}`

Режим ввода команд: глобальная конфигурация

auto-negotiate

Эта команда включает автоматическое согласование для отдельного порта или диапазона портов.

Данная команда устарела. Возможность включения/выключения режима автосогласования с помощью команды auto-negotiate не поддерживается. Вместо этой команды используются варианты команды speed (т. е. speed для выключения и speed auto для включения автосогласования). Тем не менее в целях обеспечения обратной совместимости сценарии конфигурации с использованием команды auto-negotiate по-прежнему поддерживаются. Для обеспечения обратной совместимости данной команды может выполняться перенос конфигурации как в текстовом формате, так и в формате бинарного файла.

Значение по умолчанию: включено

Формат: `auto-negotiate`

Режим ввода команд: конфигурирование интерфейса

no auto-negotiate

Команда выключает автоматическое согласование порта.

При выключении автоматического согласования выключается и автоматическое распознавание порта.

Формат: `no auto-negotiate`

Режим ввода команд: конфигурирование интерфейса

auto-negotiate all

Данная команда включает автоматическое согласование для всех портов.

Значение по умолчанию: включено

Формат: `auto-negotiate all`

Режим ввода команд: глобальная конфигурация

no auto-negotiate all

Команда выключает автоматическое согласование для всех портов.

Формат: `no auto-negotiate all`

Режим ввода команд: глобальная конфигурация

description

Команда используется для создания описания интерфейса или диапазона интерфейсов в буквенно-цифровом формате.

Формат: `description description`

Режим ввода команд: конфигурирование интерфейса

no description

Удаляет описание интерфейса или диапазона интерфейсов.

Формат: `no description`

Режим ввода команд: конфигурирование интерфейса

media-type

Команда переключения режимов оптического волокна и медного кабеля для комбинированных портов.

- Комбинированный порт — это порт или интерфейс, способный работать как в оптическом, так и в медном режиме.
- Медный порт и оптический порт. Медный порт использует в качестве среды передачи медный кабель (примером могут служить порты RJ45). Оптический порт использует в качестве среды передачи оптическое волокно (примером могут служить порты SFP).

Значение по умолчанию: Auto-select, SFP preferred

Формат: `media-type {auto-select | rj45 | sfp }`

Режим ввода команд: конфигурирование интерфейса

Команда media-type поддерживает следующие режимы.

- ***Auto-select, SFP preferred:*** носитель определяется автоматически на основании фактического физического носителя. Если обнаружены оба соединения (и оптическое, и медное), приоритет устанавливается за оптическим соединением, оно становится активным.
- ***Auto-select, RJ45 preferred:*** носитель определяется автоматически на основании фактического физического носителя. Если обнаружены оба соединения (и оптическое, и медное), приоритет устанавливается за медным, это соединение становится активным.
- ***SFP:*** работает только оптическое соединение. Соединение по медному кабелю всегда выключено.
- ***RJ45:*** работает только соединение по медному кабелю. Оптическое соединение всегда выключено.

no media-type

Данная команда отменяет настройки, выполненные с помощью команды media-type, и возвращает настройки интерфейса к значению по умолчанию.

Формат: `no media-type`

Режим ввода команд: конфигурирование интерфейса

mtu

Команда mtu служит для настройки размера Maximum Transmit Unit (MTU) в байтах для входящих и исходящих кадров данного интерфейса. Дополнительно эту команду можно использовать, чтобы настроить поддержку сверхдлинного кадра для физических и агрегированных (LAG) интерфейсов. В стандартной конфигурации размер MTU может быть целым числом в интервале 1504–12270 для тегированных пакетов и целым числом в интервале 1500–12270 для нетегированных пакетов.

Для приема пакетов и их обработки размер Ethernet MTU должен включать дополнительные байты, достаточные для передачи заголовков уровня 2. По вопросу настройки IP MTU, максимального размера входного пакета (заголовок + полезная нагрузка входного пакета), см. команду ip mtu на стр. 819.

Значение по умолчанию: 1500 (для нетегированных пакетов)

Формат: `mtu 1500-12270`

Режим ввода команд: конфигурирование интерфейса

no mtu

Команда возвращает размер MTU (в байтах) для интерфейса к значению по умолчанию.

Формат: `no mtu`

Режим ввода команд: конфигурирование интерфейса

shutdown

Эта команда выключает порт или диапазон портов.

Команду shutdown можно использовать при работе с физическим и агрегированным (LAG) интерфейсом, однако она не подходит для выключения виртуального интерфейса маршрутизации.

Значение по умолчанию: включено

Формат: `shutdown`

Режим ввода команд: конфигурирование интерфейса

no shutdown

Данная команда включает порт.

Формат: `no shutdown`

Режим ввода команд: конфигурирование интерфейса

shutdown all

Команда выключает все порты.

Команду shutdown all можно использовать при работе с физическими и агрегированными (LAG) интерфейсами, однако она не подходит для выключения виртуальных интерфейсов маршрутизации.

Значение по умолчанию: включено

Формат: `shutdown all`

Режим ввода команд: глобальная конфигурация

no shutdown all

Данная команда включает все порты.

Формат: `no shutdown all`

Режим ввода команд: глобальная конфигурация

speed

Команда используется для включения или выключения автосогласования и для настройки скорости, анонсированной для данного порта. Параметр duplex позволяет устанавливать анонсированную скорость как для полудуплексов, так и для полного дуплекса.

Ключевое слово auto используется для включения автосогласования для порта. Если ключевое слово auto не указано, автосогласование будет выключено, а скорость и режим порта будут настроены в соответствии со значениями команды. При выключении автосогласования необходимо указывать настройки скорости и дуплексного режима.

Значение по умолчанию: включено автосогласование.

Формат: `speed auto {10|100|1000|2.5G|10G|20G|25G|40G} [10|100|1000|2.5G|10G|20G|25G|40G] [half-duplex|full-duplex]`

`speed {10|100|1000|2.5G|10G|20G|25G|40G} {half-duplex|full-duplex}.`

Режим ввода команд: конфигурирование интерфейса

speed all

Данная команда устанавливает скорость и настройки дуплекса для всех интерфейсов, если автосогласование выключено. Если автоматическое согласование включено, команда вернет сообщение об ошибке. Для выключения автоматического согласования можно использовать команду no auto-negotiate.

Значение по умолчанию: включено автосогласование. Значения объявляемых скоростей: 10h, 10f, 100h, 100f, 1000f.

Формат: `speed all {100 | 10} {half-duplex | full-duplex}`

Режим ввода команд: глобальная конфигурация

hardware profile portmode

Данная команда используется для смены режима работы интерфейсов x/0/49-52.

Формат: `hardware profile portmode {1x40G | 4x10G}`

Режим ввода команд: конфигурирование интерфейса

show interface media-type[1]

Команда отображает конфигурацию типа носителя для интерфейса.

Формат: `show interface media-type`

Режим ввода команд: привилегированный

В рамках данной команды отображается следующая информация.

Параметр	***Описание***
Port	Интерфейс в формате unit/slot/port.
Configured Media Type	Тип среды передачи для данного интерфейса. auto-select — тип среды передачи выбран автоматически. Отображается предпочтительный тип среды передачи. RJ45 — порт RJ45 SFP — порт SFP-порт
Active	Текущее оперативное состояние комбинированного порта

[1] Отсутствует в текущей версии ПО.

show interfaces status

Используйте эту команду для отображения информации интерфейса, включая описание, статус порта, скорость. Команда похожа на *show port*, но отображает дополнительные поля, такие как описание интерфейса и возможности порта. Описание интерфейса сопоставимо с существующим описанием поля <*name*>, которое ограничено до 28 символов.

Значение по умолчанию: выключено

Формат: `show interfaces status [{unit/slot/port | vlan id | all}]`

Режим ввода команды: привилегированный

Параметр	***Описание***
Port	Интерфейс в формате unit/slot/port.
Name	Название интерфейса, созданное пользователем.
Admin Mode	Административное состояние управления портами. Порт должен быть включен в соответствии с требованиями доступа к сети. Возможные значения: enabled или disabled. В качестве заводской настройки используется enabled (включено).
Link State	Показывает, создано или разорвано соединение.
Physical Mode	Скорость и дуплексный режим порта. Если выбрана поддержка автосогласования, скорость и дуплексный режим устанавливаются в процессе автоматического согласования. Обратите внимание: анонсируется максимальная мощность порта (полный дуплекс — 100M). Если нет, данный параметр определяет дуплексный режим порта и скорость передачи. В качестве заводской настройки используется auto (автосогласование).
Physical Status	Скорость порта и дуплексный режим.
Media Type	Тип подключенного SFP-модуля.
Flow Control Status	Состояние Flow Control.

show port

Эта команда отображает информацию о порте.

Формат: `show port {intf-range | all}`

Режим ввода команд: привилегированный

Параметр	***Описание***
Interface	Интерфейс в формате unit/slot/port.
Type	Если поле заполнено, оно определяет, что порт относится к особому типу. Возможные значения приведены далее. *Mirror* — данный порт является портом мониторинга. Подробнее об этом см. в теме «Команды зеркального копирования порта» на стр. 617. *PC Mbr* — порт является частью агрегированного интерфейса (LAG). *Probe* — данный порт является тестовым.
Admin Mode	Административное состояние управления портами. Порт должен быть включен в соответствии с требованиями доступа к сети. Возможные значения: enabled или disabled. В качестве заводской настройки используется enabled (включено).

Physical Mode	Скорость и дуплексный режим порта. Если выбрана поддержка автосогласования, скорость и дуплексный режим устанавливаются в процессе автоматического согласования. Обратите внимание: анонсируется максимальная мощность порта (полный дуплекс — 100M). Если нет, данный параметр определяет дуплексный режим порта и скорость передачи. В качестве заводской настройки используется auto (автосогласование).
Physical Status	Скорость порта и дуплексный режим.
Link Status	Создано или разорвано соединение.
Link Trap	Данный параметр определяет, нужно ли отправлять SNMP-трап при смене состояния соединения. В качестве заводской настройки используется enabled (включено).
LACP Mode	Определяет, включен или выключен LACP для данного порта.

show port advertise

Данная команда отображает настройки анонсирования для локального административного соединения, локального оперативного соединения и интерфейса соединения партнёра. Она также показывает приоритет очередности выбора скорости и дуплекса согласно стандарту 802.3, приложение 28B.3. Отображает состояние автоматического согласования, физическую конфигурацию для ведущего/ведомого таймера и состояние соединения порта.

Если соединение выключено, состояние таймера будет показано как No Link, а в строках параметров Oper Peer advertisement и Priority Resolution будут стоять прочерки. Если автоматическое согласование выключено, поля Admin Local Link advertisement, Operational local link advertisement, Operational peer advertisement и Priority resolution fields не отображаются.

Если в команде не указан необязательный параметр unit/slot/port, вывод отображает состояние автоматического согласования и оперативное анонсирование локального соединения всех портов. Оперативное анонсирование соединения будет отображать скорость только при условии, что она поддерживается и локальным, и партнерским соединением. Если автосогласование недоступно, оперативное анонсирование локального соединения не отображается.

Формат: `show port advertise [unit/slot/port]`

Режим ввода команд: привилегированный

show port description

Эта команда отображает описание интерфейса. Вместо параметра unit/slot/port можно использовать lag lag-intf-num как альтернативный вариант определения LAG-интерфейса. Параметр lag lag-intf-num можно использовать для определения конкретного LAG-интерфейса, при этом значение lag-intf-num должно указывать номер порта LAG.

Формат: `show port description unit/slot/port`

Режим ввода команд: привилегированный

Параметр	***Описание***
Interface	Интерфейс в формате unit/slot/port.
Index	Индекс интерфейса, связанный с данным портом.
Description	Буквенно-цифровое описание интерфейса, созданное с помощью команды «description».

MAC address	MAC-адрес порта. В формате шести двузначных номеров шестнадцатеричной системы, разделенных двоеточиями, например: 01:23:45:67:89:AB.
Bit Offset Val	Величина смещения битов.

show interfaces hardware profile

Эта команда отображает текущий режим работы интерфейсов x/0/49-52, а также режим, который будет активирован после перезагрузки устройства.

Формат: `show interfaces hardware profile [unit/slot/port]`

Режим ввода команд: привилегированный

9.2 Команды настройки протокола STP

В этой части представлены команды, которые используются для настройки Spanning Tree Protocol (STP). STP помогает предотвратить образование сетевых петель и дублирование сообщений, а также уменьшает нестабильность сети.

STP на коммутаторе и всех портах, а также LAG-интерфейсах включен по умолчанию.

spanning-tree

Данная команда устанавливает оперативный режим остовного дерева в состояние «включено».

Значение по умолчанию: включено

Формат: `spanning-tree`

Режим ввода команд: глобальная конфигурация

no spanning-tree

Команда устанавливает оперативный режим остовного дерева в состояние «выключено». Если остовное дерево выключен, его конфигурация сохраняется и доступна для редактирования, но не может быть активирована.

Формат: `no spanning-tree`

Режим ввода команд: глобальная конфигурация

spanning-tree auto-edge

Эта команда позволяет интерфейсу стать периферийным портом, если за установленный период времени он не получит ни одного BPDU.

Значение по умолчанию: включено

Формат: `spanning-tree auto-edge`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree auto-edge

Данная команда возвращает настройку режима auto-edge для порта к значению по умолчанию.

Формат: `no spanning-tree auto-edge`

Режим ввода команд: конфигурирование интерфейса

spanning-tree backbonefast

Команда используется для включения обнаружения сбоев непрямых соединений и ускорения конвергенции на коммутаторах, настроенных с использованием PVSTP.

Функция backbonefast ускоряет поиск альтернативных путей, когда непрямое соединение с корневым портом выключается.

Настроить backbonefast можно даже в тех случаях, когда коммутатор настроен на использование режимов MST (RSTP) или PVST. Однако работает эта функция, только если коммутатор настроен на использование режима PVST.

Когда коммутатор с настроенной функцией backbonefast получает сбойный BPDU от назначенного корневого коммутатора или заблокированного порта, если существуют альтернативные пути доступа к ним, коммутатор устанавливает максимальное время хранения адреса для интерфейсов, от которых получен сбойный BPDU. Это позволяет заблокированному порту незамедлительно перейти в режим ожидания, из которого он сможет обычным образом вернуться в состояние переадресации.

При получении сбойного BPDU от назначенного моста коммутаторы с настроенной функцией backbonefast отправляют запрос Root Link Query (RLQ) всем неназначенным портам, за исключением порта, с которого был получен сбойный BPDU. Такая проверка подтверждает, что коммутатор может получать корневые пакеты на портах, где ожидается получение BPDU. Порт, из которого был получен первичный сбойный BPDU, исключается из списка, поскольку продемонстрировал ошибку. Назначенные порты исключаются, поскольку они не ведут к корню.

Если на RLQ-запрос получен отрицательный ответ, принимающий порт утерял соединение с корнем, поэтому его BPDU сразу же объявляются устаревшими. Если отрицательный ответ получен по всем неназначенным портам, весь мост утерял соединение с корнем и может начинать расчет STP заново.

Если получен утвердительный ответ, т.е. коммутатор может получить доступ к корневому мосту по одному из портов, порт, на котором был получен первичный сбойный BPDU, сразу же объявляется устаревшим

Мост, который отправляет RLQ-запрос, записывает свой идентификатор моста в PDU. Это позволяет не передавать ответ на назначенные порты.

Мост, который получает RLQ и может соединиться с корнем, перенаправляет запрос к корню через свой корневой порт.

Мост, который получает RLQ и не может соединиться с корнем (идентификатор моста коммутатора отличается от идентификатора корневого моста в запросе) или является корневым мостом, сразу отправляет в ответ на запрос идентификатор своего корневого моста.

Ответы на RLQ-запрос передаются на назначенные порты.

Значение по умолчанию: не определено

Формат: `spanning-tree backbonefast`

Режим ввода команд: глобальная конфигурация

no spanning-tree backbonefast

Данная команда выключает функцию backbonefast.

Использование PVRSTP подразумевает поддержку backbonefast и uplinkfast. Даже если функции uplinkfast и backbonefast настроены, они действуют только в режиме PVSTP.

Формат: `no spanning-tree backbonefast`

Режим ввода команд: глобальная конфигурация

spanning-tree bpdufilter

Используйте данную команду для включения фильтра BPDU на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `spanning-tree bpdufilter`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree bpdufilter

Команда используется для выключения фильтра BPDU на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `no spanning-tree bpdufilter`

Режим ввода команд: конфигурирование интерфейса

spanning-tree bpdufilter default

Данная команда используется для включения фильтра BPDU на всех периферийных интерфейсах.

Значение по умолчанию: выключено

Формат: `spanning-tree bpdufilter default`

Режим ввода команд: глобальная конфигурация

no spanning-tree bpdufilter default

Команда используется для выключения фильтра BPDU на всех периферийных интерфейсах.

Значение по умолчанию: выключено

Формат: `no spanning-tree bpdufilter default`

Режим ввода команд: глобальная конфигурация

spanning-tree bpduflood

Данная команда используется для включения BPDU Flood на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `spanning-tree bpduflood`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree bpduflood

Команда для выключения BPDU Flood на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `no spanning-tree bpduflood`

Режим ввода команд: конфигурирование интерфейса

spanning-tree bpduguard

Данная команда используется для включения BPDU Guard на коммутаторе.

Значение по умолчанию: выключено

Формат: `spanning-tree bpduguard`

Режим ввода команд: глобальная конфигурация

no spanning-tree bpduguard

Команда используется для выключения BPDU Guard на коммутаторе.

Значение по умолчанию: выключено

Формат: `no spanning-tree bpduguard`

Режим ввода команд: глобальная конфигурация

spanning-tree bpdumigrationcheck

Команда используется для принудительной передачи BPDU, связанных с протоколами Rapid spanning tree (RSTP) и Multiple spanning tree (MSTP). Параметр *unit/slot/port* включает передачу BPDU из определенного интерфейса. Ключевое слово *all* позволяет передавать BPDU протоколов RST или MST из всех интерфейсов. Принудительная передача BPDU выполняется только при выполнении данной команды, поэтому она не влияет на системные настройки и не имеет соответствующей no-команды.

Формат: `spanning-tree bpdumigrationcheck {unit/slot/port | all}`

Режим ввода команд: глобальная конфигурация

spanning-tree configuration name

Данная команда устанавливает Configuration Identifier Name для обозначения конфигурации, которую данный коммутатор использует в данный момент. Параметр name является строкой длиной до 32 символов.

Значение по умолчанию: основной MAC-адрес в шестнадцатеричном формате

Формат: `spanning-tree configuration name name`

Режим ввода команд: глобальная конфигурация

no spanning-tree configuration name

Команда возвращает Configuration Identifier Name к значению по умолчанию.

Формат: `no spanning-tree configuration name`

Режим ввода команд: глобальная конфигурация

spanning-tree configuration revision

Команда устанавливает значение Configuration Identifier Revision Level для обозначения конфигурации, которую данный коммутатор использует в данный момент. Параметр Configuration Identifier Revision Level представляет собой число в диапазоне от 0 до 65535.

Значение по умолчанию: 0

Формат: `spanning-tree configuration revision 0-65535`

Режим ввода команд: глобальная конфигурация

no spanning-tree configuration revision

Эта команда возвращает параметр Configuration Identifier Revision Level для обозначения конфигурации, которую данный коммутатор использует в данный момент, к значению по умолчанию.

Формат: `no spanning-tree configuration revision`

Режим ввода команд: глобальная конфигурация

spanning-tree cost

Используйте данную команду для конфигурации стоимости внешнего пути для порта, использованного MST. Если использовано ключевое слово auto, стоимость пути от порта до корневого моста определяется автоматически по скорости интерфейса. Чтобы настроить затраты вручную, укажите значение параметра cost в диапазоне 1–200000000.

Значение по умолчанию: auto

Формат: `spanning-tree cost {cost | auto}`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree cost

Данная команда возвращает настройку затрат внешнего пути для порта к значению по умолчанию.

Формат: `no spanning-tree cost`

Режим ввода команд: конфигурирование интерфейса

spanning-tree edgeport

Данная команда определяет интерфейс (или диапазон интерфейсов) как периферийный порт (порты) в рамках общего и внутреннего остовного дерева. Такая настройка позволяет порту без задержки переходить к состоянию переадресации.

Формат: `spanning-tree edgeport`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree edgeport

Команда определяет, что данный порт не является периферийным портом в рамках общего и внутреннего остовного дерева.

Формат: `no spanning-tree edgeport`

Режим ввода команд: конфигурирование интерфейса

spanning-tree forward-time

Эта команда устанавливает параметр Bridge Forward Delay на новое значение в рамках общего и внутреннего остовного дерева. Значение времени переадресации указывается в секундах в диапазоне от 4 до 30, при этом оно должно быть равным или превышать результат выражения «(Bridge Max Age / 2) + 1».

Значение по умолчанию: 15

Формат: `spanning-tree forward-time 4-30`

Режим ввода команд: глобальная конфигурация

no spanning-tree forward-time

Данная команда устанавливает параметр Bridge Forward Delay в значение для общего и внутреннего остовного дерева по умолчанию.

Формат: `no spanning-tree forward-time`

Режим ввода команд: глобальная конфигурация

spanning-tree guard

Данная команда определяет включение функций контроля петель или контроля корня для интерфейса или диапазона интерфейсов. В случае если ни одна из них не включена, порт работает в соответствии с MSTP.

Значение по умолчанию: none

Формат: `spanning-tree guard {none | root | loop}`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree guard

Команда выключает функции контроля петель или контроля корня для интерфейса.

Формат: `no spanning-tree guard`

Режим ввода команд: конфигурирование интерфейса

spanning-tree max-age

Эта команда устанавливает новое значение параметра Bridge Max Age для общего и внутреннего остовного дерева. Значение максимального времени указывается в секундах в

диапазоне от 4 до 30, при этом оно должно быть равным или меньше результата выражения «2 x (Bridge Forward Delay – 1)».

Значение по умолчанию: 20

Формат: `spanning-tree max-age` *`6-40`*

Режим ввода команд: глобальная конфигурация

no spanning-tree max-age

Команда возвращает параметр Bridge Max Age для общего и внутреннего остовного дерева к значению по умолчанию.

Формат: `no spanning-tree` *`max-age`*

Режим ввода команд: глобальная конфигурация

spanning-tree max-hops

Эта команда устанавливает новое значение параметра Bridge Max Hops для общего и внутреннего остовного дерева. Значение максимального количества хопов указывается в диапазоне от 6 до 40.

Значение по умолчанию: 20

Формат: `spanning-tree max-hops` *`6-40`*

Режим ввода команд: глобальная конфигурация

no spanning-tree max-hops

Эта команда возвращает значение параметра Bridge Max Hops для общего и внутреннего остовного дерева к значению по умолчанию.

Формат: `no spanning-tree max-hops`

Режим ввода команд: глобальная конфигурация

spanning-tree mode

Данная команда настраивает режим глобального остовного дерева посредством остовного дерева VLAN, Rapid-PVST, MST, RSTP или STP. Для коммутатора можно включить только один из протоколов MSTP (RSTP), PVST или RPVST.

При включении PVSTP или Rapid-PVSTP (PVRSTP) протоколы MSTP/RSTP/STP выключаются в оперативном порядке. При переключении на MSTP/RSTP/STP выключается PVSTP/PVRSTP. По умолчанию в включен протокол MSTP. При активном PVSTP или PVRSTP в BPDU содержится информация по сетям VLAN, а не сводная информация остовного дерева (MST/RSTP).

PVSTP обрабатывает независимые данные по каждому остовному дереву настроенных сетей VLAN. PVSTP использует транкинг IEEE 802.1Q и позволяет транкинговой VLAN обслуживать статус блокировки или переадресации каждого порта по каждой сети VLAN. Это позволяет транкинговому порту выполнять переадресацию на одном VLAN и быть заблокированным в других VLAN.

Работа PVRSTP основана на стандарте IEEE 802.1w. Он поддерживает быструю конвергенцию IEEE 802.1D. PVRSTP совместим с остовным деревом IEEE 802.1D. PVRSTP отправляет BPDU всем портам, а не только на корневой мост, и поддерживает состояния удаления, определения и переадресации.

Когда режим меняется на PVRSTP, передача STP BPDU версии 0 прекращается, и во включенные для данного основного дерева сети VLAN передаются PVRSTP BPDU версии 2 с информацией по каждой VLAN. При наличии BPDU версии 0 PVRSTP возвращается отправке BPDU версии 0.

Rapid Spanning Tree Protocol (PVRSTP) при работе по каждой VLAN обеспечивает поддержку функций PVSTP backbonefast и uplinkfast. Включение или выключение этих функций в PVRSTP не предусмотрено.

Значение по умолчанию: выключено

Формат: `spanning-tree mode {mst | pvst | rapid-pvst | stp | rstp }`

Режим ввода команд: глобальная конфигурация

no spanning-tree mode

Данная команда глобально возвращает режим остовного дерева по умолчанию.

Формат: `no spanning-tree mode { pvst | rapid-pvst }`

Режим ввода команд: глобальная конфигурация

spanning-tree mst

Эта команда устанавливает стоимость пути или значение приоритета порта для конкретного порта при использовании экземпляра multiple spanning tree (MST) или common and internal spanning tree (CIST). Если параметр *mstid* определен в соответствии с экземпляром MST, конфигурация выполняется для этого MST. Если параметр *mstid* задан как 0 (идентификатор CIST по умолчанию), конфигурация будет выполнена для CIST.

Если указать опцию **cost**, команда будет устанавливать стоимость пути для порта в экземпляре MST или в CIST, в зависимости от параметра *mstid*. Значение стоимости пути можно установить в диапазоне от 1 до 200000000 или как **auto**. При настройке стоимости как **auto** стоимость пути устанавливается на основании скорости соединения.

Если определена опция **port-priority**, данная команда устанавливает приоритет для данного порта в экземпляре MST или в CIST, в зависимости от параметра *mstid*. Значение **port-priority** можно указать в диапазоне от 0 до 240 с шагом в 16 единиц.

Значение по умолчанию: cost—auto
port-priority—128

Формат: `spanning-tree mst` *`mstid`* `{{cost` *`1-200000000`* `| auto} | port-priority` *`0-240`*`}`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree mst

Данная команда устанавливает стоимость пути или значение приоритета порта для конкретного порта при использовании экземпляра multiple spanning tree (MST) или common and internal spanning tree (CIST) в значение по умолчанию. Если параметр *mstid* определен в соответствии

с экземпляром MST, настройка выполняется для этого MST. Если параметр mstid задан как 0 (идентификатор CIST по умолчанию), настройка будет выполнена для экземпляра CIST.

Если указать опцию **cost**, команда установит значение стоимости пути для порта по умолчанию в экземпляре MST или в CIST, в зависимости от параметра *mstid*, то есть стоимость пути будет определяться на основании скорости соединения.

Если определена опция **port-priority**, данная команда устанавливает приоритет для данного порта в значение по умолчанию в экземпляре MST или в CIST, в зависимости от параметра *mstid*.

Формат: `no spanning-tree mst mstid {cost | port-priority}`

Режим ввода команд: конфигурирование интерфейса

spanning-tree mst instance

Команда добавляет к коммутатору экземпляр MST. Параметр mstid представляет собой число в диапазоне от 1 до 4094, которое соответствует идентификатору добавляемого экземпляра. Коммутатор может поддерживать до 32 экземпляров MST.

Значение по умолчанию: отсутствует

Формат: `spanning-tree mst instance mstid`

Режим ввода команд: глобальная конфигурация

no spanning-tree mst instance

Данная команда удаляет экземпляр MST из настроек коммутатора и выполняет привязку всех связанных с удаленным экземпляром сетей VLAN к CIST. Параметр *mstid* представляет собой число, которое соответствует идентификатору удаляемого экземпляра.

Формат: `no spanning-tree mst instance mstid`

Режим ввода команд: глобальная конфигурация

spanning-tree mst priority

Данная команда устанавливает приоритет моста для конкретного экземпляра MST. Параметр *mstid* представляет собой число, которое соответствует идентификатору соответствующего экземпляра MST. Значение приоритета можно указать как число в диапазоне от 0 до 4094.

Если параметр *mstid* задан как 0 (идентификатор CIST по умолчанию), приоритет моста будет настроен в новое значение для CIST. Значение приоритета моста можно указать как число в диапазоне от 0 до 4094. В соответствии со спецификацией 802.1s 12 наименее значимых битов скрываются. В таких случаях приоритет округляется в меньшую сторону до следующего действительного значения.

Значение по умолчанию: 32768

Формат: `spanning-tree mst priority mstid 0-4094`

Режим ввода команд: глобальная конфигурация

Для настройки приоритета моста в режиме STP,RSTP необходимо использовать команду `spanning-tree mst priority` для нулевого экземпляра MST (Пример: `spanning-tree mst priority 0 <0-61440>`)

no spanning-tree mst priority

Команда устанавливает приоритет моста для конкретного экземпляра MST в значение по умолчанию. Параметр *mstid* представляет собой число, которое соответствует идентификатору соответствующего экземпляра MST.

Если параметр *mstid* передается как 0 (идентификатор CIST по умолчанию), приоритет моста будет настроен в значение по умолчанию для CIST.

Формат: `no spanning-tree mst priority` *`mstid`*

Режим ввода команд: глобальная конфигурация

spanning-tree mst vlan

Данная команда добавляет связь между экземпляром MST и одной или несколькими VLAN таким образом, что эти VLAN перестают быть связанными с CIST. Параметр *mstid* указывается в диапазоне от 0 до 4094 и является идентификатором экземпляра MST. Значение *vlanid* может быть задано как отдельная VLAN, список или диапазон значений. Список VLAN необходимо указывать как список идентификаторов VLAN в диапазоне от 1 до 4093, разделенных запятыми без пробелов. Для указания диапазона VLAN между начальным и конечным идентификатором VLAN ставится дефис (-). Использовать пробелы и нули нельзя. Указанные идентификаторы VLAN могут быть существующими или несуществующими в данной системе.

Формат: `spanning-tree mst vlan` *`mstid vlanid`*

Режим ввода команд: глобальная конфигурация

no spanning-tree mst vlan

Эта команда удаляет связь между экземпляром MST и одной или несколькими VLAN, в результате эти VLAN опять оказываются связаны с CIST.

Формат: `no spanning-tree mst vlan` *`mstid vlanid`*

Режим ввода команд: глобальная конфигурация

spanning-tree port mode

Данная команда устанавливает административный статус порта коммутатора в состояние, когда он включен для использования остовным деревом.

Значение по умолчанию: включено

Формат: `spanning-tree port mode`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree port mode

Эта команда устанавливает административный статус порта коммутатора в состояние, когда он выключен для использования остовным деревом.

Формат: `no spanning-tree port mode`

Режим ввода команд: конфигурирование интерфейса

spanning-tree port mode all

Данная команда устанавливает административный статус всех портов коммутатора во включенное состояние.

Значение по умолчанию: включено

Формат: `spanning-tree port mode all`

Режим ввода команд: глобальная конфигурация

no spanning-tree port mode all

Данная команда устанавливает административный статус всех портов коммутатора в выключенное состояние.

Формат: `no spanning-tree port mode all`

Режим ввода команд: глобальная конфигурация

spanning-tree port-priority

Команда используется для смены значения приоритета порта и позволяет оператору выбирать относительную значимость порта в процессе переадресации. Чтобы данный порт был предпочтительным для переадресации кадров, нужно установить меньшее значение.

Для всех портов LAN значение приоритета по умолчанию установлено как 128. PVSTP/PVRSTP настраивает порт LAN с наименьшим номером в состояние переадресации и блокирует все остальные порты LAN.

Когда конкретный порт LAN настроен как периферийный порт, приложение использует значение приоритета порта.

Значение по умолчанию: включено

Формат: `spanning-tree port-priority` *`0-240`*

Режим ввода команд: конфигурирование интерфейса

spanning-tree tcnguard

Команда включает TCN guard на данном интерфейсе. Во включенном состоянии TCN guard предотвращает дальнейшее распространение любой информации, полученной через данный интерфейс, если она связана с изменением топологии.

Значение по умолчанию: выключено

Формат: `spanning-tree tcnguard`

Режим ввода команд: конфигурирование интерфейса

no spanning-tree tcnguard

Команда устанавливает состояние TCN guard на данном интерфейсе в значение по умолчанию.

Формат: `no spanning-tree tcnguard`

Режим ввода команд: конфигурирование интерфейса

spanning-tree transmit

Данная команда устанавливает параметр отсчета задержки для передающего моста.

Значение по умолчанию: 6

Формат: `spanning-tree transmit hold-count`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
hold-count	Параметр отсчета задержки для передающего моста (целое число в промежутке от 1 до 10).

spanning-tree uplinkfast

Используйте данную команду для настройки частоты отправки пустых кадров (в пакетах за секунду) после переключения коммутатора, настроенного на использование PVSTP, на альтернативный порт, а также для включения на PVSTP-коммутаторе режима uplinkfast. Диапазон значений — от 0 до 32000; по умолчанию — 150. Дополнительным эффектом при выполнении данной команды становится ускоренная конвергенция остовного дерева после переключения на альтернативный порт.

Настройка uplinkfast может быть выполнена, даже если коммутатор настроен для MST (RSTP), но действовать она будет только тогда, когда коммутатор находится в режиме PVST. Включение uplinkfast повышает приоритет на 3000. Пути стоимостью менее 3000 при включении uplinkfast получают дополнительно 3000. Это сокращает для коммутатора возможность стать корневым коммутатором.

При обнаружении ошибки корневого порта uplinkfast незамедлительно переключается на альтернативный корневой порт и изменяет состояние нового корневого порта непосредственно на переадресацию. Для таких событий выполняется отправка TCN.

После переключения на альтернативный порт (новый коневой порт) uplinkfast выполняет многоадресную рассылку на новый корневой порт пустых кадров от имени каждого присоединенного устройства, чтобы остальные устройства в сети знали, как использовать второстепенное соединения для доступа к этому устройству.

Использование PVRSTP подразумевает поддержку backbonefast и uplinkfast. Включение или выключение этих функций в настроенном на PVRSTP коммутаторе не предусмотрено.

Значение по умолчанию: 150

Формат: `spanning-tree uplinkfast [max-update-rate` *`packets`*`]`

Режим ввода команд: глобальная конфигурация

no spanning-tree uplinkfast

Данная команда выключает uplinkfast в настроенных на PVRSTP коммутаторах. При этом все значения приоритетов коммутатора и стоимости пути, которые не изменялись относительно настроек по умолчанию, устанавливаются в значения по умолчанию.

Формат: `no spanning-tree uplinkfast [max-update-rate]`

Режим ввода команд: глобальная конфигурация

spanning-tree vlan

Данная команда используется для включения или выключения остовного дерева в сети VLAN.

Значение по умолчанию: отсутствует

Формат: `spanning-tree vlan vlan-list`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
vlan list	Сети VLAN, к которым будет применена команда,

spanning-tree vlan cost

Команда назначает стоимость пути для порта в сети VLAN. Допустимые значения — от 1 до 200000000 или auto. При выборе значения auto стоимость пути устанавливается на основании скорости соединения.

Значение по умолчанию: отсутствует

Формат: `spanning-tree vlan vlan-id cost {auto |1-200000000}`

Режим ввода команд: конфигурирование интерфейса

spanning-tree vlan forward-time

Команда используется для настройки времени задержки переадресации остовного дерева для одной или нескольких сетей VLAN. Значение по умолчанию — 15 секунд.

Установите меньшее значение, чтобы ускорить переход к переадресации. При настройке данного параметра сетевой оператор должен учитывать совокупную задержку распространения BPDU, максимальное время жизни кадра, максимальную задержку передачи и предельное значение для времени жизни сообщения для конкретной сети.

Значение по умолчанию: 15 секунд

Формат: `spanning-tree vlan vlan-list forward-time 4-30`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
vlan list	Сети VLAN, к которым будет применена команда.
forward-time	Задержка переадресации остовного дерева от 4 до 30 секунд.

spanning-tree vlan hello-time

Данная команда используется для настройки периода «hello» остовного дерева для одной или нескольких сетей VLAN. Значение по умолчанию — 2 секунды. Установите меньшее значение, чтобы ускорить обнаружение изменений топологии.

Значение по умолчанию: 2 секунды

Формат: `spanning-tree vlan vlan-list hello-time 1-10`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
vlan-list	Сети VLAN, к которым будет применена команда,
hello-time	Задержка переадресации остовного дерева от 1 до 10 секунд.

spanning-tree vlan max-age

Используйте данную команду для конфигурации максимального срока жизни остовного дерева для одной или нескольких сетей VLAN. Значение по умолчанию — 20 секунд.

Установите меньшее значение, чтобы ускорить обнаружение изменений топологии. При настройке данного параметра сетевой оператор должен учитывать совокупную задержку распространения BPDU и предельное значение для времени жизни сообщения для топологии конкретной сети.

Настройка по умолчанию составляет 20 секунд и подходит для соединения диаметром 7 с величиной потерянных сообщений 3, задержкой передачи 1, периодом «hello» 2 с, переоценкой на мост 1 с и задержкой BPDU 1 с. Для соединения диаметром 4 приемлема настройка 16 секунд, если все остальные значения времени используются в значениях по умолчанию.

Значение по умолчанию: 20 секунд

Формат: `spanning-tree vlan` *`vlan-list`* `max-age` *`6-40`*

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
vlan-list	Сети VLAN, к которым будет применена команда.
hello-time	Задержка переадресации остовного дерева от 1 до 10 секунд.

spanning-tree vlan root

Используйте данную команду для настройки коммутатора в качестве корневого моста или резервного корневого моста за счет изменения приоритета моста со значения по умолчанию (32768) на меньшее значение, соответствующее роли корневого (или резервного) моста.

Логика выполнения команды обеспечивает настройку приоритета моста в минимальное (для основного моста) или соседнее с минимальным значение (для резервного моста) для данной сети VLAN или диапазона VLAN.

Значение по умолчанию: 32768

Формат: `spanning-tree vlan` *`vlan-list`* `root {primary|secondary}`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
vlan-list	Сети VLAN, к которым будет применена команда.

spanning-tree vlan port-priority

Команда используется для изменения значения приоритета порта в рамках сети VLAN, чтобы позволить оператору выбирать относительную значимость порта VLAN в процессе выбора переадресации, если порт настроен на двухточечный тип соединения. Чтобы данный порт был предпочтительным для переадресации кадров, нужно установить меньшее значение.

Значение по умолчанию: отсутствует

Формат: `spanning-tree vlan` *`vlan-id`* `port-priority` *`priority`*

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
vlan-list	Сети VLAN, к которым будет применена команда.

priority	Приоритет порта VLAN. Диапазон значений: 0-255.

spanning-tree vlan priority

Используйте данную команду для настройки приоритета моста в рамках VLAN. Значение по умолчанию — 32768.

Если выбранное значение не является одним из установленных значений, оно будет округлено до ближайшего действительного значения.

Значение по умолчанию: 32768

Формат: `spanning-tree vlan` *`vlan-list`* `priority` *`priority`*

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
vlan-list	Сети VLAN, к которым будет применена команда.
Priority	Приоритет моста VLAN. Действительные значения: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 и 61440

show spanning-tree

Данная команда отображает настройки остовного дерева для CIST. Выводятся следующие подробности.

Формат: `show spanning-tree`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
Bridge Priority	Определяет приоритет моста для Common and Internal Spanning Tree (CIST). Величина в целых числах между 0 и 61440. Приоритет порта отображается в цифрах, кратных 4096.
Bridge Identifer	Идентификатор моста для CIST. Составлен из приоритета моста и основного MAC-адреса моста.
Time Since Topology Change	Время в секундах.
Topology Change Count	Счетчик количества изменений.
Topology Change in Progress	Логическое значение параметра изменения топологии для коммутатора, показывающее, есть ли в данный момент незавершенные изменения топологии на каком-либо порте, связанном с данным CIST.
Designated Root	Идентификатор корневого моста. Состоит из приоритета моста и основного MAC-адреса моста.
Root Path Cost	Параметр, указывающий значение стоимости корневого пути для CIST.
Root Port Identifier	Идентификатор порта для получения доступа к назначенному корню CIST.
Bridge Max Age	Выведенное значение.
Bridge Max Hops	Счетчик максимального количества хопов моста для устройства.
Root Port Bridge Forward Delay	Выведенное значение.
Hello Time	Настроенное значение параметра для CIST.

Bridge Hold Time	Минимальное время между передачей конфигурационных Bridge Protocol Data Units (BPDU).
CST Regional Root	Идентификатор моста для регионального корня CIST. Составлен из приоритета моста и основного MAC-адреса моста.
Regional Root Path Cost	Стоимость пути для регионального корня CIST.
Associated FIDs	Список идентификаторов таблиц коммутации, связанных на данный момент с этим экземпляром.
Associated VLANs	Список идентификаторов сетей VLAN, связанных на данный момент с этим экземпляром.

show spanning-tree active

Используйте эту команду для отображения значений остовного дерева на активных портах для соответствующих режимов (xSTP и PV(R)STP).

Формат: show spanning-tree active

Режим ввода команд: привилегированный
пользовательский

show spanning-tree backbonefast

Данная команда отображает информацию остовного дерева для backbonefast.

Формат: `show spanning-tree backbonefast`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
Transitions via Backbonefast	Количество переходов backbonefast.
Inferior BPDUs received (all VLANs)	Количество сбойных BPDU, полученных по всем VLAN.
RLQ request PDUs received (all VLANs)	Количество PDU с запросами Root Link Query (RLQ), полученных по всем VLAN.
RLQ response PDUs received (all VLANs)	Количество PDU с ответами RLQ, полученных по всем VLAN.
RLQ request PDUs sent (all VLANs)	Количество PDU с запросами RLQ, отправленных по всем VLAN.
RLQ response PDUs sent (all VLANs)	Количество PDU с ответами RLQ, отправленных по всем VLAN.

show spanning-tree brief

Команда для отображения настроек остовного дерева для моста. Отображается следующая информация.

Формат: `show spanning-tree brief`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
Bridge Priority	Настраиваемое значение.
Bridge Identifier	Идентификатор моста для выбранного экземпляра MST. Составлен из приоритета моста и основного MAC-адреса моста.
Bridge Max Age	Настраиваемое значение.
Bridge Max Hops	Счетчик максимального количества хопов моста для устройства.

Bridge Hello Time	Настраиваемое значение.
Bridge Forward Delay	Настраиваемое значение.
Bridge Hold Time	Минимальное время между передачей конфигурационных Bridge Protocol Data Units (BPDU).

show spanning-tree interface

Данная команда отображает настройки и параметры для определенного порта коммутатора в рамках CIST. Параметр *unit/slot/port* определяет нужный порт коммутатора. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG. В результате выполнения команды отображаются следующие данные:

Формат: `show spanning-tree interface` *`unit/slot/port`*`|lag` *`lag-intf-num`*

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
Hello Time	Административный период «hello» для данного порта.
Port Mode	Включен или выключен.
BPDU Guard Effect	Включен или выключен.
Root Guard	Включен или выключен.
Loop Guard	Включен или выключен.
TCN Guard	Включено или выключено распространение полученных уведомлений об изменениях топологии и топологических изменений на другие порты.
BPDU Filter Mode	Включен или выключен.
BPDU Flood Mode	Включен или выключен.
Auto Edge	Включена или выключена функция, под действием которой порт, не получивший ни одного BPDU за настроенный период **edge delay**, становится периферийным портом и быстрей переходит в режим переадресации.
Port Up Time Since Counters Last Cleared	Время с последней перезагрузки порта, отображается в днях, часах, минутах и секундах.
STP BPDUs Transmitted	Отправленные BPDU для STP-протокола.
STP BPDUs Received	Полученные BPDU для STP-протокола.
RSTP BPDUs Transmitted	Отправленные BPDU для RSTP-протокола.
RSTP BPDUs Received	Полученные BPDU для RSTP-протокола.
MSTP BPDUs Transmitted	Отправленные BPDU для MSTP-протокола.
MSTP BPDUs Received	Полученные BPDU для MSTP-протокола.

show spanning-tree mst detailed

Данная команда отображает подробные настройки экземпляра MST.

Формат: `show spanning-tree mst detailed` *`mstid`*

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***

mstid	Идентификатор экземпляра MST. Диапазон значений: от 0 до 4094.

show spanning-tree mst port detailed

Данная команда отображает подробные настройки и параметры для определенного порта коммутатора в рамках конкретного экземпляра MST. Параметр *mstid* представляет собой число, которое соответствует идентификатору соответствующего экземпляра MST. Параметр *unit/slot/port* определяет нужный порт коммутатора. Вместо параметра *unit/slot/port* можно использовать lag lag-intf-num как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `show spanning-tree mst port detailed` *mstid* *unit/slot/port*|`lag` *lag-intf-num*

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
MST Instance ID	Идентификатор существующего экземпляра MST. Диапазон значений: от 0 до 4094.
Port Identifier	Идентификатор выбранного порта в рамках выбранного экземпляра MST. Состоит из приоритета порта и номера интерфейса порта.
Port Priority	Приоритет для определенного порта в рамках выбранного экземпляра MST. Приоритет порта выражается в числах, кратных 16.
Port Forwarding State	Текущий статус остовного дерева данного порта.
Port Role	Каждый включенный порт моста MST получает роль порта для каждого остовного дерева. Возможны следующие значения для роли порта: Root Port, Designated Port, Alternate Port, Backup Port, Master Port или Disabled Port.
Auto-Calculate Port Path Cost	Показывает, включено ли автоматическое вычисление стоимости пути для порта.
Port Path Cost	Настраиваемая величина параметра стоимости пути внутреннего порта.
Designated Root	Идентификатор назначенного корня для данного порта.
Root Path Cost	Стоимость пути до корневого моста для данного экземпляра. Если данный мост является корневым для данного экземпляра, стоимость пути будет равна нулю.
Designated Bridge	Идентификатор для моста с назначенным портом.
Designated Port Identifier	Порт назначенного моста, который предлагает наименьшую стоимость пути для LAN.
Loop Inconsistent State	Непостоянное состояние текущей петли данного порта в экземпляре MST. При непостоянном состоянии петли порт не может получить BPDU, если в настройках включена функция loop guard. Непостоянное состояние петли поддерживает порт в состоянии блокировки, пока не получен следующий BPDU.
Transitions Into Loop Inconsistent State	Счетчик переходов интерфейса в непостоянное состояние петли.
Transitions Out of Loop Inconsistent State	Счетчик выхода интерфейса из непостоянного состояния петли.

Если параметр *mstid* задан как 0 (идентификатор CIST по умолчанию), данная команда отображает настройки и параметры для конкретного порта коммутатора в рамках CIST. Параметр *unit/slot/port* определяет нужный порт коммутатора. В данном случае отображается следующее.

Параметр	***Описание***
Port Identifier	Идентификатор данного порта в рамках CIST.
Port Priority	Приоритет порта в рамках CIST.
Port Forwarding State	Состояние переадресации данного порта в рамках CIST.
Port Role	Роль данного интерфейса в рамках CIST.
Auto-Calculate Port Path Cost	Показывает, включено или выключено автоматическое вычисление стоимости пути для порта.
Port Path Cost	Настроенная стоимость пути для данного интерфейса.
Auto-Calculate External Port Path Cost	Показывает, включено ли автоматическое вычисление стоимости внешнего пути для порта.
External Port Path Cost	Стоимость пути до корневого моста CIST через границы региона. В случае если порт является граничным портом для региона MSTP, используется стоимость внешнего пути.
Designated Root	Идентификатор назначенного корня для данного порта в рамках CIST.
Root Path Cost	Стоимость корневого пути к LAN для данного порта.
Designated Bridge	Мост, содержащий назначенный порт.
Designated Port Identifier	Порт назначенного моста, который предлагает наименьшую стоимость пути для LAN.
Topology Change Acknowledgment	Значение флага при передаче следующего конфигурационного BPDU, показывающее, происходит ли в данный момент изменение топологии для данного порта.
Hello Time	Период «hello», используемый для данного порта.
Edge Port	Настроенное значение, показывающее, является ли данный порт периферийным портом.
Edge Port Status	Выведенное значение состояния периферийного порта. Если данный порт работает как периферийный, значение — true, если нет — false.
Point To Point MAC Status	Выведенное значение, которое показывает, является ли данный порт частью двухточечного соединения.
CST Regional Root	Идентификатор регионального корня для данного порта.
CST Internal Root Path Cost	Стоимость внутреннего корневого пути к LAN для назначенного внешнего порта.
Loop Inconsistent State	Непостоянное состояние текущей петли данного порта в экземпляре MST. При непостоянном состоянии петли порт не может получить BPDU, если в настройках включена функция loop guard. Непостоянное состояние петли поддерживает порт в состоянии блокировки, пока не получен следующий BPDU.
Transitions Into Loop Inconsistent State	Счетчик переходов интерфейса в непостоянное состояние петли.
Transitions Out of Loop Inconsistent State	Счетчик выхода интерфейса из непостоянного состояния петли.

show spanning-tree mst port summary

Данная команда отображает настройки одного или всех портов в рамках определенного экземпляра MST. Параметр *mstid* определяет экземпляр MST. Параметр *{unit/slot/port|all}* определяет нужный порт коммутатора порта или все порты. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр

lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf- num* должно указывать номер порта LAG.

Если параметр *mstid* задан как 0 (идентификатор CIST по умолчанию), отображается сводное состояние для одного или всех портов в рамках CIST.

Формат: `show spanning-tree mst port summary` *mstid* *{unit/slot/port* `|lag` *lag-intf-num*`|` `all}`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
MST Instance ID	Экземпляр MST, связанный с данным портом.
Interface	Интерфейс в формате unit/slot/port.
STP Mode	Определяет состояние остовного дерева на данном порте (включено или выключено).
Type	В настоящий момент не используется.
STP State	Состояние переадресации порта в данном экземпляре остовного дерева.
Port Role	Роль определенного порта в рамках остовного дерева.
Desc	Определяет, находится ли порт в непостоянном состоянии петли. Если функция loop guard не доступна, это поле остается пустым.

show spanning-tree mst port summary active

Эта команда отображает настройки для портов, представляющих собой активные соединения, в рамках определенного экземпляра MST.

Формат: `show spanning-tree mst port summary` *mstid* `active`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
MST Instance ID	Экземпляр MST, связанный с данным портом.
Interface	Интерфейс в формате unit/slot/port.
STP Mode	Определяет состояние основного дерева на данном порте (включено или выключено).
Type	В настоящий момент не используется.
STP State	Состояние переадресации порта в данном экземпляре остовного дерева.
Port Role	Роль определенного порта в рамках остовного дерева.
Desc	Определяет, находится ли порт в непостоянном состоянии петли. Если функция loop guard не доступна, это поле остается пустым.

show spanning-tree mst summary

Данная команда отображает сводные данные обо всех экземплярах MST в коммутаторе. По итогам выполнения команды отображается следующее.

Формат: `show spanning-tree mst summary`

Режим ввода команд: привилегированный
пользовательский

Параметр	*Описание*
MST Instance ID List	Список идентификаторов MST, настроенных на данный момент.
For each MSTID: • Associated FIDs • Associated VLANs	• Список идентификаторов таблиц коммутации, связанных с этим экземпляром; • Список идентификаторов сетей VLAN, связанных с этим экземпляром.

show spanning-tree summary

Эта команда отображает настройки и параметры остовного дерева для коммутатора. В результате выполнения команды отображаются следующие данные:

Формат: `show spanning-tree summary`

Режим ввода команд: привилегированный
пользовательский

Параметр	*Описание*
Spanning Tree Adminmode	Включено или выключено.
Spanning Tree Version	В настоящее время поддерживается версия 802.1 (IEEE 802.1s, IEEE 802.1w или IEEE 802.1d), основанная на параметре Force Protocol Version (FPV).
BPDU Guard Mode	Включен или выключен.
BPDU Filter Mode	Включен или выключен.
Configuration Name	Идентификатор, используемый для определения текущей конфигурации.
Configuration Revision Level	Идентификатор, используемый для определения текущей конфигурации.
Configuration Digest Key	Сгенерированный ключ, используемый при обмене BPDU.
Configuration Format Selector	Определяет версию формата конфигурации, используемой при обмене BPDU. Значение по умолчанию — ноль.
MST Instances	Список всех экземпляров MST, настроенных на коммутаторе.

show spanning-tree uplinkfast

Данная команда отображает информацию остовного дерева для uplinkfast.

Формат: `show spanning-tree uplinkfast`

Режим ввода команд: привилегированный
пользовательский

Параметр	*Описание*
Uplinkfast transitions (all VLANs)	Список идентификаторов MST, настроенных на данный момент.
Proxy multicast addresses transmitted (all VLANs)	Количество групповых прокси-адресов, переданных на все VLAN.

show spanning-tree vlan

Команда отображает информацию остовного дерева по каждой VLAN, а также список ролей и состояний порта с соответствующей стоимостью порта. Параметр *vlan-list* представляет собой список сетей VLAN, перечисленных через запятую без пробелов, либо диапазон VLAN. Диапазон сетей VLAN задается в виде X-Y, где X и Y являются действительными идентификаторами VLAN, при этом X<Y.

Параметр *vlanid* соответствует существующему идентификатору VLAN.

Формат: `show spanning-tree vlan {vlanid | vlan-list}`

Режим ввода команд: привилегированный
пользовательский

spanning-tree mac-address dot1d

Команда устанавливает режим обработки Bridge PDU на основании их MAC адреса назначения и позволяет использовать протокол STP с мостами, работающими по стандарту 802.1ad (Provider Bridges). Изменяет MAC-адрес, с которым отправляются и принимаются BPDU на 01-80-C2-00-00-00. Входящие BPDU с адресом, не соответствующим режиму, отбрасываются.

Значение по умолчанию: включено

Формат: `spanning-tree mac-address dot1d`

Режим ввода команды: режим конфигурации интерфейса

no spanning-tree mac-address

Отключить режим обработки Bridge PDU на основании их MAC адреса назначения.

Формат: `no spanning-tree mac-address`

Режим ввода команд: Режим конфигурации интерфейса

spanning-tree mac-address dot1ad

Изменяет MAC-адрес, с которым отправляются и принимаются BPDU на 01-80-C2-00-00-08. В режиме dot1ad обрабатываются и передаются кадры с Provider Bridge Group Address. Входящие BPDU с адресом, не соответствующим режиму, отбрасываются.

Значение по умолчанию: выключено

Формат: `spanning-tree mac-address dot1ad`

Режим ввода команды: режим конфигурации интерфейса

no spanning-tree mac-address

Отключить режим обработки Bridge PDU на основании их MAC адреса назначения.

Формат: `no spanning-tree mac-address`

Режим ввода команд: режим конфигурации интерфейса

spanning-tree mac-address auto

Изменяет MAC-адрес, с которым принимаются BPDU на 01-80-C2-00-00-08, на прочих изменяет MAC-адрес на 01-80-C2-00-00-00.

Значение по умолчанию: выключено

Формат: `spanning-tree mac-address auto`

Режим ввода команды: режим конфигурации интерфейса

no spanning-tree mac-address

Отключить режим обработки Bridge PDU на основании их MAC адреса назначения.

Формат: `no spanning-tree mac-address`

Режим ввода команд: режим конфигурации интерфейса

9.3 Команды настройки защиты от петель

В этой части описаны команды, которые используются для настройки защиты от петель. Защита от петель определяет физические и локальные петли между Ethernet-портами в устройстве. Перед включением на уровне интерфейса защита от петель должна быть включена глобально.

keepalive (режим глобальной конфигурации)

Данная команда включает защиту от петель на уровне системы.

Значение по умолчанию: выключено

Формат: `keepalive`

Режим ввода команд: глобальная конфигурация

no keepalive

Эта команда выключает защиту от петель на уровне системы. Команда также устанавливает интервал передачи и число повторных попыток в значение по умолчанию.

Формат: `no keepalive`

Режим ввода команд: глобальная конфигурация

keepalive (режим конфигурирования интерфейса)

Данная команда включает функцию keepalive для определенного интерфейса.

Значение по умолчанию: отсутствует

Формат: `keepalive`

Режим ввода команд: конфигурирование интерфейса

no keepalive

Эта команда выключает функцию keepalive для определенного интерфейса.

Формат: `keepalive`

Режим ввода команд: конфигурирование интерфейса

keepalive action

Эта команда настраивает действие, которое должно выполняться на порте при обнаружении петли.

Значение по умолчанию: выключено.

Формат: `keepalive receive-action {log|disable|both}`

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
log	Только запись сообщения. В режиме log выполняется только запись сообщения в журнал буфера, работа порта не прекращается.

disable	Прекращение работы порта. Это значение используется по умолчанию.
both	Запись сообщения и выключение порта.

no keepalive action

Данная команда возвращает значение по умолчанию (выключение порта) для действия, выполняемого при обнаружении петли.

Формат: `no keepalive action`

Режим ввода команд: конфигурирование интерфейса

keepalive disable-timer

Данная команда настраивает время (в секундах), на которое порт прекращает работу при обнаружении петли. Значение по умолчанию — ноль, т. е. повторное включение порта выполняется вручную.

Значение по умолчанию: 0

Формат: `keep-alive disable-timer` *`value`*

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
log	Только запись сообщения. В режиме log выполняется только запись сообщения в журнал буфера, работа порта не прекращается.
disable	Прекращение работы порта. Это значение используется по умолчанию.
both	Запись сообщения и выключение порта.

no keepalive action

Данная команда возвращает значение по умолчанию (выключение порта) для действия, выполняемого при обнаружении петли.

Формат: `no keepalive action`

Режим ввода команд: конфигурирование интерфейса

keepalive disable-timer

Данная команда настраивает время (в секундах), на которое порт прекращает работу при обнаружении петли. Значение по умолчанию — ноль, т. е. повторное включение порта выполняется вручную.

Значение по умолчанию: 0

Формат: `keep-alive disable-timer` *`value`*

Режим ввода команд: глобальная конфигурация

keepalive retry

Данная команда настраивает время в секундах между передачей пакетов keepalive. Retry — дополнительный параметр, который задает количество пакетов keepalive, после получения которого коммутатором интерфейс будет выключен.

Значение по умолчанию: 5

Формат: `keepalive val [retry]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
val	Время (в секундах) между передачей пакетов keepalive.
retry	Устанавливает количество пакетов keepalive, после получения которого коммутатором интерфейс будет выключен.

show keepalive

Команда для отображения глобальной конфигурации функции keepalive.

Значение по умолчанию: отсутствует

Формат: `show keepalive`

Режим ввода команд: привилегированный

show keepalive statistics

Данная команда отображает статистику keepalive для каждого порта или для определенного порта.

Значение по умолчанию: отсутствует

Формат: `show keepalive statistics {`*`port-num`* `| all }`

Режим ввода команд: привилегированный

Параметр	*Описание*
port-num	Номер порта, для которого нужно вывести статистику.
all	Отображает статистику для всех портов.

clear counters keepalive

Эта команда сбрасывает статистику keepalive, связанную с портами (например, количество отправленных пакетов, принятых пакетов и пакетов петли).

Значение по умолчанию: отсутствует

Формат: `clear counters keepalive`

Режим ввода команд: привилегированный

9.4 Команды настройки VLAN

В этой части описаны команды, которые используются для настройки VLAN.

vlan database

Данная команда предоставляет доступ к режиму конфигурирования VLAN, который позволяет настраивать характеристики VLAN.

Формат: `vlan database`

Режим ввода команд: привилегированный

vlan

Эта команда создает новую сеть VLAN и назначает ей идентификатор. ID — это действительный идентификационный номер (для VLAN по умолчанию зарезервирован ID 1). Диапазон идентификаторов VLAN — от 2 до 4094.

Формат: `vlan` *`2-4094`*

Режим ввода команд: конфигурирование VLAN

no vlan

Команда для удаления существующей VLAN. ID — это действительный идентификационный номер (для VLAN по умолчанию зарезервирован ID 1). Диапазон идентификаторов VLAN — от 2 до 4094.

Формат: `no vlan` *`2-4094`*

Режим ввода команд: конфигурирование VLAN

vlan acceptframe

Эта команда устанавливает режим принятия кадров на интерфейсе или диапазоне интерфейсов. В режиме VLAN Only нетегированные кадры и кадры приоритета на этом интерфейсе отбрасываются. В режиме Admit All нетегированные кадры и кадры приоритета на этом интерфейсе принимаются и связываются со значением идентификатора VLAN интерфейса для данного порта. В режиме admituntaggedonly на данном интерфейсе принимаются только нетегированные кадры, а тегированные — отбрасываются. В любом из вариантов тегированные кадры VLAN переадресуются в соответствии со спецификацией IEEE 802.1Q для VLAN.

Значение по умолчанию: all

Формат: `vlan acceptframe {admituntaggedonly | vlanonly | all}`

Режим ввода команд: конфигурирование интерфейса

no vlan acceptframe

Данная команда возвращает режим принятия кадров на интерфейсе или диапазоне интерфейсов в значение по умолчанию.

Формат: `no vlan acceptframe`

Режим ввода команд: конфигурирование интерфейса

vlan ingressfilter

Эта команда включает фильтрацию входящих пакетов на интерфейсе или диапазоне интерфейсов. Если фильтрация входящих пакетов выключена, при получении кадров, идентификатор VLAN у которых не соответствуют набору VLAN интерфейса принимающего устройства, выполняется прием и переадресация на порты, которые входят в состав нужной VLAN.

Значение по умолчанию: выключено

Формат: `vlan ingressfilter`

Режим ввода команд: конфигурирование интерфейса

no vlan ingressfilter

Данная команда выключает фильтрацию входящих пакетов. Если фильтрация входящих пакетов выключена, при получении кадров, идентификатор VLAN у которых не соответствуют набору VLAN интерфейса принимающего устройства, выполняется прием и переадресация на порты, которые входят в состав нужной VLAN.

Формат: `no vlan ingressfilter`

Режим ввода команд: конфигурирование интерфейса

vlan internal allocation

Команда, выполняющая настройку идентификаторов VLAN для использования с интерфейсами маршрутизации на основе портов. Когда интерфейс маршрутизации на основе порта создан, ему автоматически назначается неиспользуемый идентификатор VLAN.

Формат: `vlan internal allocation {base` *`vlan-id`* `| policy ascending | policy decending}`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
base vlan-id	Первый идентификатор VLAN, который будет назначен интерфейсу маршрутизации на основе порта.
policy ascending	Идентификаторы VLAN, назначаемые интерфейсам маршрутизации на основе портов, начинаются с первого и следуют в порядке увеличения.
policy descending	Идентификаторы VLAN, назначаемые интерфейсам маршрутизации на основе портов, начинаются с первого и следуют в порядке уменьшения.

vlan makestatic

Данная команда превращает динамически созданную VLAN (созданную при регистрации GVRP) в статичную VLAN (которая настраивается и определяется на постоянной основе). ID — действительный идентификационный номер VLAN. Диапазон идентификаторов VLAN — от 2 до 4094.

Формат: `vlan makestatic` *`2-4094`*

Режим ввода команд: конфигурирование VLAN

vlan name

Эта команда изменяет имя VLAN. Имя состоит из буквенно-цифровых символов (максимум 32), а ID — это действительный идентификационный номер VLAN. Диапазон идентификаторов — от 1 до 4094.

Значение по умолчанию: VLAN ID 1 — значение по умолчанию
другие VLAN — пустая строка

Формат: `vlan name` *`1-4094 name`*

Режим ввода команд: конфигурирование VLAN

no vlan name

Эта команда устанавливает имя VLAN как пустую строку.

Формат: `no vlan name 1-4094`

Режим ввода команд: конфигурирование VLAN

vlan participation

Данная команда настраивает степень участия определенного интерфейса или диапазона интерфейсов в сети VLAN. ID — это действительный идентификационный номер VLAN; interface — это действительный номер интерфейса.

Формат: `vlan participation {exclude | include | auto} 1-4094`

Режим ввода команд: конфигурирование интерфейса

Возможные опции степени участия.

Опции	***Значение***
include	Интерфейс всегда входит в данную VLAN. Эквивалентно фиксированной регистрации.
exclude	Интерфейс никогда не входит в данную VLAN. Эквивалентно запрету регистрации.
auto	Интерфейс динамически регистрируется в данной VLAN с помощью GVRP и не входит в нее до тех пор, пока на интерфейс не поступит запрос на присоединение. Это эквивалентно нормальной регистрации.

vlan participation all

Эта команда настраивает степень участия всех интерфейсов в сети VLAN. ID — действительный идентификационный номер VLAN.

Формат: `vlan participation all {exclude | include | auto} 1-4094`

Режим ввода команд: глобальная конфигурация

Можно использовать следующие опции степени участия.

Опции	***Значение***
include	Интерфейс всегда входит в данную VLAN. Эквивалентно фиксированной регистрации.
exclude	Интерфейс никогда не входит в данную VLAN. Эквивалентно запрету регистрации.
auto	Интерфейс динамически регистрируется в данной VLAN с помощью GVRP. Интерфейс не входит в VLAN до тех пор, пока не поступит запрос на присоединение. Это эквивалентно нормальной регистрации.

vlan port acceptframe all

Данная команда устанавливает режим принятия кадров для всех интерфейсов.

Значение по умолчанию: all

Формат: `vlan port acceptframe all {vlanonly | admituntaggedonly |all}`

Режим ввода команд: глобальная конфигурация

Варианты режимов приведены ниже.

Режим	***Значение***
Режим VLAN Only	Нетегированные кадры и кадры приоритета на этом интерфейсе отбрасываются.

Режим Admit Untagged Only	Тегированные VLAN-кадры и кадры приоритета на этом интерфейсе отбрасываются.
Режим Admit All	Нетегированные кадры и кадры приоритета на этом интерфейсе принимаются и связываются со значением идентификатора VLAN-интерфейса для данного порта.

В любом из режимов тегированные кадры VLAN переадресуются в соответствии со спецификацией IEEE 802.1Q для VLAN.

no vlan port acceptframe all

Данная команда устанавливает режим принятия кадров для всех интерфейсов в значение Admit All. В режиме Admit All нетегированные кадры и кадры приоритета на этом интерфейсе принимаются и связываются со значением идентификатора VLAN-интерфейса для данного порта. В любом из режимов тегированные кадры VLAN переадресуются в соответствии со спецификацией IEEE 802.1Q для VLAN.

Формат: `no vlan port acceptframe all`

Режим ввода команд: глобальная конфигурация

vlan port ingressfilter all

Эта команда включает фильтрацию входящих пакетов для всех портов. Если фильтрация входящих пакетов выключена, при получении кадров, идентификатор VLAN у которых не соответствуют набору VLAN интерфейса принимающего устройства, выполняется прием и переадресация на порты, которые входят в состав нужной VLAN.

Значение по умолчанию: выключено

Формат: vlan port ingressfilter all

Режим ввода команд: глобальная конфигурация

no vlan port ingressfilter all

Данная команда выключает фильтрацию входящих пакетов для всех портов. Если фильтрация входящих пакетов выключена, при получении кадров, идентификатор VLAN у которых не соответствуют набору VLAN-интерфейса принимающего устройства, выполняется прием и переадресация на порты, которые входят в состав нужной VLAN.

Формат: `no vlan port ingressfilter all`

Режим ввода команд: глобальная конфигурация

vlan port pvid all

Эта команда изменяет идентификатор VLAN для всех интерфейсов.

Значение по умолчанию: 1

Формат: `vlan port pvid all` *`1-4094`*

Режим ввода команд: глобальная конфигурация

no vlan port pvid all

Эта команда устанавливает значение идентификатора VLAN для всех интерфейсов как 1.

Формат: `no vlan port pvid all`

Режим ввода команд: глобальная конфигурация

vlan port tagging all

Данная команда включает настройку тегирования для всех интерфейсов в сети VLAN. Если тегирование включено, трафик передается в виде тегированных кадров. Если тегирование выключено, трафик передается в виде нетегированных кадров. ID — действительный идентификационный номер VLAN.

Формат: `vlan port tagging all` *`1-4094`*

Режим ввода команд: глобальная конфигурация

no vlan port tagging all

Эта команда выключает настройку тегирования для всех интерфейсов в сети VLAN. Если тегирование выключено, трафик передается в виде нетегированных кадров. ID — действительный идентификационный номер VLAN.

Формат: `no vlan port tagging all`

Режим ввода команд: глобальная конфигурация

vlan protocol group

Эта команда добавляет в систему группы протоколов для классификации VLAN. groupid — это уникальный номер от 1 до 128, который используется как идентификатор группы в последующих командах.

Формат: `vlan protocol group` *`groupid`*

Режим ввода команд: глобальная конфигурация

vlan protocol group name

Эта команда назначает имена группам протоколов для классификации VLAN. Переменная *groupname* может быть строкой длиной от 0 до 16 символов.

Формат: `vlan protocol group name` *`groupid groupname`*

Режим ввода команд: глобальная конфигурация

no vlan protocol group name

Эта команда удаляет имя группы, определенной параметром *groupid*.

Формат: `no vlan protocol group name` *`groupid`*

Режим ввода команд: глобальная конфигурация

vlan protocol group add protocol

Данная команда добавляет значение *protocol-list* к группе протоколов для классификации VLAN, определенной параметром *groupid*. С одной группой можно связать более одного протокола.

Каждое сочетание интерфейса и протокола может быть связано только с одной группой. Если добавление протокола к группе вызывает конфликт с интерфейсами, которые в данный момент связаны с данной группой, данная команда завершается ошибкой и протокол к группе не добавляется. Возможные значения *protocol-list* включают ключевые слова *ip*, *arp*, и *ipx*, а также шестнадцатеричные и десятичные значения в диапазоне от 0x0600 (1536) до 0xFFFF (65535). В списке можно указать до 16 протоколов, разделенных запятой.

Значение по умолчанию: отсутствует

Формат: `vlan protocol group add protocol` *`groupid ethertype protocol-list`*

Режим ввода команд: глобальная конфигурация

no vlan protocol group add protocol

Данная команда удаляет протоколы, определенные параметром *protocol-list*, из группы протоколов для классификации VLAN, которая определяется параметром *groupid*.

Формат: `no vlan protocol group add protocol` *`groupid ethertype protocol-list`*

Режим ввода команд: глобальная конфигурация

protocol group

Эта команда присоединяет сеть *vlanid* к группе VLAN на основе протоколов, которая определяется параметром *groupid*. Группу можно связать за один раз только с одной VLAN, однако связанные VLAN можно изменять.

Значение по умолчанию: отсутствует

Формат: `protocol group` *`groupid vlanid`*

Режим ввода команд: конфигурирование VLAN

no protocol group

Эта команда удаляет сеть *vlanid* из группы протоколов для классификации VLAN, которая определяется параметром *groupid*.

Формат: `no protocol group` *`groupid vlanid`*

Режим ввода команд: конфигурирование VLAN

protocol vlan group

Данная команда добавляет физический интерфейс или диапазон интерфейсов к группе протоколов для классификации VLAN, которая определяется параметром *groupid*. К группе можно присоединять несколько интерфейсов, но каждое сочетание интерфейса и протокола может быть связано только с одной группой. Если добавление интерфейса к группе вызывает конфликт с протоколами, которые в данный момент связаны с данной группой, данная команда завершается ошибкой, и интерфейс к группе не добавляется.

Значение по умолчанию: отсутствует

Формат: `protocol vlan group` *`groupid`*

Режим ввода команд: конфигурирование интерфейса

no protocol vlan group

Эта команда удаляет интерфейс из группы протоколов для классификации VLAN, которая определяется параметром *groupid*.

Формат: `no protocol vlan group` *groupid*

Режим ввода команд: конфигурирование интерфейса

protocol vlan group all

Эта команда добавляет все физические интерфейсы к группе протоколов для классификации VLAN, которая определяется параметром *groupid*. К группе можно присоединять несколько интерфейсов, но каждое сочетание интерфейса и протокола может быть связано только с одной группой. Если добавление интерфейса к группе вызывает конфликт с протоколами, которые в данный момент связаны с данной группой, данная команда завершается ошибкой, и интерфейс не будет добавлен к группе.

Значение по умолчанию: отсутствует

Формат: `protocol vlan group all` *groupid*

Режим ввода команд: глобальная конфигурация

no protocol vlan group all

Эта команда удаляет все интерфейсы из группы протоколов для классификации VLAN, которая определяется параметром *groupid*.

Формат: `no protocol vlan group all` *groupid*

Режим ввода команд: глобальная конфигурация

show port protocol

Данная команда отображает информацию о группе протоколов для классификации VLAN для всей системы или для указанной группы.

Формат: `show port protocol {`*groupid* `|` `all}`

Режим ввода команд: привилегированный

Термин	***Описание***
Group Name	Имя группы в записи таблицы протоколов для классификации VLAN.
Group ID	Идентификатор группы на основе протоколов.
VLAN	VLAN, связанная с группой на основе протоколов.
Protocol(s)	Тип протокола/протоколов для данной группы.
Interface(s)	Перечисляет интерфейсы, связанные с данной группой на основе протоколов, в формате unit/slot/port.

vlan pvid

Данная команда меняет идентификатор VLAN на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: 1

Формат: `vlan pvid` *1-4094*

Режим ввода команд: конфигурирование интерфейса конфигурирование диапазона интерфейсов

no vlan pvid

Эта команда устанавливает идентификатор VLAN на интерфейсе или диапазоне интерфейсов в значение 1.

Формат: `no vlan pvid`

Режим ввода команд: конфигурирование интерфейса

vlan tagging

Данная команда включает настройку тегирования для указанного интерфейса или диапазона интерфейсов VLAN. Если тегирование включено, трафик передается в виде тегированных кадров. Если тегирование выключено, трафик передается в виде нетегированных кадров. ID — действительный идентификационный номер VLAN.

Формат: `vlan tagging` *`1-4094`*

Режим ввода команд: конфигурирование интерфейса

no vlan tagging

Данная команда выключает тегирование для указанного интерфейса или диапазона интерфейсов VLAN. Если тегирование выключено, трафик передается в виде нетегированных кадров. ID — действительный идентификационный номер VLAN.

Формат: `no vlan tagging` *`1-4094`*

Режим ввода команд: конфигурирование интерфейса

vlan association subnet

Эта команда связывает VLAN с указанной IP-подсетью.

Формат: `vlan association subnet` *`ipaddr netmask vlanid`*

Режим ввода команд: конфигурирование VLAN

no vlan association subnet

Эта команда разрывает связь VLAN с указанной IP-подсетью.

Формат: `no vlan association subnet ipaddr netmask`
Режим ввода команд: конфигурирование VLAN

vlan association mac

Эта команда связывает сеть VLAN с определенным MAC-адресом.

Формат: `vlan association mac` *`macaddr vlanid`*

Режим ввода команд: VLAN database

no vlan association mac

Данная команда разрывает связь VLAN с определенным MAC-адресом.

Формат: `no vlan association mac` *`macaddr`*

Режим ввода команд: таблица VLAN

remote-span

Эта команда определяет VLAN как RSPAN VLAN и отключает обучение mac-адресов для данного интерфейса VLAN.

Значение по умолчанию: отсутствует

Формат: `remote-span`

Режим ввода команд: конфигурирование VLAN

Максимальное количество RSPAN VLAN равно 7.

no remote-span

Данная команда удаляет информацию RSPAN для VLAN и включает обучение MAC-адресов для данного интерфейса VLAN.

Формат: `no remote-span`

Режим ввода команд: конфигурирование VLAN

show vlan

Команда отображает информацию о настроенных VLAN и Private VLAN, включая первичные и вторичные идентификаторы VLAN, типы (community, isolated или primary) и порты, которые относятся к Private VLAN.

Формат: `show vlan {`*`vlanid`*`|private-vlan [`*`type`*`]}`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
Primary	Первичный идентификатор VLAN. Диапазон идентификатора VLAN: 1–40934094.
Secondary	Вторичный идентификатор VLAN.
Type	Вторичный тип VLAN (community, isolated или primary).
Ports	Порты, связанные с Private VLAN.
VLAN ID	Идентификатор VLAN (VID), связанный с каждой VLAN. Диапазон идентификатора VLAN: 1–4094.
VLAN Name	Строка, связанная с этой VLAN для удобства наименования. Может содержать до 32 буквенно-цифровых символов, включая пробелы. Значение по умолчанию: пустая строка. VLAN ID 1 всегда имеет имя **Default**. Это необязательное поле.
VLAN Type	Тип VLAN, который может иметь значения Default (VLAN ID = 1), Static (настраивается и определяется на постоянной основе) или Dynamic. Динамический тип VLAN может быть создан регистрацией GVRP или

	во время процесса аутентификации 802.1X (DOT1X), если на данном коммутаторе не существует связанная с RADIUS VLAN.
Interface	Интерфейс в формате *unit/slot/port*. Можно настроить параметры для всех портов, используя селекторы в верхней строке.
Current	Степень участия этого порта в данной VLAN. Возможны следующие значения. **Include** — порт всегда входит в данную VLAN. Эквивалентно фиксированной регистрации согласно стандарту IEEE 802.1Q. **Exclude** — порт никогда не входит в данную VLAN. Эквивалентно запрещенной регистрации согласно стандарту IEEE 802.1Q. **Autodetect** — позволяет динамическую регистрацию порта в данной VLAN посредством GVRP. Порт не входит в VLAN до тех пор, пока на него не поступит запрос на присоединение. Эквивалентно нормальной регистрации согласно стандарту IEEE 802.1Q.
Configured	Настроенная степень участия порта в данной VLAN. Возможны следующие значения. **Include** — порт всегда входит в данную VLAN. Эквивалентно фиксированной регистрации согласно стандарту IEEE 802.1Q. **Exclude** — порт никогда не входит в данную VLAN. Эквивалентно запрещенной регистрации согласно стандарту IEEE 802.1Q. **Autodetect** — позволяет динамическую регистрацию порта в данной VLAN посредством GVRP. Порт не входит в VLAN до тех пор, пока на него не поступит запрос на присоединение. Эквивалентно нормальной регистрации согласно стандарту IEEE 802.1Q.
Tagging	Настройки тегирования для порта в данной VLAN. **Tagged** — передает трафик для данной VLAN в виде тегированных кадров. **Untagged** — передает трафик для данной VLAN в виде нетегированных кадров.

show vlan tag

Показать конфигурацию для одного VLAN в кратком формате.

Формат: `show vlan tag`

Режим ввода команд: привилегированный
пользовательский

show vlan internal usage

Команда отображает информацию о привязке идентификаторов VLAN на коммутаторе.

Формат: `show vlan internal usage`
Режим ввода команд: привилегированный
пользовательский

Термин	*Описание*
Base VLAN ID	Определяет базовый идентификатор VLAN для внутренней привязки сетей VLAN к интерфейсу маршрутизации.
Allocation policy	Показывает, в каком порядке система выделяет идентификаторы VLAN (в восходящем или в нисходящем).

show vlan brief

Эта команда отображает список всех настроенных VLAN.

Формат: show vlan brief

Режим ввода команд: привилегированный
пользовательский

Термин	*Описание*
VLAN ID	Идентификатор VLAN (vlanid) для каждой VLAN. Диапазон идентификатора VLAN: 1–4094.
VLAN Name	Строка, связанная с этой VLAN для удобства наименования. Может содержать до 32 буквенно-цифровых символов, включая пробелы. Значение по умолчанию: пустая строка. VLAN ID 1 всегда имеет имя Default. Это необязательное поле.
VLAN Type	Тип VLAN, который может иметь значения Default (VLAN ID = 1), Static (настраивается и определяется на постоянной основе) или Dynamic (созданный регистрацией GVRP).

show vlan association subnet

Эта команда отображает VLAN, связанную с определенным настроенным IP-адресом и маской подсети. Если IP-адрес и маска подсети не настроены, отображаются связи VLAN со всеми IP-подсетями.

Формат: `show vlan association subnet [ipaddr netmask]`

Режим ввода команд: привилегированный

Термин	*Описание*
IP Address	IP-адрес, назначенный каждому интерфейсу.
Net Mask	Маска подсети.
VLAN ID	Идентификатор VLAN (VID).

show vlan association mac

Эта команда отображает VLAN, связанную с определенным настроенным MAC-адресом. Если конкретный MAC-адрес не настроен, отображаются связи VLAN со всеми настроенными MAC-адресами.

Формат: `show vlan association mac [macaddr]`

Режим ввода команд: привилегированный

Термин	*Описание*
MAC Address	MAC-адрес, для которого коммутатор имеет данные о переадресации и/или фильтрации. В формате 6 или 8 двузначных номеров шестнадцатеричной системы, разделенных двоеточиями, например: 01:23:45:67:89:AB. В системе IVL MAC-адрес будет отображаться как 8 байт.
VLAN ID	Идентификатор VLAN (VID).

9.5 Команды настройки Double VLAN

В этой части приводятся команды, используемые для настройки Double VLAN (DVLAN). Двойное тегирование трафика — это способ передать трафик VLAN от одного домена клиента к другому через городскую магистральную сеть простым и экономичным образом. Дополнительный тег трафика помогает отличать клиентов в городской сети, при этом сохраняя идентификацию VLAN индивидуальных клиентов, когда они входят в свой собственный домен IEEE 802.1Q.

dvlan-tunnel ethertype (режим конфигурирования интерфейса)

Данная команда доступна не на всех платформах.

Эта команда настраивает значение Ethertype для указанного интерфейса. Двухбайтное шестнадцатеричное значение Ethertype используется в качестве первых 16 битов тега DVLAN. Ethertype может иметь значения *802.1Q*, *vman*, или *custom*. Если для Ethertype указано необязательное значение custom, это пользовательское значение туннеля, и значение Ethertype должен быть установлен в диапазоне от 1 до 65535.

Значение по умолчанию: 802.1Q

Формат: `dvlan-tunnel ethertype {802.1Q | vman | custom` *`1-65535`*`}`

Режим ввода команд: глобальная конфигурация

Термин	***Описание***
802.1Q	Настраивает Ethertype как 0x8100.
custom	Настраивает значение пользовательского тега в диапазоне от 1 до 65535.
vman	Представляет наиболее часто используемое значение 0x88A8.

no dvlan-tunnel ethertype (режим конфигурирования интерфейса)

Данная команда доступна не на всех платформах. Эта команда удаляет значение Ethertype для указанного интерфейса.

Формат: `no dvlan-tunnel ethertype`

Режим ввода команд: глобальная конфигурация

dvlan-tunnel ethertype primary-tpid

Используйте данную команду, чтобы создать новый TPID и связать его со следующим доступным регистром TPID. Если регистры TPID пустые, система вернет ошибку. При указании необязательного ключевого слова [primary–tpid] значение TPID будет принудительно настроено как TPID по умолчанию с индексом 0.

Формат: `dvlan-tunnel ethertype {802.1Q | vman | custom` *`1–65535`*`} [primary-tpid]`

Режим ввода команд: глобальная конфигурация

Термин	***Описание***
802.1Q	Настраивает Ethertype как 0x8100.

custom	Настраивает значение пользовательского тега в диапазоне от 1 до 65535.
vman	Представляет наиболее часто используемое значение 0x88A8.

no dvlan-tunnel ethertype primary–tpid

Этот вариант no-команды используется, чтобы установить регистр TPID в значение 0. (При инициализации все регистры будут установлены в свои значения по умолчанию.)

Формат: `no dvlan-tunnel ethertype {802.1Q | vman | custom` *`1–65535`*`} [primary-tpid]`

Режим ввода команд: глобальная конфигурация

mode dot1q-tunnel

Эта команда используется для включения Double VLAN Tunneling на указанном интерфейсе.

Значение по умолчанию: выключено

Формат: `mode dot1q-tunnel`

Режим ввода команд: конфигурирование интерфейса

no mode dot1q-tunnel

Команда используется для выключения Double VLAN Tunneling на указанном интерфейсе. По умолчанию Double VLAN Tunneling выключено.

Формат: `no mode dot1q-tunnel`

Режим ввода команд: конфигурирование интерфейса

mode dvlan-tunnel

Команда используется для включения Double VLAN Tunneling на указанном интерфейсе.

Когда вы используете команду mode dvlan-tunnel на интерфейсе, он становится портом провайдера сервиса. Порты, на которых Double VLAN Tunneling не включен, являются пользовательскими портами.

Значение по умолчанию: выключено

Формат: `mode dvlan-tunnel`

Режим ввода команд: конфигурирование интерфейса

no mode dvlan-tunnel

Команда используется для выключения Double VLAN Tunneling на указанном интерфейсе. По умолчанию Double VLAN Tunneling выключено.

Формат: `no mode dvlan-tunnel`

Режим ввода команд: конфигурирование интерфейса

show dot1q-tunnel

Используйте эту команду без необязательных параметров, чтобы отобразить все интерфейсы с включенным Double VLAN Tunneling. Используйте необязательные параметры, чтобы отобразить подробную информацию о Double VLAN Tunneling для указанного интерфейса или интерфейсов.

Формат: `show dot1q-tunnel [interface {`*`unit/slot/port`*` | all}]`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Interface	Интерфейс в формате unit/slot/port
Mode	Административный режим, в котором Double VLAN Tunneling можно включить или выключить. Значение этого поля по умолчанию — disabled.
EtherType	Двухбайтное шестнадцатеричное значение Ethertype, используемое в качестве первых 16 битов тега DVLAN tunnel. Существует 3 разных тега Ethertype. Первый — 802.1Q, который представляет собой часто используемое значение 0x8100. Второй — vMAN, который представляет собой часто используемое значение 0x88A8. Если Ethertype не является одним из этих двух значений, то это значение пользовательского туннеля, представляющее собой любое значение от 1 до 65535.

9.6 Команды настройки Private VLAN

Эта часть описывает команды, используемые для Private VLAN. Private VLAN обеспечивают изоляцию уровня 2 между портами, которые находятся в одной широковещательной области. Другими словами, это позволяет широковещательной области VLAN быть поделенным на более мелкие поддомены типа «точка-многоточка». Порты, задействованные в Private VLAN, находятся в любом месте сети уровня 2.

switchport private-vlan

Эта команда определяет связь Private VLAN с изолированным или общим портом или привязку для смешанного порта.

Формат: `switchport private-vlan {host-association primary-vlan-id secondary-vlan-id | mapping primary-vlan-id {add | remove} secondary-vlan-list}`

Режим ввода команд: конфигурирование интерфейса

Термин	*Значение*
host-association	Устанавливает связь VLAN с общими портами или портами узла.
mapping	Устанавливает привязку Private VLAN для случайных портов.
primary-vlan-id	Первичный идентификатор Private VLAN.
secondary-vlan-id	Вторичный (изолированный или общий) идентификатор Private VLAN.
add	Связывает вторичный VLAN с первичным.
remove	Удаляет связи вторичных VLAN с первичным VLAN.
secondary-vlan- list	Список вторичных VLAN, которые будут привязаны к первичной VLAN.

no switchport private-vlan

Эта команда удаляет связи Private VLAN или привязку для порта.

Формат: `no switchport private-vlan {host-association|mapping}`

Режим ввода команд: конфигурирование интерфейса

switchport mode private-vlan

Эта команда настраивает порт как смешанный или узловой порт Private VLAN. Обратите внимание: свойства каждого режима могут быть настроены даже тогда, когда коммутатор не находится в нужном режиме. Однако они будут применены только тогда, когда коммутатор перейдет в заданный режим.

Значение по умолчанию: general

Формат: `switchport mode private-vlan {host|promiscuous}`

Режим ввода команд: конфигурирование интерфейса

Термин	***Значение***
host	Настраивает интерфейс как узловой порт Private VLAN. Порт может быть изолированным или общим в зависимости от вторичной VLAN, с которой он связан.
promiscuous	Настраивает интерфейс как смешанный порт Private VLAN. Смешанные порты входят в первичную VLAN.

no switchport mode private-vlan

Эта команда удаляет связи Private VLAN или привязку для порта.

Формат: `no switchport mode private-vlan`

Режим ввода команд: конфигурирование интерфейса

private-vlan

Эта команда настраивает Private VLAN и связи между первичными и вторичными Private VLAN.

Формат: `private-vlan {association [add|remove] secondary-vlan-list|community|isolated|primary}`

Режим ввода команд: конфигурирование VLAN

Параметр	***Описание***
association	Связывает первичную и вторичную VLAN.
secondary-vlan-list	Список вторичных VLAN, которые будут привязаны к первичной VLAN.
community	Назначает VLAN общей.
isolated	Назначает VLAN изолированной.
primary	Назначает VLAN первичной.

no private-vlan

Команда восстанавливает нормальную конфигурацию VLAN.

Формат: `no private-vlan {association}`

Режим ввода команд: конфигурирование VLAN

9.7 Настройка портов коммутатора

В этой части описаны команды, используемые для настройки режима порта коммутатора.

switchport mode

Используйте эту команду, чтобы настроить режим порта коммутатора как access, trunk or general.

В режиме Trunk порт становится частью всех VLAN на коммутаторе, если он не указан в списке разрешений команды *switchport trunk allowed vlan*. PVID порта в этом случае установлен в значение Native VLAN, как указано в команде switchport trunk native vlan. Это означает, что порты Trunk принимают как тегированные, так и нетегированные пакеты, при этом нетегированные пакеты обрабатываются в основной VLAN, а тегированные обрабатываются в сетях VLAN, идентификаторы которых указаны в пакетах. Определение MAC выполняется на пакетах обоих типов. Тегированные пакеты с идентификатором VLAN, которые не связаны с данным портом, отбрасываются, определение MAC не выполняется. Порты в режиме Trunk всегда передают нетегированные пакеты в основную VLAN.

В режиме Access порт становится частью только одной VLAN. Порт отсылает и получает нетегированный трафик. Он также может получать тегированный трафик. На порте включена фильтрация входящих пакетов. Это значит, что если идентификатор VLAN полученного пакета не идентичен идентификатору доступной VLAN, такой пакет отбрасывается.

В режиме General пользователь может выполнять пользовательскую настройку принадлежности к VLAN, PVID, тегирования, фильтрации входящих пакетов и т. д. Это устаревший вариант настройки для конфигурации порта коммутатора. Устаревшие команды CLI настраивали порт в режиме General.

Значение по умолчанию: режим General

Формат: `switchport mode {access | trunk | general}`

Режим ввода команд: конфигурирование интерфейса

no switchport mode

Эта команда устанавливает режим порта коммутатора в значение по умолчанию.

Формат: `no switchport mode`

Режим ввода команд: конфигурирование интерфейса

switchport trunk allowed vlan

Используйте данную команду для настройки списка доступа VLAN, которые могут получать и отправлять трафик на данном интерфейсе в тегированном формате, когда интерфейс находится в режиме Trunk. Значение по умолчанию: все VLAN.

Список VLAN может быть изменен с помощью опций add и remove, или заменен другим списком с помощью опций vlan-list, all, или except. Если выбрано all, все VLAN добавляются в список VLAN, имеющих доступ. Опция except предоставляет список исключений.

Порты в режиме Trunk принимают тегированные пакеты, и они обрабатываются в сетях VLAN, идентификаторы которых указаны в пакетах, если VLAN находятся в списке доступа VLAN. Тегированные пакеты с идентификатором VLAN, которые не связаны с данным портом, отбрасываются, определение MAC не выполняется. Если VLAN добавлена в систему после того, как порт настроен в режим Trunk, и при этом находится в списке доступа VLAN, данная VLAN назначается этому порту автоматически.

Значение по умолчанию: All

Формат: `switchport trunk allowed vlan {`*`vlan-list`* `| all | {add` *`vlan-list`*`} | {remove` *`vlan-list`*`}| {except` *`vlan-list`* `}}`

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
all	Обозначает все VLAN от 1 до 4094. Это ключевое слово не допускается в командах, которые не разрешают сразу использовать полный список VLAN.
add	Добавляет определенный список VLAN к тем, что уже установлены, не заменяя их.
remove	Удаляет установленный список VLAN, не заменяя его. Действительные идентификаторы — от 1 до 4094; в данной команде действует расширенный диапазон идентификаторов VLAN в форме X-Y ил X,Y,Z.
except	Задает список VLAN, которые рассчитывается путем инвертирования указанного списка VLAN (т. е. все VLAN, за исключением указанных).
vlan-list	Отдельный номер VLAN от 1 до 4094 или непрерывный диапазон VLAN, заданный двумя VLAN номерами, разделенными дефисом, от меньшего к большему.

no switchport trunk allowed vlan

Данная команда сбрасывает список доступа VLAN для порта в режиме Trunk в значение по умолчанию.

Формат: `no switchport trunk allowed vlan`

Режим ввода команд: конфигурирование интерфейса

switchport trunk native vlan

Используйте данную команду для настройки параметра Native VLAN порта в режиме Trunk. Любым входящим нетегированным пакетам присваивается тег со значением Native VLAN. Для тегирования нетегированных пакетов Native VLAN должна быть в списке доступа VLAN. В противном случае нетегированные пакеты отбрасываются. Пакеты, тегированные значением Native VLAN, передаются нетегированными от Trunk-порта. Значение по умолчанию: 1.

Значение по умолчанию: 1 (Default VLAN)

Формат: `switchport trunk native vlan` *`vlan-id`*

Режим ввода команд: конфигурирование интерфейса

no switchport trunk native vlan

Используйте эту команду, чтобы установить Native VLAN для Trunk-порта в значение по умолчанию.

Формат: `no switchport trunk native vlan`

Режим ввода команд: конфигурирование интерфейса

switchport access vlan

Используйте данную команду для настройки VLAN на порте в режиме Access. Для Access-порта можно назначить только одну VLAN. По умолчанию Access-порты являются членами VLAN 1. Access-порты можно связать с другими VLAN, помимо VLAN 1. При удалении связанной VLAN на коммутаторе Access-порт становится членом VLAN 1. Настройка связи Access-порта с несуществующей VLAN заканчивается ошибкой и не меняет конфигурацию.

Значение по умолчанию: 1 (Default VLAN)

Формат: `switchport access vlan` *`vlan-id`*

Режим ввода команд: конфигурирование интерфейса

no switchport access vlan

Эта команда устанавливает VLAN для порта в режиме Access в значение по умолчанию.

Формат: `no switchport access vlan`

Режим ввода команд: конфигурирование интерфейса

show interfaces switchport

Команда для отображения состояния порта коммутатора для всех интерфейсов или указанного интерфейса.

Формат: `show interfaces switchport` *`unit/slot/port`*

Режим ввода команд: привилегированный

show interfaces switchport

Используйте данную команду для отображения конфигурации порта коммутатора для выбранного режима по каждому интерфейсу. Если интерфейс не указан, отображается конфигурация для всех интерфейсов.

Формат: `show interfaces switchport {access | trunk | general} [`*`unit/slot/port`*`]`

Режим ввода команд: привилегированный

9.8 Команды настройки Voice VLAN

В этой части описаны команды, используемые для Voice VLAN. Voice VLAN позволяет портам коммутатора передавать голосовой трафик с заданным приоритетом, чтобы обеспечить разделение голосового трафика и трафика данных, поступающих на порт. Преимущество использования Voice VLAN в том, что она гарантирует, что качество звука IP-телефона защищено от ухудшения при высоком потоке данных.

Кроме того, свойственная VLAN изоляция гарантирует, что внутренний трафик VLAN находится под административным контролем и что соединенные с сетью клиенты не смогут инициировать прямую атаку на голосовые компоненты. QoS на основе класса обслуживания (CoS) IEEE 802.1p использует классификацию и планирование отправки сетевого трафика с коммутатора предсказуемым образом. Система использует исходный MAC-адрес трафика, проходящего через порт, чтобы идентифицировать данные IP-телефонии.

voice vlan (режим глобальной конфигурации)

Используйте эту команду, чтобы включить функционал Voice VLAN на коммутаторе.

Значение по умолчанию: выключено

Формат: `voice vlan`

Режим ввода команд: глобальная конфигурация

no voice vlan (Global Config)

Используйте данную команду, чтобы выключить Voice VLAN на коммутаторе.

Формат: `no voice vlan`

Режим ввода команд: глобальная конфигурация

voice vlan (режим конфигурирования интерфейса)

Команда для включения функционала Voice VLAN на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `voice vlan {vlanid` *`id`* `| dot1p` *`priority`* `| none | untagged}`

Режим ввода команд: конфигурирование интерфейса

Настроить Voice VLAN можно одним из четырех способов.

Параметр	***Описание***
vlan-id	Настраивает IP-телефон направлять весь голосовой трафик через указанную VLAN. Действительные идентификаторы VLAN — от 1 до 4094 (максимальный диапазон, поддерживаемый платформой).
dot1p	Настраивает IP-телефон использовать для голосового трафика приоритетное тегирование 802.1p и значение Native VLAN (VLAN 0) по умолчанию для всего трафика. Действительный диапазон значений priority — от 0 до 7.
none	Позволяет IP-телефону использовать собственные настройки для отправки нетегированного голосового трафика.
untagged	Настраивает телефон отправлять нетегированный голосовой трафик.

no voice vlan (Interface Config)

Используйте эту команду, чтобы выключить Voice VLAN на интерфейсе.

Формат: `no voice vlan`

Режим ввода команд: конфигурирование интерфейса

voice vlan data priority

Команда используется, чтобы позволить или запретить настройку трафика, приходящего на интерфейс или диапазон интерфейсов Voice VLAN.

Значение по умолчанию: trust

Формат: `voice vlan data priority {untrust | trust}`

Режим ввода команд: конфигурирование интерфейса

show voice vlan

Формат: `show voice vlan [interface {unit/slot/port | all}]`

Режим ввода команд: привилегированный

Если параметр *interface* не задан, отображается только глобальный режим Voice VLAN.

Параметр	***Описание***
Administrative Mode	Глобальный режим Voice VLAN

Если параметр *interface* указан:

Параметр	***Описание***
Voice VLAN Mode	Административный режим Voice VLAN на интерфейсе.
Voice VLAN ID	Идентификатор Voice VLAN.
Voice VLAN Priority	do1p-приоритет для Voice VLAN порта.
Voice VLAN Untagged	Опция тегирования для трафика Voice VLAN.
Voice VLAN CoS Override	Опция перезаписи для голосового трафика, приходящего на порт.
Voice VLAN Status	Оперативный статус Voice VLAN на порте.

9.9 Команды настройки моста провайдера

Команды для моста провайдера настраивают коммутатор для использования стекированных VLAN по стандарту IEEE 802.1ad. Сервисные провайдеры используют стекированные VLAN, в которых содержатся теги 801.Q VLAN на втором уровне тегов 802.Q (802.1Q-inQ), чтобы позволить одной сети VLAN поддерживать клиентов, у которых есть несколько внутренних VLAN.

Команды настройки моста провайдера включают в себя команды туннелирования данных и команды туннелирования протоколов L2.

- Команды туннелирования данных определяют сервисные экземпляры и применяют их к определенным портам.
- Команды туннелирования протоколов L2 позволяют использовать протоколы второго уровня сети клиента на различных площадках, подключенных через сеть сервисного провайдера.

Команды настройки туннелирования данных

Чтобы на коммутаторе создать мост в рамках всей сети поставщика услуг, требуется определить экземпляры сервисов. Определение экземпляра сервисов включает в себя указание имени сервиса, используемого типа переадресации и данных QoS. Экземпляр сервиса может также быть связан с уникальной сервисной меткой VLAN (*SVLAN*), которая определяется значением идентификатора VLAN (*S-VID*).

Администратор может приписать к сервису отдельные порты. Когда порт приписывается к сервису, на коммутаторе создается VLAN (если она еще не существует), и приписанный порт настраивается как участник SVLAN. Порт сервисного поставщика (называемый портом Network-to-Network, или NNI) также настраивается как участник SVLAN для того, чтобы передавать исходящий и получать входящий трафик.

Приписка включает критерии сопоставления, такие как идентификатор VLAN клиента, C-VID, приоритет, S-VID. Когда входящий пакет на UNI-P соответствует критерию приписанного порта, коммутатор добавляет тег сервисной VLAN к пакету, и дополнительно может менять тег C-VID/удалять C-тег пакета перед тем, как направлять/перенаправлять его в сеть сервисного провайдера. Когда входящий пакет на UNI-S соответствует критерию приписанного порта, коммутатор может менять тег S-VID и/или менять тег C-VID/удалять C-тег пакета перед тем, как направлять/перенаправлять его в сеть сервисного провайдера. CLI поддерживает до 4 тыс. приписок сервиса на один коммутатор/порт.

Если сервис TLS приписан к порту, то P-VID порта настраивается на функционирование в качестве S-VID сервиса TLS. P-VID NNI-порта устанавливается как управляющая VLAN. По умолчанию управляющей является VLAN 1. Настройки создания и участия VLAN на коммутаторе одинаковы для всех типов сервисов (TLS, E-LAN, E-Tree, ELine).

Сети VLAN и участие портов (клиентских и сервисного провайдера) настраиваются автоматически на основе конфигурации сервиса и приписок. Администраторам не рекомендуется создавать или изменять VLAN и участие портов в VLAN на каких-либо портах. Ручная настройка VLAN и участия портов может привести к непредсказуемым последствиям.

dot1ad mode

Эта команда включает режим UNI/NNI и устанавливает тип dot1ad для интерфейса или диапазона интерфейсов. UNI-P предназначен для интерфейсов на основе портов, а UNI-S — для интерфейсов на основе сервисов. Сопоставление на основе S-VID/C-VID и CVID/Priority может быть настроено на порте UNI-S. Порт UNI-P может быть настроен с критериями сопоставления на основе C-VID/Priority/Untagged. Сервисы dot1ad не могу быть приписаны к порту в режиме switchport. Если режим установлен как switchport, порт можно использовать для нормальной коммутации/маршрутизации трафика.

Значение по умолчанию: отсутствует

Формат: `dot1ad mode {uni-p | uni-s | nni | switchport}`

Режим ввода команд: конфигурирование интерфейса

Пример:

Команда может выглядеть следующим образом:

```
(Switch)(Config)(interface 1/0/6)#dot1ad mode nni
```

dot1ad service

Эта команда настраивает сервис заданного типа по имени. Команда предоставляет настройку связи S–VID и NNI-портов на уровне сервисов.

Формат: `dot1ad service` *`service-name`* `svid` *`svid`* `{e-lan | e-line | e-tree | tls} [nni` *`port list`*`]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
service-name	Название сервиса, заданное пользователем.
svid	Идентификатор сервисной VLAN (S–VID).
e-lan | e-line | e- tree | tls	Эти параметры определяют тип трафика, связанного с экземпляром сервиса. • **e-lan** — коммутируемый или общий сервис, в котором связанный трафик пересылается на основе стандартного коммутационного поиска уровня 2 с использованием S-VID и MAC-адреса пункта назначения в качестве ориентиров в FDB. **Порт может быть участником нескольких сервисов E-LAN. Если коммутируемый сервис присоединен к нескольким UNI-портам, эти порты смогут передавать трафик друг другу так же, как и портам NNI. Этот же сервис E-LAN может быть применен к портам UNI-P и UNI-S.** • **e-line** — параметр e-line создает сервис «точка-точка», в котором трафик передается напрямую к NNI-порту в восходящем направлении и к подсоединенным UNI-портам в нисходящем направлении. Сервис e-line обходит стандартные решения коммутации на основе VLAN/MAC, в том числе определение MAC-адреса источника. По умолчанию система не определяет принадлежность трафика, принадлежащего сервису e-line. Экземпляр сервиса e-line определяет сервис «точка-точка», в котором участвует только порт UNI-P или UNI-S. **Примечание.** Важно отметить, что нисходящая передача данных и многоадресный трафик по-прежнему будут перенаправляться к связанному UNI-порту, участвующему в сервисе e-line. • **e-tree** — параметр e-tree создает сервис «точка-многоточка», в котором трафик, связанный с этим сервисом, передается напрямую к NNI-порту в восходящем направлении и напрямую к подсоединенным UNI-портам в нисходящем направлении. Если экземпляр службы e-tree применяется к нескольким UNI-портам, он становится сервисом «точка-многоточка», в котором участвующие порты пользователя по-прежнему изолированы друг от друга. **Примечание.** Важно отметить, что нисходящая передача данных, многоадресная передача трафика и трафик неизвестного назначения (DLF) по-прежнему будут перенаправляться (реплицироваться) на все порты, участвующие в сервисе e-tree. • **tls (Transparent LAN Service).** Администраторы могут настроить TLS на портах UNI-P и UNI-S. TLS используется для подключения удаленных клиентов с прозрачным C-Tag. Критериев соответствия для TLS не существует. – Если на порте UNI-P не настроена служба TLS, все пакеты, не совпадающие ни с одним экземпляром сервисов, настроенным на портах, будут отброшены. Если служба TLS настроена, то все пакеты, не совпадающие с другими экземплярами служб на порте, будут отмечены в соответствии с описанием TLS для этого порта. Заданный пользователем сервис TLS будет использоваться для нетегированных, приоритетно тегированных пакетов и пакетов с тегами C-VLAN, которые не совпадают с другими экземплярами служб на порте. – Если служба TLS настроена на порте UNI-S, кадры с тегами сервиса VLAN (включая двойные теги), не совпадающие с другими экземплярами служб на порте, будут переданы к соответствующим NNI-портам на основе S-VID, связанным с сервисом, без каких-либо изменения в VLAN. Пакеты без маркировки и пакеты приоритетов, не

	совпадающие с другими экземплярами служб на порте, будут отброшены.
port-list	Список NNI-портов.

no dot1ad service

Используйте форму no-команды, чтобы удалить сервис.

Формат: `no dot1ad service` *`service-name`*

Режим ввода команд: глобальная конфигурация

subscribe match untagged–pkt

Команда настраивает соответствие назначения VLAN для нетегированных пакетов (только UNI-P) на интерфейсе или диапазоне интерфейсов. Восходящий трафик идет к настроенным NNI-портам, основанным на коммутации или перенаправлении, в зависимости от сервиса, к которому они приписаны.

Формат: `subscribe` *`service-name subscription-name`* `match untagged–pkt [assign–cvid` *`cvid`*`] [nni` *`port-list`*`]`

Режим ввода команд: конфигурирование интерфейса

no subscribe match untagged–pkt

Используйте форму no-команды, чтобы отменить приписку нетегированных пакетов.

Формат: `no subscribe` *`service-name subscription-name`* `match untagged–pkt [assign–cvid` *`cvid`*`] [nni` *`port-list`*`]`

Режим ввода команд: конфигурирование интерфейса

subscribe match priority

Команда используется для настройки критериев назначения VLAN для пакетов с приоритетным тегированием на интерфейсе или диапазоне интерфейсов. Восходящий трафик идет к настроенным NNI-портам, основанным на коммутации или перенаправлении, в зависимости от сервиса, к которому они приписаны.

Формат: `subscribe` *`service-name subscription-name`* `match priority` *`pri`* `[assign–cvid` *`cvid`*`] [nni` *`port-list`*`]`

Режим ввода команд: конфигурирование интерфейса

subscribe match cvid

Используйте данную команду для настройки критериев соответствия назначения VLAN для пакетов с С-тегом. Восходящий трафик идет к настроенным NNI-портам, основанным на коммутации или перенаправлении, в зависимости от сервиса, к которому они приписаны. Эта команда применима только для портов UNI-P.

Формат: `subscribe` *`service-name subscription-name`* `match cvid` *`cvid`* `[[remark–cvid]` *`cvid]`* `| [remove–ctag]] [nni` *`port-list`*`]`

Режим ввода команд: конфигурирование интерфейса

subscribe match cvid priority

Команда для настройки критериев соответствия назначения VLAN для пакетов с C-тегом на основе C-VID, и, дополнительно, на основе значения Priority в C-теге. Восходящий трафик идет к настроенным NNI-портам, основанным на коммутации или перенаправлении, в зависимости от сервиса, к которому они приписаны. Эта команда применима только для портов UNI-P.

Формат: `subscribe *service-name subscription-name* match cvid *cvid* [priority *pri* [[remark-cvid] *cvid*] | [remove-ctag]] [nni *port-list*]`

Режим ввода команд: конфигурирование интерфейса

subscribe match svid

Используйте данную команду для настройки критериев соответствия назначения VLAN для одиночных пакетов с S-тегом. Восходящий трафик идет к настроенным NNI-портам, основанным на коммутации или перенаправлении, в зависимости от сервиса, к которому они приписаны.

Формат: `subscribe *service-name subscription-name* match svid *svid* [nni *port-list*]`

Режим ввода команд: конфигурирование интерфейса

subscribe match svid cvid

Используйте эту команду, чтобы настроить критерии соответствия назначения VLAN для пакетов с двойными тегами. Восходящий трафик идет к настроенным NNI-портам, основанным на коммутации или перенаправлении, в зависимости от сервиса, к которому они приписаны.

Формат: `subscribe *service-name subscription-name* match svid *svid* [cvid *cvid* [[remark-cvid *cvid*] | [remove-ctag]]] [nni *port list*]`

Режим ввода команд: конфигурирование интерфейса

subscribe

Используйте эту команду, чтобы приписать TLS-сервис к порту. Восходящий трафик идет к настроенным NNI-портам на основе коммутационных решений.

Формат: `subscribe *service-name subscription-name* [nni *port list*]`

Режим ввода команд: конфигурирование интерфейса

show dot1ad service

Команда отображает информацию об указанном сервисе или обо всех сервисах (т. е. название сервиса, тип сервиса и S-VID), настроенных на CPE.

Формат: `show dot1ad service [[*service-name*] [*unit/slot/port*]]`

Режим ввода команд: привилегированный

show dot1ad service-subscription

Данная команда показывает все сервисы, приписанные к интерфейсам.

Формат: `show dot1ad service-subscription {*unit/slot/port* | all | *service-name*}`

Режим ввода команд: привилегированный

Параметр	*Описание*
unit/slot/port	Показывает все подписки для указанного unit/slot/port.
all	Показывает подписки всех сервисов.
service-name	Показывает все подписки для указанного имени сервиса.
e-lan | e-line | e- tree | tls	Эти параметры определяют тип трафика, связанного с экземпляром сервиса. • **e-lan** — коммутируемый или общий сервис, в котором связанный трафик пересылается на основе стандартного коммутационного поиска уровня 2 с использованием S-VID и MAC-адреса пункта назначения в качестве ориентиров в FDB. **Порт может быть участником нескольких сервисов E-LAN. Если коммутируемый сервис присоединен к нескольким UNI-портам, эти порты смогут передавать трафик друг другу так же, как и портам NNI. Этот же сервис E-LAN может быть применен к портам UNI-P и UNI-S.** • **e-line** — параметр e-line создает сервис «точка-точка», в котором трафик передается напрямую к NNI-порту в восходящем направлении и к подсоединенным UNI-портам в нисходящем направлении. Сервис e-line обходит стандартные решения коммутации на основе VLAN/MAC, в том числе определение MAC-адреса источника. По умолчанию система не определяет принадлежность трафика, принадлежащего сервису e-line. Экземпляр сервиса e-line определяет сервис «точка-точка», в котором участвует только порт UNI-P или UNI-S. Примечание. Важно отметить, что нисходящая передача данных и многоадресный трафик по-прежнему будут перенаправляться к связанному UNI-порту, участвующему в сервисе e-line. • **e-tree** — параметр e-tree создает сервис «точка-многоточка», в котором трафик, связанный с этим сервисом, передается напрямую к NNI-порту в восходящем направлении и напрямую к подсоединенным UNI-портам в нисходящем направлении. Если экземпляр службы e-tree применяется к нескольким UNI-портам, он становится сервисом «точка-многоточка», в котором участвующие порты пользователя по-прежнему изолированы друг от друга. **Примечание.** Важно отметить, что нисходящая передача данных, многоадресная передача трафика и трафик неизвестного назначения (DLF) по-прежнему будут перенаправляться (реплицироваться) на все порты, участвующие в сервисе e-tree. • **tls** (Transparent LAN Service). Администраторы могут настроить TLS на портах UNI-P и UNI-S. TLS используется для подключения удаленных местоположений клиента клиентов с прозрачным C-Tag. Критериев соответствия для TLS не существует. – Если на порте UNI-P не настроена служба TLS, все пакеты, не совпадающие ни с одним экземпляром сервисов, настроенным на портах, будут отброшены. Если служба TLS настроена, то все пакеты, не совпадающие с другими экземплярами служб на порте, будут отмечены в соответствии с описанием TLS для этого порта. Заданный пользователем сервис TLS будет использоваться для нетегированных, приоритетно тегированных пакетов и пакетов с тегами C-VLAN, которые не совпадают с другими экземплярами служб на порте. – Если служба TLS настроена на порте UNI-S, кадры с тегами сервиса VLAN (включая двойные теги), не совпадающие с другими экземплярами служб на порте, будут переданы к соответствующим NNI-портам на основе S-VID, связанным с сервисом, без каких-либо изменения в VLAN. Пакеты без маркировки и пакеты приоритетов, не совпадающие с другими экземплярами служб на порте, будут отброшены.

port-list	Список NNI-портов.

Команды настройки туннелирования протоколов L2

Туннелирование второго уровня может использоваться для расширения сети к отдаленным местоположениям через сеть поставщика услуг. Эти команды настраивают туннелирование второго уровня на интерфейсах коммутаторов.

Чтобы настроить протокол туннелирования L2 на интерфейсе, необходимо настроить его как интерфейс 802.1ad типа «сеть-сеть» (NNI) или «пользователь-сеть» (UNI). Затем нужно настроить действие (туннелирование, завершение, отбрасывание или отбрасывание и выключение), которое выполняется интерфейсом, когда он получает PDU с указанной комбинацией MAC-адреса места назначения и идентификатора протокола. Если интерфейс настроен туннелировать по протоколу/MAC-адресу PDU, то он добавляет к пакету соответствующий тег с сервисным определением (S-тег), и необязательный тег идентификатора VLAN пользователя (C-тег), а затем перенаправляет его к NNI-порту.

dot1ad l2tunnel

Данная команда настраивает действие (tunnel или terminate) для данного MAC-адреса определенного сервиса.

Все зарезервированные MAC-адреса в диапазоне от 01:80:C2:00:00:00 до 01:80:C2:00:00:3F по умолчанию настраиваются с действием terminate. Когда зарезервированный MAC-адрес настроен с действием terminate, он не отображается при выполнении любых команд show или show running-config.

Значение по умолчанию: terminate

Формат: `dot1ad l2tunnel vlan` *`vlan id`* `mac-address` *`reserved-mac`* `protocol-id` *`proto-id`* `{tunnel | terminate | discard [shutdown]}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
protocol-id	Поле идентификатора протокола, которое должно совпадать во входящем пакете, чтобы провести протокольное туннелирование. Диапазон protocol-id — от 0x0001 до 0xffff.
reserved-mac	Поле MAC-адреса назначения во входящем пакете, которое должно совпадать с настройками для протокольного туннелирования. Диапазон MAC-адресов — от 01:80:c2:00:00:00 до 01:80:c2:00:00:3F.
tunnel | terminate | discard [shutdown]	Это действие предпринимается для любых пакетов, соответствующих сочетанию MAC-адрес/protocol-id. • **tunnel** — пакету присваивается два тега: с определением сервиса (S-VID) и с идентификатором VLAN клиента (C-VID), после чего пакет переадресуется на NNI-порт на основании S-VID. Это действие предпринимается независимо от того, был ли включен протокол на интерфейсе или нет. • **terminate** — если на интерфейсе включен протокол, то контрольный PDU передается приложению, обрабатывающему протокол. Если протокол не включен, то контрольный пакет отбрасывается. • **discard [shutdown]** — пакет отбрасывается вне зависимости от того, включен на интерфейсе протокол или нет. Используйте необязательное ключевое слово shutdown, чтобы выключить интерфейс и сгенерировать SNMP-трап.
vlan id	Идентификатор сервисной VLAN.

no dot1ad l2tunnel

Эта команда удаляет любую обработку dot1ad-протокола для данного порта.

Формат: `no dot1ad l2tunnel vlan` *`vlan id`* `MAC-address` *`reserved MAC`* `protocol-id` *`proto-id`*

Режим ввода команд: глобальная конфигурация

show dot1ad mode

Данная команда отображает тип порта (UNI-P, UNI-S, NNI или Switchport), и настройку приоритета C-тега.

Формат: `show dot1ad mode {all |` *`unit/slot/port`*`}`

Режим ввода команд: привилегированный

show dot1ad l2tunnel

Данная команда отображает конфигурацию фильтрации зарезервированных MAC-адресов.

Формат: `show dot1ad l2tunnel {all | mac-address` *`mac-addr`* `| protocol-id` *`proto-id`*`} | vlan` *`vlan- id`*`}`

Режим ввода команд: привилегированный

Параметры MAC-address и protocol-id могут быть использованы для индексирования при отображении записей.

9.10 Команды настройки распределения ресурсов (IEEE 802.1p)

В этой части описаны команды для настройки распределения ресурсов (IEEE 802.1p), которые позволяют настроить приоритеты портов.

vlan port priority all

Эта команда назначает приоритет портов для нетегированных пакетов для всех портов, подключенных в данный момент к устройству. Диапазон значений приоритета — от 0 до 7. Любая последующая настройка отдельных портов заменяет данный параметр конфигурации.

Формат: `vlan port priority all` *`priority`*

Режим ввода команд: глобальная конфигурация

vlan priority

Эта команда назначает приоритет порта 802.1p по умолчанию для нетегированных пакетов для определенного интерфейса. Диапазон значений приоритета — от 0 до 7.

Значение по умолчанию: 0

Формат: `vlan priority` *`priority`*

Режим ввода команд: конфигурирование интерфейса

9.11 Команды настройки сквозного режима (ASF)

Сквозной режим (иначе называемый Alternative Store and Forward Mode, ASF) позволяет коммутатору работать в режиме, когда исходящий конвейер начинает передачу пакета до того, как

пакет поступил на входящий конвейер полностью. Включение этого режима сокращает задержку при передаче больших пакетов.

В этом режиме диспетчеру оперативной памяти (MMU) разрешается направлять пакет на исходящий порт до того, как пакет полностью был загружен в память Cell Buffer Pool (CBP).

cut-through mode

Используйте данную команду, чтобы включить или выключить сквозной режим на коммутаторе. После включения или выключения режима необходимо перезагрузить коммутатор, чтобы изменения вступили в силу.

Значение по умолчанию: выключено

Формат: `cut-through mode`

Режим ввода команд: глобальная конфигурация.

no cut-through mode

Эта команда устанавливает сквозной режим в значение по умолчанию.

Формат: `no cut-through mode`

Режим ввода команд: глобальная конфигурация.

show cut-through mode

Команда для отображения текущего и настроенного статуса сквозного режима.

Формат: `show cut-through mode`

Режим ввода команд: глобальная конфигурация

Пример:

Результат выполнения команды в CLI.

```
(Routing) #show cut-through

mode Current mode :Disable
Configured mode :Enable (This mode is effective on next reload)
```

9.12 Настройки асимметричного управления потоком

В режиме асимметричного управления потоком коммутатор отвечает на PAUSE-кадры, полученные от других устройств, останавливая передачу пакетов, но при этом коммутатор не инициирует PAUSE-кадры управления MAC.

Если настроить коммутатор в режим асимметричного управления потоком (или в режим без управления потоком), устройство переходит в режим отбрасывания исходящих данных. Этот режим максимально увеличивает пропускную способность системы за счет потери пакетов в сильно перегруженной системе и позволяет избежать блокировки очереди.

flowcontrol {symmetric|asymmetric}

Используйте данную команду, чтобы включить или выключить симметричное или асимметричное управление потоком на коммутаторе. Режим асимметричного управления подразумевает, что настройка Tx Pause не может быть включена. Включена может быть только Rx Pause.

Значение по умолчанию: управление потоком выключено.

Формат: `flowcontrol {symmetric|asymmetric}`

Режим ввода команд: глобальная конфигурация

no flowcontrol {symmetric|asymmetric}

Используйте no-форму команды, чтобы выключить симметричное или асимметричное управление потоком.

Формат: `no flowcontrol {symmetric|asymmetric}`

Режим ввода команд: глобальная конфигурация

flowcontrol

Используйте данную команду, чтобы включить или выключить симметричное управление потоком на коммутаторе.

Значение по умолчанию: управление потоком выключено.

Формат: `flowcontrol`

Режим ввода команд: глобальная конфигурация

no flowcontrol

Используйте no-форму команды, чтобы выключить симметричное управление потоком.

Формат: `no flowcontrol`

Режим ввода команд: глобальная конфигурация

show flowcontrol

Данная команда используется для отображения конфигурации и статуса управления потоком стандарта IEEE 802.3 (Приложение 31B) для конкретного интерфейса или всех интерфейсов. Команда также отображает счетчики пауз для 802.3 Tx и Rx. Счетчики кадров приоритета для управления потоком не отображаются. Если порт включен для приоритетного управления потоком, оперативный статус управления отображается как **Inactive**. Оперативный статус управления потоком для портов в стеке всегда отображается как **N/A**.

Формат: show flowcontrol [*unit/slot/port*]

Режим ввода команд: привилегированный

9.13 Настройка защищенных портов

Эта часть описывает команды, используемые для настройки и просмотра защищенных портов на коммутаторе. Защищенные порты не перенаправляют трафик друг другу, даже если находятся в одной VLAN. При этом защищенные порты могут перенаправлять трафик на все незащищенные порты в своей группе. Незащищенные порты могут перенаправлять данные защищенным и незащищенным портам. По умолчанию порты являются незащищенными.

Если интерфейс настроен как защищенный порт и вы добавляете его к агрегированному интерфейсу или группе агрегации каналов (LAG), статус защищенного порта на интерфейсе оперативно выключается, при этом интерфейс принимает конфигурацию LAG-порта. Тем не менее

настройка защищенного порта на интерфейсе остается без изменений. Как только интерфейс выходит из LAG, текущая конфигурация этого интерфейса автоматически вступает в действие.

switchport protected (режим глобальной конфигурации)

Используйте данную команду, чтобы создать защищенную группу портов. Параметр groupid определяет набор защищенных портов. Используйте параметры name name, чтобы назначить имя защищенной группы портов. Имя может включать до 32 буквенно-цифровых символов, включая пробелы. Значение по умолчанию: пустая строка.

Защита портов происходит в рамках одного коммутатора. Конфигурация защищенного порта не влияет на трафик между портами двух разных коммутаторов. Между двумя защищенными портами переадресация трафика невозможна.

Значение по умолчанию: не защищен

Формат: `switchport protected` *`groupid`* `name` *`name`*

Режим ввода команд: глобальная конфигурация

no switchport protected (Global Config)

Команда удаляет защищенную группу портов. Параметр groupid определяет набор защищенных портов. Ключевое слово name указывает имя группы, подлежащей удалению.

Формат: `no switchport protected` *`groupid`* `name`

Режим ввода команд: глобальная конфигурация

switchport protected (режим конфигурирования интерфейса)

Используйте данную команду, чтобы добавить интерфейс к группе защищенных портов. Параметр *groupid* определяет набор защищенных портов, к которым подключается интерфейс. Только один интерфейс может быть настроен как защищенный в одной группе.

Защита портов происходит в рамках одного коммутатора. Конфигурация защищенного порта не влияет на трафик между портами двух разных коммутаторов. Между двумя защищенными портами переадресация трафика невозможна.

Значение по умолчанию: не защищен

Формат: `switchport protected` *`groupid`*

Режим ввода команд: конфигурирование интерфейса

no switchport protected (режим конфигурирования интерфейса)

Команда настраивает порт как незащищенный. Параметр *groupid* определяет набор защищенных портов, к которым подключается интерфейс.

Формат: `no switchport protected` *`groupid`*

Режим ввода команд: конфигурирование интерфейса

show switchport protected

Эта команда отображает статус всех интерфейсов, включая защищенные и незащищенные.

Формат: `show switchport protected` *`groupid`*

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Group ID	Номер, обозначающий защищенную группу портов.
Name	Необязательное название группы защищенных портов. Имя может включать до 32 буквенно-цифровых символов, включая пробелы. Значение по умолчанию: пустая строка.
List of Physical Ports	Список портов, которые настроены как защищенные для группы, определенной параметром *groupid*. Если в этой группе ни один порт не настроен как защищенный, поле пустое.

show interfaces switchport

Данная команда отображает статус интерфейса (защищенный/незащищенный) для группы, определенной параметром *groupid*.

Формат: `show interfaces switchport` *`unit/slot/port groupid`*

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Name	Строка, связанная с этой группой для удобства наименования. Может содержать до 32 буквенно-цифровых символов, включая пробелы. Значение по умолчанию: пустая строка. Это необязательное поле.
Protected	Указывает, является ли интерфейс защищенным. Значения: TRUE или FALSE.

9.14 Команды настройки протокола GARP

Этот подраздел описывает команды, используемые для настройки протокола GARP (Generic Attribute Registration Protocol) и отображения статуса GARP. Команды этой части влияют и на GARP VLAN Registration Protocol (GVRP) и на GARP Multicast Registration Protocol (GMRP). GARP — это протокол, позволяющий станциям клиента регистрироваться на коммутаторе для участия в сетях VLAN (используя GVRP) или многоадресных группах (используя GMRP).

set garp timer join

Эта команда устанавливает время регистрации GVRP каждого GARP для одного интерфейса, диапазона интерфейсов или всех интерфейсов. Время регистрации — это интервал между передачей Protocol Data Units (PDU) GARP, регистрирующих (или перерегистрирующих) членство для VLAN или группы многоадресной рассылки. Команда выполняется только тогда, когда GVRP включен. Значения времени — от 10 до 100 сантисекунд. 20 сантисекунд равны 0,2 секунды.

Значение по умолчанию: 20

Формат: `set garp timer join` *`10-100`*

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

no set garp timer join

Данная команда устанавливает время регистрации GVRP в значение по умолчанию и действует только при включенном GVRP.

Формат: `no set garp timer join`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

set garp timer leave

Команда устанавливает время выхода GVRP для одного интерфейса, диапазона интерфейсов, всех интерфейсов или всех портов и действует только при включенном GVRP. Время выхода — это время ожидания после получения запроса об отмене регистрации в VLAN или в группе многоадресной рассылки, по истечении которого удаляется запись VLAN. Может считаться буферным временем для другой станции, чтобы она утвердила регистрацию для того же атрибута и обеспечила непрерывную работу сервиса. Значения времени выхода — от 20 до 600 сантисекунд. 60 сантисекунд равны 0,6 секунды. Время выхода должно быть равно утроенному времени регистрации либо превышать это значение.

Значение по умолчанию: 60

Формат: `set garp timer leave` *`20-600`*

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

no set garp timer leave

Эта команда устанавливает время выхода GVRP в значение по умолчанию и действует только при включенном GVRP.

Формат: `no set garp timer leave`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

set garp timer leaveall

Данная команда устанавливает, как часто генерируются PDU Leave All. PDU Leave All указывает, что все регистрации будут удалены. Участникам необходимо выполнить повторное подключение, чтобы сохранить регистрацию. Значение применяется для каждого порта и каждого участия GARP. Значение времени — от 200 до 6000 сантисекунд. 1000 сантисекунд равны 10 секундам. Команда может применяться для всех портов (режим глобальной конфигурации), для одного порта или диапазона портов (режим конфигурирования интерфейса) и действует только при включенном GVRP. Значение времени leave all должно быть больше времени выхода.

Значение по умолчанию: 1000

Формат: `set garp timer leaveall` *`200-6000`*

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

no set garp timer leaveall

Эта команда устанавливает частоту генерации PDU Leave All в значение по умолчанию и действует только при включенном GVRP.

Формат: `no set garp timer leaveall`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

show garp

Команда для отображения информации о GARP.

Формат: `show garp`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
GMRP Admin Mode	Административный режим GARP Multicast Registration Protocol (GMRP) данной системы.
GVRP Admin Mode	Административный режим GARP VLAN Registration Protocol (GVRP) данной системы.

9.15 Команды настройки протокола GVRP

Эта часть описывает команды, используемые для настройки и отображения информации GVRP (GARP VLAN Registration Protocol). Коммутаторы с включенным GVRP обмениваются информацией о настройках VLAN, которая позволяет GVRP обеспечивать динамическое создание и удаление VLAN на магистральных портах.

Если GVRP выключен, система не переадресует GVRP-сообщения.

set gvrp adminmode

Эта команда включает GVRP в системе.

Значение по умолчанию: выключено

Формат: `set gvrp adminmode`

Режим ввода команд: привилегированный

no set gvrp adminmode

Данная команда выключает GVRP.

Формат: `no set gvrp adminmode`

Режим ввода команд: привилегированный

set gvrp interfacemode

Эта команда включает GVRP на одном порте (режим конфигурирования интерфейса), диапазоне портов (режим диапазона интерфейсов) или на всех портах (режим глобальной конфигурации).

Значение по умолчанию: выключено

Формат: `set gvrp interfacemode`

Режим ввода команд: конфигурирование интерфейса
диапазон интерфейсов
глобальная конфигурация

no set gvrp interfacemode

Эта команда выключает GVRP на одном порте (режим конфигурирования интерфейса) или на всех портах (режим глобальной конфигурации). Если GVRP выключен, параметры Join Time, Leave Time и Leave All Time не действуют.

Формат: `no set gvrp interfacemode`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

show gvrp configuration

Эта команда отображает информацию о GVRP для одного или всех интерфейсов.

Формат: `show gvrp configuration {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
Interface	unit/slot/port
Join Timer	Интервал между передачей PDU GARP, регистрирующих (или перерегистрирующих) членство для атрибута. Текущие атрибуты — группа многоадресной рассылки или VLAN. Для этого таймера существует экземпляр на каждый порт на основе участия каждого GARP. Возможные значения — от 10 до 100 сантисекунд (от 0,1 до 1,0 секунды). По умолчанию — 20 сантисекунд (0,2 секунды). Минимальная детализация – 1 сантисекунда (0,01 секунды).
Leave Timer	Время ожидания после получения запроса об отмене регистрации для атрибута, прежде чем удалить атрибут. Текущие атрибуты — группа многоадресной рассылки или VLAN. Может считаться буферным временем для другой станции, чтобы она утвердила регистрацию для того же атрибута и обеспечила непрерывную работу сервиса. Для этого таймера существует экземпляр на каждый порт на основе участия каждого GARP. Возможные значения — от 20 до 600 сантисекунд (от 0,2 до 6,0 секунды). По умолчанию — 60 сантисекунд (0,6 секунды).
LeaveAll Timer	Время Leave All определяет, как часто генерируются PDU LeaveAll. PDU LeaveAll указывает, что все регистрации скоро будут удалены. Участникам необходимо выполнить повторное подключение, чтобы сохранить регистрацию. Для этого таймера существует экземпляр на

	каждый порт на основе участия каждого GARP. Таймер Leave All установлен на случайное значение в пределах от LeaveAllTime до 1,5 LeaveAllTime. Возможные значения — от 200 до 6000 сантисекунд (от 2 до 60 секунды). По умолчанию — 1000 сантисекунд (10 секунды).
Port GMRP Mode	Административный режим GMRP порта, который может быть включен или выключен (по умолчанию). Если этот параметр выключен, параметры Join Time, Leave Time и Leave All Time не действуют.

show mac-address-table gmrp

Данная команда отображает GMRP-записи в таблице коммутации многоадресной рассылки (MFDB).

Формат: `show mac-address-table gmrp`

Режим ввода команд: привилегированный

Термин	***Значение***
VLAN ID	VLAN, в которой был определен MAC-адрес.
MAC Address	Одноадресный MAC-адрес, для которого коммутатор переадресует или фильтрует данные. В формате шести двузначных номеров шестнадцатеричной системы, разделенных двоеточиями, например: 01:23:45:67:89:AB.
Type	Тип записи. Статичные записи — записи, которые настраиваются конечным пользователем. Динамические добавляются в таблицу как результат процесса определения или протокола.
Description	Текстовое описание данной записи таблицы многоадресной коммутации.
Interfaces	Список интерфейсов, которые назначены для переадресации (Fwd:) и фильтрации (Flt:).

9.16 Команды настройки управления сетевым доступом на основе портов

Эта часть описывает команды, которые можно использовать для настройки управления доступом к сети на базе IEEE 802.1X. Управление доступом к сети на основе портов позволяет разрешать доступ к службам сети только устройствам, которые прошли авторизацию и аутентификацию.

aaa authentication dot1x default

Используйте эту команду, чтобы настроить на коммутаторе метод аутентификации для доступа на базе 802.1x. Дополнительные методы аутентификации используются только в случае получения сообщения об ошибке указанного метода, но не в случае ошибки аутентификации. Ниже перечислены возможные методы.

- ias. Использует для аутентификации базу данных внутреннего сервера аутентификации пользователей. Этот способ может использоваться вместе с любым уже существующим способом — **local**, **radius** и т. д.
- local. Использует для аутентификации локальную базу имен пользователей.
- none. Аутентификация не используется.
- radius. Использует для аутентификации список всех RADIUS-серверов.

Формат: `aaa authentication dot1x default {[ias]|[`*`method1 [method2 [method3]]]`*`}`

Режим ввода команд: глобальная конфигурация

clear dot1x statistics

Эта команда сбрасывает статистику 802.1X для указанного порта или всех портов.

Формат: `clear dot1x statistics {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный

clear dot1x authentication-history

Эта команда очищает таблицу истории аутентификации, записанную во время успешных и неудачных аутентификаций на указанном интерфейсе или всех интерфейсах.

Формат: `clear dot1x authentication-history [`*`unit/slot/port`*`]`

Режим ввода команд: привилегированный

clear radius statistics

Данная команда очищает всю статистику RADIUS.

Формат: `clear radius statistics`

Режим ввода команд: привилегированный

dot1x eapolflood

Используйте эту команду, чтобы включить на коммутаторе поддержку потоков EAPOL.

Значение по умолчанию: выключено

Формат: `dot1x eapolflood`

Режим ввода команд: глобальная конфигурация

no dot1x eapolflood

Эта команда выключает потоки EAPOL на коммутаторе.

Формат: `no dot1x eapolflood`

Режим ввода команд: глобальная конфигурация

dot1x dynamic-vlan enable

Используйте эту команду, чтобы позволить коммутатору динамично создавать VLAN, не существующей на коммутаторе, на основе RADIUS авторизации.

Значение по умолчанию: выключено

Формат: `dot1x dynamic-vlan enable`

Режим ввода команд: глобальная конфигурация

no dot1x dynamic-vlan enable

Используйте эту команду, чтобы запретить коммутатору динамично создавать VLAN.

Формат: `no dot1x dynamic-vlan enable`

Режим ввода команд: глобальная конфигурация

dot1x guest-vlan

Данная команда настраивает гостевую VLAN на интерфейсе или диапазоне интерфейсов по стандарту IEEE 802.1X. Диапазон — от 1 до максимального значения идентификатора VLAN, поддерживаемого платформой.

Значение по умолчанию: выключено

Формат: `dot1x guest-vlan` *`vlan-id`*

Режим ввода команд: конфигурирование интерфейса

no dot1x guest-vlan

Эта команда выключает гостевую VLAN на интерфейсе.

Значение по умолчанию: выключено

Формат: `no dot1x guest-vlan`

Режим ввода команд: конфигурирование интерфейса

dot1x initialize

Команда начинает процедуру инициализации на указанном порте. Эта команда действительна только в случае, если режим управления для указанного порта автоматический или основан на MAC. Если это условие не выполнено, команда вернет ошибку.

Формат: `dot1x initialize` *`unit/slot/port`*

Режим ввода команд: привилегированный

dot1x max-req

Эта команда устанавливает максимальное число запросов аутентификации статуса устройства на интерфейсе или диапазоне интерфейсов с помощью EAPOL EAP Request/Identity. Значение count должно быть от 1 до 10.

Значение по умолчанию: 2

Формат: `dot1x max-req` *`count`*

Режим ввода команд: конфигурирование интерфейса

no dot1x max-req

Эта команда устанавливает максимальное число запросов аутентификации статуса устройства на интерфейсе или диапазоне интерфейсов с помощью EAPOL EAP Request/Identity к значению по умолчанию.

Формат: `no dot1x max-req`

Режим ввода команд: конфигурирование интерфейса

dot1x max-users

Используйте данную команду, чтобы установить максимальное количество клиентов, поддерживающихся интерфейсом или диапазоном интерфейсов, если на порте включена dot1x-аутентификация на основе MAC. Значение count — от 1 до 48.

Значение по умолчанию: 48

Формат: `dot1x max-users count`

Режим ввода команд: конфигурирование интерфейса

no dot1x max-users

Эта команда возвращает максимальное количество клиентов на каждый порт в значение по умолчанию.

Формат: `no dot1x max-users`

Режим ввода команд: конфигурирование интерфейса

dot1x port-control

Эта команда устанавливает режим аутентификации для использования на указанном интерфейсе или диапазоне интерфейсов. Используйте параметр *force-unauthorized*, чтобы PAE-аутентификатор безоговорочно установил управляемый порт как неавторизованный. Используйте параметр force-authorized, чтобы PAE-аутентификатор установил управляемый порт как авторизованный. Используйте параметр auto, чтобы PAE-аутентификатор установил управляемый порт на основе результата обменов аутентификационными данными между клиентом, коммутатором и сервером аутентификации. Если указана опция mac-based, на порте включается dot1x-аутентификация на основе MAC.

Значение по умолчанию: auto

Формат: `dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}`

Режим ввода команд: конфигурирование интерфейса

no dot1x port-control

Данная команда устанавливает режим 802.1X-управления указанного порта в значение по умолчанию.

Формат: `no dot1x port-control`

Режим ввода команд: конфигурирование интерфейса

dot1x port-control all

Эта команда устанавливает режим аутентификации для использования на всех портах. Выберите `force-unauthorized`, чтобы PAE-аутентификатор безоговорочно установил управляемый порт как неавторизованный. Выберите force-authorized, чтобы PAE-аутентификатор безоговорочно установил управляемый порт как авторизованный. Выберите auto, чтобы PAE-аутентификатор установил управляемый порт на основе результата обменов аутентификационными данными между клиентом, коммутатором и сервером аутентификации. Если указана опция mac-based, на порте включается dot1x-аутентификация на основе MAC.

Значение по умолчанию: auto

Формат: `dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}`

Режим ввода команд: глобальная конфигурация

no dot1x port-control all

Эта команда возвращает режим аутентификации для всех портов в значение по умолчанию.

Формат: `no dot1x port-control all`

Режим ввода команд: глобальная конфигурация

dot1x mac-auth-bypass

Если режим 802.1X на интерфейсе работает на основе MAC, можно использовать данную команду, чтобы включить на интерфейсе MAC Authentication Bypass (MAB). MAB — это дополнительный механизм аутентификации, который позволяет не распознающим 802.1X клиентам (таким как принтеры, факсы, а также некоторые IP-телефоны) аутентифицироваться в сети с помощью клиентского MAC-адреса в качестве идентификатора. Эта команда также предоставляет варианты для указания типа используемой аутентификации — EAP-MD5, PAP или CHAP.

Значение по умолчанию: выключено

Формат: `dot1x mac-auth-bypass [auth-type {pap | eap-md5 | chap}]`

Режим ввода команд: конфигурирование интерфейса

no dot1x mac-auth-bypass

Данная команда устанавливает режим MAB на портах в значение по умолчанию.

Формат: `no dot1x mac-auth-bypass`

Режим ввода команд: конфигурирование интерфейса

dot1x re-authenticate

Эта команда начинает процедуру повторной аутентификации на указанном порте. Данная команда действует только в случае, если режим управления для данного порта настроен как auto или mac-based. Если это условие не выполнено, команда вернет ошибку.

Формат: `dot1x re-authenticate` *`unit/slot/port`*

Режим ввода команд: привилегированный

dot1x re-authentication

Эта команда включает повторную аутентификацию клиента для указанного интерфейса или диапазона интерфейсов.

Значение по умолчанию: выключено

Формат: `dot1x re-authentication`

Режим ввода команд: конфигурирование интерфейса

no dot1x re-authentication

Эта команда выключает повторную аутентификацию клиента для указанного порта.

Формат: `no dot1x re-authentication`

Режим ввода команд: конфигурирование интерфейса

dot1x system-auth-control

Используйте данную команду, чтобы запустить dot1x-аутентификацию на коммутаторе. В выключенном состоянии конфигурация dot1x сохраняется и может быть изменена, но не является активной.

Значение по умолчанию: выключено

Формат: `dot1x system-auth-control`

Режим ввода команд: глобальная конфигурация

no dot1x system-auth-control

Эта команда используется для выключения поддержки dot1x-аутентификации на коммутаторе.

Формат: `no dot1x system-auth-control`

Режим ввода команд: глобальная конфигурация

dot1x system-auth-control monitor

Используйте данную команду, чтобы включить режим мониторинга 802.1X на коммутаторе. Задача режима мониторинга — помочь в решении проблем, связанных с конфигурацией аутентификации на базе портов без прерывания доступа к сети хостов, подключенных к коммутатору. В режиме мониторинга у хоста есть сетевой доступ к порту с включенным 802.1X, даже если он не прошел аутентификацию. Результаты процесса записываются в целях диагностики.

Значение по умолчанию: выключено

Формат: `dot1x system-auth-control monitor`

Режим ввода команд: глобальная конфигурация

no dot1x system-auth-control monitor

Эта команда выключает на коммутаторе режим мониторинга 802.1X.

Формат: `no dot1x system-auth-control monitor`

Режим ввода команд: глобальная конфигурация

dot1x timeout

Данная команда устанавливает значение таймера в секундах, который используется Dot1x на интерфейсе или диапазоне интерфейсов. В зависимости от используемого таймера и прошедшего времени (в секундах) устанавливаются различные настраиваемые параметры времени жизни. Поддерживается настройка следующих таймеров.

Таймер	***Значение***
guest-vlan- period	Время в секундах, которое аутентификатор ждет поступления на порт EAPOL-пакетов, прежде чем авторизовать порт и поместить его в гостевую VLAN (если настроена). Таймер гостевой VLAN применим только в случае, если на данном порте настроена гостевая VLAN.
reauth-period	Значение в секундах для таймера, используемого аутентификатором состояния на данном порте для определения, когда будет

	происходить повторная аутентификация запрашивающего. Значение должно быть в диапазоне от 1 до 65535.
quiet-period	Значение в секундах для таймера, используемого аутентификатором состояния на данном порте для того, чтобы определить периоды времени, в которые он не будет пытаться искать запрашивающего. Это значение должно быть в диапазоне от 0 до 65535.
tx-period	Значение в секундах для таймера, используемого аутентификатором состояния на данном порте для того, чтобы определить, когда отсылать кадр EAPOL EAP Request/Identity запрашивающему. Это значение должно быть в диапазоне от 1 до 65535.
supp-timeout	Значение в секундах для таймера, используемого аутентификатором состояния на данном порте для того, чтобы определить время жизни записи для запрашивающего. Значение должно быть в диапазоне от 1 до 65535.
server-timeout	Значение в секундах для таймера, используемого аутентификатором состояния на данном порте для того, чтобы определить время жизни записи для сервера аутентификации. Значение должно быть в диапазоне от 1 до 65535.

Значение по умолчанию: guest-vlan-period: 90 секунд

reauth-period: 3600 секунд

quiet-period: 60 секунд

tx-period: 30 секунд

supp-timeout: 30 секунд

server-timeout: 30 секунд

Формат: `dot1x timeout {{guest-vlan-period` *`seconds`*`} |{reauth-period` *`seconds`*`} | {quiet-period` *`seconds`*`} | {tx-period` *`seconds`*`} | {supp-timeout` *`seconds`*`} | {server-timeout` *`seconds`*`}}`

Режим ввода команд: конфигурирование интерфейса

no dot1x timeout

Эта команда устанавливает значение времени (в секундах) для таймера, используемого аутентификатором состояния на данном порте, в значение по умолчанию. В зависимости от используемого токена устанавливаются соответствующие значения по умолчанию.

Формат: `no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supp- timeout | server-timeout}`

Режим ввода команд: конфигурирование интерфейса

dot1x unauthenticated-vlan

Используйте эту команду, чтобы настроить неаутентифицированную VLAN, связанную с указанным интерфейсом или диапазоном интерфейсов. Идентификатор неаутентифицированной VLAN может быть действительным идентификатором VLAN из в диапазоне от 0 до максимального поддерживаемого значения. Для работы неаутентифицированная VLAN должна быть настроена статично в базе данных VLAN. По умолчанию неаутентифицированная VLAN обозначена как 0, т. е. недействительна и не работает.

Значение по умолчанию: 0

Формат: `dot1x unauthenticated-vlan` *`vlan id`*

Режим ввода команд: конфигурирование интерфейса

no dot1x unauthenticated-vlan

Данная команда устанавливает неаутентифицированную VLAN, связанную с портом, в значение по умолчанию.

Формат: `no dot1x unauthenticated-vlan`

Режим ввода команд: конфигурирование интерфейса

dot1x user

Эта команда добавляет указанного пользователя в список пользователей, имеющих доступ к указанному порту или всем портам. Параметр *user* должен быть настроенным пользователем.

Формат: `dot1x user` *`user`* {*`unit/slot/port`* | `all`}

Режим ввода команд: глобальная конфигурация

no dot1x user

Эта команда удаляет пользователя из списка пользователей, имеющих доступ к указанному порту или всем портам.

Формат: `no dot1x user` *`user`* {*`unit/slot/port`* | `all`}

Режим ввода команд: глобальная конфигурация

authentication enable

Эта команда глобально включает диспетчер аутентификации. Конфигурация интерфейса будет действовать только в случае, если диспетчер аутентификации включен с помощью этой команды.

Значение по умолчанию: выключено

Формат: `authentication enable`

Режим ввода команд: глобальная конфигурация

no authentication enable

Эта команда выключает диспетчер аутентификации.

Формат: `no authentication enable`

Режим ввода команд: глобальная конфигурация

authentication order

Эта команда устанавливает порядок способов аутентификации, используемых на порте. Доступные способы аутентификации: Dot1x, MAB и captive portal. Порядок устанавливает последовательность способов, которые коммутатор будет пытаться применить при аутентификации нового устройства, подключенного к порту. Если способ не завершился успехом или был просрочен, применяется следующий способ.

Каждый способ может быть введен только один раз. Установить порядок можно только для 802.1x и MAB. Captive portal может быть настроен как единственный метод или как последний способ в очереди.

Формат: `authentication order {dot1x [mab [captive-portal] | captive-portal] | mab [dot1x [captive-portal]| captive-portal] | captive-portal}`

Режим ввода команд: конфигурирование интерфейса

no authentication order

Эта команда возвращает порт к порядку способов аутентификации по умолчанию.

Формат: `no authentication order`

Режим ввода команд: конфигурирование интерфейса

authentication priority

Эта команда устанавливает приоритет способов аутентификации, используемых на порте. Доступные способы аутентификации: Dot1x, MAB и captive portal. Приоритет аутентификации определяет, будет ли прежде аутентифицированный клиент проходить повторную аутентификацию с помощью способа с более высоким приоритетом, когда таковой получен. Captive portal всегда находится последним в списке способов.

Значение по умолчанию: `authentication order dot1x mab captive portal`

Формат: `authentication priority {dot1x [mab [captive portal] | captive portal] | mab [dot1x [captive portal]| captive portal] | captive portal}`

Режим ввода команд: конфигурирование интерфейса

no authentication priority

Эта команда возвращает порт к настройкам приоритета способов аутентификации по умолчанию.

Формат: `no authentication priority`

Режим ввода команд: конфигурирование интерфейса

authentication timer restart

Данная команда устанавливает время в секундах, после которого начинается повторная аутентификация. (Значение по умолчанию — 300 секунд.) Таймер начинает повторную аутентификацию только после того, как все способы аутентификации завершились неудачей. По истечении времени таймера для порта запускается повторная аутентификация.

Формат: `authentication timer restart <300-65535>`

Режим ввода команд: конфигурирование интерфейса

no authentication timer restart

Эта команда устанавливает время повторной аутентификации в значение по умолчанию — 3600 секунд.

Формат: `no authentication timer restart`

Режим ввода команд: конфигурирование интерфейса

show authentication authentication-history

Используйте эту команду, чтобы отобразить данные истории аутентификации для определенного интерфейса.

Формат: `show authentication authentication-history` *`unit/slot/port`*

Режим ввода команд: привилегированный

Для каждого интерфейса отображается следующая информация.

Термин	***Значение***
Time Stamp	Время аутентификации.
Interface	Интерфейс.
MAC-Address	MAC-адрес интерфейса.
Auth Status Method	Способ аутентификации и его статус для интерфейса.

show authentication interface

Используйте данную команду, чтобы отобразить информацию о способах аутентификации для всех интерфейсов либо для указанного порта.

Формат: `show authentication interface {all | `*`unit/slot/port`*` }`

Режим ввода команд: привилегированный

Для каждого интерфейса отображается следующая информация.

Термин	***Значение***
Interface	Интерфейс, для которого отображается конфигурация аутентификации.
Authentication Restart timer	Время в секундах, по прошествии которого начинается повторная аутентификация.
Configured method order	Порядок способов аутентификации, настроенный на порте.
Enabled method order	Порядок способов аутентификации, используемый на порте.
Configured method priority	Приоритет способов аутентификации, настроенный на порте.
Enabled method priority	Приоритет способов аутентификации, используемый на порте.
Number of authenticated clients	Количество аутентифицированных клиентов.
Logical Interface	Логический интерфейс.
Client MAC addr	MAC-адрес клиента.
Authenticated Method	Текущий способ аутентификации.
Auth State	Была ли аутентификация успешной.
Auth Status	Текущий статус аутентификации.
Authentication Login List	Название списка аутентификации подключения.
Method 1	Первый метод в указанном списке входной аутентификации, если имеется.
Method 2	Второй метод в указанном списке входной аутентификации, если имеется.
Method 3	Третий метод в указанном списке входной аутентификации, если имеется.

show authentication statistics

Используйте данную команду, чтобы отобразить статистику аутентификации для интерфейса.

Формат: `show authentication statistics` *`unit/slot/port`*

Режим ввода команд: привилегированный

Для каждого интерфейса отображается следующая информация.

show authentication methods

Команда отображает информацию о способах аутентификации.

Формат: `show authentication methods`

Режим ввода команд: привилегированный

Термин	*Значение*
Authentication Login List	Название списка аутентификации подключения.
Method 1	Первый метод в указанном списке входной аутентификации, если имеется.
Method 2	Второй метод в указанном списке входной аутентификации, если имеется.
Method 3	Третий метод в указанном списке входной аутентификации, если имеется.

show authentication statistics

Используйте данную команду, чтобы отобразить статистику аутентификации для интерфейса.

Формат: show authentication statistics *unit/slot/port*

Режим ввода команд: привилегированный

Для каждого интерфейса отображается следующая информация.

Термин	*Значение*
Port	Порт, для которого отображается информация.
802.1X attempts	Количество попыток аутентификации Dot1x на порте.
802.1X failed attempts	Количество неудавшихся попыток аутентификации Dot1x на порте.
Mab attempts	Количество попыток аутентификации MAB (MAC authentication bypass) на порте.
Mab failed attempts	Количество неудавшихся попыток аутентификации MAB на порте.
Captive-portal attempts	Количество попыток аутентификации с помощью captive portal (веб-авторизация).
Captive-portal failed attempts	Количество неудавшихся попыток аутентификации с помощью captive portal.

clear authentication statistics

Используйте данную команду, чтобы очистить статистику аутентификации на интерфейсе.

Формат: `clear authentication authentication-history {unit/slot/port] | all}`

Режим ввода команд: привилегированный

clear authentication authentication-history

Используйте данную команду, чтобы очистить журнал истории аутентификации для интерфейса.

Формат: `clear authentication authentication-history {unit/slot/port | all}`

Режим ввода команд: привилегированный

show dot1x

Эта команда используется для того, чтобы отобразить сводную информацию глобальной конфигурации dot1x, сводную информацию конфигурации dot1x для указанного порта или всех портов, подробную информацию конфигурации dot1x для указанного порта и статистику dot1x для указанного порта.

Формат: `show dot1x [{summary {unit/slot/port | all} | detail unit/slot/port | statistics unit/ slot/port]`

Режим ввода команд: привилегированный

Если не использовать необязательные параметры unit/slot/port или vlanid, команда отобразит параметры Global dot1x mode, VLAN Assignment mode и Dynamic VLAN Creation mode.

Термин	***Значение***
Administrative Mode	Показывает, включен ли на коммутаторе режим управления аутентификацией.
VLAN Assignment Mode	Показывает, разрешено назначение авторизованного порта к VLAN, назначенной RADIUS (enabled) или нет (disabled).
Dynamic VLAN Creation Mode	Показывает, может ли коммутатор динамически создавать VLAN, связанную с RADIUS, если таковая еще не существует на коммутаторе.
Monitor Mode	Показывает, включен ли на коммутаторе режим мониторинга Dot1x.

Если использовать необязательный параметр summary {unit/slot/port | all}, отображаются все настройки dot1x для указанного порта или всех портов.

Термин	***Значение***
Interface	Интерфейс, для которого отображается конфигурация.
Control Mode	Настроенный режим управления для данного порта. Возможные значения: force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	Текущий режим управления, с которым работает порт. Возможные значения: authorized | unauthorized.
Reauthentication Enabled	Показывает, включена ли на данном порте повторная аутентификация.
Port Status	Показывает, авторизован ли порт. Возможные значения: authorized | unauthorized.

Если использовать необязательный параметр detail unit/slot/port, отображаются подробные настройки dot1x для указанного порта.

Термин	***Значение***
Port	Интерфейс, для которого отображается конфигурация.
Protocol Version	Версия протокола, связанная с данным портом. Единственное возможное значение — 1, соответствующее первой версии спецификации dot1x.
PAE Capabilities	PAE-функциональность данного порта. Возможные значения: Authenticator или Supplicant.

Control Mode	Настроенный режим управления для данного порта. Возможные значения: force-unauthorized | force-authorized | auto | mac-based.
Authenticator PAE State	Текущий статус PAE-состояния аутентификатора. Возможные значения: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized и ForceUnauthorized. Если на порте включена MAC-аутентификация, этот параметр становится устаревшим.
Backend Authentication State	Текущий статус серверного аутентификатора. Возможные значения: Request, Response, Success, Fail, Timeout, Idle и Initialize. Если на порте включена MAC-аутентификация, этот параметр становится устаревшим.
Quiet Period	Таймер, используемый аутентификатором состояния на данном порте для того, чтобы определить периоды времени, в которые он не будет пытаться искать запрашивающего. Значение выражается в секундах в диапазоне от 0 до 65535.
Transmit Period	Таймер, используемый аутентификатором статуса на указанном порте для определения времени, когда он будет посылать кадры EAPOL EAP Request/Identity запрашивающему. Значение выражается в секундах в диапазоне от 1 до 65535.
Guest-VLAN ID	Идентификатор гостевой VLAN, настроенной на интерфейсе.
Guest VLAN Period	Время в секундах, в течение которого аутентификатор ждет поступления на порт EAPOL-пакетов, прежде чем поместить порт в гостевую VLAN.
Supplicant Timeout	Таймер, используемый аутентификатором статуса на данном порте для того, чтобы определить время жизни записи запрашивающего. Значение выражается в секундах в диапазоне от 1 до 65535.
Server Timeout	Таймер, используемый аутентификатором статуса на данном порте для того, чтобы определить время жизни записи сервера аутентификации. Значение выражается в секундах в диапазоне от 1 до 65535.
Maximum Requests	Максимальное количество раз, которое устройство аутентификации статуса на данном порте будет повторять передачу кадра EAPOL EAP Request/Identity до прекращения передачи. Значение будет в диапазоне от 1 до 10.
Configured MAB Mode	Административный режим функции MAC authentication bypass на коммутаторе.
Operational MAB Mode	Рабочий режим функции MAC authentication bypass на коммутаторе. MAB может быть административно включена, но не функционировать, если действует режим управления не на основе MAC.
Vlan-ID	VLAN, назначенная порту сервером RADIUS. Действительно только в том случае, если действует режим управления порта не на основе MAC.
VLAN Assigned Reason	Причина, по которой VLAN идентифицируемая в поле VLAN-assigned, была назначена порту. Возможные значения: RADIUS, Unauthenticated VLAN, Guest VLAN, default, или Not Assigned. Если причина указана как Not Assigned, это означает, что dot1x не назначал порту никаких VLAN. Действительно только в том случае, если действует режим управления порта не на основе MAC.
Reauthentication Period	Таймер, используемый идентификатором статуса данного порта, чтобы определить, когда происходит повторная аутентификация запрашивающего. Значение выражается в секундах в диапазоне от 1 до 65535.
Reauthentication Enabled	Показывает, включена ли повторная аутентификация на данном порте. Возможные значения: True или False.
Key Transmission Enabled	Показывает, передается ли ключ запрашивающему на указанном порте. Возможные значения: True или False.

EAPOL Flood Mode Enabled	Показывает, включена ли поддержка потоков EAPOL на коммутаторе. Возможные значения: True или False.
Control Direction	Направление контроля для указанного порта или портов. Возможные значения: both или in.
Maximum Users	Максимальное количество клиентов, которые могут быть аутентифицированы на порте в режиме dot1x-аутентификации на базе MAC. Это значение используется только в том случае, если действует режим управления порта не на основе MAC.
Unauthenticated VLAN ID	Указывает неаутентифицированные VLAN, настроенные для данного порта. Это значение действительно для порта только в том случае, если действует режим управления порта не на основе MAC.
Session Timeout	Указывает время, в течение которого данная сессия является действительной. Период времени в секундах возвращается RADIUS-сервером после аутентификации порта. Это значение действительно для порта только в том случае, если действует режим управления порта не на основе MAC.
Session Termination Action	Указывает действие, выполняемое по истечении времени сессии. Возможные значения: Default и Radius-Request. Default обозначает, что сессия прекращается и порт возвращается в неавторизованное состояние. При значении Radius-Request на данном порте выполняется повторная аутентификация клиента. Это значение действительно для порта только в том случае, если действует режим управления порта не на основе MAC.

Для каждого клиента, аутентифицированного на порте, команда *show dot1x detail unit/slot/port* отобразит следующие параметры dot1x на основе MAC, если действует режим управления указанного порта на основе MAC.

Термин	***Значение***
Supplicant MAC Address	MAC-адрес запрашивающего.
Authenticator PAE State	Текущий статус PAE-состояния аутентификатора. Возможные значения: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized и ForceUnauthorized.
Backend Authentication State	Текущий статус серверного аутентификатора. Возможные значения: Request, Response, Success, Fail, Timeout, Idle и Initialize.
VLAN-Assigned	VLAN, назначенный клиенту сервером RADIUS.
Logical Port	Номер логического порта, назначенного клиенту.

Если использовать необязательный параметр *statistics unit/slot/port*, появится следующая статистика dot1x для указанного порта.

Термин	***Значение***
Port	Интерфейс, для которого отображается статистика.
EAPOL Frames Received	Количество действительных EAPOL-кадров любого типа, полученных данным аутентификатором.
EAPOL Frames Transmitted	Количество EAPOL-кадров любого типа, переданных данным аутентификатором.
EAPOL Start Frames Received	Количество EAPOL-кадров типа start, полученных данным аутентификатором.
EAPOL Logoff Frames Received	Количество EAPOL-кадров типа logoff, полученных данным аутентификатором.
Last EAPOL Frame Version	Номер версии протокола, присутствующий в последнем полученном EAPOL-кадре.
Last EAPOL Frame Source	MAC-адрес источника, присутствующий в последнем полученном EAPOL-кадре.

EAP Response/ Id Frames Received	Количество EAP-кадров типа response/identity, полученных данным аутентификатором.
EAP Response Frames Received	Количество действительных EAP-кадров типа response (помимо response/identity), полученных данным аутентификатором.
EAP Request/Id Frames Transmitted	Количество EAP-кадров типа request/identity, переданных данным аутентификатором.
EAP Request Frames Transmitted	Количество EAP-кадров типа request (помимо request/identity), переданных данным аутентификатором.
Invalid EAPOL Frames Received	Количество EAPOL-кадров с нераспознанным типом кадра, полученных данным аутентификатором.
EAP Length Error Frames Received	Количество EAPOL-кадров с нераспознанным типом кадра, полученных данным аутентификатором.

show dot1x authentication-history

Эта команда отображает события аутентификации 802.1X и информацию успешных и неудачных процессов аутентификации Dot1x для всех интерфейсов или определенного интерфейса. Используйте необязательные ключевые слова, чтобы кратко или подробно отобразить только неудачные события аутентификации.

Формат: `show dot1x authentication-history {`*`unit/slot/port`* `| all} [failed-auth-only] [detail]`

Режим ввода команд: привилегированный

Термин	***Значение***
Time Stamp	Точное время события.
Interface	Физический порт, на котором произошло событие.
Mac-Address	MAC-адрес запрашивающего/клиента.
VLAN assigned	VLAN, назначенная клиенту/порту аутентификации.
VLAN assigned Reason	Тип назначенного идентификатора VLAN; может иметь значения Guest VLAN, Unauth, Default, RADIUS Assigned или Monitor Mode VLAN ID.
Auth Status	Статус аутентификации.
Reason	Фактическая причина успешной или неудачной аутентификации.

show dot1x clients

Данная команда отображает информацию 802.1X-клиента. Эта команда также отображает информацию о количестве клиентов, которые прошли аутентификацию с помощью режима мониторинга и применения 802.1X.

Формат: `show dot1x clients {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный

Термин	***Значение***
Clients Authenticated using Monitor Mode	Указывает количество dot1x-клиентов, аутентифицированных с помощью режима мониторинга.
Clients Authenticated using Dot1x	Указывает количество dot1x-клиентов, аутентифицированных с помощью процесса аутентификации 802.1X.
Logical Interface	Номер логического порта, назначенного клиенту.
Interface	Физический порт, с которым связан запрашивающий.

User Name	Имя пользователя, используемое клиентом для аутентификации на сервере.
Supplicant MAC Address	MAC-адрес запрашивающего устройства.
Session Time	Время с момента входа запрашивающего.
Filter ID	Указывает идентификатор фильтра, возвращающийся на RADIUS-сервер, когда клиент аутентифицируется. Является настраиваемым именем политики DiffServ на коммутаторе.
VLAN ID	VLAN, назначенная порту.
VLAN Assigned	Причина, по которой указанная в поле VLAN ID сеть VLAN была назначена порту. Возможные значения: RADIUS, Unauthenticated VLAN, Monitor Mode или Default. Default означает, что VLAN назначена порту по причине того, что P-VID порта совпал с идентификатором VLAN.
Session Timeout	Это значение указывает время действия сессии. Период времени в секундах возвращается RADIUS-сервером после аутентификации порта. Это значение действительно для порта только в том случае, если действует режим управления порта не на основе MAC.
Session Termination Action	Указывает действие, выполняемое по истечении времени сессии. Возможные значения: Default и Radius-Request. Default обозначает, что сессия прекращается и данные клиента удаляются. При значении Radius-Request, на данном порте выполняется повторная аутентификация клиента.

show dot1x users

Данная команда отображает информацию о защите 802.1X-порта для локально настроенных пользователей.

Формат: `show dot1x users` *`unit/slot/port`*

Режим ввода команд: привилегированный

Термин	***Значение***
Users	Пользователи, локально настроенные для получения доступа к указанному порту.

9.17 Команды клиента 802.1X

Система поддерживает функционал клиента 802.1X (dot1x) на портах типа «точка-точка». Администратор может настроить имя пользователя и пароль, используемые для аутентификации.

dot1x pae

Эта команда устанавливает dot1x-роль порта. Порт может быть клиентом либо аутентификатором.

Формат: `dot1x pae {supplicant | authenticator}`

Режим ввода команд: конфигурирование интерфейса

dot1x supplicant port-control

Эта команда устанавливает статус авторизации порта (Authorized или Unauthorized) вручную или с помощью настройки порта на автоматическую авторизацию при запуске. По умолчанию все порты — аутентификаторы. Если атрибут порта необходимо сменить в направлении <authenticator to supplicant> или <supplicant to authenticator>, используйте эту команду.

Формат: `dot1x supplicant port-control {auto | force-authorized | force_unauthorized}`

Режим ввода команд: конфигурирование интерфейса

Термин	*Значение*
auto	Порт находится в неавторизованном статусе до тех пор, пока он не предоставит свое имя пользователя и пароль аутентификатору. Если аутентификатор авторизует порт, порт переходит в авторизованный статус.
force-authorized	Устанавливает статус авторизации порта в значение Authorized, обходя процесс аутентификации.
force-unauthorized	Устанавливает статус авторизации порта в значение Unauthorized, обходя процесс аутентификации.

no dot1x supplicant port-control

Эта команда устанавливает режим контроля порта в значение по умолчанию (автоматический).

Значение по умолчанию: auto

Формат: `no dot1x supplicant port-control`

Режим ввода команд: конфигурирование интерфейса

dot1x supplicant max-start

Данная команда настраивает количество попыток поиска аутентификатора, которые предпринимаются запрашивающим до того, как он предположит, что аутентификатора не существует.

Значение по умолчанию: 3

Формат: `dot1x supplicant max-start <1-10>`

Режим ввода команд: конфигурирование интерфейса

no dot1x supplicant max-start

Эта команда устанавливает значение количества попыток max-start в значение по умолчанию.

Формат: `no dot1x supplicant max-start`

Режим ввода команд: конфигурирование интерфейса

dot1x supplicant timeout start-period

Данная команда настраивает интервал таймера начального периода ожидания от аутентификатора запроса идентификации EAP.

Значение по умолчанию: 30 секунд

Формат: `dot1x supplicant timeout start-period <1-65535 seconds>`

Режим ввода команд: конфигурирование интерфейса

no dot1x supplicant timeout start-period

Эта команда устанавливает start-period в значение по умолчанию.

Формат: `no dot1x supplicant timeout start-period`

Режим ввода команд: конфигурирование интерфейса

dot1x supplicant timeout held-period

Эта команда настраивает интервал таймера удержания для ожидания следующей аутентификации после неудачной попытки.

Значение по умолчанию: 60 секунд

Формат: `dot1x supplicant timeout held-period <1-65535 seconds>`

Режим ввода команд: конфигурирование интерфейса

no dot1x supplicant timeout held-period

Эта команда устанавливает held-period в значение по умолчанию.

Формат: `no dot1x supplicant timeout held-period`

Режим ввода команд: конфигурирование интерфейса

dot1x supplicant timeout auth-period

Эта команда настраивает интервал таймера аутентификации для ожидания следующего EAP-запроса от аутентификатора.

Значение по умолчанию: 30 секунд

Формат: `dot1x supplicant timeout auth-period <1-65535 seconds>`

Режим ввода команд: конфигурирование интерфейса

no dot1x supplicant timeout auth-period

Эта команда устанавливает auth-period в значение по умолчанию.

Формат: `no dot1x supplicant timeout auth-period`

Режим ввода команд: конфигурирование интерфейса

dot1x supplicant user

Используйте данную команду, чтобы привязать пользователя к порту.

Формат: `dot1x supplicant user`

Режим ввода команд: конфигурирование интерфейса

show dot1x statistics

Данная команда отображает подробную статистику dot1x-порта.

Формат: `show dot1x statistics slot/port`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
EAPOL Frames Received	Отображает количество действительных EAPOL-кадров, полученных портом.
EAPOL Frames Transmitted	Отображает количество EAPOL-кадров, переданных через порт.

EAPOL Start Frames Transmitted	Отображает количество EAPOL-кадров типа Start, переданных через порт.
EAPOL Logoff Frames Received	Отображает количество EAPOL-кадров типа Log off, полученных портом.
EAP Resp/ID Frames Received	Отображает количество EAP-кадров типа Respond ID, полученных портом.
EAP Response Frames Received	Отображает количество действительных EAP-кадров типа Respond, полученных портом.
EAP Req/ID Frames Transmitted	Отображает количество EAP-кадров типа Requested ID, переданных через порт.
EAP Req Frames Transmitted	Отображает количество EAP-кадров типа Request, переданных через порт.
Invalid EAPOL Frames Received	Отображает количество нераспознанных EAPOL-кадров, полученных данным портом.
EAP Length Error Frames Received	Отображает количество EAPOL-кадров с неверной длиной содержимого пакета, полученных данным портом.
Last EAPOL Frames Version	Отображает номер версии протокола, связанного с последним полученным EAPOL-кадром.
Last EAPOL Frames Source	Отображает MAC-адрес источника, связанный с последним полученным EAPOL-кадром.

9.18 Авторизация на основе задач

Авторизация на основе задач позволяет установить пользователям разные уровни доступа (read, write, execute, debug) на уровне каждого компонента. Авторизация на основе задач использует понятие компонентов/задач для того, чтобы определить разрешенные команды для конкретного пользователя.

Пользователи назначаются в группы пользователей, которые, в свою очередь, связываются с группами задач. Каждая группа задач связывается с одним или несколькими компонентами/задачами. Данная версия поддерживает компоненты AAA, BGP и OSPF. Данная функция также поддерживается только для пользователей, которые были локально аутентифицированы через интерфейс CLI.

usergroup

Эта команда создает группу пользователей с указанным именем и входит в режим конфигурирования групп пользователей.

Формат: `usergroup` *`usergroup-name`*

Режим ввода команд: глобальная конфигурация

no usergroup

Команда удаляет группу пользователей с указанным именем.

Формат: `no usergroup` *`usergroup-name`*

Режим ввода команд: глобальная конфигурация

taskgroup

Данная команда создает группу задач с указанным именем и входит в режим конфигурирования групп задач.

Формат: `taskgroup` *`taskgroup-name`*

Режим ввода команд: глобальная конфигурация

no taskgroup

Команда удаляет группу задач с указанным именем.

Формат: `no taskgroup` *`taskgroup-name`*

Режим ввода команд: глобальная конфигурация

username usergroup

Данная команда назначает указанного пользователя в определенную группу пользователей.

Формат: `username <`*`username`*`> usergroup` *`usergroup-name`*

Режим ввода команд: глобальная конфигурация

no username usergroup

Эта команда удаляет пользователя из указанной группы пользователей.

Формат: `no usergroup` *`usergroup-name`*

Режим ввода команд: глобальная конфигурация

description (режим настройки групп пользователей)

Данная команда добавляет группе пользователей описание.

Формат: `description` *`description`*

Режим ввода команд: настройка групп пользователей

no description (режим настройки групп пользователей)

Команда удаляет описание группы пользователей.

Формат: `no description`

Режим ввода команд: настройка групп пользователей

inherit usergroup

Данная команда устанавливает родительскую группу для текущей группы пользователей. Эта группа пользователей наследует права доступа указанной родительской группы.

Формат: `inherit usergroup` *`usergroup-name`*

Режим ввода команд: настройка групп пользователей

no inherit usergroup

Команда удаляет связь текущей группы пользователей с родительской группой.

Формат: `no inherit usergroup` *`usergroup-name`*

Режим ввода команд: настройка групп пользователей

taskgroup (режим настройки групп пользователей)

Эта команда связывает группу пользователей с указанной группой задач.

Формат: `taskgroup` *`taskgroup-name`*

Режим ввода команд: настройка групп пользователей

no taskgroup (режим настройки групп пользователей)

Эта команда удаляет связь группы пользователей с группой задач.

Формат: no taskgroup *taskgroup-name*

Режим ввода команд: настройка групп пользователей

description (режим настройки групп задач)

Данная команда добавляет описание группы задач.

Формат: `description` *`description`*

Режим ввода команд: настройка групп задач

no description (режим настройки групп задач)

Команда удаляет описание группы задач.

Формат: `no description`

Режим ввода команд: настройка групп задач

inherit taskgroup

Эта команда устанавливает родительскую группу задач для текущей группы задач. Эта группа задач наследует права доступа указанной родительской группы.

Формат: `inherit taskgroup` *`taskgroup-name`*

Режим ввода команд: настройка групп задач

no inherit taskgroup

Команда удаляет связь текущей группы задач с родительской группой.

Формат: `no inherit taskgroup` *`taskgroup-name`*

Режим ввода команд: настройка групп задач

task [read] [write] [debug] [execute]

Данная команда связывает группу задач с набором разрешений для задач.

Значение по умолчанию: разрешений нет

Формат: `task [read] [write] [debug] [execute] {aaa | ospf | bgp}`

Режим ввода команд: настройка групп задач

no task {aaa | ospf | bgp}

Эта команда удаляет связи для указанной задачи.

Формат: no task {aaa | ospf | bgp}

Режим ввода команд: настройка групп задач

show aaa usergroup

Эта команда отображает список групп пользователей и их настройки.

Формат: `show aaa usergroup [usergroup-name]`

Режим ввода команд: привилегированный

show aaa taskgroup

Данная команда отображает список групп задач и их настройки.

Формат: `show aaa taskgroup [taskgroup-name]`

Режим ввода команд: привилегированный

show aaa userdb

Команда отображает список пользователей и список групп пользователей, в которых они участвуют.

Формат: `show aaa userdb [username]`

Режим ввода команд: привилегированный

9.19 Команды настройки контроля шторма

Эта часть описывает команды, используемые для настройки контроля шторма и просмотра информации о конфигурации контроля шторма. Трафик-шторм — это состояние, когда входящие пакеты переполняют LAN, что приводит к ухудшению производительности сети. Функция контроля шторма защищает сеть от этого состояния.

Система обеспечивает контроль широковещательного, многоадресного и одноадресного шторма для отдельных интерфейсов. Одноадресный контроль шторма защищает от трафика, MAC-адреса которого не знакомы системе. Для широковещательного, многоадресного и одноадресного контроля шторма трафик отбрасывается в случае, если скорость входящего трафика возрастает выше настроенного для данного типа порога.

Для настройки контроля шторма необходимо включить эту функцию для всех интерфейсов или отдельных интерфейсов и установить пороговое значение (уровень контроля шторма), при превышении которого широковещательный, многоадресный и одноадресный трафик будет отбрасываться. Функция контроля шторма позволяет ограничивать скорость указанных типов пакетов через коммутатор на основе каждого порта и каждого типа.

Выключение уровня контроля шторма (с помощью no-форм команд) устанавливает уровень контроля шторма в значение по умолчанию. Используя no-форму команды storm-control (без указания level), можно выключить форму контроля шторма, но сохранить при этом настроенный уровень (чтобы активировать в следующий раз, когда контроль шторма будет включен).

Действительная скорость входящего трафика, необходимая для активации контроля шторма, основывается на размере входящих пакетов, и для расчета скорости pps (пакет/с) используется жестко установленный средний размер пакета в 512 байт, в то время как плоскость передачи данных требует pps в отношении к абсолютной скорости в кбит/с. Например, если настроено ограничение 10 %, оно конвертируется в ~25000 pps, и этот лимит pps устанавливается на уровне передачи данных (в аппаратном обеспечении). В итоге вы получите приблизительный желаемый результат при использовании пакетов размером в 512 байт.

storm-control broadcast

Используйте данную команду, чтобы включить функцию контроля широковещательного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса). Если режим включен, контроль широковещательного шторма активирован, и когда скорость входящего широковещательного трафика второго уровня превысит настроенное пороговое значение, трафик будет отброшен. Следовательно, скорость широковещательного трафика будет ограничена в соответствии с настроенным порогом.

Значение по умолчанию: выключено

Формат: `storm-control broadcast`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control broadcast

Команда используется, чтобы выключить режим контроль широковещательного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса).

Формат: `no storm-control broadcast`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control broadcast action

Эта команда настраивает действие контроля широковещательного шторма как shutdown или trap для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса). Если настроено значение shutdown, интерфейс, получающий широковещательные пакеты со скоростью, превышающей пороговое значение, переходит в состояние errdisable. Если настроено значение trap, интерфейс отправляет трап-сообщения примерно каждые 30 секунд, пока контроль широковещательного шторма восстанавливается.

Значение по умолчанию: отсутствует

Формат: `storm-control broadcast action {shutdown | trap}`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control broadcast action

Эта команда устанавливает действие контроля широковещательного шторма в значение по умолчанию для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса).

Формат: `no storm-control broadcast action`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control broadcast level

Используйте данную команду, чтобы настроить пороговое значение скорости широковещательного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) как процент от скорости соединения и включить контроль широковещательного шторма. Если режим включен, контроль широковещательного шторма запущен, и если скорость входящего широковещательного трафика второго уровня превысит настроенное пороговое значение, трафик будет отброшен. Следовательно, скорость широковещательного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: 5

Формат: `storm-control broadcast level` *`0-100`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control broadcast level

Эта команда устанавливает порог контроля широковещательного шторма в значение по умолчанию для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса), а также выключает контроль широковещательного шторма.

Формат: `no storm-control broadcast level`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control broadcast rate

Используйте данную команду для настройки порога скорости широковещательного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) в пакетах в секунду. Если режим включен, контроль широковещательного шторма запущен, и если скорость входящего широковещательного трафика второго уровня превысит настроенное пороговое значение, трафик будет отброшен. Следовательно, скорость широковещательного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: 0

Формат: `storm-control broadcast rate` *`0-33554431`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control broadcast rate

Эта команда устанавливает порог скорости широковещательного шторма в значение по умолчанию для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса), а также выключает контроль широковещательного шторма.

Формат: `no storm-control broadcast rate`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control multicast

Данная команда включает режим контроля многоадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса). Если режим включен, контроль многоадресного шторма запущен, и если скорость входящего многоадресного трафика второго уровня превысит настроенное пороговое значение, трафик будет отброшен. Следовательно, скорость многоадресного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: выключено

Формат: `storm-control multicast`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control multicast

Данная команда выключает режим контроля многоадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса).

Формат: `no storm-control multicast`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control multicast action

Эта команда настраивает действие контроля многоадресного шторма как shutdown или trap для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса). Если настроено значение shutdown, интерфейс, получающий многоадресные пакеты со скоростью, превышающей пороговое значение, переходит в состояние errdisable. Если настроено значение trap, интерфейс отправляет трап-сообщения примерно каждые 30 секунд, пока контроль многоадресного шторма восстанавливается.

Значение по умолчанию: отсутствует

Формат: `storm-control multicast action {shutdown | trap}`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control multicast action

Эта команда устанавливает действие контроля многоадресного шторма в значение по умолчанию для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса).

Формат: `no storm-control multicast action`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control multicast level

Используйте эту команду, чтобы настроить пороговое значение скорости многоадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) как процент от скорости соединения и включить контроль многоадресного шторма. Если режим включен, контроль многоадресного шторма запущен, и если скорость входящего многоадресного трафика второго уровня превысит настроенное пороговое значение, трафик будет отброшен. Следовательно, скорость многоадресного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: 5

Формат: `storm-control multicast level` *`0-100`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control multicast level

Эта команда устанавливает порог скорости многоадресного шторма в значение по умолчанию для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса), а также выключает восстановление после многоадресного шторма.

Формат: `no storm-control multicast level` *`0-100`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control multicast rate

Используйте данную команду для настройки порога скорости многоадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) в пакетах в секунду. Если режим включен, контроль многоадресного шторма запущен, и если скорость входящего многоадресного трафика второго уровня превысит настроенное пороговое значение, трафик будет отброшен. Следовательно, скорость многоадресного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: 0

Формат: `storm-control multicast rate` *`0-33554431`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control multicast rate

Эта команда устанавливает порог скорости многоадресного шторма в значение по умолчанию для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса), а также выключает восстановление после многоадресного шторма.

Формат: `no storm-control multicast rate`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control unicast

Данная команда включает режим контроля одноадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса). Если режим включен, контроль одноадресного шторма запущен, и если скорость входящего на интерфейс неизвестного (отказ поиска пункта назначения) одноадресного трафика второго уровня превысит настроенное пороговое значение, трафик будет сброшен. Следовательно, скорость неизвестного одноадресного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: выключено

Формат: storm-control unicast

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control unicast

Данная команда выключает режим контроля одноадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса).

Формат: `no storm-control unicast`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control unicast action

Эта команда настраивает действие контроля одноадресного шторма как shutdown или trap для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса). Если настроено значение shutdown, интерфейс, получающий одноадресные пакеты со скоростью, превышающей пороговое значение, переходит в состояние errdisable. Если настроено значение trap, интерфейс отправляет трап-сообщения примерно каждые 30 секунд, пока контроль одноадресного шторма восстанавливается.

Значение по умолчанию: отсутствует

Формат: `storm-control unicast action {shutdown | trap}`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control unicast action

Эта команда устанавливает действие контроля одноадресного шторма в значение по умолчанию для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса).

Формат: `no storm-control unicast action`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control unicast level

Используйте данную команду, чтобы настроить порог скорости одноадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) как процент от скорости соединения и включить контроль одноадресного шторма. Если режим включен, контроль одноадресного шторма запущен, и если скорость входящего на интерфейс неизвестного одноадресного трафика второго уровня превысит настроенное пороговое значение, трафик будет сброшен. Следовательно, скорость неизвестного одноадресного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: 5

Формат: `storm-control unicast level` *`0-100`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control unicast level

Эта команда устанавливает порог скорости одноадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) в значение по умолчанию и выключает контроль одноадресного шторма.

Формат: `no storm-control unicast level`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

storm-control unicast rate

Используйте данную команду для настройки порога скорости одноадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) в пакетах в секунду. Если режим включен, контроль одноадресного шторма запущен, и если скорость входящего одноадресного трафика второго уровня превысит настроенное пороговое значение, трафик будет отброшен. Следовательно, скорость одноадресного трафика будет ограничена в соответствии с настроенным пороговым значением.

Значение по умолчанию: 0

Формат: `storm-control unicast rate` *`0-33554431`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no storm-control unicast rate

Эта команда устанавливает порог скорости одноадресного шторма для всех интерфейсов (режим глобальной конфигурации) или для одного или нескольких интерфейсов (режим конфигурирования интерфейса) в значение по умолчанию и выключает контроль одноадресного шторма.

Формат: `no storm-control unicast rate`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

show storm-control

Команда отображает информацию о конфигурации контроля шторма коммутатора. Если вы не используете необязательные параметры, эта команда отобразит глобальные параметры конфигурации контроля шторма.

Используйте ключевое слово all, чтобы отобразить параметры конфигурации для каждого интерфейса, или укажите *unit/slot/port*, чтобы отобразить информацию для определенного интерфейса.

Формат: `show storm-control [all | unit/slot/port]`

Режим ввода команд: привилегированный

Термин	***Значение***
Bcast Mode	Показывает, включен ли режим контроля широковещательного шторма. Заводская настройка: disabled.
Bcast Level	Уровень контроля широковещательного шторма.
Mcast Mode	Показывает, включен ли режим контроля многоадресного шторма.
Mcast Level	Уровень контроля многоадресного шторма.
Ucast Mode	Показывает, включен ли режим контроля одноадресного шторма или DLF-шторма (Destination Lookup Failure).
Ucast Level	Уровень контроля одноадресного шторма или DLF-шторма.

9.20 Команды настройки установления зависимости состояния соединений

В этой части описаны команды, используемые для настройки зависимости соединений. Зависимости соединений позволяют статусу соединения указанных портов зависеть от статуса соединения других портов. Как следствие, если порт, от которого зависят остальные порты, потеряет соединение, зависимые порты административно выключаются или административно включаются для того, чтобы соединения зависимых портов соответственно сбрасывались или восстанавливались.

no link state track

Данная команда удаляет опции зависимости соединений для выбранного идентификатора группы.

Формат: `no link state track group-id`

Режим ввода команд: глобальная конфигурация

link state group

Используйте эту команду, чтобы установить, должны ли расположенные ниже по порядку интерфейсы повторять или инвертировать статус интерфейсов, находящихся выше. Настройка по умолчанию для группы — down (т. е. все интерфейсы ниже по порядку будут повторять статус соединения выше по порядку, если все интерфейсы выше выключены). Настройка up значит, что интерфейсы, находящиеся ниже по порядку, будут работать, когда все интерфейсы выше будут выключены.

Значение по умолчанию: Down

Формат: `link state group` *`group-id`* `action {up | down}`

Режим ввода команд: глобальная конфигурация

no link state group

Используйте данную команду, чтобы установить статус соединения для группы в значение по умолчанию.

Формат: `no link state group` *`group-id`* `action`

Режим ввода команд: глобальная конфигурация

link state group downstream

Используйте эту команду, чтобы добавить интерфейсы в список интерфейсов, находящихся ниже по порядку. Добавление интерфейса в такой список перемещает интерфейс ниже по порядку, пока в группу не добавляется интерфейс выше. Статус соединения следует интерфейсу, указанному в команде upstream. Чтобы избежать выключения интерфейсов, необходимо ввести команду upstream до ввода команды downstream.

Формат: `link state group` *`group-id`* `downstream`

Режим ввода команд: конфигурирование интерфейса

no link state group downstream

Используйте данную команду, чтобы удалить выбранный интерфейс из списка интерфейсов ниже по порядку.

Формат: `no link state group` *`group-id`* `downstream`

Режим ввода команд: конфигурирование интерфейса

link state group upstream

Используйте эту команду для добавления интерфейсов в список интерфейсов, находящихся выше по порядку. Стоит отметить, что интерфейс, определенный как находящийся выше по порядку, может быть также определен как находящийся ниже в той же самой группе статуса соединения или же в другой группе статуса соединения, если одна из этих конфигураций создает круговую зависимость между группами.

Формат: `link state group` *`group-id`* `upstream`

Режим ввода команд: конфигурирование интерфейса

no link state group upstream

Команда удаляет выбранный интерфейс из списка интерфейсов выше по порядку.

Формат: `no link state group group-id upstream`

Режим ввода команд: конфигурирование интерфейса

show link state group

Используйте данную команду, чтобы отобразить состояние настроенных групп зависимых соединений или указанной группы.

Формат: `show link state group group-id`

Режим ввода команд: привилегированный

show link state group detail

Используйте данную команду для отображения подробной информации о состоянии интерфейсов выше или ниже по порядку для указанной группы зависимых соединений. Group Transitions — это счетчик событий, когда интерфейс ниже по порядку переходил в состояние action в результате изменения статуса интерфейса выше.

Формат: `show link state group group-id detail`

Режим ввода команд: привилегированный

9.21 Команды настройки LLPF

Link Local Protocol Filtering (LLPF) позволяет коммутатору фильтровать PDU проприетарных протоколов, таких как Port Aggregation Protocol (PAgP), если с проприетарными протоколами, запущенными на стандартных коммутаторах, возникают проблемы. Если PDU определенного протокола приводят к непредсказуемым результатам, LLPF может быть включен для того, чтобы коммутатор не обрабатывал PDU этого протокола.

llpf

Используйте эту команду, чтобы блокировать LLPF протокол/протоколы на порте.

Значение по умолчанию: включено для параметра blockudld; выключено для остальных.

Формат: `llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall}`

Режим ввода команд: конфигурирование интерфейса

no llpf

Команда для разблокирования LLPF протокола/протоколов на порте.

Формат: `no llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall }`

Режим ввода команд: конфигурирование интерфейса

show llpf interface

Команда для отображения статуса правил LLPF, настроенных для определенного порта или всех портов.

Формат: `show llpf interface [all | unit/slot/port]`

Режим ввода команд: привилегированный

Термин	*Значение*
Block ISDP	Показывает, блокирует ли порт PDU ISDP.
Block VTP	Показывает, блокирует ли порт PDU VTP.
Block DTP	Показывает, блокирует ли порт PDU DTP.
Block UDLD	Показывает, блокирует ли порт PDU UDLD.
Block PAGP	Показывает, блокирует ли порт PDU PAgP.
Block SSTP	Показывает, блокирует ли порт PDU SSTP.
Block All	Показывает, блокирует ли порт все проприетарные PDU, доступные для функции LLPF.

9.22 Команды настройки MVR

В этой части перечислены команды настройки Multicast VLAN Registration (MVR).

mvr

Используйте эту команду, чтобы включить MVR. По умолчанию MVR выключен.

Значение по умолчанию: выключено

Формат: `mvr`

Режим ввода команд: конфигурирование интерфейса, глобальная конфигурация

no mvr

Эта команда выключает MVR.

Формат: `no mvr`

Режим ввода команд: конфигурирование интерфейса, глобальная конфигурация

mvr group

Команда добавляет принадлежность к группе MVR.

Формат: `mvr group`

Режим ввода команд: глобальная конфигурация

no mvr group

Используйте эту команду, чтобы выключить принадлежность к группе MVR.

Формат: `no mvr group`

Режим ввода команд: глобальная конфигурация

mvr immediate

Используйте эту команду, чтобы включить режим MVR Immediate Leave. Если интерфейс настроен как порт-источник, режим MVR Immediate Leave включить нельзя. По умолчанию этот режим выключен.

Значение по умолчанию: выключено

Формат: `mvr immediate`

Режим ввода команд: конфигурирование интерфейса

no mvr immediate

Используйте эту команду, чтобы выключить режим MVR Immediate Leave.

Формат: `mvrm immediate`

Режим ввода команд: конфигурирование интерфейса

mvr mode

Команда используется, чтобы установить тип режима MVR. Тип режима по умолчанию — compatible.

Формат: `mvr mode [compatible | dynamic]`

Режим ввода команд: глобальная конфигурация

no mvr mode

Используйте эту команду, чтобы установить тип режима MVR в значение по умолчанию (compatible).

Формат: `no mvr mode`

Режим ввода команд: глобальная конфигурация

mvr querytime

Используйте данную команду, чтобы установить время отклика на MVR-запрос в десятых долях секунды. Время запроса — это максимальное время ожидания отчета об IGMP-членстве на порте принимающего устройства, прежде чем удалить порт из группы многоадресного вещания. Время запроса применяется только к принимающим портам и указывается в десятых долях секунды. Значение по умолчанию — 5.

Формат: `mvr querytime` *`1-100`*

Режим ввода команд: глобальная конфигурация

no mvr querytime

Данная команда устанавливает время отклика на запрос в значение по умолчанию.

Формат: `no mvr querytime`

Режим ввода команд: глобальная конфигурация

mvr type

Используйте данную команду, чтобы установить тип MVR-порта. По умолчанию тип порта отсутствует.

Формат: `mvr type [receiver | source]`

Режим ввода команд: конфигурирование интерфейса

no mvr type

Используйте данную команду, чтобы сбросить тип MVR-порта в значение по умолчанию.

Формат: `no mvr type`

Режим ввода команд: конфигурирование интерфейса

mvr vlan

Используйте эту команду, чтобы установить MVR VLAN.

Значение по умолчанию: 1

Формат: `mvr vlan 1-4093`

Режим ввода команд: глобальная конфигурация

no mvr vlan

Команда устанавливает MVR VLAN в значение по умолчанию.

Формат: `no mvr vlan`

Режим ввода команд: глобальная конфигурация

mvr vlan group

Используйте эту команду, чтобы добавить порт в определенную MVR-группу. Значение по умолчанию отсутствует.

Формат: `mvr vlan mvlan group A.B.C.D.`

Режим ввода команд: конфигурирование интерфейса

no mvr vlan group

Команда удаляет порт из определенной MVR-группы.

Формат: `no mvr vlan mvlan group A.B.C.D.`

Режим ввода команд: конфигурирование интерфейса

show mvr

Команда для отображения глобальных настроек MVR.

Формат: `show mvr`

Режим ввода команд: привилегированный

show mvr members

Используйте эту команду, чтобы отобразить распределенные MVR-группы.

Формат: `show mvr members [A.B.C.D.]`

Режим ввода команд: привилегированный

show mvr interface

Данная команда отображает конфигурацию интерфейсов с включенным MVR.

Формат: `show mvr interface [interface-id [members [vlan vlan-id]]]`

Режим ввода команд: привилегированный

show mvr traffic

Используйте эту команду, чтобы отобразить глобальную статистику MVR.

Формат: `show mvr traffic`

Режим ввода команд: привилегированный

debug mvr trace

Команда для включения трассировки отладки MVR. Значение по умолчанию — выключено.

Формат: `debug mvr trace`

Режим ввода команд: привилегированный

no debug mvr trace

Используйте эту команду, чтобы выключить трассировку отладки MVR.

Формат: `no debug mvr trace`

Режим ввода команд: привилегированный

debug mvr packet

Используйте эту команду, чтобы включить трассировку отладки приема/передачи MVR-пакетов. Если команда выполняется без указания аргументов, включается отладка пакетов и приема, и передачи. Значение по умолчанию — включено.

Формат: `debug mvr packet [receive | transmit]`

Режим ввода команд: привилегированный

no debug mvr packet

Используйте эту команду, чтобы выключить трассировку отладки приема/передачи MVR-пакетов.

Формат: `no debug mvr packet [receive | transmit]`

Режим ввода команд: привилегированный

9.23 Команды настройки агрегированного интерфейса (802.3ad)

Данная часть описывает команды для настройки агрегированных интерфейсов, или link aggregation group (LAG), определение которых дается в спецификации 802.3ad. Агрегация интерфейсов позволяет совмещать несколько полнодуплексных соединений Ethernet в одно логическое соединение. Устройства сети воспринимают LAG как одиночное соединение, что повышает отказоустойчивость и обеспечивает распределение нагрузки. Функция LAG первоначально загружает общий трафик на основании MAC-адреса источника и места назначения. После создания канала агрегированного интерфейса необходимо назначить канал порта (LAG) участником VLAN. Если этого не сделать, канал порта может стать участником управляющей VLAN, что может привести к проблемам при определении и коммутации.

LAG-интерфейс может быть статичным или динамичным. Все участники LAG-интерфейса должны использовать одинаковые протоколы. Статичный LAG-интерфейс не требует от партнерской системы возможности объединить свои порты.

Если настроить максимальное количество LAG-интерфейсов для данной платформы, настраиваемые дополнительные порт-каналы автоматически будут статичными.

port-channel

Данная команда настраивает новый агрегированный интерфейс и генерирует для него логический номер *unit/slot/port*. Поле name field является строкой и может состоять из буквенных символов и тире. Используйте команду show port channel для отображения значения *unit/slot/port* для логического интерфейса. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Перед тем, как добавлять порт в агрегированный интерфейс, необходимо установить его в физический режим. Подробнее см. в описании команды speed на странице 307.

Формат: `port-channel` *`name`*

Режим ввода команд: глобальная конфигурация

addport

Эта команда добавляет один порт к агрегированному интерфейсу. Первый интерфейс — это логический номер *unit/slot/port* настроенного агрегированного интерфейса. Можно добавить диапазон портов, указав диапазон портов при входе в режим конфигурирования интерфейса, например interface 1/0/1-1/0/4. Вместо параметра unit/slot/port можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение lag-intf-num должно указывать номер порта LAG.

Если настроить максимальное количество LAG-интерфейсов для данной платформы, настраиваемые дополнительные порт-каналы автоматически будут статичными.

Формат: `addport` *`logical unit/slot/port`*

Режим ввода команд: конфигурирование интерфейса

deleteport (режим конфигурирования интерфейса)

Эта команда удаляет порт или диапазон портов из агрегированного интерфейса. Интерфейс — это логический номер *unit/slot/port* настроенного агрегированного интерфейса (или диапазона LAG). Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `deleteport` *`logical unit/slot/port`*

Режим ввода команд: конфигурирование интерфейса

deleteport (Global Config)

Эта команда удаляет все настроенные порты из LAG-интерфейса. Интерфейс — это логический номер *unit/slot/port* настроенного агрегированного интерфейса. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `deleteport {logical unit/slot/port | all}`

Режим ввода команд: глобальная конфигурация

lacp admin key

Команда настраивает административное значение ключа для агрегированного интерфейса. Диапазон значений key — от 0 до 65535. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Значение по умолчанию: 0x8000

Формат: `lacp admin key key`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на агрегированных интерфейсах.

no lacp admin key

Используйте эту команду, чтобы установить административное значение ключа для агрегированного интерфейса в значение по умолчанию.

Формат: `no lacp admin key`

Режим ввода команд: конфигурирование интерфейса

lacp collector max-delay

Команда позволяет настроить максимальную задержку коллектора агрегированного интерфейса. Эта команда может использоваться для настройки одного интерфейса или диапазона интерфейсов. Диапазон действительных значений параметра delay — от 0 до 65535.

Значение по умолчанию: 0x8000

Формат: `lacp collector max delay delay`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на агрегированных интерфейсах.

no lacp collector max delay

Используйте эту команду, чтобы установить максимальную задержку коллектора агрегированного интерфейса в значение по умолчанию.

Формат: `no lacp collector max delay`

Режим ввода команд: конфигурирование интерфейса

lacp actor admin key

Используйте данную команду, чтобы настроить административное значение ключа-исполнителя LACP на интерфейсе или диапазоне интерфейсов. Диапазон значения key — от 0 до 65535.

Значение по умолчанию: внутренний номер интерфейса данного физического порта.

Формат: `lacp actor admin key key`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на агрегированных интерфейсах.

no lacp actor admin key

Команда устанавливает административное значение ключа в значение по умолчанию.

Формат: `no lacp actor admin key`

Режим ввода команд: конфигурирование интерфейса

lacp actor admin state individual

Используйте эту команду, чтобы установить административный статус исполнителя LACP как individual.

Формат: `lacp actor admin state individual`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp actor admin state individual

Используйте эту команду, чтобы установить административный статус исполнителя LACP как aggregation.

Формат: `no lacp actor admin state individual`
Режим ввода команд: конфигурирование интерфейса

lacp actor admin state longtimeout

Данная команда устанавливает административный статус исполнителя LACP как longtimeout.

Формат: `lacp actor admin state longtimeout`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp actor admin state longtimeout

Используйте эту команду, чтобы установить административный статус исполнителя LACP как shorttimeout.

Формат: `no lacp actor admin state longtimeout`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

lacp actor admin state passive

Команда устанавливает административный статус исполнителя LACP как passive.

Формат: `lacp actor admin state passive`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp actor admin state passive

Используйте эту команду, чтобы установить административный статус исполнителя LACP как активный.

Формат: `no lacp actor admin state passive`

Режим ввода команд: конфигурирование интерфейса

lacp actor admin state

Используйте данную команду, чтобы настроить административное значение статуса исполнителя в соответствии с исполнителем в LACPDU. Команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Значение по умолчанию: 0x07

Формат: `lacp actor admin state {individual|longtimeout|passive}`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp actor admin state

Используйте эту команду, чтобы вернуть установку административного значения статуса исполнителя в соответствии с исполнителем в LACPDU в значение по умолчанию.

Обе команды (no port lacptimeout и no lacp actor admin state) возвращают значения по умолчанию, независимо от того, какая команда использовалась для настройки порта. Как следствие, обе эти команды отображаются в выводе команды show running-config.

Формат: `no lacp actor admin state {individual|longtimeout|passive}`

Режим ввода команд: конфигурирование интерфейса

lacp actor port priority

Используйте эту команду, чтобы настроить значение приоритета, назначенного агрегированному порту, для интерфейса или диапазона интерфейсов. Диапазон значений *priority* — от 0 до 65535.

Значение по умолчанию: 0x80

Формат: `lacp actor port priority` *`0-65535`*

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp actor port priority

Команда устанавливает значение приоритета, назначенного агрегированному порту, в значение по умолчанию.

Формат: `no lacp actor port priority`

Режим ввода команд: конфигурирование интерфейса

lacp partner admin key

Используйте эту команду, чтобы установить административное значение ключа для партнера по протоколу. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов. Диапазон значения *key* — от 0 до 65535.

Значение по умолчанию: 0x0

Формат: `lacp partner admin key` *key*

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner admin key

Команда устанавливает административное значение ключа для партнера по протоколу в значение по умолчанию.

Формат: `no lacp partner admin key`

Режим ввода команд: конфигурирование интерфейса

lacp partner admin state individual

Используйте эту команду, чтобы установить административный статус LACP-партнера как individual.

Формат: `lacp partner admin state individual`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner admin state individual

Используйте эту команду, чтобы установить административный статус LACP-партнера как aggregation.

Формат: `no lacp partner admin state individual`

Режим ввода команд: конфигурирование интерфейса

lacp partner admin state longtimeout

Команда устанавливает административный статус LACP-партнера как longtimeout.

Формат: `lacp partner admin state longtimeout`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner admin state longtimeout

Используйте эту команду, чтобы установить административный статус LACP-партнера как shorttimeout.

Формат: `no lacp partner admin state longtimeout`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

lacp partner admin state passive

Используйте эту команду, чтобы установить административный статус LACP-партнера как passive.

Формат: `lacp partner admin state passive`

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner admin state passive

Используйте эту команду, чтобы установить административный статус LACP-партнера как active.

Формат: `no lacp partner admin state passive`

Режим ввода команд: конфигурирование интерфейса

lacp partner port id

Используйте эту команду, чтобы настроить идентификатор порта LACP-партнера. Команда может использоваться для настройки одного интерфейса или диапазона интерфейсов. Диапазон значения port-id — от 0 до 65535.

Значение по умолчанию: 0x80

Формат: `lacp partner port-id` *`port-id`*

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner port id

Используйте эту команду, чтобы установить идентификатор порта LACP-партнера в значение по умолчанию.

Формат: `no lacp partner port-id`

Режим ввода команд: конфигурирование интерфейса

lacp partner port priority

Используйте эту команду, чтобы настроить приоритет порта-партнера LACP. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов. Диапазон значений priority — от 0 до 65535.

Значение по умолчанию: 0x0

Формат: `lacp partner port priority` *`priority`*

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner port priority

Команда устанавливает приоритет порта-партнера LACP в значение по умолчанию.

Формат: `no lacp partner port priority`

Режим ввода команд: конфигурирование интерфейса

lacp partner system-id

Используйте эту команду, чтобы настроить шестиоктетное значение MAC-адреса, обозначающее административное значение идентификатора партнерской системы протокола агрегированного порта. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов. Диапазон значения system-id — от 00:00:00:00:00:00 до FF:FF:FF:FF:FF.

Значение по умолчанию: 00:00:00:00:00:00

Формат: `lacp partner system-id` *`system-id`*

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner system-id

Используйте эту команду, чтобы установить административное значение идентификатора партнерской системы протокола агрегированного порта в значение по умолчанию.

Формат: `no lacp partner system-id`

Режим ввода команд: конфигурирование интерфейса

lacp partner system priority

Команда настраивает административное значение приоритета, связанное с идентификатором партнерской системы. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов. Диапазон значений priority — от 0 до 65535.

Значение по умолчанию: 0x0

Формат: `lacp partner system priority` *`0-65535`*

Режим ввода команд: конфигурирование интерфейса

Данная команда применима только на физических интерфейсах.

no lacp partner system priority

Команда настраивает административное значение приоритета, связанное с идентификатором партнерской системы, в значение по умолчанию.

Формат: `no lacp partner system priority`

Режим ввода команд: конфигурирование интерфейса

interface lag

Используйте данную команду, чтобы войти в режим конфигурирования интерфейса для указанного LAG.

Формат: `interface lag` *`lag-interface-number`*

Режим ввода команд: глобальная конфигурация

port-channel static

Данная команда включает статичный режим на LAG-интерфейсе или диапазоне интерфейсов. По умолчанию статичный режим для нового LAG-интерфейса включен, что означает, что агрегированный интерфейс является статичным. Если максимальное количество разрешенных динамических агрегированных интерфейсов уже присутствует в системе, статичный режим для нового агрегированного интерфейса будет включен, а значит, он будет статичным. Эта команда используется только на агрегированных интерфейсах.

Значение по умолчанию: включено

Формат: `port-channel static`

Режим ввода команд: конфигурирование интерфейса

no port-channel static

Эта команда устанавливает статичный режим на определенном LAG-интерфейсе в значение по умолчанию. Команда может использоваться только на агрегированных интерфейсах.

Формат: `no port-channel static`

Режим ввода команд: конфигурирование интерфейса

port lacpmode

Данная команда включает Link Aggregation Control Protocol (LACP) на порте или диапазоне портов.

Значение по умолчанию: включено

Формат: `port lacpmode`

Режим ввода команд: конфигурирование интерфейса

no port lacpmode

Команда выключает Link Aggregation Control Protocol (LACP) на порте.

Формат: `no port lacpmode`

Режим ввода команд: конфигурирование интерфейса

port lacpmode enable all

Данная команда включает Link Aggregation Control Protocol (LACP) на всех портах.

Формат: `port lacpmode enable all`

Режим ввода команд: глобальная конфигурация

no port lacpmode enable all

Команда выключает Link Aggregation Control Protocol (LACP) на всех портах.

Формат: `no port lacpmode enable all`

Режим ввода команд: глобальная конфигурация

port lacptimeout (Interface Config)

Данная команда устанавливает время жизни записи на физическом интерфейсе или диапазоне интерфейсов определенного типа устройств (исполнителя или партнера) в длинное или короткое значение.

Значение по умолчанию: long

Формат: `port lacptimeout {actor | partner} {long | short}`

Режим ввода команд: конфигурирование интерфейса

no port lacptimeout

Команда устанавливает время жизни записи на физическом интерфейсе или диапазоне интерфейсов определенного типа устройств (исполнителя или партнера) в значение по умолчанию.

Формат: `no port lacptimeout {actor | partner}`

Режим ввода команд: конфигурирование интерфейса

Обе команды (no port lacptimeout и no lacp actor admin state) возвращают значения по умолчанию, независимо от того, какая команда использовалась для настройки порта. Как следствие, обе эти команды отображаются в выводе команды show running-config.

port lacptimeout (Global Config)

Данная команда устанавливает время жизни записи для всех интерфейсов определенного типа устройств (исполнителя или партнера) в длинное или короткое значение.

Значение по умолчанию: long

Формат: `port lacptimeout {actor | partner} {long | short}`

Режим ввода команд: глобальная конфигурация

no port lacptimeout

Команда устанавливает время жизни записи для всех физических интерфейсов определенного типа устройств (исполнителя или партнера) в значение по умолчанию.

Формат: `no port lacptimeout {actor | partner}`

Режим ввода команд: глобальная конфигурация

Обе команды (no port lacptimeout и no lacp actor admin state) возвращают значения по умолчанию, независимо от того, какая команда использовалась для настройки порта. Как следствие, обе эти команды отображаются в выводе команды show running-config.

port-channel adminmode

Эта команда включает все настроенные агрегированные интерфейсы с одинаковыми установками административного режима.

Формат: `port-channel adminmode all`

Режим ввода команд: глобальная конфигурация

no port-channel adminmode

Команда выключает все настроенные агрегированные интерфейсы с одинаковыми установками административного режима.

Формат: `no port-channel adminmode all`

Режим ввода команд: глобальная конфигурация

port-channel linktrap

Эта команда включает уведомления о трапах соединений для LAG-интерфейса. Параметр interface — это логическое значение *unit/slot/port* для настроенного агрегированного интерфейса. Опция *all* настраивает все настроенные LAG-интерфейсы с одинаковыми параметрами административного режима. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Значение по умолчанию: включено

Формат: `port-channel linktrap {`*`logical unit/slot/port`*` | all}`

Режим ввода команд: глобальная конфигурация

no port-channel linktrap

Команда выключает уведомления о трапах соединений для LAG-интерфейса. Параметр interface — это логическое значение *unit/slot/port* для настроенного агрегированного интерфейса. Опция all настраивает все настроенные LAG-интерфейсы с одинаковыми параметрами административного режима.

Формат: `no port-channel linktrap {`*`logical unit/slot/port`*` | all}`

Режим ввода команд: глобальная конфигурация

port-channel load-balance

Эта команда выбирает опцию балансировки нагрузки для агрегированного интерфейса. Трафик балансируется на агрегированном интерфейсе путем выбора одного из соединений интерфейса, через который будут передаваться определенные пакеты. Физический интерфейс выбирается с помощью создания двоичного шаблона из выбранных полей пакета и связывания этого шаблона с определенным физическим интерфейсом.

Данная команда может выполняться на одном интерфейсе, диапазоне интерфейсов или на всех интерфейсах. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как

альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Значение по умолчанию: 3

Формат: `port-channel load-balance { dst-ip | dst-mac | enhanced | src-dst-ip | src-dst-mac | src-ip | src-mac } {`*`unit/slot/port`* `| all}`

Режим ввода команд: конфигурирование интерфейса глобальная конфигурация

Термин	***Значение***
src-mac	MAC-адрес источника, VLAN, EtherType и входящий порт, связанные с пакетом.
dst-mac	MAC-адрес места назначения, VLAN, EtherType и входящий порт, связанные с пакетом.
src-dst-mac	MAC-адрес источника/места назначения, VLAN, EtherType и входящий порт, связанные с пакетом.
src-ip	IP-адрес источника и TCP/UDP-порт источника.
dst-ip	IP-адрес места назначения и TCP/UDP-порт места назначения.
src-dst-ip	IP-адреса источника/места назначения и TCP/UDP-порты источника/места назначения.
enhanced	Режим расширенного хеширования.
unit/slot/port| all	Только в режиме глобальной конфигурации. Интерфейс — это логический номер *unit/slot/port* настроенного агрегированного интерфейса. *All* применяет команду ко всем настроенным на данный момент агрегированным интерфейсам.

no port-channel load-balance

Данная команда возвращает конфигурацию балансировки нагрузки в значение по умолчанию.

Формат: `no port-channel load-balance {`*`unit/slot/port`* `| all}`

Режим ввода команд: конфигурирование интерфейса глобальная конфигурация

Термин	***Значение***
unit/slot/ port| all	Только в режиме глобальной конфигурации. Интерфейс — это логический номер *unit/slot/port* настроенного агрегированного интерфейса. *All* применяет команду ко всем настроенным на данный момент агрегированным интерфейсам.

port-channel local-preference

Данная команда включает режим локального предпочтения для LAG-интерфейса или диапазона интерфейсов. По умолчанию режим локального предпочтения для агрегированного интерфейса выключен. Команда может использоваться только на LAG-интерфейсах.

Значение по умолчанию: выключено

Формат: `port-channel local-preference`

Режим ввода команд: конфигурирование интерфейса

no port-channel local-preference

Команда выключает режим локального предпочтения на канале порта.

Формат: `no port-channel local-preference`

Режим ввода команд: конфигурирование интерфейса

port-channel min-links

Данная команда настраивает минимальные число физических интерфейсов для LAG-интерфейса.

Значение по умолчанию: 1

Формат: `port-channel min-links` *`1-8`*

Режим ввода команд: конфигурирование интерфейса

port-channel name

Команда задает имя для агрегированного интерфейса. Параметр interface — это логическое значение *unit/slot/port* для настроенного агрегированного интерфейса, а name — это строка, содержащая до 15 буквенно-цифровых символов. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `port-channel name {`*`logical unit/slot/port`*`}` *`name`*

Режим ввода команд: глобальная конфигурация

port-channel system priority

Используйте данную команду, чтобы настроить системный приоритет агрегированного интерфейса. Диапазон значений priority — от 0 до 65535.

Значение по умолчанию: 0x8000

Формат: `port-channel system priority` *`priority`*

Режим ввода команд: глобальная конфигурация

no port-channel system priority

Используйте данную команду, чтобы установить системный приоритет агрегированного интерфейса в значение по умолчанию.

Формат: `no port-channel system priority`

Режим ввода команд: глобальная конфигурация

show hashdest

Команда определяет, как пакеты будут направляться через LAG или на ближайшее устройство, если местом назначения является ECMP. С помощью метода агрегации соединений, входящего физического порта и значений различных полей пакетов эта команда определяет исходящий физический порт в пределах LAG или ECMP для пакета.

Формат: `show hashdest {lag` *`lag-id`* `|` `ecmp` *`prefix/prefix-length`*`} in_port` *`unit/slot/port`* `src-mac` *`macaddr`* `dst-mac` *`macaddr`* `[vlan` *`vlan-id`*`] ethertype` *`0xXXXX`* `[src-ip {`*`ipv4-addr`* `|` *`ipv6- addr`*`} dst-ip`

{*ipv4-addr* | *ipv6-addr*} protocol *pid* src-l4-port *port-num* dst-l4-port *port-num*]

Режим ввода команд: привилегированный

Термин	***Значение***
lag	Группа LAG, для которой рассчитывается исходящий физический порт.
ecmp	IP-адрес EMC-группы, для которой рассчитывается исходящий физический порт.
in_port	Входящий физический порт для системы.
src-mac	MAC-адрес источника.
dst-mac	MAC-адрес места назначения.
vlan	Идентификатор VLAN для пакетов с тегами VLAN. Для пакетов, не относящихся к тегированным VLAN, параметр не используется или равен нулю.
ethertype	16-битное значение EtherType в формате 0xXXXX. Для пакетов 3 уровня прогноз хеширования доступен только для IPv4 (0x0800) и IPv6 (0x86DD).
src-ip	IP-адрес источника, вводимый в формате x.x.x.x для IPv4-пакетов и в формате x:x:x:x:x:x:x:x для IPv6-пакетов.
dst-ip	IP-адрес места назначения, вводимый в формате x.x.x.x для IPv4 и в формате x:x:x:x:x:x:x:x для IPv6-пакетов.
protocol	Идентификатор протокола.
src-l4-port	Порт-источник 4 уровня.
dst-l4-port	Порт места назначения 4 уровня.

show lacp actor

Используйте эту команду, чтобы отобразить атрибуты исполнителя LACP. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: show lacp actor {*unit/slot/port*|all}

Режим ввода команд: глобальная конфигурация

Отображаться будут следующие выходные параметры.

Термин	***Значение***
System Priority	Административное значение ключа.
Actor Admin Key	Административное значение ключа.
Port Priority	Значение приоритета, назначенное агрегированному порту.
Admin State	Административные значения статуса исполнителя в соответствии с тем, что было передано исполнителем в LACPDU.

show lacp partner

Используйте эту команду, чтобы отобразить атрибуты LACP-партнера. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: show lacp actor {*unit/slot/port*|all}

Режим ввода команд: привилегированный

Отображаться будут следующие выходные параметры.

Термин	*Значение*
System Priority	Административное значение приоритета, связанного с идентификатором партнерской системы.
System ID	Отображает административное значение идентификатора системы партнёра.
Admin Key	Административное значение ключа для партнера по протоколу.
Port Priority	Административное значение ключа для партнера по протоколу.
Port-ID	Административное значение номера порта для партнера по протоколу.
Admin State	Административные значения статуса исполнителя для партнера по протоколу.

show port-channel brief

Данная команда отображает статичную пропускную способность всех LAG-интерфейсов устройства, а также сводную информацию по отдельным LAG-интерфейсам. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `show port-channel brief`

Режим ввода команд: пользовательский

Для каждого LAG-интерфейса отображается следующая информация:

Термин	*Значение*
Logical Interface	unit/slot/port логического интерфейса.
Port-channel Name	Имя LAG-интерфейса.
Link-State	Показывает, создано или разорвано соединение.
Trap Flag	Показывает, включены ли флаги трапов.
Type	Показывает, является агрегированный интерфейс статичным или динамическим.
Mbr Ports	Участники данного агрегированного интерфейса.
Active Ports	Порты, участвующие в агрегированном интерфейсе на данный момент.

show port-channel

Данная команда отображает обзор всех агрегированных интерфейсов на коммутаторе. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `show port-channel`

Режим ввода команд: привилегированный

Термин	*Значение*
Logical Interface	Действительный номер unit/slot/port.

Port-Channel Name	Имя данного LAG-интерфейса. Строка длиной до 15 буквенно-цифровых символов.
Link State	Показывает, создано или разорвано соединение.
Admin Mode	Возможные значения: enabled или disabled. В качестве заводской настройки используется enabled (включено).
Type	Показывает, является агрегированный интерфейс статичным или динамическим. • **Static** — агрегированный интерфейс является статичным. • **Dynamic** — агрегированный интерфейс является динамическим.
Load Balance Option	Опция балансировки нагрузки, связанная с данным LAG. См. команду port-channel load-balance.
Local Preference	Показывает, включен ли режим локального предпочтения.
Mode	Список портов-участников данного агрегированного интерфейса, в формате *unit/slot/port*.
Mbr Ports	Одному агрегированному интерфейсу может быть назначено до 8 портов.
Device Timeout	Перечисляет время жизни записи (**long** или **short**) каждого типа устройства (**actor** или **partner**) для каждого порта.
Port Speed	Скорость агрегированного интерфейса.
Active Ports	Это поле перечисляет порты, участвующие в агрегированном интерфейсе на данный момент.

show port-channel system priority

Используйте данную команду, чтобы отобразить системный приоритет агрегированного интерфейса.

Формат: `show port-channel system priority`

Режим ввода команд: привилегированный

show port-channel counters

Используйте данную команду, чтобы отобразить счетчики агрегированного интерфейса для указанного порта.

Формат: `show port-channel` *`unit/slot/port`* `counters`

Режим ввода команд: привилегированный

Термин	***Значение***
Local Interface	Действительный номер slot/port.
Channel Name	Имя данного LAG-интерфейса.
Link State	Показывает, создано или разорвано соединение.
Admin Mode	Возможные значения: enabled или disabled. В качестве заводской настройки используется enabled (включено).
Port Channel Flap Count	Количество случаев неактивности агрегированного интерфейса.
Mbr Ports	Значение slot/port для порта-участника.
Mbr Flap Counters	Количество случаев неактивности порта-участника из-за отсутствующего соединения или из-за выключенного административного режима.

clear port-channel counters

Используйте данную команду, чтобы очистить и сбросить счетчики ошибок соединения для указанного агрегированного интерфейса и его участников.

Формат: `clear port-channel {lag-intf-num | unit/slot/port} counters`

Режим ввода команд: привилегированный

clear port-channel all counters

Используйте данную команду, чтобы очистить и сбросить все счетчики ошибок соединения для указанного агрегированного интерфейса и его участников для определенного интерфейса.

Формат: `clear port-channel all counters`

Режим ввода команд: привилегированный

9.24 Команды настройки протокола VPC

VPC (также известный как MLAG) позволяет создавать LAG через два независимых коммутатора таким образом, чтобы некоторые порты-участники VPC могли находиться на одном коммутаторе, а другие участники — на другом. Партнерское устройство на удаленной стороне может не знать про VPC. Такое устройство будет принимать VPC за отдельный LAG-интерфейс, соединенный с одним коммутатором.

vpc domain

Используйте данную команду, чтобы войти в режим конфигурирования VPC и создать домен VPC с указанным domain-id. Только один домен VPC может быть создан на одном устройстве. Значение domain-id домена VPC должен равняться тому, что настроено на соседнем устройстве VPC, с которым данное устройство планирует образовать общий VPC. Обмен настроенными domain-id для VPC происходит во время распределения ролей, и если их настройки соседних устройств отличаются, VPC не начнет функционировать.

Администратор должен убедиться, что ни одна пара доменов VPC не занимает одно и тот же значение domain-id VPC. Идентификатор домена используется для вывода автоматически сгенерированного VPC MAC-адреса, который используется в поле идентификатора исполнителя в LACP PDU и STP BPDU при отправке на интерфейсы VPC. Если два домена VPC имеют одинаковый domain-id, это приведет к одинаковому значению поля идентификатора исполнителя и к последующим проблемам конвергенции LACP и STP.

Диапазон значений domain-id — от 1 до 255.

Формат: `vpc domain` *`domain-id`*

Режим ввода команд: глобальная конфигурация

no vpc domain

Используйте данную команду для удаления VPC-домена, выключения peer-keepalive и peer-detection и сбрасывания настроенных параметров (приоритет роли, MAC-адрес VPC, системный приоритет VPC) для VPC-домена.

Формат: `no vpc domain` *`domain-id`*

Режим ввода команд: глобальная конфигурация

feature vpc

Эта команда включает VPC глобально. Распределение ролей VPC происходит, когда и VPC и механизм статуса keepalive включены (см. команду peer-keepalive timeout на стр. 606). Чтобы произошло распределение ролей, также должно быть настроено одноранговое соединение.

Формат: `feature vpc`

Режим ввода команд: глобальная конфигурация

no feature vpc

Данная команда выключает VPC.

Формат: `no feature vpc`

Режим ввода команд: глобальная конфигурация

vpc isolate-orphans

Запрещает прохождение трафика между хостами, подключенными в интерфейсы разных устройств VPC-пары. При этом, данные интерфейсы не должны являться участниками VPC.

Значение по умолчанию: включено

Формат: `vpc isolate-orphans`

Режим ввода команд: глобальная конфигурация

no vpc isolate-orphans

Разрешает прохождение трафика между хостами, подключенными в интерфейсы разных устройств VPC-пары. При этом, данные интерфейсы не должны являться участниками VPC.

Формат: `no vpc isolate-orphans`

Режим ввода команд: глобальная конфигурация

vpc arp-synchronize

Данная команда включает синхронизацию ARP-таблиц между коммутаторами VPC-пары. После включения происходит синхронизация только вновь изученных ARP-записей.

Значение по умолчанию: выключено

Формат: `vpc arp-synchronize`

Режим ввода команд: глобальная конфигурация

no vpc arp-synchronize

Данная команда выключает синхронизацию ARP-таблиц между коммутаторами VPC-пары.

Формат: `no vpc arp-synchronize`

Режим ввода команд: глобальная конфигурация

peer detection enable

Эта команда запускает Dual control plane detection protocol (DCPDP) на VPC-коммутаторе. Чтобы DCPDP запустился на VPC-коммутаторе, там должен быть настроен IP-адрес соседнего устройства.

Значение по умолчанию: отсутствует

Формат: `peer detection enable`

Режим ввода команд: конфигурирование VPC

no peer detection enable

Эта команда выключает DCPDP на VPC-коммутаторе.

Формат: `no peer detection enable`

Режим ввода команд: конфигурирование VPC

peer detection interval

Используйте данную команду, чтобы настроить интервал передачи и время жизни записи для приема DCPDP.

Настраиваемый диапазон интервала передачи — от 200 до 4000 миллисекунд. Настраиваемый диапазон времени жизни записи для приема — от 700 до 14 000 миллисекунд. По умолчанию интервал передачи равен 1000 миллисекунд; время жизни записи для приема — 3500 миллисекунд.

Значение по умолчанию: Интервал передачи: 1000 мс
Время жизни записи для приема: 3500 мс

Формат: `peer detection interval` *`msecs`* `timeout` *`seconds`*

Режим ввода команд: конфигурирование VPC

no peer detection interval

Используйте данную команду, чтобы установить интервал передачи и время жизни записи для приема DCPDP в значения по умолчанию.

Формат: `no peer detection interval` *`msecs`* `timeout` *`seconds`*

Режим ввода команд: конфигурирование VPC

peer-keepalive destination

Эта команда настраивает IP-адрес соседнего VPC-коммутатора, который является IP-адресом места назначения DCPDP на соседнем VPC-коммутаторе. Эта конфигурация используется только протоколом DCPDP на VPC-коммутаторах. Команда также настраивает IP-адрес источника DCPDP-сообщения, который является IP самого VPC-коммутатора. UDP-порт, через который VPC-коммутатор получает DCPDP-сообщения, может быть также настроен с помощью этой команды.

Настраиваемый диапазон UDP-порта — от 1 до 65535 (по умолчанию — 60000).

Формат: `peer-keepalive destination` *`ipaddress`* `switch` *`ipaddress`* `[udp-port` *`port`*`]`

Режим ввода команд: конфигурирование VPC

no peer-keepalive destination

Команда сбрасывает настройки IP-адреса устройства, IP-адреса соседнего устройства и UDP-порта.

Формат: `no peer-keepalive destination` *`ipaddress`* `switch` *`ipaddress`* `[udp-port` *`port`*`]`

Режим ввода команд: конфигурирование VPC

peer-keepalive enable

Эта команда запускает keepalive-механизм на VPC-устройстве, если VPC глобально включен.

Значение по умолчанию: выключено

Формат: `peer-keepalive enable`

Режим ввода команд: конфигурирование VPC

no peer-keepalive enable

Эта команда останавливает keepalive-механизм на VPC-коммутаторе.

Формат: `no peer-keepalive enable`

Режим ввода команд: конфигурирование VPC

peer-keepalive timeout

Эта команда настраивает время жизни механизма поддержки активности (в секундах). Если VPC-коммутатор не получает сообщения поддержки активности от соседнего парного устройства за указанное время, он передает свою роль (если требуется).

Механизм поддержки активности не перезапускается, если keepalive timeout был изменен после назначения роли.

Настраиваемый диапазон — от 2 до 15 секунд. Значение по умолчанию — 5 секунд.

Формат: `peer-keepalive timeout` *`value`*

Режим ввода команд: конфигурирование VPC

no peer-keepalive timeout

Эта команда устанавливает значение время жизни механизма поддержки активности в значение 5 секунд.

Формат: `no keepalive timeout`

Режим ввода команд: конфигурирование VPC

role priority

Эта команда настраивает приоритет VPC-коммутатора. Значение приоритета используется для выбора роли VPC. Значение приоритета посылается партнеру в VPC-сообщениях поддержки активности. VPC-коммутатор с более низким приоритетом становится первичным, а коммутатор с более высоким приоритетом становится вторичным. Если оба партнерских VPC-коммутатора имеют одинаковый приоритет роли, первичным становится устройство с более низким системным MAC-адресом.

Механизм поддержки активности не перезапускается, если role priority был изменен после назначения роли.

Приоритет может находиться в диапазоне от 1 до 255.

Значение по умолчанию: 100.

Формат: `role priority` *`value`*

Режим ввода команд: конфигурирование VPC

no role priority

Эта команда устанавливает значение приоритета VPC-коммутатора время жизни механизма поддержки активности в значение 100 .

Формат: `no role priority`

Режим ввода команд: конфигурирование VPC

system-mac

Используйте эту команду, чтобы настроить MAC-адрес VPC-домена вручную. MAC-адрес VPC должен быть настроен одинаково на обоих партнерских устройствах. Указанный MAC-адрес должен быть MAC-адресом одноадресной передачи в формате <aa:bb:cc:dd:ee:ff> и не может равняться MAC-адресу первичного или вторичного устройства VPC. Настроенные MAC-адреса VPC передаются во время выбора ролей, и если они настроены по-разному на партнерских устройствах, VPC не начнет работать.

mac-address используется в LACP PDU и STP BPDU, отправляемых к портам-участникам VPC, если выбор первичного устройства VPC происходит после того, как MAC-адрес был настроен. Если MAC-адрес VPC настраивается после выбора первичного устройства VPC, операционный MAC-адрес VPC используется в LACP PDU и STP BPDU вместо настроенного MAC-адреса VPC.

Формат: `system-mac` *`mac-address`*

Режим ввода команд: VPC Domain

no system-mac

Эта команда сбрасывает настроенный вручную MAC-адрес для VPC-домена.

Формат: `no system-mac`

Режим ввода команд: домен VPC

system-priority

Используйте эту команду, чтобы вручную настроить системный приоритет для VPC-домена. Параметр *system-priority* должен быть настроен одинаково на обоих партнерских VPC-устройствах. Если системный приоритет VPC настроен по-разному на партнерских устройствах, VPC не будет работать.

system-priority используется в LACP PDU и STP BPDU, отправляемых к портам-участникам VPC, если выбор первичного устройства VPC происходит после того, как приоритет был настроен. Если системный приоритет VPC настраивается после выбора первичного устройства VPC, оперативный приоритет VPC будет использоваться в LACP PDU и STP BPDU вместо настроенного системного приоритета VPC.

Настраиваемый диапазон — от 1 до 65535.

Значение по умолчанию: 32767.

Формат: `system-priority` *`priority`*

Режим ввода команд: домен VPC

no system-priority

Эта команда устанавливает системный приоритет VPC в значение по умолчанию.

Формат: `no system-priority priority`

Режим ввода команд: домен VPC

vpc

Эта команда настраивает LAG-интерфейс как часть VPC. При исполнении команды канал порта выключен до того, пока партнерские коммутаторы не обменяются данными и не утвердят информацию LAG-интерфейса как участника.

Настраиваемый диапазон для VPC id — от 1 до значения «максимальное число LAG-интерфейсов (64) — 1».

Значение по умолчанию: отсутствует

Формат: `vpc id`

Режим ввода команд: LAG-интерфейс

no vpc

Эта команда сбрасывает настройки канала порта как части VPC.

Формат: `no vpc id`

Режим ввода команд: LAG-интерфейс

vpc peer-link

Эта команда настраивает LAG-интерфейс как партнерское соединение VPC.

Формат: `vpc peer-link`

Режим ввода команд: LAG-интерфейс

no vpc peer-link

Команда удаляет настройки LAG-интерфейса как партнерского соединения VPC.

Формат: `no vpc peer-link`

Режим ввода команд: LAG-интерфейс

show running-config vpc

Используйте данную команду для отображения информации о текущей конфигурации для виртуальных каналов порта (VPC).

Формат: `show running-config vpc`

Режим ввода команд: привилегированный

show vpc

Данная команда отображает информацию о VPC. Отображаются конфигурационный и оперативный режимы VPC; при этом VPC оперативно включается, если выполнены все предварительные условия. Агрегированный интерфейс, который настроен как VPC-интерфейс, также отображается с портами-участниками на текущем коммутаторе и коммутаторе-партнере (с соответствующим статусом соединения).

Формат: `show vpc id`

Режим ввода команд: пользовательский

show vpc brief

Эта команда отображает глобальный статус VPC и текущий оперативный режим VPC (VPC оперативно включена, если все предварительные условия выполнены). Отображаются статусы *peerlink* и *keepalive*, а также количество настроенных и действующих VPC, системные MAC-адреса и роли.

Формат: `show vpc brief`

Режим ввода команд: привилегированный

show vpc consistency-parameters

Используйте данную команду, чтобы отобразить глобальные параметры согласованности и параметры согласованности LAG-интерфейса для виртуальных каналов порта (VPC) на коммутаторе.

Формат: `show vpc consistency-parameters {global | interface lag lag-id}`

Режим ввода команд: привилегированный

show vpc peer-keepalive

Данная команда отображает IP-адрес соседнего VPC-коммутатора, используемый протоколом DCPDP. Отображается порт, используемый для DCPDP. Команда также показывает, включено ли обнаружение партнера. Если включено, отображается статус обнаружения. Отображаются также интервал передачи DCPDP-сообщений и время ожидания принятия.

Формат: `show vpc peer-keepalive`

Режим ввода команд: пользовательский

show vpc role

Данная команда отображает информацию о статусе keepalive и его параметры. Отображаются также роль VPC-коммутатора, системный MAC-адрес и приоритет.

Формат: `show vpc role`

Режим ввода команд: пользовательский

show vpc statistics

Эта команда показывает счетчики keepalive-сообщений, переданных и полученных VPC-коммутатором.

Формат: `show vpc statistics {peer-keepalive | peer-link}`

Режим ввода команд: пользовательский

clear vpc statistics

Эта команда очищает всю статистику keepalive.

Формат: `clear vpc statistics {peer-keepalive | peer-link}`

Режим ввода команд: пользовательский

debug vpc peer-keepalive

Эта команда включает трассировку отладки для переходов статуса keepalive.

Формат: `debug vpc peer-keepalive`

Режим ввода команд: пользовательский

debug vpc peer-link data-message

Эта команда включает трассировку отладки для контрольных сообщений, которыми обмениваются VPC-устройства через партнерское соединение.

Формат: `debug vpc peer-link data-message`

Режим ввода команд: пользовательский

debug vpc peer-link control-message async

Эта команда включает трассировку отладки для асинхронных достоверных контрольных сообщений, которыми обмениваются устройства MLAG через партнерское соединение. С ключевым словом error отслеживаются только ошибки в коммуникации. С ключевым слово msg можно отследить содержание обмениваемых контрольных сообщений. Содержание можно отслеживать как для передаваемых, так и для получаемых контрольных сообщений.

Формат: `debug vpc peer-link control-message async {error | msg [receive | transmit]}`

Режим ввода команд: пользовательский

debug vpc peer-link control-message bulk

Эта команда включает трассировку отладки для периодических контрольных сообщений, которыми обмениваются устройства MLAG через партнерское соединение. С ключевым словом error отслеживаются только ошибки в коммуникации. С ключевым слово msg можно отследить содержание обмениваемых контрольных сообщений. Содержание можно отслеживать как для передаваемых, так и для получаемых контрольных сообщений.

Формат: `debug vpc peer-link control-message bulk {error | msg [receive | transmit]}`

Режим ввода команд: пользовательский

debug vpc peer-link control-message ckpt

Эта команда включает трассировку отладки для контрольных сообщений контрольных точек, которыми обмениваются устройства MLAG через партнерское соединение. С ключевым словом *error* отслеживаются только ошибки в коммуникации. С ключевым слово *msg* можно отследить содержание обмениваемых контрольных сообщений. Содержание можно отслеживать как для передаваемых, так и для получаемых контрольных сообщений.

Формат: `debug vpc peer-link control-message ckpt {error | msg [receive | transmit]}`

Режим ввода команд: пользовательский

debug vpc peer detection

Эта команда включает трассировку отладки для протокола DCPDP. Записи видны, когда DCPDP передает или получает пакеты обнаружения от соседнего VPC-коммутатора.

Формат: `debug vpc peer detection`

Режим ввода команд: пользовательский

9.25 Команды настройки зеркалирования интерфейсов

Зеркальное копирование порта, также называемое мониторингом портов, выбирает сетевой трафик, который можно проанализировать с помощью сетевого анализатора, например устройства SwitchProbe или другого тестового устройства удаленного мониторинга (RMON).

monitor session source

Команды, описанные ниже, добавляют зеркалируемый порт (порт-источник) к сессии, обозначенной *session-id*. Параметр *session-id* — это целочисленное значение, используемое для идентификации сессии. Максимальное количество сессий, которое может быть настроено 7. Используйте параметр *source interface unit/slot/port*, чтобы указать интерфейс для мониторинга. Используйте параметры rx для мониторинга только входящих пакетов или tx для мониторинга только исходящих пакетов. Если не указывать опции {rx | tx}, порт назначения будет выполнять мониторинг для обоих типов пакетов.

Если используется VLAN как источник для сессии, выполняется мониторинг всех портов-участников этой VLAN.

Для настройки удаленного зеркалирования интерфейса используйте параметр remote vlan vlan-id.

Источник и место назначения не могут быть настроены как удаленные на одном и том же устройстве.

Если интерфейс участвует в какой-либо VLAN и входит в LAG, эта VLAN не может быть назначена как источник для сессии мониторинга. Однако если интерфейс участвует в какой-либо VLAN, и эта VLAN назначена источником сессии мониторинга, интерфейс может быть назначен в качестве участника LAG.

Если в качестве источника указать интерфейс VLAN, то зеркалирование TX трафика с CPU коммутатора в этом VLAN осуществляться не будет. Для зеркалирования данного трафика необходимо указать в качестве порта-источника CPU интерфейс (`monitor session session-id source interface cpu`).

Значение по умолчанию: отсутствует

Формат: `monitor session` *`session-id`* `source {interface {`*`unit/slot/port`* `| cpu | lag } | vlan` *`vlan- id`* `| remote vlan` *`vlan-id`* `}[{rx | tx}]`

Режим ввода команд: глобальная конфигурация

no monitor session source

Эта команда удаляет указанный зеркалируемый порт из указанной сессии мониторинга.

Значение по умолчанию: отсутствует

Формат: `no monitor session` *`session-id`* `source {interface {`*`unit/slot/port`* `| cpu | lag } | vlan| remote vlan}`

Режим ввода команд: глобальная конфигурация

monitor session destination

Эта команда добавляет зеркалирующий порт (порт-получатель) к выбранной сессии, обозначенной *session-id*. Параметр *session-id* — это целочисленное значение, используемое для идентификации сессии. Максимальное количество сессий, которое может быть настроено 7.

Используйте destination interface *unit/slot/port*, чтобы указать интерфейс, который будет передавать зеркалируемый трафик.

Удаленное зеркалирования портов настраивается путем добавления RSPAN VLAN ID. Для настройки удалённого зеркалирования RSPAN используйте параметр *remote vlan vlan- id*.

Параметр *reflector-port* настраивается на коммутаторе-источнике вместе с RSPAN VLAN места назначения. Назначенный *reflector-port* передает зеркалируемый трафик к коммутатору места назначения.

Данный порт должен быть настроен как участник RSPAN VLAN.

На промежуточном коммутаторе должна быть создана RSPAN VLAN, и все порты, соединенные с коммутаторами источника и места назначения, должны быть включены в RSPAN VLAN. Тегирование исходящего трафика RSPAN VLAN должно быть включено на интерфейсе промежуточного коммутатора, расположенного на пути к коммутатору места назначения.

Значение по умолчанию: отсутствует

Формат: `monitor session` *`session-id`* `destination {interface` *`unit/slot/port`* `|remote vlan` *`vlan- id`* `reflector-port` *`unit/slot/port`*`}`

Режим ввода команд: глобальная конфигурация

no monitor session destination

Эта команда удаляет указанный зеркалирующий порт из выбранной сессии мониторинга.

Формат: `no monitor session` *`session-id`* `destination {interface` *`unit/slot/port`* `|remote vlan` *`vlan- id`* `reflector-port` *`unit/slot/port`*`}`

Режим ввода команд: глобальная конфигурация

monitor session filter

Данная команда подключает список IP/MAC ACL к выбранной сессии мониторинга, обозначенной *session-id*. Используйте параметр *filter*, чтобы фильтровать зеркалируемые пакеты по IP- или MAC-адресам в соответствии с указанным ACL.

IP/MAC ACL можно подключать к сессии путем предоставления номера или имени ACL.

Значение по умолчанию: отсутствует

Формат: `monitor session` *`session-id`* `filter {ip access-group` *`acl-id/aclname`* `| mac access-group` *`acl-name`*`}`

Режим ввода команд: глобальная конфигурация

no monitor session filter

Эта команда удаляет указанный IP/MAC ACL из выбранной сессии мониторинга.

Формат: `no smonitor session` *`session-id`* `filter {ip access-group|mac access-group}`

Режим ввода команд: глобальная конфигурация

monitor session mode

Эта команда включает режим мониторинга для выбранной сессии мониторинга.

Значение по умолчанию: отсутствует

Формат: `monitor session session-id mode`

Режим ввода команд: глобальная конфигурация

no monitor session mode

Команда выключает режим мониторинга для выбранной сессии мониторинга.

Формат: no monitor session *session-id* mode

Режим ввода команд: глобальная конфигурация

no monitor session

Используйте данную команду без необязательных параметров, чтобы удалить выбранную сессию мониторинга со всеми сконфигурированными необязательными параметрами и возвращает режим мониторинга для выбранной сессии в значение по умолчанию.

Формат: no monitor session *session-id*

Режим ввода команд: глобальная конфигурация

no monitor

Данная команда возвращает все настроенные на коммутаторе сессии мониторинга к значению по умолчанию.

Данная команда является автономной no-формой командой. Команда не имеет «утвердительной» формы.

Значение по умолчанию: отсутствует

Формат: `no monitor`

Режим ввода команд: глобальная конфигурация

show monitor session

Данная команда отображает информацию мониторинга портов для указанной сессии мониторинга или для всех доступных сессий мониторинга.

Формат: `show monitor session {session-id {1-7} | all}`

Режим ввода команд: привилегированный

Термин	*Значение*
Session ID	Целое число, соответствующее индикатору сессии в диапазоне от 1 до 7.
Admin Mode	Показывает включена ли функция зеркалирования портов для сессии, обозначенной параметром session-id. Возможные значения: enabled и disabled.
Probe Port	Зеркалирующий (порт места назначения) для сессии, обозначенной параметром session-id. Если зеркалирующий порт не назначен, поле остается пустым.

Src RVLAN	Зеркалируемая VLAN. Если зеркалируемая VLAN не настроена, поле остается пустым.
Mirrored Port	Порт, настроенный как зеркалируемый (порт-источник) для сессии, обозначенной параметром session-id. Если для сессии не настроен порт-источник, поле остается пустым.
Ref. Port	Этот порт передает весь копируемый трафик.
Src RVLAN	Входящая RSPAN VLAN, настроенная на коммутаторе. Если RSPAN VLAN не настроена, это поле остается пустым.
Dst RVLAN	Исходящая RSPAN VLAN места, настроенная на коммутаторе. Если RSPAN VLAN не настроена, это поле остается пустым.
Type	Тип зеркалируемых пакетов. Возможные значения: tx для передаваемых пакетов и rx для принимаемых пакетов.
IP ACL	Идентификатор или имя списка контроля доступа IP, связанного с сессией мониторинга портов.
MAC ACL	Имя списка контроля доступа MAC, связанного с сессией мониторинга портов.

show vlan remote-span

Эта команда отображает настроенные RSPAN VLAN.

Формат: `show vlan remote-span`

Режим ввода команд: привилегированный

9.26 Команды настройки статичной MAC-фильтрации

Команды в этой части описывают процесс настройки статической MAC-фильтрации. Статическая MAC-фильтрация позволяет настроить порты места назначения для статического MAC-фильтра многоадресной рассылки.

macfilter

Эта команда добавляет запись статического MAC-фильтра для MAC-адреса macaddr в сети VLAN vlanid. Значение macaddr — это 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Запрещёнными MAC-адресами являются 00:00:00:00:00:00, с 01:80:C2:00:00:00 по 01:80:C2:00:00:0F, с 01:80:C2:00:00:20 по 01:80:C2:00:00:21, а также FF:FF:FF:FF:FF:FF. Параметр vlanid должен определять действительную VLAN.

Количество статических MAC-фильтров, поддерживаемых в системе, отличается для MAC-фильтров с настроенными портами-источниками и MAC-фильтров с настроенными портами места назначения.

Можно настроить следующие комбинации:

- одноадресный MAC и порт-источник;
- многоадресный MAC и порт-источник;
- многоадресный MAC и только порт места назначения;
- многоадресный MAC с портами-источниками и портами места назначения.

Формат: `macfilter` *`macaddr vlanid`*

Режим ввода команд: глобальная конфигурация

no macfilter

Эта команда удаляет все ограничения фильтрации и запись статического MAC-фильтра для MAC-адреса macaddr в сети VLAN vlanid. Значение параметра macaddr должно определяться как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6.

Параметр *vlanid* должен определять действительную VLAN.

Формат: no macfilter *macaddr vlanid* **Mode**

Режим ввода команд: глобальная конфигурация

macfilter adddest

Используйте данную команду для добавления интерфейса или диапазона интерфейсов к набору фильтров мест назначения MAC-фильтра с данным *macaddr* и VLAN *vlanid*. Значение параметра *macaddr* должно определяться как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр vlanid должен определять действительную VLAN.

Настройка списка портов места назначения возможна только для действительных MAC-адресов многоадресной рассылки.

Формат: `macfilter adddest` *`macaddr`*

Режим ввода команд: конфигурирование интерфейса

no macfilter adddest

Эта команда удаляет порт из набора фильтров мест назначения MAC-фильтра с данным macaddr и VLAN vlanid. Значение параметра macaddr должно определяться как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр vlanid должен определять действительную VLAN.

Формат: `no macfilter adddest` *`macaddr`*

Режим ввода команд: конфигурирование интерфейса

macfilter adddest all

Эта команда добавляет все интерфейсы к набору фильтров мест назначения MAC-фильтра с данным *macaddr* и VLAN *vlanid*. Значение параметра *macaddr* должно определяться как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр *vlanid* должен определять действительную VLAN.

Настройка списка портов места назначения возможна только для действительных MAC-адресов многоадресной рассылки.

Формат: `macfilter adddest all` *`macaddr`*

Режим ввода команд: глобальная конфигурация

no macfilter adddest all

Эта команда удаляет все порты из набора фильтров мест назначения MAC-фильтра с данным *macaddr* и VLAN *vlanid*. Значение параметра *macaddr* должно определяться как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр vlanid должен определять действительную VLAN.

Формат: `no macfilter adddest all` *`macaddr`*

Режим ввода команд: глобальная конфигурация

macfilter addsrc

Данная команда добавляет интерфейс или диапазон интерфейсов к набору фильтров источников MAC-фильтра с данным macaddr и VLAN vlanid. Значение параметра macaddr должно определяться как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр vlanid должен определять действительную VLAN.

Формат: `macfilter addsrc` *`macaddr vlanid`*

Режим ввода команд: конфигурирование интерфейса

no macfilter addsrc

Данная команда удаляет порт из набора фильтров источников MAC-фильтра с данным *macaddr* и VLAN *vlanid*. Значение параметра macaddr должно определяться как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр *vlanid* должен определять действительную VLAN.

Формат: `no macfilter addsrc` *`macaddr vlanid`*

Режим ввода команд: конфигурирование интерфейса

macfilter addsrc all

Данная команда добавляет все интерфейсы к набору фильтров источников MAC-фильтра с данным *macaddr* и VLAN *vlanid*. Значение *macaddr* нужно определять как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6. Параметр vlanid должен определять действительную VLAN.

Формат: `macfilter addsrc all` *`macaddr vlanid`*

Режим ввода команд: глобальная конфигурация

no macfilter addsrc all

Данная команда удаляет все интерфейсы из набора фильтров источников MAC-фильтра с данным *macaddr* и VLAN *vlanid*. Значение macaddr нужно определять как 6-битное шестнадцатеричное число в формате b1:b2:b3:b4:b5:b6.

Параметр *vlanid* должен определять действительную VLAN.

Формат: `no macfilter addsrc all` *`macaddr vlanid`*

Режим ввода команд: глобальная конфигурация

show mac-address-table static

Эта команда отображает данные о статической MAC-фильтрации для всех статических MAC-фильтров. Если указать ключевое слово *all*, будут отображены все статические MAC-фильтры в системе. Если указано значение для *macaddr*, необходимо также ввести значение *vlanid*, и тогда система отобразит информацию статической MAC-фильтрации только для данного MAC-адреса и VLAN.

Формат: `show mac-address-table static {`*`macaddr vlanid`*` | all}`

Режим ввода команд: привилегированный

Термин	***Значение***
MAC Address	MAC-адрес записи статической MAC-фильтрации.

VLAN ID	Идентификатор VLAN-записи статичной MAC-фильтрации.
Source Port(s)	Порт(ы) набора фильтров.

Списки портов места назначения будут только у фильтров групповых адресов.

show mac-address-table staticfiltering

Эта команда отображает записи статической фильтрации в таблице коммутации многоадресной рассылки (MFDB).

Формат: `show mac-address-table staticfiltering`

Режим ввода команд: привилегированный

Термин	*Значение*
VLAN ID	VLAN, в которой был определен MAC-адрес.
MAC Address	Одноадресный MAC-адрес, для которого коммутатор переадресует или фильтрует данные. Как только будет определена информация из таблицы MFDB, адрес станет групповым. Указывается в формате шести двузначных номеров шестнадцатеричной системы, разделенных двоеточиями, например: 01:23:45:67:89:AB.
Type	Тип записи.
Description	Текстовое описание данной записи таблицы многоадресной коммутации.
Interfaces	Список интерфейсов, которые назначены для переадресации (Fwd:) и фильтрации (Flt:).

9.27 Настройка агента DHCP-ретранслятора уровня 2

Коммутатор можно настроить как агент DHCP-ретранслятора уровня 2 для ретрансляции DHCP-запросов от клиентов к агенту-ретранслятору уровня 3 или серверу. К DHCP-запросам, ретранслированным от клиентов к DHCP-серверу, можно добавить значения Circuit ID и Remote ID. Эта информация будет включена в DHCP-опцию 82, как указано в разделах 3.1 и 3.2 стандарта RFC3046.

dhcp l2relay

Эта команда включает агент DHCP-ретранслятора уровня 2 для интерфейса, диапазона интерфейсов или всех интерфейсов. Последующие команды этой части могут быть выполнены только в случае, если агент DHCP-ретранслятора уровня 2 включен.

Формат: `dhcp l2relay`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no dhcp l2relay

Команда выключает агент DHCP-ретранслятора уровня 2 для интерфейса или диапазона интерфейсов.

Формат: `no dhcp l2relay`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

dhcp l2relay circuit-id subscription

Эта команда устанавливает Circuit ID в DHCP-опции 82 для указанной сервисной подписки *subscription-string* на данном интерфейсе. *subscription-string* — это ряд символов, который для правильной работы должен совпадать с настроенным значением подписки DOT1AD. Если *circuit-id* включен с помощью этой команды, все запросы DHCP-клиентов, подпадающие под эту подписку, добавляются в circuit-id опции-82 как входящий номер интерфейса.

Значение по умолчанию: выключено

Формат: `dhcp l2relay circuit-id subscription subscription-string`

Режим ввода команд: конфигурирование интерфейса

no dhcp l2relay circuit-id subscription

Эта команда сбрасывает значение Circuit ID в DHCP-опции 82 для указанной сервисной подписки, обозначающейся как *subscription-string* на данном интерфейсе.

Формат: `no dhcp l2relay circuit-id subscription` *`subscription-string`*

Параметр	***Описание***
vlan–list	Идентификатор VLAN. Диапазон значений: 1–4094. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).

no dhcp l2relay circuit-id vlan

Этот параметр удаляет значение Circuit ID DHCP-опции 82 для VLAN.

Формат: `no dhcp l2relay circuit-id vlan` *`vlan-list`*

Режим ввода команд: глобальная конфигурация

dhcp l2relay remote-id subscription

Эта команда устанавливает строку *Remote-ID* DHCP-опции 82 для сервисной подписки subscription-string на данном интерфейсе или диапазоне интерфейсов. *subscription-string* — это ряд символов, который для правильной работы должен совпадать с настроенным значением подписки DOT1AD. *remoteid-string* — это строка символов. Если *remote-id* включен с помощью этой команды, все запросы DHCP-клиентов, подпадающие под эту подписку, добавляются в *Remote-id* опции-82 как настроенная строка *remote-id*.

Значение по умолчанию: пустая строка

Формат: `dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*

Режим ввода команд: конфигурирование интерфейса

no dhcp l2relay remote-id subscription

Эта команда сбрасывает строку Remote-ID DHCP-опции 82 для сервисной подписки subscription-string на данном интерфейсе.

Формат: `no dhcp l2relay remote-id` *`remoteid-string`* `subscription-name` *`subscription-string`*

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
vlan–list	Идентификатор VLAN. Диапазон значений: 1–4094. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).

no dhcp l2relay remote-id vlan

Этот параметр удаляет Remote-ID DHCP-опции 82 для VLAN и сервисной подписки (на основе имени подписки).

Формат: `no dhcp l2relay remote-id vlan` *`vlan-list`*

Режим ввода команд: глобальная конфигурация

dhcp l2relay subscription

Эта команда включает ретрансляцию DHCP-пакетов на интерфейсе или диапазоне интерфейсов, которые подпадают под указанную сервисную подписку. *subscription-string* — это ряд символов, который для правильной работы должен совпадать с настроенным значением подписки DOT1AD.

Значение по умолчанию: выключено (т. е. DHCP-пакеты не ретранслируются)

Формат: `dhcp l2relay subscription-name` *`subscription-string`*

Режим ввода команд: конфигурирование интерфейса

no dhcp l2relay subscription

Эта команда выключает ретрансляцию DHCP-пакетов на интерфейсе или диапазоне интерфейсов, которые подпадают под указанную сервисную подписку.

Формат: `no dhcp l2relay subscription-name` *`subscription-string`*

Режим ввода команд: конфигурирование интерфейса

dhcp l2relay trust

Используйте данную команду для настройки интерфейса или диапазона интерфейсов как доверенных для принятия DHCP-пакетов с Опцией 82.

Значение по умолчанию: не доверенный
Формат: `dhcp l2relay trust`

Режим ввода команд: конфигурирование интерфейса

no dhcp l2relay trust

Используйте данную команду для настройки интерфейса или диапазона интерфейсов как не доверенных для принятия DHCP-пакетов с Опцией 82.

Формат: `no dhcp l2relay trust`

Режим ввода команд: конфигурирование интерфейса

dhcp l2relay vlan

Используйте данную команду, чтобы включить агента DHCP-ретранслятора уровня 2 для набора VLAN. Все DHCP-пакеты, попадающие на интерфейсы в настроенных VLAN, подлежат ретрансляции уровня 2.

Значение по умолчанию: выключено

Формат: `dhcp l2relay vlan vlan-list`

Режим ввода команд: глобальная конфигурация

dhcp l2relay remote-id vlan

Этот параметр устанавливает Remote-ID DHCP-опции 82 для VLAN и сервисной подписки (на основе имени подписки).

Формат: `dhcp l2relay remote-id remote-id-string vlan vlan-list`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
vlan–list	Идентификатор VLAN. Диапазон значений: 1–4094. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).

no dhcp l2relay vlan

Используйте данную команду, чтобы выключить агента DHCP-ретранслятора уровня 2 для набора VLAN.

Формат: `no dhcp l2relay vlan vlan-list`

Режим ввода команд: глобальная конфигурация

show dhcp l2relay all

Эта команда отображает сводную информацию настроек DHCP-ретранслятора уровня 2.

Формат: `show dhcp l2relay all`

Режим ввода команд: привилегированный

show dhcp l2relay circuit-id vlan

Эта команда отображает конфигурацию circuit-id DHCP для VLAN.

Формат: `show dhcp l2relay circuit-id vlan vlan-list`

Режим ввода команд: привилегированный
конфигурирование интерфейса

dhcp l2relay circuit-id vlan

Этот параметр устанавливает значение Circuit ID DHCP-опции 82 для VLAN. После включения номер интерфейса добавляется как Circuit ID в DHCP-опции 82.

Формат: `dhcp l2relay circuit-id vlan vlan-list`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
vlan–list	Идентификатор VLAN в диапазоне от 1 до 4094. Используйте дефис (-) для диапазона или запятые (,) для разделения отдельных идентификаторов VLAN. Использовать пробелы и нули нельзя.

show dhcp l2relay interface

Эта команда отображает настройки DHCP ретранслятора для указанных интерфейсов.

Формат: `show dhcp l2relay interface {all | interface-num}`

Режим ввода команд: привилегированный

show dhcp l2relay remote-id vlan

Данная команда отображает конфигурацию Remote-id DHCP для VLAN.

Формат: `show dhcp l2relay remote-id vlan` *`vlan-list`*

Режим ввода команд: привилегированный

Параметр	*Описание*
vlan–list	Идентификатор VLAN в диапазоне от 1 до 4094. Используйте дефис (-) для диапазона или запятые (,) для разделения отдельных идентификаторов VLAN. Использовать пробелы и нули нельзя.

show dhcp l2relay stats interface

Данная команда отображает статистику интерфейсов с настроенными DHCP-ретрансляторами уровня 2.

Формат: `show dhcp l2relay stats interface {all | interface-num}`

Режим ввода команд: привилегированный

show dhcp l2relay subscription interface

Эта команда отображает настройки DHCP-ретранслятора уровня 2 для указанных сервисных подписок на интерфейсе.

Формат: `show dhcp l2relay subscription interface {all|interface-num}`

Режим ввода команд: привилегированный

show dhcp l2relay agent-option vlan

Данная команда отображает настройки Опции-82 DHCP-ретранслятора уровня 2 для конкретных VLAN.

Формат: `show dhcp l2relay agent-option vlan vlan-range`

Режим ввода команд: привилегированный

show dhcp l2relay vlan

Эта команда отображает VLAN-настройки DHCP.

Формат: `show dhcp l2relay vlan vlan-list`

Режим ввода команд: привилегированный

Параметр	*Описание*
vlan–list	Идентификатор VLAN в диапазоне от 1 до 4094. Используйте дефис (-) для диапазона или запятые (,) для разделения отдельных идентификаторов VLAN. Использовать пробелы и нули нельзя.

clear dhcp l2relay statistics interface

Используйте эту команду, чтобы сбросить счетчики DHCP-ретранслятора уровня 2. Необходимо указать порт, на котором нужно сбросить счетчики, или использовать ключевое слово all, чтобы сбросить счетчики на всех портах.

Формат: `clear dhcp l2relay statistics interface {unit/slot/port | all}`

Режим ввода команд: привилегированный

9.28 Команды настройки DHCP-клиента

Система может включать данные источника запросов DHCP-клиента, передаваемые DHCP-серверу. Эта информация включена в параметр Vendor Class Identifier DHCP-опции 60. Информация является строкой, состоящей из 128 октетов.

dhcp client vendor-id-option

Эта команда включает добавление Vendor Class Identifier DHCP-опции 60 в запросы, передаваемые DHCP-серверу DHCP-клиентами, работающими на коммутаторе.

Формат: `dhcp client vendor-id-option` *`string`*

Режим ввода команд: глобальная конфигурация

no dhcp client vendor-id-option

Эта команда выключает добавление Vendor Class Identifier DHCP-опции 60 в запросы, передаваемые DHCP-серверу DHCP-клиентами, работающими на коммутаторе.

Формат: `no dhcp client vendor-id-option`

Режим ввода команд: глобальная конфигурация

dhcp client vendor-id-option-string

Этот параметр устанавливает строку DHCP-опции 60 для добавления к запросам, передаваемым DHCP-серверу DHCP-клиентами, работающими на коммутаторе.

Формат: `dhcp client vendor-id-option-string` *`string`*

Режим ввода команд: глобальная конфигурация

no dhcp client vendor-id-option-string

Этот параметр удаляет строку DHCP-опции 60.

Формат: `no dhcp client vendor-id-option-string`

Режим ввода команд: глобальная конфигурация

show dhcp client vendor-id-option

Эта команда отображает настроенный административный режим для VendorID Option и VendorID String, которые будут включены в опцию 60 DHCP-запросов.

Формат: `show dhcp client vendor-id-option`

Режим ввода команд: привилегированный

9.29 Команды настройки DHCP Snooping

Эта часть описывает команды, используемые для настройки DHCP Snooping.

ip dhcp snooping

Используйте данную команду, чтобы включить DHCP Snooping глобально.

Значение по умолчанию: выключено

Формат: `ip dhcp snooping`

Режим ввода команд: глобальная конфигурация

no ip dhcp snooping

Команда выключает DHCP Snooping глобально.

Формат: `no ip dhcp snooping`

Режим ввода команд: глобальная конфигурация

ip dhcp snooping vlan

Используйте эту команду, чтобы включить DHCP Snooping на списке диапазонов VLAN, перечисленных через запятую.

Значение по умолчанию: выключено

Формат: `ip dhcp snooping vlan` *`vlan-list`*

Режим ввода команд: глобальная конфигурация

no ip dhcp snooping vlan

Используйте эту команду, чтобы выключить DHCP Snooping на указанных VLAN.

Формат: `no ip dhcp snooping vlan` *`vlan-list`*

Режим ввода команд: глобальная конфигурация

ip dhcp snooping verify mac-address

Команда включает проверку MAC-адреса источника в полученном DHCP-сообщении.

Значение по умолчанию: включено

Формат: `ip dhcp snooping verify mac-address`

Режим ввода команд: глобальная конфигурация

no ip dhcp snooping verify mac-address

Используйте эту команду, чтобы выключить проверку MAC-адреса источника.

Формат: `no ip dhcp snooping verify mac-address`

Режим ввода команд: глобальная конфигурация

ip dhcp snooping database

Используйте эту команду, чтобы настроить постоянное расположение для базы данных DHCP Snooping. Расположение может быть локальным или в виде удаленного файла на устройстве с указанным IP-адресом.

Значение по умолчанию: local

Формат: `ip dhcp snooping database {local|tftp://hostIP/filename}`

Режим ввода команд: глобальная конфигурация

ip dhcp snooping database write-delay

Используйте эту команду, чтобы настроить интервал в секундах, за который база данных DHCP Snooping должна быть сохранена. Значение интервала находится в диапазоне от 15 до 86400 секунд.

Значение по умолчанию: 300 секунд

Формат: `ip dhcp snooping database write-delay in seconds`

Режим ввода команд: глобальная конфигурация

no ip dhcp snooping database write-delay

Команда устанавливает *write-delay* в значение по умолчанию.

Формат: `no ip dhcp snooping database write-delay`

Режим ввода команд: глобальная конфигурация

ip dhcp snooping binding

Команда для настройки статичной привязки DHCP Snooping.

Формат: `ip dhcp snooping binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Режим ввода команд: глобальная конфигурация

no ip dhcp snooping binding

Команда удаляет статичную запись DHCP из базы данных DHCP Snooping.

Формат: `no ip dhcp snooping binding` *`mac-address`*

Режим ввода команд: глобальная конфигурация

ip dhcp filtering trust

Используйте эту команду, чтобы включить доверенный режим на интерфейсе, если сохраненная в прошлый раз конфигурация или примененный сценарий содержали эту команду.

Формат: `ip dhcp filtering trust` *`interface id`*

Режим ввода команд: глобальная конфигурация

no ip dhcp filtering trust

Используйте эту команду, чтобы выключить доверенный режим на интерфейсе.

Формат: `no ip dhcp filtering trust` *`interface id`*

Режим ввода команд: глобальная конфигурация

ip verify binding

Используйте данную команду, чтобы настроить статичные записи IP Source Guard (IPSG).

Формат: `ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Режим ввода команд: глобальная конфигурация

no ip verify binding

Используйте данную команду, чтобы удалить статичную запись IPSG из базы данных IPSG.

Формат: `no ip verify binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Режим ввода команд: глобальная конфигурация

ip dhcp snooping limit

Команда помогает управлять скоростью, с которой сообщения DHCP Snooping приходят на интерфейс или диапазон интерфейсов. По умолчанию ограничение скорости выключено. Если ограничение включено, скорость может составлять от 0 до 300 пакетов в секунду. Диапазон уровней всплесков — от 1 до 15 секунд.

Значение по умолчанию: выключено (нет ограничений)

Формат: `ip dhcp snooping limit {rate pps [`*`burst interval seconds`*`]}`

Режим ввода команд: конфигурирование интерфейса

no ip dhcp snooping limit

Команда устанавливает значение скорости, с которой приходят сообщения DHCP Snooping, и уровень всплесков в значения по умолчанию.

Формат: `no ip dhcp snooping limit`

Режим ввода команд: конфигурирование интерфейса

ip dhcp snooping log-invalid

Используйте данную команду, чтобы управлять фильтрацией DHCP-сообщений для журнала DHCP Snooping. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Значение по умолчанию: выключено

Формат: `ip dhcp snooping log-invalid`

Режим ввода команд: конфигурирование интерфейса

no ip dhcp snooping log-invalid

Используйте данную команду, чтобы выключить фильтрацию DHCP-сообщений для журнала DHCP Snooping.

Формат: `no ip dhcp snooping log-invalid`

Режим ввода команд: конфигурирование интерфейса

ip dhcp snooping trust

Используйте эту команду, чтобы настроить интерфейс или диапазон интерфейсов как доверенные.

Значение по умолчанию: выключено

Формат: `ip dhcp snooping trust`

Режим ввода команд: конфигурирование интерфейса

no ip dhcp snooping trust

Команда настраивает порт как не доверенный.

Формат: no ip dhcp snooping trust

Режим ввода команд: конфигурирование интерфейса

ip verify source

Используйте эту команду, чтобы настроить ID-атрибут IPSG-источника на аппаратную фильтрацию трафика. ID источника — это сочетание IP-адреса и MAC-адреса. Обычная команда позволяет фильтрацию трафика на основе IP-адреса. С опцией *port-security* трафик данных будет фильтроваться на основе IP-адресов и MAC-адресов.

Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Значение по умолчанию: IP-адрес — это ID источника

Формат: `ip verify source {port-security}`

Режим ввода команд: конфигурирование интерфейса

no ip verify source

Используйте эту команду, чтобы выключить IPSG. Невозможно выключить отдельно *port-security*, если этот параметр настроен.

Формат: `no ip verify source`

Режим ввода команд: конфигурирование интерфейса

show ip dhcp snooping

Используйте эту команду, чтобы отобразить глобальные настройки DHCP Snooping и настройки для каждого порта.

Формат: `show ip dhcp snooping`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Interface	Интерфейс, для которого отображается информация.
Trusted	Если включено, DHCP Snooping считает этот порт доверенным. Заводская настройка: disabled.
Log Invalid Pkts	Если включено, DHCP Snooping вносит в журнал на данном интерфейсе сбойные пакеты.

show ip dhcp snooping binding

Используйте эту команду, чтобы отобразить записи привязки DHCP Snooping. Чтобы упорядочить вывод информации, используйте следующие опции:

- Dynamic: Ограничить вывод по DHCP Snooping.
- Interface: Ограничить вывод по определенному интерфейсу.
- Static: Ограничить вывод по статичным записям.
- VLAN: Ограничить вывод по VLAN.

Формат: `show ip dhcp snooping binding [{static/dynamic}] [interface unit/slot/port] [vlan id]`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
MAC Address	Отображает MAC-адрес для добавленной привязки. MAC-адрес — это ключ к базе данных привязки.
IP Address	Отображает действительный IP-адрес для правил привязки.
VLAN	VLAN для правил привязки.
Interface	Интерфейс, к которому добавляется привязка интерфейса DHCP Snooping.
Type	Тип привязки: статично настроенная в CLI или определённая динамически.
Lease (sec)	Оставшийся срок аренды для записи.

show ip dhcp snooping database

Используйте эту команду, чтобы отобразить настройки DHCP Snooping, относящиеся к сохранению базы данных.

Формат: `show ip dhcp snooping database`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
Agent URL	Привязки URL-агента базы данных.
Write Delay	Максимальное время записи базы данных (локальной или удаленной).

show ip dhcp snooping interfaces

Используйте эту команду, чтобы отобразить статус DHCP Snooping интерфейсов.

Формат: `show ip dhcp snooping interfaces`

Режим ввода команд: привилегированный

show ip dhcp snooping statistics

Используйте эту команду, чтобы перечислить статистику нарушений безопасности DHCP Snooping на ненадежных портах.

Формат: `show ip dhcp snooping statistics`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
Interface	IP-адрес интерфейса в формате *unit/slot/port*.
MAC Verify Failures	Отображает количество DHCP-сообщений, отфильтрованных на ненадежных интерфейсах из-за несовпадения MAC-адреса источника и аппаратного адреса клиента.
Client Ifc Mismatch	Отображает количество DHCP-релизов и сообщений отказов, полученных на разных портах, определенных ранее.

DHCP Server Msgs Rec'd	Отображает количество сообщений DHCP-сервера, полученных от ненадежных портов.

clear ip dhcp snooping binding

Используйте данную команду, чтобы удалить все привязки DHCP Snooping на всех интерфейсах или указанном интерфейсе.

Формат: `clear ip dhcp snooping binding [interface unit/slot/port]`

Режим ввода команд: привилегированный
пользовательский

clear ip dhcp snooping statistics

Команда очищает всю статистику DHCP Snooping.

Формат: `clear ip dhcp snooping statistics`

Режим ввода команд: привилегированный
пользовательский

show ip verify source

Используйте данную команду, чтобы отобразить настройки IPSG на всех портах.

Формат: `show ip verify source`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
Interface	IP-адрес интерфейса в формате *unit/slot/port*.
Filter Type	Может принимать одно из значений. • ip-mac: Для фильтрации трафика на данном интерфейсе используется IP+MAC. • ip: Для фильтрации трафика на данном интерфейсе используется только IP.
IP Address	IP-адрес интерфейса.
MAC Address	Если на интерфейсе не настроена фильтрация по MAC-адресу фильтрации, это поле остается пустым. Если на интерфейсе выключена защита портов, поле MAC Address отображает «permit-all».
VLAN	VLAN для правил привязки.

show ip verify interface

Используйте данную команду, чтобы отобразить тип IPSG-фильтра для указанного интерфейса.

Формат: `show ip verify interface unit/slot/port`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
Interface	IP-адрес интерфейса в формате *unit/slot/port*.
Filter Type	Может принимать одно из значений. • ip-mac: Для фильтрации трафика на данном интерфейсе используется IP+MAC.

	• ip: Для фильтрации трафика на данном интерфейсе используется только IP.

show ip source binding

Используйте данную команду, чтобы отобразить привязки IPSG.

Формат: `show ip source binding [{dhcp-snooping|static}] [interface` *`unit/slot/port`*`] [vlan id]`

Режим ввода команд: привилегированный

пользовательский

Термин	***Значение***
MAC Address	MAC-адрес обновленной записи.
IP Address	IP-адрес добавленной записи.
Type	Тип записи; статично настроенный с консоли или динамически определенный с помощью DHCP Snooping.
VLAN	VLAN записи.
Interface	IP-адрес интерфейса в формате unit/slot/port.

9.30 Команды настройки Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) — это функционал безопасности, который отклоняет недопустимые и вредоносные пакеты ARP. DAI предотвращает класс атак «man-in-the-middle», при которых недружественная станция перехватывает трафик других станций путем отравления ARP-кэша своих ничего не подозревающих соседей. Злоумышленник отправляет запросы ARP или ответы отображающие IP-адрес другой станции на свой собственный MAC-адрес.

DAI базируется на функционале DHCP Snooping. DHCP Snooping прослушивает обмен DHCP-сообщениями и создает базу данных привязки действительных {MAC-адрес, IP-адрес, VLAN и интерфейс} кортежей.

Если DAI включен, коммутатор отбрасывает ARP-пакеты, чьи MAC-адрес и IP-адрес отправителя не соответствуют записи в базе данных привязок DHCP Snooping. При желании можно настроить дополнительную проверку пакетов ARP.

ip arp inspection vlan

Используйте данную команду, чтобы включить Dynamic ARP Inspection на списке диапазонов VLAN, разделенных запятой.

Значение по умолчанию: выключено

Формат: `ip arp inspection vlan vlan-list`

Режим ввода команд: глобальная конфигурация

no ip arp inspection vlan

Команда выключает Dynamic ARP Inspection на списке диапазонов VLAN, разделенных запятой.

Формат: `no ip arp inspection vlan vlan-list`

Режим ввода команд: глобальная конфигурация

ip arp inspection validate

Используйте данную команду, чтобы включить дополнительные проверки source-mac, destination-mac и ip address для принятых ARP-пакетов. Каждая команда перекрывает настройки предыдущей команды. Например, если команда включает проверку достоверности src-mac и dst-mac, вторая команда включает только проверку IP, то src-mac и dst-mac будут выключены в результате выполнения второй команды.

Значение по умолчанию: выключено

Формат: `ip arp inspection validate {[src-mac] [dst-mac] [ip]}`

Режим ввода команд: глобальная конфигурация

no ip arp inspection validate

Данная команда выключает дополнительные проверки для принятых ARP-пакетов.

Формат: `no ip arp inspection validate {[src-mac] [dst-mac] [ip]}`

Режим ввода команд: глобальная конфигурация

ip arp inspection vlan logging

Используйте эту команду, чтобы включить запись в журнал неверных ARP-пакетов на списке диапазонов VLAN, разделенных запятой.

Значение по умолчанию: включено

Формат: `ip arp inspection vlan vlan-list logging`

Режим ввода команд: глобальная конфигурация

no ip arp inspection vlan logging

Используйте эту команду, чтобы выключить запись в журнал неверных ARP-пакетов на списке диапазонов VLAN, разделенных запятой.

Формат: `no ip arp inspection vlan vlan-list logging`

Режим ввода команд: глобальная конфигурация

ip arp inspection trust

Используйте данную команду, чтобы настроить интерфейс или диапазон интерфейсов как доверенный для Dynamic ARP Inspection.

Значение по умолчанию: включено

Формат: `ip arp inspection trust`

Режим ввода команд: конфигурирование интерфейса

no ip arp inspection trust

Используйте данную команду, чтобы настроить интерфейс или диапазон интерфейсов как ненадежный для Dynamic ARP Inspection.

Формат: `no ip arp inspection trust`

Режим ввода команд: конфигурирование интерфейса

ip arp inspection limit

Используйте данную команду, чтобы настроить ограничение скорости входящего трафика и значения интервала всплесков для интерфейса или диапазона интерфейсов. Настройка лимита как none означает, что интерфейс не ограничен в скорости для Dynamic ARP Inspections. Максимальное значение пакетов в секунду (pps), показанное в диапазоне для опции скорости, может быть больше, чем предел возможностей аппаратного обеспечения. Поэтому необходимо быть в курсе производительности коммутатора и соответственно настраивать pps.

Интерфейс будет принимать ограничение скорости для доверенных интерфейсов, но ограничение не будет применяться, если интерфейс настроен как ненадежный.

Значение по умолчанию: 15 pps для скорости и 1 секунда для интервала-всплеска

Формат: `ip arp inspection limit {rate pps [burst interval seconds] | none}`

Режим ввода команд: конфигурирование интерфейса

no ip arp inspection limit

Используйте данную команду, чтобы установить ограничение скорости входящего трафика и значения интервала всплесков для интерфейса в значения по умолчанию.

Формат: `no ip arp inspection limit`

Режим ввода команд: конфигурирование интерфейса

ip arp inspection filter

Используйте эту команду, чтобы настроить ARP ACL, используемый для фильтрации неверных ARP-пакетов на списке диапазонов VLAN, разделенных запятой. Если указано ключевое слово static, пакеты, не совпадающие с указанным разрешением, отбрасываются без проверки соответствия с привязками DHCP Snooping.

Значение по умолчанию: ARP ACL для VLAN не настроен

Формат: `ip arp inspection filter acl-name vlan vlan-list [static]`

Режим ввода команд: глобальная конфигурация

no ip arp inspection filter

Используйте эту команду, чтобы сбросить настройки ARP ACL, используемого для фильтрации неверных ARP-пакетов на списке диапазонов VLAN, разделенных запятой.

Формат: `no ip arp inspection filter acl-name vlan vlan-list [static]`

Режим ввода команд: глобальная конфигурация

arp access-list

Команда создает ARP ACL.

Формат: `arp access-list acl-name`

Режим ввода команд: глобальная конфигурация

no arp access-list

Используйте эту команду, чтобы удалить ARP ACL.

Формат: `no arp access-list acl-name`

Режим ввода команд: глобальная конфигурация

permit ip host mac host

Используйте данную команду, чтобы настроить правило для комбинации IP-адреса и MAC-адреса, используемой при проверке ARP-пакетов.

Формат: `permit ip host sender-ip mac host sender-mac`

Режим ввода команд: конфигурирование списка контроля доступа ARP

no permit ip host mac host

Используйте данную команду, чтобы удалить правило для комбинации IP-адреса и MAC-адреса.

Формат: `no permit ip host sender-ip mac host sender-mac`

Режим ввода команд: конфигурирование списка контроля доступа ARP

show ip arp inspection

Команда отображает глобальную конфигурацию Dynamic ARP Inspection и настройки на всех VLAN. С аргументом vlan-list (т. е. диапазоны VLAN, разделенные запятой) команда отобразит глобальную конфигурацию и настройки всех VLAN для указанного списка VLAN. Режим глобальной конфигурации включает в себя информацию проверок source mac, destination mac и invalid IP.

Формат: `show ip arp inspection [{interfaces unit/slot/port| vlan vlan-list]`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
Source MAC Validation	Показывает, включена ли проверка MAC-адресов источников ARP-кадров.
Destination MAC Validation	Показывает, включена ли проверка MAC-адресов места назначения ARP-кадров.
IP Address Validation	Показывает, включена ли проверка IP-адресов.
VLAN	Идентификатор VLAN для каждой отображаемой записи.
Configuration	Показывает, включен ли DAI на каждой VLAN.
Log Invalid	Показывает, включена ли на VLAN запись в жернал неверных ARP-пакетов.
ACL Name	Имя ARP ACL, если таковой настроен на VLAN.
Static Flag	Показывает, настроен ли ARP ACL на VLAN как статичный.

show ip arp inspection statistics

Используйте данную команду для отображения статистики ARP-пакетов, обработанных функцией Dynamic ARP Inspection. Используйте аргумент vlan-list, чтобы отобразить статистику для всех VLAN в списке, где включена DAI. Укажите один аргумент vlan, чтобы команда отобразила статистику для этой VLAN. Если ни один аргумент не указан, команда перечисляет сводную информацию по переадресованным и отброшенным ARP-пакетам.

Формат: `show ip arp inspection statistics [vlan vlan-list]`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
VLAN	Идентификатор VLAN для каждой отображаемой строки.
Forwarded	Общее количество действительных ARP-пакетов, переадресованных в данной VLAN.
Dropped	Общее количество недействительных ARP-пакетов, отброшенных в данной VLAN.
DHCP Drops	Количество пакетов, отброшенных по причине несоответствия с базой данных DHCP Snooping.
ACL Drops	Количество пакетов, отброшенных по причине несоответствия с правилом ARP ACL.
DHCP Permits	Количество пакетов, разрешенных по причине соответствия с базой данных DHCP Snooping.
ACL Permits	Количество пакетов, разрешенных по причине соответствия с правилом ARP ACL.
Bad Src MAC	Количество пакетов, отброшенных по причине неудачного прохождения проверки MAC-адреса источника.
Bad Dest MAC	Количество пакетов, отброшенных по причине неудачного прохождения проверки MAC-адреса места назначения.
Invalid IP	Количество пакетов, отброшенных по причине неудачных проверок IP.

clear ip arp inspection statistics

Данная команда сбрасывает статистику Dynamic ARP Inspection на всех VLAN.

Значение по умолчанию: none

Формат: `clear ip arp inspection statistics`

Режим ввода команд: привилегированный

show ip arp inspection interfaces

Используйте данную команду для отображения настроек Dynamic ARP Inspection для всех интерфейсов с включенной DAI. Интерфейс считается доступным для DAI, если хотя бы одна VLAN, участником которой является данный интерфейс, доступна для DAI. При аргументе интерфейса *unit/slot/port* команда отобразит значения для указанного интерфейса, независимо от того, доступен он для DAI или нет.

Формат: `show ip arp inspection interfaces [`*`unit/slot/port`*`]`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
Interface	Идентификатор интерфейса для каждой отображаемой строки.
Trust State	Является ли интерфейс доверенным для DAI.
Rate Limit	Настроенное значение ограничения скорости в пакетах в секунду.
Burst Interval	Настроенное значение интервала всплеска в секундах.

show arp access-list

Команда отображает настроенные ARP ACL с правилами. При указании имени ARP ACL как аргумента, команда отобразит только правила указанного ARP ACL.

Формат: `show arp access-list [acl-name]`

Режим ввода команд: привилегированный
пользовательский

9.31 Команды настройки IGMP Snooping

В этой части перечислены команды, используемые для настройки IGMP Snooping. Программное обеспечение поддерживает IGMP версий 1, 2 и 3. Функция IGMP Snooping может помочь сохранить пропускную способность, т. к. она позволяет коммутатору пересылать многоадресный трафик только для подключенных хостов, которые запрашивают многоадресный трафик. IGMPv3 добавляет к версиям IGMP 1 и 2 возможности фильтрации трафика.

В данном примечании разъясняется определение приоритетов конфигураций MGMD Snooping. Многие команды из протокола IGMP/MLD Snooping доступны и в режиме конфигурирования интерфейса, и в режиме конфигурирования VLAN. В оперативном отношении система для большинства конфигураций выбирает значения сконфигурированные на VLAN, значениям, которые настроены на интерфейсе, если интерфейс участвует в VLAN.

set igmp

Эта команда включает IGMP Snooping в системе (в режиме глобальной конфигурации), на интерфейсе или диапазоне интерфейсов. Команда также включает IGMP Snooping в определенной VLAN (режим настройки VLAN) и может запустить IGMP Snooping на всех интерфейсах, участвующих в VLAN.

Если интерфейс, на котором включено IGMP Snooping, делают доступным для маршрутизации или включают в список участников LAG, функции IGMP Snooping на данном интерфейсе выключаются. Функции IGMP Snooping на интерфейсе включаются повторно, если интерфейс выключить для маршрутизации или удалить его из участников агрегированного интерфейса.

IGMP-snooping поддерживает следующие действия.

- Проверка контрольной суммы заголовка IP (а также контрольной суммы заголовка IGMP) и отбрасывание кадра после ошибки в контрольной сумме.
- Ведение записей таблицы пересылки на основе MAC-адресов в сравнении с IP-адресами.
- Пересылка незарегистрированных пакетов многоадресной передачи на все порты в VLAN.

Значение по умолчанию: выключено

Формат: `set igmp [vlan_id]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
конфигурирование VLAN

no set igmp

Эта команда выключает IGMP Snooping в системе, на интерфейсе, диапазоне интерфейсов или в VLAN.

Формат: `no set igmp [vlan_id]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

конфигурирование VLAN

set igmp header-validation

Эта команда включает для IGMP-сообщений проверку заголовков. Когда проверка заголовков включена, IGMP Snooping проверяет следующие параметры.

- Поле TTL в заголовке IP протокола IGMP (и отбрасывает пакеты, где TTL не равно 1). Поле TTL всегда должно быть установлено как 1 в заголовках IP отчетов и запросов IGMP.
- Наличие маршрутизатора опции оповещений (9404) в заголовке IP-пакета сообщения IGMPv2 (и отбрасывает пакеты, которые не включают эту опцию).
- Наличие маршрутизатора опции оповещений (9404) и ToS байт = 0xC0 (Internet Control) в заголовке IP-пакета для IGMPv3 сообщения (и отбрасывает пакеты, которые не включают эти варианты).

Значение по умолчанию: включено

Формат: `set igmp header-validation`

Режим ввода команд: глобальная конфигурация

no set igmp header-validation

Эта команда выключает проверку заголовков для IGMP-сообщений.

Формат: `no set igmp header-validation`

Режим ввода команд: глобальная конфигурация

set igmp interfacemode

Данная команда включает IGMP Snooping на всех интерфейсах. Если интерфейс, на котором включено IGMP Snooping, делают доступным для маршрутизации или включают в список участников LAG, функции IGMP Snooping на данном интерфейсе выключаются. Функции IGMP Snooping на интерфейсе включаются повторно, если этот интерфейс выключить для маршрутизации или удалить его из участников агрегированного интерфейса.

Значение по умолчанию: выключено

Формат: `set igmp interfacemode`

Режим ввода команд: глобальная конфигурация

no set igmp interfacemode

Эта команда выключает IGMP Snooping на всех интерфейсах.

Формат: `no set igmp interfacemode`

Режим ввода команд: глобальная конфигурация

set igmp fast-leave

Данная команда включает режим немедленного удаления групп IGMP Snooping на выбранном интерфейсе, диапазоне интерфейсов или VLAN. Запуск немедленной очистки позволяет коммутатору немедленно удалить интерфейс LAN 2 уровня из записи таблицы соответствия при получении IGMP Leave-сообщения для соответствующей многоадресной группы.

Включать административный режим немедленного удаления групп следует только на VLAN. Это предотвращает случайный сброс других хостов, которые подключены к одному порту LAN уровня, но по-прежнему заинтересованы в получении трафика многоадресной рассылки, направленного на эту группу. Кроме того, процессы немедленной очистки поддерживаются только хостами с версией IGMP 2.

Значение по умолчанию: выключено

Формат: `set igmp fast-leave [vlan_id]`

Режим ввода команд: конфигурирование интерфейса конфигурирование диапазона интерфейсов конфигурирование VLAN

no set igmp fast-leave

Эта команда выключает административный режим немедленного удаления групп IGMP Snooping на выбранном интерфейсе.

Формат: `no set igmp fast-leave [vlan_id]`

Режим ввода команд: конфигурирование интерфейса конфигурирование диапазона интерфейсов конфигурирование VLAN

set igmp groupmembership-interval

Эта команда устанавливает время интервала участия в группе IGMP на VLAN, одном интерфейсе, диапазоне интерфейсов или всех интерфейсах. Интервал участия в группе IGMP — это время в секундах, которое коммутатор ожидает получения запроса от определенной группы на определенном интерфейсе перед тем, как удалить интерфейс из записи. Это значение должно быть больше значения максимального времени отклика IGMPv3. Диапазон — от 2 до 3600 секунд.

Значение по умолчанию: 260 секунд

Формат: `set igmp groupmembership-interval [vlan_id] 2-3600`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация
конфигурирование VLAN

no set igmp groupmembership-interval

Данная команда устанавливает время интервала участия в группе IGMP в значение по умолчанию.

Формат: `no set igmp groupmembership-interval [vlan_id]`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация
конфигурирование VLAN

set igmp maxresponse

Эта команда устанавливает максимальное время отклика IGMP в системе, на определенном интерфейсе, VLAN или диапазоне интерфейсов. Максимальное время отклика IGMP — это время ожидания коммутатора в секундах после того, как коммутатор пошлет запрос на интерфейс, не получив запрос от определенной группы на этом интерфейсе. Это значение должно быть меньше, чем значение интервала запросов IGMP. Диапазон — от 1 до 25 секунд.

Значение по умолчанию: 10 секунд

Формат: `set igmp maxresponse [vlan_id] 1-25`

Режим ввода команд: глобальная конфиграция
конфигурирование интерфейса
конфигурирование VLAN

no set igmp maxresponse

Эта команда устанавливает максимальное время отклика (на интерфейсе или VLAN) в значение по умолчанию.

Формат: `no set igmp maxresponse [vlan_id]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
конфигурирование VLAN

set igmp mcrtrexpiretime

Данная команда устанавливает продолжительность для Multicast Router Present Expiration. Это значение устанавливается для системы, отдельного интерфейса или VLAN, или на диапазоне интерфейсов. Время в секундах, которое коммутатор ожидает принятия сообщений на интерфейсе, прежде чем интерфейс удаляется из списка интерфейсов с подсоединенными маршрутизаторами многоадресной рассылки. Диапазон — от 0 до 3600 секунд. Значение 0 означает бесконечное время, т. е. отсутствие срока истечения.

Значение по умолчанию: 0

Формат: `set igmp mcrtrexpiretime [vlan_id] 0-3600`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
конфигурирование VLAN

no set igmp mcrtrexpiretime

Эта команда устанавливает время Multicast Router Present Expiration в значение по умолчанию (0). Это значение устанавливается для системы, отдельного интерфейса или VLAN.

Формат: `no set igmp mcrtrexpiretime [vlan_id]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
конфигурирование VLAN

Формат: `no set igmp mcrtrexpiretime vlan_id`

Режим ввода команд: конфигурирование VLAN

set igmp mrouter

Эта команда настраивает идентификатор VLAN (*vlan_id*), на которой включен режим маршрутизатора многоадресной рассылки.

Формат: `set igmp mrouter vlan_id`

Режим ввода команд: конфигурирование интерфейса

no set igmp mrouter

Эта команда выключает режим маршрутизатора многоадресной рассылки для определенного идентификатора VLAN (*vlan_id*).

Формат: `no set igmp mrouter vlan_id`

Режим ввода команд: конфигурирование интерфейса

set igmp mrouter interface

Данная команда настраивает интерфейс или диапазон интерфейсов как интерфейс маршрутизатора многоадресной рассылки. В этом режиме интерфейс рассматривается как интерфейс маршрутизатора многоадресной рассылки во всех VLAN.

Значение по умолчанию: выключено

Формат: `set igmp mrouter interface`

Режим ввода команд: конфигурирование интерфейса

no set igmp mrouter interface

Данная команда выключает статус интерфейса как статично настроенного интерфейса маршрутизатора многоадресной рассылки.

Формат: `no set igmp mrouter interface`

Режим ввода команд: конфигурирование интерфейса

set igmp report-suppression

Используйте эту команду для сдерживания IGMP-сообщений на данном идентификаторе VLAN. Чтобы оптимизировать несколько сообщений, проходящих через сеть без каких-либо дополнительных преимуществ, применяется механизм сдерживания сообщений. Когда более одного клиента отвечают на запрос MGMD для того же адреса группы мультивещания в max-response-time, на запрос адресуется только первый отклик, а другие сдерживаются на коммутаторе.

Значение по умолчанию: выключено

Формат: `set igmp report-suppression vlan-id`

Режим ввода команд: конфигурирование VLAN

Параметр	***Описание***
vlan-id	Действительный идентификатор VLAN. Допустимые значения: от 1 до 4094.

no set igmp report-suppression

Используйте эту команду для возвращения настроек системы по умолчанию.

Формат: `no set igmp report-suppression`

Режим ввода команд: конфигурирование VLAN

show igmpsnooping

Данная команда отображает информацию IGMP Snooping для указанного *unit/slot/port* или VLAN. Настроенная информация отобразится независимо от того, включена функция IGMP Snooping или нет.

Формат: `show igmpsnooping [unit/slot/port | vlan_id]`

Режим ввода команд: привилегированный

Если необязательные аргументы *unit/slot/port* или *vlan_id* не используются, команда отобразит следующую информацию.

Термин	***Значение***
Admin Mode	Указывает, активна ли функция IGMP Snooping на коммутаторе.
Multicast Control Frame Count	Количество многоадресных кадров управления, которые обрабатываются процессором.
Interface Enabled for IGMP Snooping	Список интерфейсов, где включена IGMP Snooping.
VLANS Enabled for IGMP Snooping	Список VLAN, где включена IGMP Snooping.

Если указано значение *unit/slot/port*, отображается следующая информация:

Термин	***Значение***
IGMP Snooping Admin Mode	Указывает, активна ли IGMP Snooping на интерфейсе.
Fast Leave Mode	Указывает, активно ли на интерфейсе немедленное удаление групп IGMP Snooping.
Group Membership Interval	Время в секундах, которое коммутатор ожидает получения сообщения от определенной группы на определенном интерфейсе перед тем, как удалить интерфейс из записи. Это значение настраивается.
Maximum Response Time	Время ожидания коммутатора в секундах после того, как коммутатор пошлет запрос на интерфейс, не получив сообщение от определенной группы на этом интерфейсе. Это значение настраивается.
Multicast Router Expiry Time	Время ожидания коммутатора перед тем, как интерфейс удаляется из списка интерфейсов с подсоединенными маршрутизаторами многоадресной рассылки. Интерфейс удаляется, если не получено сообщение. Это значение настраивается.

Если указать значение *vlan_id*, отображается следующая информация.

Термин	***Значение***
VLAN ID	Идентификатор VLAN.
IGMP Snooping Admin Mode	Указывает, активна ли на VLAN функция IGMP Snooping.
Fast Leave Mode	Указывает, активно ли на VLAN немедленное удаление групп IGMP Snooping.
Group Membership Interval (secs)	Время в секундах, которое коммутатор ожидает получения сообщения от определенной группы на определенном интерфейсе, который участвует в VLAN, перед тем, как удалить интерфейс из записи. Это значение настраивается.
Maximum Response Time (secs)	Время ожидания коммутатора в секундах после того, как коммутатор пошлет запрос на интерфейс, который участвует в VLAN, не получив сообщения от определенной группы на этом интерфейсе. Это значение настраивается.
Multicast Router Expiry Time (secs)	Время ожидания коммутатора перед тем, как интерфейс, который участвует в VLAN, удаляется из списка интерфейсов с подсоединенными маршрутизаторами многоадресной рассылки. Интерфейс удаляется, если не получено сообщение. Это значение настраивается.
Report Suppression Mode	Указывает, включено ли сдерживание IGMP-сообщений.

show igmpsnooping mrouter interface

Данная команда отображает информацию о статично настроенных портах IGMP-маршрутизатора.

Формат: `show igmpsnooping mrouter interface` *`unit/slot/port`*

Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Порт, для которого отображается информация маршрутизатора многоадресной рассылки.
Multicast Router Attached	Указывает, включен ли на интерфейсе маршрутизатор многоадресной рассылки статично.
VLAN ID	Список VLAN, участником которых является интерфейс.

show igmpsnooping mrouter vlan

Данная команда отображает информацию о статично настроенных портах IGMP-маршрутизатора.

Формат: `show igmpsnooping mrouter vlan` *`unit/slot/port`*

Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Порт, для которого отображается информация маршрутизатора многоадресной рассылки.
VLAN ID	Список VLAN, участником которых является интерфейс.

show igmpsnooping ssm

Эта команда отображает информацию об операциях Source Specific Multicasting (SSM) по записи, группе или статистике. SSM доступны только при использовании IGMPv3 и MLDv2.

Формат: `show igmpsnooping ssm {entries | groups | stats}`

Режим ввода команд: привилегированный

show mac-address-table igmpsnooping

Данная команда отображает записи IGMP Snooping в таблице MFDB.

Формат: `show mac-address-table igmpsnooping`

Режим ввода команд: привилегированный

Термин	*Значение*
VLAN ID	VLAN, в которой был определен MAC-адрес.
MAC Address	Групповой MAC-адрес, для которого коммутатор переадресует или фильтрует информацию. Указывается в формате шести двузначных номеров шестнадцатеричной системы, разделенных двоеточиями, например: 01:23:45:67:89:AB.
Type	Тип записи, который может быть статичным (добавлена пользователем) или динамическим (добавлен в таблицу в результате процесса работы протокола).
Description	Текстовое описание данной записи таблицы многоадресной коммутации.

Interfaces	Список интерфейсов, которые назначены для переадресации (Fwd:) и фильтрации (Flt:).

9.32 Команды настройки опрашивающего устройства IGMP Snooping

В IGMP Snooping требуется, чтобы центральный коммутатор или маршрутизатор периодически отправляли запросы на все конечные устройства сети для анонсирования участия в многоадресных рассылках. Центральное устройство называется опрашивающим устройством IGMP. Ответы на IGMP-запросы (IGMP Query), известные как IGMP-сообщения (IGMP Report), держат коммутатор в курсе текущего участия каждого порта в многоадресной рассылке. Если коммутатор периодически не получает обновленной информации об участниках, он останавливает переадресацию многоадресного трафика на соответствующие порты конечных устройств.

Эта часть описывает команды, используемые для настройки и отображения информации об опрашивающих устройствах IGMP Snooping в сети и отдельно на VLAN.

В данном примечании разъясняется определение приоритетов конфигураций MGMD Snooping. Многие команды из протокола IGMP/MLD Snooping доступны и в режиме конфигурирования интерфейса, и в режиме конфигурирования VLAN. В оперативном отношении система для большинства конфигураций выбирает значения сконфигурированные на VLAN, значениям, которые настроены на интерфейсе, если интерфейс участвует в VLAN.

set igmp querier

Используйте данную команду, чтобы включить опрашивающее устройство IGMP Snooping в системе (в режиме глобальной конфигурации) или на VLAN. С помощью команды можно указать IP-адрес, который опрашивающее устройство отслеживания будет использовать в качестве адреса-источника во время генерации периодических запросов.

Если на VLAN включено опрашивающее устройство IGMP Snooping, а сама функция выключена, опрашивание на этой VLAN также будет выключено. Опрашивающее устройство включится снова, когда на VLAN будет включена функция IGMP Snooping.

IP-адрес опрашивающего устройства IGMP-отслеживания, назначенный VLAN, имеет более высокий приоритет, чем сконфигурированный глобально.

Приложение опрашивающего устройства IGMP Snooping поддерживает отправку периодических общих запросов на VLAN, чтобы запросить отчет об участии.

Значение по умолчанию: выключено

Формат: `set igmp querier [vlan-id] [address ipv4_address]`

Режим ввода команд: глобальная конфигурация
VLAN Mode

no set igmp querier

Используйте данную команду, чтобы выключить в системе опрашивающее устройство IGMP Snooping. Используйте необязательный параметр address, чтобы установить адрес опрашивающего как 0.0.0.0.

Формат: `no set igmp querier [vlan-id] [address]`

Режим ввода команд: глобальная конфигурация

VLAN Mode

set igmp querier query-interval

Используйте эту команду, чтобы установить интервал запроса опрашивающего устройства IGMP. Это время в секундах, которое коммутатор ожидает перед тем, как повторно послать общий запрос.

Значение по умолчанию: 60

Формат: `set igmp querier query-interval` *`1-1800`*

Режим ввода команд: глобальная конфигурация

no set igmp querier query-interval

Используйте данную команду, чтобы установить интервал запроса опрашивающего устройства IGMP в значение по умолчанию.

Формат: `no set igmp querier query-interval`

Режим ввода команд: глобальная конфигурация

set igmp querier timer expiry

Используйте данную команду, чтобы установить период истечения запроса IGMP. Это период времени, в течение которого коммутатор остается в режиме Non-Querier с тех пор, как он обнаружил, что в сети присутствует многоадресное опрашивающее устройство.

Значение по умолчанию: 125 секунд

Формат: `set igmp querier timer expiry` *`60-300`*

Режим ввода команд: глобальная конфигурация

no set igmp querier timer expiry

Используйте эту команду, чтобы установить период истечения запроса IGMP в значение по умолчанию.

Формат: `no set igmp querier timer expiry`

Режим ввода команд: глобальная конфигурация

set igmp querier version

Используйте эту команду, чтобы установить версию запроса IGMP, который коммутатор будет отправлять периодически.

Значение по умолчанию: 1

Формат: `set igmp querier version` *`1-2`*

Режим ввода команд: глобальная конфигурация

no set igmp querier version

Используйте эту команду, чтобы установить версию опрашивающего устройства IGMP в значение по умолчанию.

Формат: `no set igmp querier version`

Режим ввода команд: глобальная конфигурация

set igmp querier election participate

Используйте данную команду, чтобы позволить опрашивающему устройству отслеживания участвовать в процессе выбора опрашивающего, когда оно обнаружит присутствие еще одного опрашивающего в сети VLAN. При этом режиме, если опрашивающий отслеживания обнаруживает, что адрес другого опрашивающего лучше (меньше), чем его адрес, он перестает посылать периодические запросы. Если опрашивающий выиграет в выборе, он продолжит посылать периодические запросы.

Значение по умолчанию: выключено

Формат: `set igmp querier election participate`

Режим ввода команд: конфигурирование VLAN

no set igmp querier election participate

Используйте данную команду, чтобы запретить опрашивающему устройству участвовать в процессе выбора опрашивающего, но при этом выходить из режима опрашивающего устройства, как только он обнаружит присутствие другого опрашивающего в той же VLAN.

Формат: `no set igmp querier election participate`

Режим ввода команд: конфигурирование VLAN

show igmpsnooping querier

Используйте эту команду, чтобы отобразить информацию опрашивающего устройства IGMP Snooping. Настроенная информация отобразится независимо от того, включена функция IGMP Snooping или нет.

Формат: `show igmpsnooping querier [{detail | vlan vlanid}]`

Режим ввода команд: привилегированный

Если опциональный параметр *vlanid* не используется, команда отобразит информацию, представленную в таблице ниже.

Термин	***Значение***
Admin Mode	Указывает, активно ли на коммутаторе опрашивающее устройство IGMP Snooping.
Admin Version	Версия IGMP, которая будет использоваться при отправке запросов.
Querier Address	IP-адрес, используемый в IPv4-заголовке при отправке IGMP-запросов. Настраивается с помощью соответствующей команды.
Query Interval	Время в секундах, которое ожидает опрашивающее устройство перед тем, как отправить периодический общий запрос.
Expiry Interval	Количество времени, которое ожидает не опрашивающее устройство перед тем, как перейти в режим опрашивающего.

Если указать значение *vlanid*, команда отобразит информацию, представленную в таблице ниже.

Термин	***Значение***
VLAN Admin Mode	Указывает, активно ли опрашивающее устройство IGMP Snooping на данной VLAN.

VLAN Operational State	Указывает, в каком статусе находится опрашивающее устройство IGMP Snooping. Если коммутатор находится в статусе *Querier*, он будет отправлять периодические общие запросы. При статусе *Non-Querier* он будет ожидать перемещения в статус *Querier* и не будет отправлять запросов.
VLAN Operational Max Response Time	Время ожидания после получения Leave-сообщения, прежде чем удалить Leave хоста. Это значение рассчитывается динамически на основании запросов, получаемых от сети. Если коммутатор Snooping находится в режиме опрашивающего, это значение будет равно настроенному.
Querier Election Participation	Указывает, участвует ли опрашивающее устройство IGMP Snooping в выборах опрашивающего, если обнаруживает присутствие другого опрашивающего в VLAN.
Querier VLAN Address	IP-адрес, используемый в IPv4-заголовке при отправке IGMP-запросов в данной VLAN. Настраивается с помощью соответствующей команды.
Operational Version	Версия IGMP, используемая при отправке IGMP-запросов на данной VLAN.
Last Querier Address	Указывает IP-адрес опрашивающего устройства, с которого был получен последний запрос.
Last Querier Version	Указывает версию IGMP последнего опрашивающего, от которого был получен запрос на данной VLAN.

При использовании необязательного аргумента *detail* команда отображает глобальную информацию и данные по всем сетям VLAN, включенным для данного опрашивающего устройства.

9.33 Команды настройки MLD Snooping

Этот раздел описывает команды, используемые для настройки MLD Snooping. В IPv4 коммутаторы уровня 2 могут использовать IGMP Snooping, чтобы ограничить поток многоадресного трафика путем динамической конфигурации интерфейсов уровня 2 таким образом, чтобы многоадресный трафик направлялся только интерфейсам, связанным с IP-адресами многоадресной рассылки. MLD Snooping в IPv6 выполняет похожую функцию. С функцией MLD Snooping данные многоадресной рассылки IPv6 выборочно направляется к списку портов, которые желают получить данные, вместо передачи на все порты VLAN. Список портов составляется путем отслеживания многоадресных IPv6-пакетов управления.

В данном примечании разъясняется определение приоритетов конфигураций MGMD Snooping. Многие команды из протокола IGMP/MLD Snooping доступны и в режиме конфигурирования интерфейса, и в режиме конфигурирования VLAN. В оперативном отношении система для большинства конфигураций выбирает значения сконфигурированные на VLAN, значениям, которые настроены на интерфейсе, если интерфейс участвует в VLAN.

set mld

Эта команда включает MLD Snooping в системе (режим глобальной конфигурации) или на интерфейсе (режим конфигурирования интерфейса). Команда также включает MLD Snooping на определенной VLAN и на всех интерфейсах, участвующих в данной VLAN.

Если интерфейс, на котором включено MLD Snooping, делают доступным для маршрутизации или включают в список участников LAG, функции MLD Snooping на данном интерфейсе выключаются. MLD Snooping запускается на нем снова, если выключить маршрутизацию или удалить интерфейс из участников LAG.

MLD Snooping поддерживает следующие действия.

- Подтверждение адреса, версии, согласованность длины полезной нагрузки и отбрасывание кадра при ошибке.
- Ведение записей таблицы пересылки на основе MAC-адресов в сопоставлении с IPv6-адресами.
- Пересылка незарегистрированных пакетов многоадресной передачи на все порты в VLAN.

Значение по умолчанию: выключено

Формат: `set mld vlanid`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
VLAN Mode

no set mld

Используйте эту команду для выключения MLD Snooping в системе.

Формат: `set mld vlanid`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
VLAN Mode

set mld interfacemode

Эта команда включает MLD Snooping на всех интерфейсах. Если интерфейс, на котором включено MLD Snooping, делают доступным для маршрутизации или включают в список участников LAG, функции MLD Snooping на данном интерфейсе выключаются. MLD Snooping запускается на нем снова, если выключить маршрутизацию или удалить интерфейс из участников LAG.

Значение по умолчанию: выключено

Формат: `set mld interfacemode`

Режим ввода команд: глобальная конфигурация

no set mld interfacemode

Используйте данную команду, чтобы выключить MLD Snooping на всех интерфейсах.

Формат: `no set mld interfacemode`

Режим ввода команд: глобальная конфигурация

set mld fast-leave

Используйте данную команду, чтобы включить административный режим быстрого удаления групп MLD Snooping на выбранном интерфейсе или VLAN. Запуск быстрого удаления позволяет коммутатору немедленно удалять интерфейс LAN уровня 2 из записи таблицы переадресации при получении MLD-сообщения о удалении для многоадресной группы без предварительной отправки общих запросов на основе MAC к тому интерфейсу.

Включать административный режим быстрого удаления следует только на VLAN, где хост соединен с каждым портом LAN 2 уровня. Это предотвращает случайный сброс других хостов, которые подключены к тому же порту LAN 2 уровня, но по-прежнему заинтересованных в получении трафика многоадресной рассылки, направленного на эту группу.

Значение по умолчанию: выключено

Формат: `set mld fast-leave vlanid`

Режим ввода команд: конфигурирование интерфейса
VLAN Mode

no set mld fast-leave

Используйте эту команду, чтобы выключить административный режим быстрого удаления групп MLD Snooping на выбранном интерфейсе.

Формат: `no set mld fast-leave vlanid`

Режим ввода команд: конфигурирование интерфейса
VLAN Mode

set mld groupmembership-interval

Используйте данную команду, чтобы установить время интервала участия в группе MLD на VLAN, одном интерфейсе или всех интерфейсах. Интервал участия в группе MLD — это время в секундах, которое коммутатор ожидает получения сообщения от определенной группы на определенном интерфейсе перед тем, как удалить интерфейс из группы. Это значение должно быть больше значения максимального времени отклика MLDv2. Диапазон — от 2 до 3600 секунд.

Значение по умолчанию: 260 секунд

Формат: `set mld groupmembership-interval vlanid 2-3600`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация
VLAN Mode

no set groupmembership-interval

Используйте эту команду, чтобы установить интервал участия в группе MLD в значение по умолчанию.

Формат: `no set mld groupmembership-interval`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация
VLAN Mode

set mld maxresponse

Используйте данную команду, чтобы установить максимальное время отклика MLDv2 для всей системы, на определенном интерфейсе или VLAN. Максимальное время отклика MLDv2 — это время ожидания коммутатора в секундах после того, как пошлет запрос на интерфейс, не получив сообщение от определенной группы на этом интерфейсе. Это значение должно быть меньше, чем значение интервала запросов MLD. Диапазон — от 1 до 65 секунд.

Значение по умолчанию: 10 секунд

Формат: `set mld maxresponse 1-65`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
VLAN Mode

no set mld maxresponse

Используйте эту команду, чтобы установить максимальное время отклика (на интерфейсе или VLAN) в значение по умолчанию.

Формат: `no set mld maxresponse`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
VLAN Mode

set mld mcrtexpiretime

Данная команда устанавливает время Multicast Router Present Expiration. Это время устанавливается для системы, отдельного интерфейса или VLAN. Время в секундах, которое коммутатор ожидает принятия запросов на интерфейсе, прежде чем интерфейс удаляется из списка интерфейсов с подсоединенными маршрутизаторами многоадресной рассылки. Диапазон — от 0 до 3600 секунд. Значение 0 означает бесконечное время, т. е. отсутствие срока истечения.

Значение по умолчанию: 0

Формат: `set mld mcrtexpiretime` *`vlanid 0-3600`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no set mld mcrtexpiretime

Эта команда устанавливает время Multicast Router Present Expiration в значение по умолчанию (0). Это значение устанавливается для системы, отдельного интерфейса или VLAN.

Формат: `no set mld mcrtexpiretime` *`vlanid`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

set mld mrouter

Используйте эту команду для настройки VLAN, на которой включен режим маршрутизатора многоадресной рассылки.

Формат: `set mld mrouter` *`vlanid`*

Режим ввода команд: конфигурирование интерфейса

no set mld mrouter

Используйте эту команду для выключения режима маршрутизатора многоадресной рассылки для VLAN с указанным идентификатором.

Формат: `no set mld mrouter` *`vlanid`*

Режим ввода команд: конфигурирование интерфейса

set mld mrouter interface

Используйте данную команду для настройки интерфейса как интерфейса с подключенным маршрутизатором многоадресной рассылки. В этом режиме интерфейс во всех VLAN рассматривается как интерфейс маршрутизатора многоадресной рассылки.

Значение по умолчанию: выключено

Формат: `set mld mrouter interface`

Режим ввода команд: конфигурирование интерфейса

no set mld mrouter interface

Используйте данную команду для выключения статуса интерфейса как статично настроенного интерфейса маршрутизатора многоадресной рассылки.

Формат: `no set mld mrouter interface`

Режим ввода команд: конфигурирование интерфейса

show mldsnooping

Данная команда используется для отображения информации MLD Snooping. Настроенная информация отображается независимо от того, включена функция MLD Snooping или нет.

Формат: `show mldsnooping [unit/slot/port | vlanid]`

Режим ввода команд: привилегированный

Если необязательные аргументы *unit/slot/port* или *vlanid* не используются, команда отобразит следующую информацию.

Термин	***Значение***
Admin Mode	Указывает, активна ли функция MLD Snooping на коммутаторе.
Interfaces Enabled for MLD Snooping	Список интерфейсов, на которых включена функция MLD Snooping.
MLD Control Frame Count	Отображает количество MLD-кадров управления, обработанных процессором.
VLANs Enabled for MLD Snooping	Список VLAN, на которых включена MLD Snooping.

Если указано значение *unit/slot/port*, отображается следующая информация.

Термин	***Значение***
MLD Snooping Admin Mode	Указывает, активна ли MLD Snooping на интерфейсе.
Fast Leave Mode	Указывает, активно ли на интерфейсе быстрое удаление MLD Snooping.
Group Membership Interval	Время в секундах, которое коммутатор ожидает сообщения от определенной группы на определенном интерфейсе, прежде чем удалить интерфейс из записи. Это значение настраивается.
Max Response Time	Отображает время ожидания коммутатора после того, как пошлет запрос на интерфейс, который участвует в VLAN, не получив сообщения от определенной группы на этом интерфейсе. Это значение настраивается.
Multicast Router Present Expiration Time	Отображает время ожидания коммутатора перед тем, как интерфейс, который участвует в VLAN, удаляется из списка интерфейсов с подсоединенными маршрутизаторами многоадресной рассылки. Интерфейс удаляется, если не получен запрос. Это значение настраивается.

Если указать значение для *vlanid*, команда отобразит следующую информацию:

Термин	***Значение***
VLAN Admin Mode	Указывает, активна ли на VLAN функция MLD Snooping.

show mldsnooping mrouter interface

Команда для отображения информации о статически настроенных интерфейсах с подключенными маршрутизаторами многоадресной рассылки.

Формат: `show mldsnooping mrouter interface` *`unit/slot/port`*

Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Порт, для которого отображается информация маршрутизатора многоадресной рассылки.
Multicast Router Attached	Указывает, включен ли на интерфейсе маршрутизатор многоадресной рассылки статически.
VLAN ID	Список VLAN, участником которых является интерфейс.

show mldsnooping mrouter vlan

Используйте эту команду для отображения информации о статически настроенных интерфейсах с подключенными маршрутизаторами многоадресной рассылки.

Формат: `show mldsnooping mrouter vlan` *`unit/slot/port`*

Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Порт, для которого отображается информация маршрутизатора многоадресной рассылки.
VLAN ID	Список VLAN, участником которых является интерфейс.

show mldsnooping ssm entries

Команда используется для отображения таблицы коммутации многоадресной рассылки, созданной с помощью MLD Snooping.

Данная комбинация {Source, Group, VLAN} может иметь несколько интерфейсов в режиме INCLUDE, и несколько — в режиме EXCLUDE. Для таких случаев для одинаковых комбинаций {Source, Group, VLAN} отображаются две строки.

Формат: `show mldsnooping ssm entries`

Режим ввода команд: привилегированный

Термин	*Значение*
VLAN	VLAN, на которой определена запись.
Group	IPv6-адрес группы многоадресной рассылки.
Source	IPv6-адрес источника.
Source Filter Mode	Режим фильтра источника (Include/Exclude) для указанной группы. 1) Если фильтр источника находится в режиме Include, то IP-адрес источника равен источнику текущей записи, IP-адрес места назначения равен текущей группе записи, и идентификатор VLAN, на который он прибыл, — это VLAN текущей записи. 2) Если фильтр источника находится в режиме Exclude, то IP- адрес источника *не* равен источнику текущей записи, IP-адрес места

	назначения равен текущей группе записи, и идентификатор VLAN, на которую он прибыл, — это VLAN текущей записи.
Interfaces	Указывает список интерфейсов, на которые направляется входящий пакет.

show mldsnooping ssm stats

Используйте данную команду для отображения статистики SSMFDB MLD Snooping. Дополнительных опций у команды нет.

Формат: `show mldsnooping ssm stats`

Режим ввода команд: привилегированный

Термин	*Значение*
Total Entries	Общее возможное количество записей, которые могут быть в SSMFDB MLD Snooping.
Most SSMFDB Entries Ever Used	Наибольшее количество записей, которое было зарегистрировано в SSMFDB MLD Snooping.
Current Entries	Текущее количество записей в SSMFDB MLD Snooping.

show mldsnooping ssm groups

Используйте эту команду, чтобы отобразить информацию об участниках SSM-группы MLD.

Формат: `show mldsnooping ssm groups`

Режим ввода команд: привилегированный

Термин	*Значение*
VLAN	VLAN, на которой получено сообщение MLD v2.
Group	IPv6-адрес группы многоадресной рассылки.
Interface	Интерфейс, на котором получено сообщение MLD v2.
Reporter	IPv6-адрес хоста, который отправил сообщение MLD v2.
Source Filter Mode	Режим источника (Include/Exclude) для указанной группы.
Source Address List	Список IP-адресов источника, для которых запрошена фильтрация источника.

show mac-address-table mldsnooping

Используйте данную команду, чтобы отобразить записи MLD Snooping в таблице коммутации многоадресной рассылки (MFDB).

Формат: `show mac-address-table mldsnooping`

Режим ввода команд: привилегированный

Термин	*Значение*
VLAN ID	VLAN, в которой был определен MAC-адрес.
MAC Address	Групповой MAC-адрес, для которого коммутатор переадресует или фильтрует информацию. Указывается в формате шести двузначных номеров шестнадцатеричной системы, разделенных двоеточиями, например: 01:23:45:67:89:AB.

Type	Тип записи, который может быть статичным (добавлена пользователем) или динамическим (добавлен в таблицу в результате процесса или работы протокола).
Description	Текстовое описание данной записи таблицы многоадресной коммутации.
Interfaces	Список интерфейсов, которые назначены для переадресации (Fwd:) и фильтрации (Flt:).

clear mldsnooping

Данная команда удаляет все записи MLD Snooping в таблице MFDB.

Формат: clear mldsnooping

Режим ввода команд: привилегированный

9.34 Команды настройки опрашивающего устройства MLD Snooping

В контексте IPv6 MLD Snooping требует, чтобы один центральный коммутатор или маршрутизатор периодически отправляли запросы на все конечные устройства сети для подтверждения их участия в многоадресных рассылках. Такое центральное устройство называется опрашивающим устройством MLD. Сообщения на MLD-запросы, также называемые MLD-сообщениями, обновляют данные коммутатора о текущем составе группы многоадресной рассылки с детализацией на уровне портов. Если коммутатор периодически не получает обновленной информации об участниках, он останавливает переадресацию многоадресного трафика на соответствующие порты конечных устройств.

Этот подраздел описывает команды, используемые для настройки и отображения информации о запросах MLD Snooping в сети и отдельно на VLAN.

В данном примечании разъясняется определение приоритетов конфигураций MGMD Snooping. Многие команды из протокола IGMP/MLD Snooping доступны и в режиме конфигурирования интерфейса, и в режиме конфигурирования VLAN. В оперативном отношении система для большинства конфигураций выбирает значения сконфигурированные на VLAN, значениям, которые настроены на интерфейсе, если интерфейс участвует в VLAN.

set mld querier

Используйте данную команду, чтобы включить опрашивающее устройство MLD Snooping в системе (в режиме глобальной конфигурации) или на VLAN. С помощью этой команды можно указать IP-адрес, который опрашивающее устройство будет использовать в качестве адреса-источника при генерации периодических запросов.

Если на VLAN включено опрашивающее устройство MLD Snooping, а сама функция оперативно выключена, опрашивание на этой VLAN также будет выключено. Опрашивающее устройство включится снова на VLAN, когда будет включена функция MLD Snooping.

Опрашивающее устройство MLD Snooping отправляет периодические общие запросы на VLAN, чтобы получить отчет об участниках.

Значение по умолчанию: выключено

Формат: `set mld querier [`*`vlan-id`*`] [address `*`ipv6_address`*`]`

Режим ввода команд: глобальная конфигурация
VLAN Mode

no set mld querier

Используйте эту команду для выключения опрашивающего устройства MLD Snooping в системе. Используйте необязательный параметр address, чтобы сбросить адрес опрашивающего устройства.

Формат: `no set mld querier [vlan-id][address]`

Режим ввода команд: глобальная конфигурация
конфигурирование VLAN

set mld querier query_interval

Используйте эту команду, чтобы установить интервал запроса опрашивающего устройства MLD. Это время в секундах, которое коммутатор ожидает перед тем, как повторно послать общий запрос.

Значение по умолчанию: 60 секунд

Формат: `set mld querier query_interval 1-1800`

Режим ввода команд: глобальная конфигурация

no set mld querier query_interval

Используйте данную команду, чтобы установить интервал запроса опрашивающего устройства MLD в значение по умолчанию.

Формат: `no set mld querier query_interval`

Режим ввода команд: глобальная конфигурация

set mld querier timer expiry

Используйте данную команду, чтобы установить период истечения запроса MLD. Это период времени, в течение которого коммутатор остается в режиме Non-Querier с тех пор, как он обнаружил, что в сети присутствует многоадресное опрашивающее устройство.

Значение по умолчанию: 60 секунд

Формат: `set mld querier timer expiry 60-300`

Режим ввода команд: глобальная конфигурация

no set mld querier timer expiry

Используйте эту команду, чтобы установить период истечения запроса MLD в значение по умолчанию.

Формат: `no set mld querier timer expiry`

Режим ввода команд: глобальная конфигурация

set mld querier election participate

Используйте данную команду, чтобы позволить опрашивающему устройству участвовать в процессе выбора опрашивающего, когда оно обнаружит присутствие еще одного опрашивающего в сети VLAN. При этом режиме, если опрашивающий обнаруживает, что адрес другого опрашивающего лучше (меньше), чем его адрес, он перестает посылать периодические запросы. Если опрашивающий выиграет в выборе, он продолжит посылать периодические запросы.

Значение по умолчанию: выключено

Формат: `set mld querier election participate`

Режим ввода команд: конфигурирование VLAN

no set mld querier election participate

Команда используется, чтобы запретить опрашивающему устройству участвовать в процессе выбора опрашивающего, но при этом выходить из режима опрашивающего устройства, как только он обнаружит присутствие другого опрашивающего в той же VLAN.

Формат: `no set mld querier election participate`

Режим ввода команд: конфигурирование VLAN

show mldsnooping querier

Данная команда используется для отображения данных опрашивающего устройства MLD Snooping. Настроенная информация отображается независимо от того, включено опрашивающее устройство MLD Snooping или нет.

Формат: `show mldsnooping querier [{detail | vlan` *`vlanid`*`}]`

Режим ввода команд: привилегированный

Если необязательный параметр *vlanid* не используется, команда отобразит следующую информацию:

Термин	***Значение***
Admin Mode	Указывает, активно ли на коммутаторе опрашивающее устройство MLD Snooping.
Admin Version	Версия MLD, которая будет использоваться при отправке запросов. Значение по умолчанию — MLD v1, изменить эту настройку нельзя.
Querier Address	IP-адрес, используемый в IPv6-заголовке при отправке MLD-запросов. Настраивается с помощью соответствующей команды.
Query Interval	Время в секундах, которое ожидает опрашивающее устройство перед тем, как отправить периодический общий запрос.
Querier Timeout	Время ожидания не опрашивающего устройства перед тем, как перейти в режим опрашивающего.

Если указать значение для *vlanid*, команда отобразит следующую информацию:

Термин	***Значение***
VLAN Admin Mode	Указывает, активно ли опрашивающее устройство MLD Snooping на данной VLAN.
VLAN Operational State	Указывает, в каком статусе находится опрашивающее устройство MLD Snooping. Если коммутатор находится в статусе Querier, он будет отправлять периодические общие запросы. При статусе Non-Querier он будет ожидать перемещения в статус Querier и не будет отправлять запросов.
VLAN Operational Max Response Time	Время ожидания после получения Leave-запроса, прежде чем удалить Leave хоста. Это значение рассчитывается динамически на основании запросов, получаемых от сети. Если коммутатор Snooping находится в режиме опрашивающего, это значение будет равно настроенному.
Querier Election Participate	Указывает, участвует ли опрашивающее устройство MLD Snooping в выборах опрашивающего, если обнаруживает присутствие другого опрашивающего в VLAN.
Querier VLAN Address	IP-адрес, используемый в IPv4-заголовке при отправке MLD-запросов в данной VLAN. Настраивается с помощью соответствующей команды.

Operational Version	Версия IPv6, используемая при отправке MLD-запросов на данной VLAN.
Last Querier Address	Указывает IP-адрес опрашивающего устройства, с которого был получен последний запрос.
Last Querier Version	Версия MLD опрашивающего устройства, с которого был получен последний запрос.

При использовании необязательного аргумента *detail* команда отображает глобальную информацию и данные по всем сетям VLAN, включенным для данного опрашивающего устройства.

9.35 Команды настройки Port Security

Этот подраздел описывает команды, используемые для настройки Port Security на коммутаторе. Port Security, известная как MAC-привязка, позволяет повысить безопасность сети путем блокировки допустимых MAC-адресов на данном порте. Пакеты с совпадающим MAC-адресом источника направляются обычным образом, все остальные пакеты отбрасываются.

Чтобы включить SNMP-трап для Port Security определенного порта, см. команду snmp-server enable traps violation.

port-security

Данная команда включает привязку MAC-адрес на интерфейсе, диапазоне интерфейсов или на системном уровне.

Значение по умолчанию: выключено

Формат: `port-security`

Режим ввода команд: глобальная конфигурация (чтобы включить привязку порта глобально) конфигурирование интерфейса (чтобы включить привязку порта на интерфейсе или диапазоне интерфейсов)

no port-security

Данная команда выключает привязку порта на одном порте (режим конфигурирования интерфейса) или всех портах (режим глобальной конфигурации).

Формат: `no port-security`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

port-security max-dynamic

Эта команда устанавливает максимальное количество динамически привязанных MAC-адресов, допустимых на определенном порте. Диапазон допустимых значений: 0–600.

Значение по умолчанию: 600

Формат: `port-security max-dynamic` *`maxvalue`*

Режим ввода команд: конфигурирование интерфейса

no port-security max-dynamic

Эта команда устанавливает максимальное количество динамически привязанных MAC-адресов, допустимых на определенном порте, в значение по умолчанию.

Формат: `no port-security max-dynamic`

Режим ввода команд: конфигурирование интерфейса

port-security max-static

Данная команда устанавливает максимальное количество статично привязанных MAC-адресов, допустимых на определенном порте. Диапазон допустимых значений: 0–20.

Значение по умолчанию: 1

Формат: `port-security max-static` *`maxvalue`*

Режим ввода команд: конфигурирование интерфейса

no port-security max-static

Эта команда устанавливает максимальное количество статично привязанных MAC-адресов, допустимых на определенном порте, в значение по умолчанию.

Формат: `no port-security max-static`

Режим ввода команд: конфигурирование интерфейса

port-security mac-address

Данная команда добавляет MAC-адрес в список статически привязанных MAC-адресов для интерфейса или диапазона интерфейсов. Параметр *vid* — это идентификатор VLAN.

Формат: `port-security mac-address` *`mac-address vid`*

Режим ввода команд: конфигурирование интерфейса

no port-security mac-address

Команда удаляет MAC-адрес из списка статически привязанных MAC-адресов.

Формат: `no port-security mac-address` *`mac-address vid`*

Режим ввода команд: конфигурирование интерфейса

port-security mac-address move

Эта команда переводит все динамически привязанные MAC-адреса в статически привязанные адреса для интерфейса или диапазона интерфейсов.

Формат: `port-security mac-address move`

Режим ввода команд: конфигурирование интерфейса

port-security mac-address sticky

Эта команда включает режим *sticky* для MAC-привязки порта на интерфейсе. Если добавить MAC-адрес и идентификатор VLAN (только в режиме конфигурирования интерфейса), то в режиме *sticky* MAC-адрес добавится в список статически привязанных MAC-адресов. Такие sticky-адреса конвертируются обратно в динамические адреса в случае, если выключить на порте режим sticky. Параметр *<vid>* — это идентификатор VLAN. При выполнении в режиме глобальной конфигурации команда применяет режим sticky ко всем действующим интерфейсам (физическим и LAG). Глобального sticky-режима как такового не существует.

Sticky-адреса, которые определяются динамически, отобразятся при команде *show running-config* как записи по схеме port-security mac-address sticky <mac> <vid>. Это отличает их от статических записей.

Формат: `port-security mac-address sticky [<mac-address> <vid>]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no port-security mac-address sticky

Форма отмены **no**-команды удаляет sticky-режим. MAC-адрес sticky может быть удален с помощью команды *no port- security mac-address <mac-address> <vid>*.

Формат: `no port-security mac-address sticky [<mac-address> <vid>]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

mac-address-table limit

Данная команда устанавливает предельное число MAC-адресов для соответствующго vlan-id.

Значение по умолчанию: выключено

Формат: `mac-address-table limit [action shutdown] [notification trap] [maximum-num] [vlan vlan-id]`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
[action shutdown]	После достижения предельного количества MAC-адресов это действие выключит все порты, участвующие в VLAN.
[notification trap]	Включает сообщения журнала по достижении предельного количества MAC-адресов.
[maximum-num]	Настраиваемое предельное количество MAC-адресов.
[vlan vlan]	VLAN, на которой применяется MAC-ограничение.

no mac-address-table limit

Данная команда выключает ограничение числа MAC-адресов для соответствующей *vlan-id*.

Значение по умолчанию: выключено

Формат: `no mac-address-table limit [action shutdown] [notification trap] [maximum-num] [vlan vlan-id]`

Режим ввода команд: глобальная конфигурация

show port-security

Эта команда отображает настройки защиты портов для порта или нескольких портов. Без использования дополнительных параметров команда отобразит административный режим защиты портов. Для отображения настроек определенного интерфейса или группы интерфейсов используйте необязательные параметры. Вместо параметра unit/slot/port можно использовать lag lag-intf-num как альтернативный вариант определения LAG-интерфейса. Параметр lag lag-intf-num также можно использовать для определения конкретного LAG-интерфейса, при этом значение lag-intf-num должно указывать номер порта LAG.

Формат: show port-security [{*unit/slot/port* | all}]
Режим ввода команд: привилегированный

Термин	*Значение*
Admin Mode	Режим привязки портов для системы в целом. Отображается при отсутствии дополнительных параметров.

При указании конкретного интерфейса выводится информация, представленная в таблице ниже.

Термин	*Значение*
Admin Mode	Режим привязки портов для данного интерфейса.
Dynamic Limit	Максимальное количество динамически присвоенных MAC-адресов.
Static Limit	Максимальное количество статически присвоенных MAC-адресов.
Violation Trap Mode	Показывает, включены ли трапы для нарушений.
Sticky Mode	Административный режим функции sticky-режима защиты портов на интерфейсе.

show port-security dynamic

Эта команда отображает динамически привязанные MAC-адреса для данного порта. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `show port-security dynamic` *`unit/slot/port`*
Режим ввода команд: привилегированный

Термин	*Значение*
MAC Address	Динамически привязанный MAC-адрес.

show port-security static

Эта команда отображает статически привязанные MAC-адреса для данного порта. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `show port-security static {`*`unit/slot/port`*` | lag `*`lag-intf-num`*`}`
Режим ввода команд: привилегированный

Параметр	*Описание*
Statically Configured MAC Address	Статично настроенный MAC-адрес.
VLAN ID	Идентификатор VLAN, включающей хост с указанным MAC-адресом.
Sticky	Указывает, добавлена ли статичная MAC-запись в sticky-режиме.

show port-security violation

Данная команда отображает MAC-адрес источника последнего пакета, отброшенного на защищённом порте. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* также можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `show port-security violation {`*`unit/slot/port`* `| lag` *`lag-id`*`}`

Режим ввода команд: привилегированный

Термин	*Значение*
MAC Address	MAC-адрес источника последнего кадра, отброшенного на защищённом интерфейсе.
VLAN ID	Идентификатор VLAN (если применимо) связанный с MAC-адресом последнего кадра, отброшенного на защищённом интерфейсе.

show mac-address-table limit

Эта команда отображает конфигурацию ограничения числа MAC-адресов.

Формат: `show mac-address-table limit [`*`vlan-id`*`]`

Режим ввода команд: привилегированный

Термин	*Значение*
VLAN ID	Идентификатор VLAN, на которой настроена привязка.

9.36 Команды настройки протокола LLDP (802.1AB)

Эта часть описывает команды, которые используются для настройки протокола Link Layer Discovery Protocol (LLDP), определенного в спецификации IEEE 802.1AB. LLDP позволяет станциям на LAN анонсировать основные возможности и физические описания устройства. Анонсирование позволяет системе управления сетью (NMS) иметь доступ к этой информации и отображать ее.

lldp transmit

Используйте данную команду, чтобы включить возможность анонсирования LLDP на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: включено

Формат: `lldp transmit`

Режим ввода команд: конфигурирование интерфейса

no lldp transmit

Используйте данную команду, чтобы выключить возможность анонсирования LLDP.

Формат: `no lldp transmit`

Режим ввода команд: конфигурирование интерфейса

lldp receive

Используйте данную команду, чтобы включить возможность получения LLDP на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: включено

Формат: `lldp receive`

Режим ввода команд: конфигурирование интерфейса

no lldp receive

Используйте данную команду, чтобы выключить возможность получения LLDPDU.

Формат: `no lldp receive`

Режим ввода команд: конфигурирование интерфейса

lldp timers

Используйте эту команду, чтобы установить параметры таймеров для передачи данных на портах с включенным LLDP. Параметр *interval-seconds* определяет ожидание в секундах перед тем, как передавать локальные данные LLDPDU. Диапазон — от 1 до 32 768 секунд. Параметр *hold-value* — это множитель интервала передачи, который устанавливает TTL для локальной данных LLDPDU. Диапазон множителя: 2–10. reinit-seconds — это задержка перед повторной инициализацией, диапазон 1–10 секунд.

Значение по умолчанию: interval — 30 секунд
hold — 4
reinit—2 секунды

Формат: `lldp timers [interval` *`interval-seconds`*`] [hold` *`hold-value`*`] [reinit` *`reinit-seconds`*`]`

Режим ввода команд: глобальная конфигурация

no lldp timers

Используйте эту команду для сброса одного или всех параметров таймеров передачи данных на портах с включенным LLDP в значения по умолчанию.

Формат: `no lldp timers [interval] [hold] [reinit]`

Режим ввода команд: глобальная конфигурация

lldp transmit-tlv

Используйте эту команду для указания необязательного значения TLV в наборе базового управления 802.1AB, которые будут передаваться в LLDPDU от интерфейса или от диапазона интерфейсов. Используйте параметр *sys-name*, чтобы передавать TLV системного имени. Используйте параметр *sys-desc*, чтобы передавать TLV системного описания. Используйте параметр

sys-cap, чтобы передавать TLV системных возможностей. Используйте параметр *port-desc*, чтобы передавать TLV описания порта.

Значение по умолчанию: необязательные TLV не включаются

Формат: `lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Режим ввода команд: конфигурирование интерфейса

no lldp transmit-tlv

Используйте данную команду, чтобы удалить необязательные значения TLV из LLDPDU. Используйте команду без параметров, чтобы удалить все необязательные TLV из LLDPDU.

Формат: `no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]`

Режим ввода команд: конфигурирование интерфейса

lldp transmit-mgmt

Команда включает передачу информации об адресе локальной системы управления в LLDPDU. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Формат: `lldp transmit-mgmt`

Режим ввода команд: конфигурирование интерфейса

no lldp transmit-mgmt

Команда выключает передачу информации об адресе локальной системы управления в LLDPDU. Используйте эту команду, чтобы выключить передачу информации об управлении в LLDPDU.

Формат: `no lldp transmit-mgmt`

Режим ввода команд: конфигурирование интерфейса

lldp notification

Используйте эту команду, чтобы включить уведомления об изменениях удаленных данных на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `lldp notification`

Режим ввода команд: конфигурирование интерфейса

no lldp notification

Эта команда выключает оповещения.

Значение по умолчанию: выключено

Формат: `no lldp notification`

Режим ввода команд: конфигурирование интерфейса

lldp notification-interval

Используйте данную команду, чтобы настроить то, как часто система будет посылать уведомления об изменениях удаленных данных. Параметр *interval* — это интервал ожидания в секундах между отправкой оповещений. Диапазон — от 5 до 3600 секунд.

Значение по умолчанию: 5

Формат: `lldp notification-interval interval`

Режим ввода команд: глобальная конфигурация

no lldp notification-interval

Используйте данную команду, чтобы вернуть интервал уведомлений в значение по умолчанию.

Формат: `no lldp notification-interval`

Режим ввода команд: глобальная конфигурация

clear lldp statistics

Команда сбрасывает всю статистику LLDP, включая информацию, относящуюся к MED.

Формат: `clear lldp statistics`

Режим ввода команд: привилегированный

clear lldp remote-data

Используйте данную команду, чтобы удалить всю информацию из таблицы удаленных данных LLDP, включая информацию, относящуюся к MED.

Формат: `clear lldp remote-data`

Режим ввода команд: глобальная конфигурация

show lldp

Данная команда отображает общую информацию о текущей конфигурации LLDP.

Формат: `show lldp`

Режим ввода команд: привилегированный

Термин	***Значение***
Transmit Interval	Как часто система передает LLDPDU локальных данных — в секундах.
Transmit Hold Multiplier	Множитель интервала передач, который устанавливает TTL в LLDPDU локальных данных.
Re-initialization Delay	Задержка в секундах перед повторной инициализацией.
Notification Interval	Как часто система отсылает уведомления об изменениях удаленных данных — в секундах.

show lldp interface

Используйте эту команду, чтобы отобразить общую информацию о текущей конфигурации LLDP для указанного интерфейса или всех интерфейсов.

Формат: `show lldp interface {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный

Термин	***Значение***
Interface	Интерфейс в формате *unit/slot/port*.
Link	Показывает, создано или разорвано соединение.
Transmit	Показывает, передает ли интерфейс LLDPDU.
Receive	Показывает, принимает ли интерфейс LLDPDU.
Notify	Показывает, отсылает ли интерфейс уведомления об изменениях.
TLVs	Показывает, отсылает ли интерфейс необязательные TLV в рамках LLDPDU. Коды TLV: 0 (описание порта), 1 (системное имя), 2 (описание системы) или 3 (возможности системы).
Mgmt	Показывает, передает ли интерфейс информацию об адресе системного управления в LLDPDU.

show lldp statistics

Команда используется, чтобы отобразить статистику LLDP для указанного интерфейса или всех интерфейсов.

Формат: `show lldp statistics {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный

Термин	***Значение***
Last Update	Время с момента последнего обновления таблицы в днях, часах, минутах и секундах.
Total Inserts	Общее количество записей в таблицу удалённых данных.
Total Deletes	Общее количество удалений из таблицы удалённых данных.
Total Drops	Общее количество случаев, когда полученный комплект удаленных данных не был внесен по причине нехватки ресурсов.
Total Ageouts	Общее количество случаев, когда запись комплекта удаленных данных была удалена по причине истечения интервала TTL.

Таблица содержит следующие заголовки колонок.

Термин	***Значение***
Interface	Интерфейс в формате *unit/slot/port*.
TX Total	Общее количество LLDP-пакетов, переданных портом.
RX Total	Общее количество LLDP-пакетов, полученных портом.
Discards	Общее количество LLDP-пакетов, отброшенных портом по какой-либо причине.
Errors	Количество LLDP-кадров с ошибками, полученных портом.
Ageouts	Общее количество случаев, когда запись комплекта удаленных данных была удалена по причине истечения TTL.
TVL Discards	Количество отброшенных TLV.

TVL Unknowns	Общее количество полученных портом TLV LLDP, тип значений которых находится в зарезервированном диапазоне и не распознается.
TLV MED	Общее количество TLV LLDP-MED, полученных интерфейсом.
TLV 802.1	Общее количество TLV LLDP типа 802.1, полученных интерфейсом.
TLV 802.3	Общее количество TLV LLDP типа 802.3, полученных интерфейсом.

show lldp remote-device

Эта команда отображает сводную информацию об удаленных устройствах, которые передают текущие данные LLDP в систему. Можно просмотреть информацию о полученных удаленных данных LLDP на всех портах или определенном порте.

Формат: `show lldp remote-device {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный

show lldp remote-device detail

Используйте эту команду, чтобы отобразить подробную информацию об удаленных устройствах, которые передают текущие LLDP-данные интерфейсу в системе.

Формат: `show lldp remote-device detail` *`unit/slot/port`*

Режим ввода команд: привилегированный

Термин	***Значение***
Local Interface	Интерфейс, который принял LLDPDU от удаленного устройства.
Remote Identifier	Внутренний идентификатор коммутатора для пометки каждого удаленного устройства системы.
Chassis ID Subtype	Тип идентификации, используемый в поле Chassis ID.
Chassis ID	Идентификатор шасси удаленного устройства.
Port ID Subtype	Тип порта на удаленном устройстве.
Port ID	Номер порта, передавшего LLDPDU.
System Name	Системное имя удаленного устройства.
System Description	Описание удаленной системы, идентифицирующее системное имя и версию аппаратного обеспечения, операционной системы и сетевого программного обеспечения, поддерживаемые удалённым устройством.
Port Description	Описывает порт в буквенно-цифровом формате. Описание порта можно настроить.
System Capabilities Supported	Указывает основные функции устройства.
System Capabilities Enabled	Показывает, какие из поддерживаемых функций устройства включены.
Management Address	Для каждого интерфейса на удаленном устройстве с LLDP-агентом перечисляет тип адреса, используемый удаленным LLDP-агентом, и указывает адрес, используемый для получения данных об устройстве.
Time To Live	Время (в секундах), в течение которого информация удаленного устройства, полученная в LLDPDU, может расцениваться как действительная.

show lldp local-device

Используйте эту команду, чтобы отобразить сводную информацию об анонсируемых локальных данных LLDP. Данная команда может отобразить сводную информацию или подробности для каждого интерфейса.

Формат: `show lldp local-device {`*`unit/slot/port`* `| all}`
Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Интерфейс в формате *unit/slot/port*.
Port ID	Идентификатор порта, связанного с интерфейсом.
Port Description	Описание порта, связанного с интерфейсом.

show lldp local-device detail

Используйте данную команду, чтобы отобразить подробную информацию о данных LLDP, передаваемых определенным интерфейсом.

Формат: `show lldp local-device detail` *`unit/slot/port`*
Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Интерфейс, отправляющий LLDPDU.
Chassis ID Subtype	Тип идентификации, используемый в поле Chassis ID.
Chassis ID	Идентификатор шасси локального устройства.
Port ID Subtype	Тип порта на локальном устройстве.
Port ID	Номер порта, передавшего LLDPDU.
System Name	Системное имя локального устройства.
System Description	Описание локальной системы, идентифицирующее системное имя и версию аппаратного обеспечения, операционной системы и сетевого программного обеспечения, поддерживаемые устройством.
Port Description	Описывает порт в буквенно-цифровом формате.
System Capabilities Supported	Указывает основные функции устройства.
System Capabilities Enabled	Показывает, какие из поддерживаемых функций устройства включены.
Management Address	Тип адреса и определенный адрес, используемый для получения и передачи данных.

9.37 Команды настройки LLDP-MED

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED), спецификация ANSI-TIA-1057, обеспечивает расширение стандарта LLDP. В частности, LLDP-MED обеспечивает расширения для сетевой конфигурации и политики, размещения устройств, управления питанием через Ethernet (PoE) и управления ресурсами.

lldp med

Используйте данную команду, чтобы включить MED на интерфейсе или диапазоне интерфейсов. Включая MED, вы активируете функцию приема и передачи LLDP.

Значение по умолчанию: выключено

Формат: `lldp med`

Режим ввода команд: конфигурирование интерфейса

no lldp med

Команда, которая выключает MED.

Формат: `no lldp med`

Режим ввода команд: конфигурирование интерфейса

lldp med confignotification

Команда настраивает интерфейс или диапазон интерфейсов на отправку оповещений об изменениях в топологии.

Значение по умолчанию: выключено

Формат: `lldp med confignotification`

Режим ввода команд: конфигурирование интерфейса

no ldp med confignotification

Эта команда выключает оповещения.

Формат: `no lldp med confignotification`

Режим ввода команд: конфигурирование интерфейса

lldp med transmit-tlv

Используйте эту команду, чтобы указать, какой необязательный набор TLV LLDP-MED будет передаваться в LLDPDU-сообщениях от этого интерфейса или диапазона интерфейсов.

Значение по умолчанию: включены возможности и политика сети TLV.

Формат: `lldp med transmit-tlv [capabilities] [network-policy]`

Режим ввода команд: конфигурирование интерфейса

Термин	***Значение***
capabilities	Передавать LLDP TLV возможности системы.
network-policy	Передача LLDP TLV политик сети.

no lldp med transmit-tlv

Используйте данную команду для удаления TLV.

Формат: `no lldp med transmit-tlv [capabilities] [network-policy]`

Режим ввода команд: конфигурирование интерфейса

lldp med all

Используйте эту команду, чтобы настроить LLDP-MED на всех портах.

Формат: `lldp med all`

Режим ввода команд: глобальная конфигурация

lldp med confignotification all

Используйте эту команду, чтобы настроить все порты на отправку оповещений об изменениях в топологии.

Формат: `lldp med confignotification all`

Режим ввода команд: глобальная конфигурация

lldp med faststartrepeatcount

Используйте данную команду, чтобы установить значения счетчика повторов быстрого старта. *[count]* — количество LLDPDU, которые будут переданы, когда функционал включен. Диапазон — от 1 до 10.

Значение по умолчанию: 3

Формат: `lldp med faststartrepeatcount` *`[count]`*

Режим ввода команд: глобальная конфигурация

no lldp med faststartrepeatcount

Используйте данную команду, чтобы вернуть настройки к заводским значениям.

Формат: `no lldp med faststartrepeatcount`

Режим ввода команд: глобальная конфигурация

lldp med transmit-tlv all

Используйте данную команду, чтобы указать какой необязательный набор TLV LLDP-MED будет передаваться в LLDPDU-сообщениях на всех портах.

Значение по умолчанию: включены возможности и политика сети TLV.

Формат: `lldp med transmit-tlv all [capabilities] [network-policy]`

Режим ввода команд: глобальная конфигурация

no lldp med transmit-tlv

Используйте данную команду для удаления TLV.

Формат: `no lldp med transmit-tlv all [capabilities] [network-policy]`

Режим ввода команд: глобальная конфигурация

show lldp med

Используйте эту команду для отображения сводной информации о текущей конфигурации LLDP-MED.

Формат: `show lldp med`

Режим ввода команд: привилегированный

show lldp med interface

Команда для отображения сводной информации о текущей конфигурации LLDP-MED для определенного интерфейса. *unit/slot/port* обозначает определенный физический интерфейс. all обозначает все действительные LLDP интерфейсы.

Формат: `show lldp med interface {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный

show lldp med local-device detail

Используйте эту команду, чтобы отобразить подробную информацию о данных LLDP MED, которые передает указанный интерфейс.

unit/slot/port обозначает определенный физический интерфейс.

Формат: `show lldp med local-device detail` *`unit/slot/port`*

Режим ввода команд: привилегированный

show lldp med remote-device

Команда отображает сводную информацию об удаленных устройствах, которые передают системе текущие данные LLDP MED. Можно просмотреть информацию об удаленных данных LLDP MED, полученных на все действительные интерфейсы LLDP или на определенный физический интерфейс.

Формат: `show lldp med remote-device {`*`unit/slot/port`* `| all}`

Режим ввода команд: привилегированный

Термин	*Значение*
Local Interface	Интерфейс, который принял LLDPDU от удаленного устройства.
Remote ID	Внутренний идентификатор коммутатора для пометки каждого удаленного устройства системы.
Device Class	Классификация удаленного устройства.

show lldp med remote-device detail

Команда отображает подробную информацию об удаленных устройствах, которые передают системе текущие данные LLDP MED.

Формат: `show lldp med remote-device detail` *`unit/slot/port`*

Режим ввода команд: привилегированный

9.38 Команды настройки управления DoS

Эта часть описывает команды, используемые для настройки управления отказом в обслуживании (DoS). Программное обеспечение обеспечивает поддержку при классификации и блокировке определенных типов DoS-атак. Вы можете настроить систему на отслеживание и блокировку следующих типов атак:

- **SIP = DIP:** IP-адрес источника = IP-адрес места назначения.
- **First Fragment:** размер заголовка TCP меньше настроенного значения.
- **TCP Fragment:** позволяет устройству отбрасывать пакеты с недостаточной полезной нагрузкой TCP, т. е. когда ее длина оказывается меньше минимально допустимого размера

заголовка TCP, если от длины полезной нагрузки входящего пакета отнять размер его заголовка.

- **TCP Flag:** TCP-флаг SYN и порт-источник < 1024, или контрольные флаги TCP = 0 и порядковый номер TCP = 0, или TCP-флаги FIN, URG, PSH и порядковый номер TCP = 0, или TCP-флаги SYN и FIN.
- **L4 Port:** TCP/UDP-порт источника = TCP/UDP-порт места назначения.
- **ICMP:** ограничение размера пакетов ICMP-пинга.
- **SMAC = DMAC:** MAC-адрес источника = MAC-адрес места назначения.
- **TCP Port:** TCP-порт источника = TCP-порт места назначения.
- **UDP Port**: UDP-порт источника = UDP-порт места назначения.
- **TCP Flag & Sequence:** TCP-флаг SYN и порт-источник < 1024, или контрольные флаги TCP = 0 и порядковый номер TCP = 0, или TCP-флаги FIN, URG, PSH и порядковый номер TCP = 0, или TCP-флаги SYN и FIN.
- **TCP Offset:** позволяет устройству отбрасывать пакеты, у которых смещение заголовка TCP установлено как 1.
- **TCP SYN:** установка TCP-флага SYN.
- **TCP SYN & FIN:** установка TCP-флагов SYN и FIN.
- **TCP FIN & URG & PSH:** TCP-флаги FIN, URG, PSH и порядковый номер TCP = 0.
- **ICMP V6**: ограничение размера ICMPv6-пакетов.
- **ICMP Fragment**: проверка фрагментированных ICMP-пакетов.

dos-control all

Данная команда включает защитные проверки DoS глобально.

Значение по умолчанию: выключено

Формат: `dos-control all`

Режим ввода команд: глобальная конфигурация

no dos-control all

Команда выключает защитные проверки DoS глобально.

Формат: `no dos-control all`

Режим ввода команд: глобальная конфигурация

dos-control sipdip

Эта команда включает DoS-защиту SIP = DIP (IP-адрес источника = IP-адрес места назначения). Соответственно, если входящие пакеты имеют SIP = DIP, то они отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control sipdip`

Режим ввода команд: глобальная конфигурация

no dos-control sipdip

Данная команда выключает DoS-защиту SIP = DIP (IP-адрес источника = IP-адрес места назначения).

Формат: `no dos-control sipdip`

Режим ввода команд: глобальная конфигурация

dos-control firstfrag

Данная команда включает DoS-защиту от недостаточного размера TCP-заголовка. Если входящие пакеты имеют размер TCP-заголовка меньше, чем настроенное значение, пакеты будут отбрасываться, если этот режим включен. Значение по умолчанию — disabled. Если включить этот режим защиты, но не указывать минимальную длину TCP-заголовка, система установит это значение как 20.

Значение по умолчанию: выключено (20)

Формат: `dos-control firstfrag [0-255]`

Режим ввода команд: глобальная конфигурация

no dos-control firstfrag

Эта команда выключает DoS-защиту от недостаточного размера TCP-заголовка.

Формат: `no dos-control firstfrag`

Режим ввода команд: глобальная конфигурация

dos-control tcpfrag

Данная команда включает DoS-защиту от TCP-фрагментов. При выявлении пакетов с недостаточной полезной нагрузкой TCP (т. е. когда ее длина оказывается меньше минимально допустимого размера заголовка TCP, если от длины полезной нагрузки входящего пакета отнять размер его заголовка) такие пакеты отбрасываются.

Значение по умолчанию: выключено

Формат: dos-control tcpfrag

Режим ввода команд: глобальная конфигурация

no dos-control tcpfrag

Эта команда выключает DoS-защиту от TCP-фрагментов.

Формат: `no dos-control tcpfrag`

Режим ввода команд: глобальная конфигурация

dos-control tcpflag

Данная команда включает DoS-защиту от TCP-флагов. Если входящие пакеты имеют настройку TCP-флага SYN и порт-источник меньше 1024, или же контрольные флаги TCP и порядковый номер TCP равный 0, или TCP-флаги FIN, URG, PSH и порядковый номер TCP равный 0, или TCP-флаги SYN и FIN, при включенном режиме защиты такие пакеты отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control tcpflag`

Режим ввода команд: глобальная конфигурация

no dos-control tcpflag

Эта команда выключает DoS-защиту от TCP-флагов.

Формат: `no dos-control tcpflag`

Режим ввода команд: глобальная конфигурация

dos-control l4port

Данная команда включает DoS-защиту портов уровня 4. Если входящие пакеты имеют номер порта-источника TCP/UDP равный номеру порта места назначения TCP/UDP, при включенном режиме защиты такие пакеты отбрасываются.

Некоторые приложения дублируют порты источника и места назначения L 4 — например RIP использует 520 для обоих. Если включить DoS-защиту портов L 4, такие приложения как RIP могут терять пакеты, что приводит к прекращению работы функционала.

Значение по умолчанию: выключено

Формат: `dos-control l4port`

Режим ввода команд: глобальная конфигурация

no dos-control l4port

Эта команда выключает DoS-защиту портов уровня 4.

Формат: `no dos-control l4port`

Режим ввода команд: глобальная конфигурация

dos-control smacdmac

Эта команда включает DoS-защиту SMAC = DMAC (MAC-адрес источника = MAC-адрес места назначения). Соответственно, если входящие пакеты имеют SMAC = DMAC, то они отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control smacdmac`

Режим ввода команд: глобальная конфигурация

no dos-control smacdmac

Данная команда выключает DoS-защиту SMAC = DMAC (MAC-адрес источника = MAC-адрес места назначения).

Формат: `no dos-control smacdmac`

Режим ввода команд: глобальная конфигурация

dos-control tcpport

Эта команда включает DoS-защиту от типа атак с номером порта-источника уровня 4 TCP равным номеру порта TCP места назначения. Соответственно, если входящие пакеты имеют одинаковые TCP-порты источника и места назначения, пакеты отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control tcpport`

Режим ввода команд: глобальная конфигурация

no dos-control tcpport

Эта команда выключает DoS-защиту от типа атак с номером порта-источника уровня 4 TCP равным номеру порта TCP места назначения.

Формат: `no dos-control tcpport`

Режим ввода команд: глобальная конфигурация

dos-control udpport

Данная команда включает DoS-защиту от типа атак с номером порта-источника уровня 4 UDP равным номеру порта UDP места назначения. Соответственно, если входящие пакеты имеют одинаковые UDP-порты источника и места назначения, пакеты отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control udpport`

Режим ввода команд: глобальная конфигурация

no dos-control udpport

Эта команда выключает DoS-защиту от типа атак с номером порта-источника уровня 4 UDP равным номеру порта UDP места назначения.

Формат: `no dos-control udpport`

Режим ввода команд: глобальная конфигурация

dos-control tcpflagseq

Данная команда включает DoS-защиту от TCP-флагов и последовательностей. Если входящие пакеты имеют настройку TCP-флага SYN и порт-источник меньше 1024, или же контрольные флаги TCP и порядковый номер TCP равный 0, или TCP-флаги FIN, URG, PSH и порядковый номер TCP равный 0, или TCP-флаги SYN и FIN, при включенном режиме защиты такие пакеты отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control tcpflagseq`

Режим ввода команд: глобальная конфигурация

no dos-control tcpflagseq

Данная команда выключает DoS-защиту от TCP-флагов и последовательностей.

Формат: `no dos-control tcpflagseq`

Режим ввода команд: глобальная конфигурация

dos-control tcpoffset

Эта команда включает DoS-защиту от TCP-смещений. Если входящие пакеты имеют TCP-смещение заголовка равное 1, они отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control tcpoffset`

Режим ввода команд: глобальная конфигурация

no dos-control tcpoffset

Данная команда выключает DoS-защиту от TCP-смещений.

Формат: `no dos-control tcpoffset`

Режим ввода команд: глобальная конфигурация

dos-control tcpsyn

Эта команда включает DoS-защиту от TCP SYN и источника уровня 4 = 0–1023. Если входящие пакеты имеют TCP-флаг SYN и порт-источник уровня 4 от 0 до 1023, они отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control tcpsyn`

Режим ввода команд: глобальная конфигурация

no dos-control tcpsyn

Данная команда выключает DoS-защиту от TCP SYN и источника уровня 4 = 0–1023.

Формат: `no dos-control tcpsyn`

Режим ввода команд: глобальная конфигурация

dos-control tcpsynfin

Эта команда включает DoS-защиту от TCP SYN и FIN. Если входящие пакеты имеют TCP-флаг SYN и FIN, они отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control tcpsynfin`

Режим ввода команд: глобальная конфигурация

no dos-control tcpsynfin

Данная команда выключает DoS-защиту от TCP SYN и FIN.

Формат: `no dos-control tcpsynfin`

Режим ввода команд: глобальная конфигурация

dos-control tcpfinurgpsh

Эта команда включает проверку TCP FIN, URG, PSH и SEQ = 0 в рамках DoS-защиты. Если входящие пакеты имеют настройки TCP FIN, URG, PSH и порядковый номер TCP равный 0, они отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control tcpfinurgpsh`

Режим ввода команд: глобальная конфигурация

no dos-control tcpfinurgpsh

Команда выключает проверку TCP FIN, URG, PSH и SEQ = 0 в рамках DoS-защиты.

Формат: `no dos-control tcpfinurgpsh`
Режим ввода команд: глобальная конфигурация

dos-control icmpv4

Данная команда включает DoS-защиту от максимального размера ICMPv4-пакета. Если входящие ответные ICMPv4-пакеты (PING) имеют размер больше, чем настроенное значение, они отбрасываются.

Значение по умолчанию: выключено (512)

Формат: `dos-control icmpv4 [0-16376]`

Режим ввода команд: глобальная конфигурация

no dos-control icmpv4

Эта команда выключает DoS-защиту от максимального размера ICMPv6-пакетов.

Формат: `no dos-control icmpv4`

Режим ввода команд: глобальная конфигурация

dos-control icmpv6

Данная команда включает DoS-защиту от максимального размера ICMPv6-пакета. Если входящие ответные ICMPv6-пакеты (PING) имеют размер больше, чем настроенное значение, они отбрасываются.

Значение по умолчанию: выключено (512)

Формат: `dos-control icmpv6 0-16376`

Режим ввода команд: глобальная конфигурация

no dos-control icmpv6

Эта команда выключает DoS-защиту от максимального размера ICMPv6-пакетов.

Формат: `no dos-control icmpv6`

Режим ввода команд: глобальная конфигурация

dos-control icmpfrag

Эта команда включает DoS-защиту от TCP-фрагментов. Соответственно, если входящие пакеты имеют фрагментированные ICMP-пакеты, они отбрасываются.

Значение по умолчанию: выключено

Формат: `dos-control icmpfrag`

Режим ввода команд: глобальная конфигурация

no dos-control icmpfrag

Эта команда выключает DoS-защиту от ICMP-фрагментов.

Формат: `no dos-control icmpfrag`

Режим ввода команд: глобальная конфигурация

show dos-control

Данная команда отображает информацию о конфигурации DoS-защиты.

Формат: `show dos-control`

Режим ввода команд: привилегированный

Термин	*Значение*
First Fragment Mode	Административный режим DoS-защиты первого фрагмента. При включенном режиме коммутатор отбрасывает пакеты, имеющие размер TCP-заголовка меньше, чем настроенное значение.
Min TCP Hdr Size	Минимальный размер заголовка TCP, который коммутатор будет принимать, если включен режим DoS-защиты первого фрагмента.
ICMPv4 Mode	Административный режим DoS-защиты ICMPv4. При включенном режиме, коммутатор отбрасывает ICMP-пакеты, имеющие тип ECHO_REQ (пинг), и если они имеют размер больше настроенного значения полезной нагрузки ICMPv4.
Max ICMPv4 Payload Size	Максимальный размер полезной нагрузки ICMPv4, который будет приниматься, если включен режим DoS-защиты ICMPv4.
ICMPv6 Mode	Административный режим DoS-защиты ICMPv6. При включенном режиме, коммутатор отбрасывает ICMP-пакеты, имеющие тип ECHO_REQ (пинг), и если они имеют размер больше настроенного значения полезной нагрузки ICMPv6.
Max ICMPv6 Payload Size	Максимальный размер полезной нагрузки ICMPv6, который будет приниматься, если включен режим DoS-защиты ICMPv6.
ICMPv4 Fragment Mode	Административный режим DoS-защиты от фрагментов ICMPv4. При включенном режиме коммутатор отбрасывает фрагментированные ICMPv4-пакеты.
TCP Port Mode	Административный режим DoS-защиты TCP-портов. При включенном режиме коммутатор отбрасывает пакеты, которые имеют одинаковые TCP-порты источника и места назначения.
UDP Port Mode	Административный режим DoS-защиты UDP-портов. При включенном режиме коммутатор отбрасывает пакеты, которые имеют одинаковые UDP-порты источника и места назначения.
SIPDIP Mode	Административный режим DoS-защиты SIP=DIP. При включенном режиме коммутатор отбрасывает пакеты, которые имеют одинаковые IP-адреса источника и места назначения. Заводская настройка: disabled.
SMACDMAC Mode	Административный режим DoS-защиты SMAC=DMAC. При включенном режиме коммутатор отбрасывает пакеты, которые имеют одинаковые MAC-адреса источника и места назначения.
TCP FIN&URG& PSH Mode	Административный режим DoS-защиты от TCP FIN & URG & PSH. При включенном режиме коммутатор отбрасывает пакеты, которые имеют TCP-флаги FIN, URG, PSH и порядковый номер TCP равный 0.

TCP Flag & Sequence Mode	Административный режим DoS-защиты от TCP-флагов. При включенном режиме коммутатор отбрасывает пакеты, которые имеют TCP-флаги контроля и порядковый номер TCP равные 0.
TCP SYN Mode	Административный режим DoS-защиты от TCP SYN. При включенном режиме коммутатор отбрасывает пакеты, которые имеют установленные TCP-флаги SYN.
TCP SYN & FIN Mode	Административный режим DoS-защиты TCP SYN & FIN. При включенном режиме коммутатор отбрасывает пакеты, которые имеют установленные TCP-флаги SYN и FIN.
TCP Fragment Mode	Административный режим DoS-защиты от фрагментов TCP. При включенном режиме коммутатор отбрасывает пакеты, которые имеют полезную нагрузку TCP меньше дозволенного минимума (если от длины полезной нагрузки входящего пакета отнять размер его заголовка).
TCP Offset Mode	Административный режим DoS-защиты от TCP-смещений. При включенном режиме коммутатор отбрасывает пакеты, которые имеют смещение TCP-заголовков, равное 1.

9.39 Команды настройки таблиц MAC-адресов

В этой части описаны команды, используемые для настройки и просмотра информации о таблицах MAC-адресов.

bridge aging-time

Эта команда настраивает время устаревания таблицы коммутации в секундах. Параметр seconds должен быть в диапазоне от 10 до 1 000 000 секунд.

Значение по умолчанию: 300

Формат: `bridge aging-time` *`10-1,000,000`*

Режим ввода команд: глобальная конфигурация

no bridge aging-time

Эта команда устанавливает время устаревания таблицы коммутации в значение по умолчанию.

Формат: `no bridge aging-time`

Режим ввода команд: глобальная конфигурация

show forwardingdb agetime

Эта команда отображает время жизни записи MAC-адресов.

Значение по умолчанию: all

Формат: `show forwardingdb agetime`

Режим ввода команд: привилегированный

Термин	***Значение***
Address Aging Timeout	Отображает значение времени жизни записи для устаревания MAC-адресов системы в секундах.

show mac-address-table multicast

Данная команда отображает информацию таблицы коммутации многоадресной рассылки (MFDB). Если ввести команду без параметров, отобразится вся таблица. Можно просмотреть запись таблицы для одного MAC-адреса, указав MAC-адрес как дополнительный параметр.

Формат: `show mac-address-table multicast` *macaddr*
Режим ввода команд: привилегированный

Термин	*Значение*
VLAN ID	VLAN, в которой был определен MAC-адрес.
MAC Address	Групповой MAC-адрес, для которого коммутатор переадресует или фильтрует информацию. Указывается в формате шести двузначных номеров шестнадцатеричной системы, разделенных двоеточиями, например: 01:23:45:67:89:AB.
Source	Компонент, от которого зависит данная запись в таблице MFDB. Источником может быть IGMP Snooping, GMRP и статическая фильтрация.
Type	Тип записи. Статические записи — записи, которые настраиваются конечным пользователем. Динамические добавляются в таблицу как результат процесса определения или протокола.
Description	Текстовое описание данной записи таблицы многоадресной коммутации.
Interfaces	Список интерфейсов, которые назначены для переадресации (Fwd:) и фильтрации (Flt:).
Fwd Interface	Список, хранящий все коммутационные интерфейсы для записи и удаляющий интерфейсы, перечисленные как статически фильтрующие интерфейсы.

show mac-address-table stats

Эта команда отображает статистику таблицы коммутации многоадресной рассылки (MFDB).

Формат: `show mac-address-table stats`

Режим ввода команд: привилегированный

Термин	*Значение*
Total Entries	Общее количество записей, возможных в MFDB.
Most MFDB Entries Ever Used	Наибольшее количество записей, которые когда-либо содержались в таблице MFDB. Обозначается также как «наивысший уровень» MFDB.
Current Entries	Текущее количество записей в MFDB.

9.40 Команды настройки ISDP

В этой части описываются команды, используемые для настройки Industry Standard Discovery Protocol (ISDP).

isdp run

Эта команда включает ISDP на коммутаторе.

Значение по умолчанию: выключено

Формат: `isdp run`

Режим ввода команд: глобальная конфигурация

no isdp run

Эта команда выключает ISDP на коммутаторе.

Формат: `no isdp run`

Режим ввода команд: глобальная конфигурация

isdp holdtime

Данная команда настраивает время удержания ISDP-пакетов, передаваемых коммутатором. Это время указывает, как долго принимающее устройство должно удерживать данные, содержащиеся в ISDP-пакете, прежде чем отбросить его. Диапазон указан в секундах.

Значение по умолчанию: 180 секунд

Формат: `isdp holdtime` *`10-255`*

Режим ввода команд: глобальная конфигурация

isdp timer

Данная команда устанавливает временной период между отправкой новых ISDP-пакетов. Диапазон указан в секундах.

Значение по умолчанию: 60 секунд

Формат: `isdp timer` *`5-254`*

Режим ввода команд: глобальная конфигурация

isdp advertise-v2

Эта команда включает отправку ISDP-пакетов версии 2 с данного устройства.

Значение по умолчанию: выключено

Формат: `isdp advertise-v2`

Режим ввода команд: глобальная конфигурация

no isdp advertise-v2

Эта команда выключает отправку ISDP-пакетов версии 2 с данного устройства.

Формат: `no isdp advertise-v2`

Режим ввода команд: глобальная конфигурация

isdp enable

Эта команда включает ISDP на интерфейсе или диапазоне интерфейсов.

Чтобы интерфейс мог передавать ISDP-пакеты, ISDP должен быть включен глобально и на интерфейсе. Если ISDP глобально выключен на коммутаторе, интерфейс не сможет передавать ISDP-пакеты независимо от статуса ISDP на интерфейсе.

Значение по умолчанию: выключено

Формат: `isdp enable`

Режим ввода команд: конфигурирование интерфейса

no isdp enable

Эта команда выключает ISDP на интерфейсе.

Формат: `no isdp enable`

Режим ввода команд: конфигурирование интерфейса

clear isdp counters

Эта команда сбрасывает счетчики ISDP.

Формат: `clear isdp counters`

Режим ввода команд: привилегированный

clear isdp table

Данная команда удаляет записи в таблице ISDP.

Формат: `clear isdp table`

Режим ввода команд: привилегированный

show isdp

Эта команда отображает глобальные настройки ISDP.

Формат: `show isdp`

Режим ввода команд: привилегированный

Термин	***Значение***
Timer	Частота, с которой данное устройство отправляет ISDP-пакеты. Значение указывается в секундах.
Hold Time	Продолжительность времени, в течение которого принимающее устройство должно сохранять данные, переданные данным устройством. Значение указывается в секундах.
Version 2 Advertisements	Настройка отправки ISDPv2-пакетов. При значении disabled отправляются пакеты версии 1.
Neighbors table time since last change	Количество времени, прошедшее с последнего изменения в ISDP-таблице соседей.
Device ID	Идентификатор, анонсируемый данным устройством. Формат данного идентификатора устройства характеризуется значением объекта Device ID Format.
Device ID Format Capability	Указывает возможности формата идентификатора устройства. • serialNumber обозначает, что устройство использует серийный номер в качестве формата для идентификатора устройства. • macAddress обозначает, что устройство использует MAC-адрес уровня 2 в качестве формата для идентификатора устройства. • other обозначает, что устройство использует особый формат, определенный платформой, на которой оно работает.
Device ID Format	Указывает формат идентификатора устройства. • serialNumber — это значение в виде строки ASCII, содержащей серийный номер устройства.

	• macAddress — это значение в виде MAC-адреса уровня 2. • other — значение в виде ASCII строки конкретной платформы, содержащей информацию, которая идентифицирует устройство. Например, ASCII-строка может включать серийный номер, предваряемый/продолженный системным именем.

show isdp interface

Используйте команду, чтобы отобразить настройки ISDP для указанного интерфейса.

Формат: `show isdp interface {all | unit/slot/port}`

Режим ввода команд: привилегированный

Термин	*Значение*
Interface	*unit/slot/port* указанного интерфейса.
Mode	Включен или выключен режим ISDP для интерфейса.

show isdp entry

Данная команда отображает записи ISDP. Если указывается идентификатор устройства, отображаются записи только для этого устройства.

Формат: `show isdp entry {all | deviceid}`

Режим ввода команд: привилегированный

Термин	*Значение*
Device ID	Идентификатор устройства, связанный с соседним устройством, которое анонсировало данные.
IP Addresses	IP-адреса, связанные с соседним устройством.
Capability	Функциональные возможности ISDP, анонсируемые соседним устройством.
Platform	Аппаратная платформа, анонсируемая соседним устройством.
Interface	Интерфейс (unit/slot/port), на котором был принят анонс соседнего устройства.
Port ID	Идентификатор порта интерфейса, с которого соседнее устройство прислало анонс.
Hold Time	Время удержания, анонсируемое соседним устройством.
Advertisement Version	Версия программного обеспечения соседнего устройства.
Entry Last Changed Time	Версия пакета-анонса, полученного от соседнего устройства.
Version	Время последнего изменения записи.

show isdp traffic

Данная команда отображает статистику ISDP.

Формат: `show isdp traffic`

Режим ввода команд: привилегированный

Термин	*Значение*
ISDP Packets Received	Общее количество полученных ISDP-пакетов.
ISDP Packets Transmitted	Общее количество переданных ISDP-пакетов.
ISDPv1 Packets Received	Общее количество полученных ISDPv1-пакетов.
ISDPv1 Packets Transmitted	Общее количество переданных ISDPv1-пакетов.
ISDPv2 Packets Received	Общее количество переданных ISDPv2-пакетов.
ISDPv2 Packets Transmitted	Общее количество переданных ISDPv2-пакетов.
ISDP Checksum Error	Количество пакетов, полученных с неверным заголовком.
ISDP Transmission Failure	Количество пакетов, которые не удалось передать.
ISDP Invalid Format	Количество полученных повреждённых пакетов.

ISDP Table Full	Количество событий, когда запись соседа не была добавлена в таблицу по причине переполнения базы данных.
ISDP IP Address Table Full	Количество событий, когда запись соседа была добавлена в таблицу без IP-адреса.

debug isdp packet

Эта команда включает трассировку ISDP-пакетов, обрабатываемых коммутатором. Для трассировки пакетов определенного интерфейса необходимо, чтобы на устройстве и на интерфейсе был включен протокол ISDP.

Формат: `debug isdp packet [{receive | transmit}]`

Режим ввода команд: привилегированный

no debug isdp packet

Эта команда выключает отслеживание ISDP-пакетов на принимаемой или передающей стороне или на обеих сторонах.

Формат: `no debug isdp packet [{receive | transmit}]`

Режим ввода команд: привилегированный

9.41 Команды настройки протокола EFM OAM

Этот подраздел описывает команды, использующиеся для настройки протокола Ethernet in the First Mile (EFM) Operations and Maintenance (OAM). Администраторы сетей используют эти команды для просмотра данных операций соединений, таких как удаленное обнаружение ошибок и управление удаленной обратной петлей, которые включают мониторинг, тестирование и решение проблем соединений протокола OAM в сети.

ethernet oam

Эта команда используется для включения Ethernet OAM на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `ethernet oam`

Режим ввода команд: конфигурирование интерфейса

no ethernet oam

Данная команда используется для выключения Ethernet OAM на интерфейсе или диапазоне интерфейсов.

Формат: `no ethernet oam`

Режим ввода команд: конфигурирование интерфейса

ethernet oam timeout

Данная команда устанавливает значение таймера хоста на 2–30 секунд на интерфейсе или диапазоне интерфейсов. Если PDU протокола OAM не получен на удаленном DTE за установленный период времени, локальный клиент фиксирует неисправность обнаружения состояния устройства.

Значение по умолчанию: 5 секунд

Формат: `ethernet oam timeout 2-30`

Режим ввода команд: конфигурирование интерфейса

no ethernet oam timeout

Данная команда устанавливает таймер хоста в значение по умолчанию.

Формат: `no ethernet oam timeout`

Режим ввода команд: конфигурирование интерфейса

ethernet oam min-rate

Данная команда устанавливает минимальную скорость передачи (pdu_timer) в секундах для отправки периодических OAM-PDU на интерфейс или диапазон интерфейсов. Диапазон — от 1 до 10.

Значение по умолчанию: 1

Формат: `ethernet oam min-rate 1-10`

Режим ввода команд: конфигурирование интерфейса

no ethernet oam min-rate

Данная команда устанавливает минимальную скорость передачи (pdu_timer) в секундах для отправки периодических OAM-PDU в значение по умолчанию.

Формат: `no ethernet oam min-rate`

Режим ввода команд: конфигурирование интерфейса

ethernet oam max-rate

Команда устанавливает максимальную скорость передачи (pdu_timer) в секундах для отправки периодических OAM-PDU на интерфейс или диапазон интерфейсов, где один PDU отсылается за секунду. Диапазон — от 1 до 10.

Значение по умолчанию: 1

Формат: `ethernet oam max-rate 1-10`

Режим ввода команд: конфигурирование интерфейса

no ethernet oam max-rate

Данная команда устанавливает максимальную скорость передачи (pdu_timer) в значение по умолчанию.

Формат: `no ethernet oam max-rate`

Режим ввода команд: конфигурирование интерфейса

ethernet oam mode

Эта команда устанавливает режим интерфейса OAM как активный или пассивный на указанном интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: пассивный

Формат: `ethernet oam mode {active | passive}`

Режим ввода команд: конфигурирование интерфейса

ethernet oam remote-loopback

Данная команда настраивает время жизни для поддержки удаленной обратной петли на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: поддержка удаленной обратной петли включена

Формат: `ethernet oam remote-loopback [supported] [timeout 1-100]`

Режим ввода команд: конфигурирование интерфейса

Термин	*Значение*
supported	Включает поддержку удаленной обратной петли. Значение по умолчанию: enabled.
timeout	Устанавливает время в секундах, после которого удаленная обратная петля устаревает. Диапазон — от 10 до 100 секунд; по умолчанию 50 секунд.

ethernet oam remote-loopback start

Данная команда включает удаленную обратную петлю на указанном OAM-интерфейсе.

Согласно IEEE 802.3ah, экземпляр должен быть в активном режиме, чтобы функция удаленной обратной петли поддерживалась.

Формат: `ethernet oam remote-loopback start unit/slot/port`

Режим ввода команд: привилегированный
пользовательский

ethernet oam remote-loopback stop

Данная команда останавливает удаленную обратную петлю на указанном OAM-интерфейсе.

Формат: `ethernet oam remote-loopback stop unit/slot/port`

Режим ввода команд: привилегированный
пользовательский

ethernet oam link-monitor supported

Данная команда включает поддержку мониторинга соединения на текущем интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: включено

Формат: `ethernet oam link-monitor supported`

Режим ввода команд: конфигурирование интерфейса

no ethernet oam link-monitor supported

Данная команда включает поддержку мониторинга соединения на текущем интерфейсе.

Формат: `no ethernet oam link-monitor supported`

Режим ввода команд: конфигурирование интерфейса

ethernet oam link-monitor

Эта команда запускает или выключает мониторинг соединения на текущем OAM-интерфейсе.

Значение по умолчанию: выключено
Формат: `ethernet oam link-monitor {on | off}`

Режим ввода команд: конфигурирование интерфейса

ethernet oam link-monitor frame

Данная команда настраивает значения событий изменения числа кадров с ошибками. Команда используется для настройки нижнего и верхнего порогов числа кадров с ошибками, по достижении которых запускается событие. Значение window — это время в секундах, в течение которого значения порогов должны быть нарушены для того, чтобы сгенерировать трап.

Формат: `ethernet oam link-monitor frame {threshold {high (`*`1-65535`*` | none) | low `*`1-65535`*`}|window `*`10-60`*`}`

Режим ввода команд: конфигурирование интерфейса

Термин	***Значение***
threshold	Максимальное и минимальное время получения кадров с ошибками в секундах. Значение по умолчанию: 1.
window	Продолжительность окна события в секундах, от 10 до 60. По умолчанию — 1.

no ethernet oam link-monitor frame

Данная команда устанавливает события числа ошибочных кадров в значение по умолчанию.

Значение по умолчанию: значения события ошибочных кадров выключены

Формат: `no ethernet oam link-monitor frame {threshold {high | low} |window}`

Режим ввода команд: конфигурирование интерфейса

ethernet oam link-monitor frame-period

Данная команда настраивает значения события периодов кадров с ошибками. Команда используется для настройки нижнего и верхнего порогов для периодов кадров с ошибками, по достижении которых запускается событие. Значение window — это время в секундах, в течение которого значения порогов должны быть нарушены для того, чтобы сгенерировать трап.

Формат: `ethernet oam link-monitor frame-period {threshold {high (`*`1-65535`*` | none) | low `*`1-65535`*`}|window `*`1-65535`*`}`

Режим ввода команд: конфигурирование интерфейса

Термин	***Значение***
threshold	Максимальное и минимальное время получения кадров с ошибками в секундах. Значение по умолчанию: 1.
window	Продолжительность окна для события голосования в секундах: от 1 до 65535. По умолчанию — 10000.

no ethernet oam link-monitor frame-period

Данная команда возвращает события периодов кадров с ошибками в значения по умолчанию.

Формат: `no ethernet oam link-monitor frame-period {threshold {high | low} |window}`

Режим ввода команд: конфигурирование интерфейса

ethernet oam link-monitor frame-seconds

Данная команда настраивает значения события продолжительности получения кадров с ошибками. Команда используется для настройки нижнего и верхнего порогов для продолжительности получения кадров с ошибками, по достижении которых запускается событие. Значение window — это время в секундах, в течение которого значения порогов должны быть нарушены для того, чтобы сгенерировать трап.

Формат: `ethernet oam link-monitor frame-seconds {threshold {high (1-65535 | none) | low 1- 65535} |window 10-900}`

Режим ввода команд: конфигурирование интерфейса

Термин	***Значение***
threshold	Максимальное и минимальное время получения кадров с ошибками в секундах. Значения по умолчанию: 1.
window	Продолжительность окна для события голосования в секундах: от 1 до 65535. По умолчанию — 10000.

no ethernet oam link-monitor frame-seconds

Данная команда сбрасывает значения события продолжительности получения кадров с ошибками.

Формат: `no ethernet oam link-monitor frame-seconds {threshold {high | low} |window}`

Режим ввода команд: конфигурирование интерфейса

show ethernet oam statistics

Эта команда показывает статистику OAM для указанного OAM-интерфейса.

Формат: `show ethernet oam statistics [interface unit/slot/port | all]`

Режим ввода команд: привилегированный
пользовательский

show ethernet oam interface

Данная команда отображает OAM-интерфейсы.

Формат: `show ethernet oam interface`

Режим ввода команд: привилегированный

show ethernet oam discovery

Эта команда показывает информацию обнаружения OAM-сущностей на указанном OAM-интерфейсе.

Формат: `show ethernet oam discovery [interface unit/slot/port | all]`

Режим ввода команд: привилегированный

show ethernet oam status

Данная команда отображает информацию статуса OAM для указанного интерфейса.

Формат: `show ethernet oam status [interface` *`unit/slot/port`* `| all]`

Режим ввода команд: привилегированный
пользовательский

show ethernet oam mode

Данная команда отображает информацию об интерфейсе указанного OAM-интерфейса.

Формат: `show ethernet oam mode` *`unit/slot/port`*`|all`

Режим ввода команд: привилегированный
пользовательский

show ethernet oam link-monitor

Данная команда отображает информацию мониторинга Ethernet OAM (Dot3ah) для OAM-интерфейса.

Формат: `show ethernet oam link-monitor` *`unit/slot/port`*

Режим ввода команд: привилегированный
пользовательский

show ethernet oam summary

Данная команда отображает общую информацию протокола для Ethernet OAM (Dot3ah).

Формат: `show ethernet oam summary [`*`unit/slot/port`* `| all]`

Режим ввода команд: привилегированный
пользовательский

debug dot3ah packet

Используйте эту команду для включения трассировки отладки Dot3ah-пакетов в консоли. Это позволит увидеть, был пакет передан или получен на интерфейс с запущенным EFM-OAM/Dot3ah.

Формат: `debug dot3ah packet`

Режим ввода команд: привилегированный
пользовательский

clear ethernet oam statistics

Данная команда очищает информацию о статистике протокола Ethernet OAM (Dot3ah) на интерфейсе/интерфейсах.

Формат: `show ethernet oam statistics [`*`unit/slot/port`* `| all]`

Режим ввода команд: привилегированный
пользовательский

loopback-test

Эта команда выполняет тестирование обратной петли на определенном порте или всех портах, подключенных к коммутатору — кроме тех, на которых запущен протокол OAM. Тест включает

тестирование MAC-уровня и физического уровня. Данные статуса и статистики возвращаются в зависимости от результатов, полученных от MAC-уровня или физического уровня, предоставляемого аппаратным обеспечением.

Формат: `loopback-test [mac | phy] unit/slot/port`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
mac	MAC-уровень тестирования обратной петли.
phy	Физический уровень тестирования обратной петли.

9.42 Команды настройки протокола CFM

Ethernet CFM (Connectivity Fault Management), IEEE802.1ag – предоставляет функции наблюдения, поиска и устранения неисправностей в сетях Ethernet, позволяя контролировать соединение, изолировать проблемные участки сети и идентифицировать клиентов, к которым применялись ограничения в сети.

Протокол оперирует следующими понятиями:

- Maintenance Domain (MD) – участок сети, принадлежащий и управляемый одним оператором;
- Maintenance Association (MA) – совокупность конечных точек (MEP), каждая из которых имеет одинаковый идентификатор MAID (Maintenance Association Identifier), определяющий тип сервиса;
- Maintenance association End Point (MEP) – конечная точка сервиса, расположенная на его границе;
- Maintenance domain Intermediate Point (MIP) – промежуточная точка домена.

ethernet cfm domain

Создание (или смена уровня) CFM домена (MD) с именем domain-name и переход в режим конфигурирования домена.

Формат: `ethernet cfm domain domain-name level 0-7`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
domain-name	Уникальный идентификатор домена
level	Уникальный идентификатор домена обслуживания. Диапазон значений: 0–7.

service vlan

Создание CFM-сервиса (MA) привязанного к VLAN с номером vlanID и переход в режим конфигурирования сервиса.

Формат: `service service-name vlan vlanID`

Режим ввода команд: обслуживание конфигурации домена

Параметр	*Описание*
service-name	Строка символов, которая идентифицирует определенную MA. В названии можно использовать до 45 буквенно-цифровых символов.
vlanID	Идентификатор VLAN MA. Диапазон значений: 1–409. Значение по умолчанию: 0. Представляет сервисный экземпляр, мониторинг которого выполняется ассоциацией обслуживания.

ethernet cfm enable

Используйте данную команду, чтобы включить на коммутаторе CFM.

Значение по умолчанию: выключено

Формат: `ethernet cfm enable`

Режим ввода команд: глобальная конфигурация

no ethernet cfm enable

Используйте no-форму команды, чтобы сбросить статус CFM в значение по умолчанию.

Формат: `no ethernet cfm enable`

Режим ввода команд: глобальная конфигурация

ethernet cfm cc level vlan interval

Используйте данную команду, чтобы настроить интервал передачи Continuity Check Message (CCM).

Формат: `ethernet cfm cc level` *`0-7`* `vlan` *`vlan-list`* `interval` *`secs`*

Режим ввода команд: ассоциация обслуживания

Параметр	*Описание*
level	Строка символов, которая идентифицирует определенную MA. В названии можно использовать до 45 буквенно-цифровых символов.
vlan–list	Идентификатор VLAN MA. Диапазон значений: 1–409. Значение по умолчанию: 0. Представляет сервисный экземпляр, мониторинг которого выполняется ассоциацией обслуживания.
secs	Время в секундах между отправкой CCM кадров, используемое всеми MEP в данной ассоциации. Возможные значения: •10 — установить интервал CCM как 10 мс •100 — установить интервал CCM как 100 мс •1000 — установить интервал CCM как 1000 мс •10000 — установить интервал CCM как 10 000 мс •3,3 — установить интервал CCM как 3,3 мс •60000 — установить интервал CCM как 60 000 мс •600000 — установить интервал CCM как 600 000 мс

ethernet cfm mep archive-hold-time

Команда настраивает период в секундах, в течение которого будут храниться данные от отсутствующей Maintenance End Point (MEP) перед удалением. Диапазон: 1–65535 секунд.

Значение по умолчанию: `600`

Формат: `ethernet cfm mep archive-hold-time` *`seconds`*

Режим ввода команд: глобальная конфигурация

no ethernet cfm mep archive-hold-time

Используйте no-форму команды чтобы установить время хранения данных на значение по умолчанию.

Формат: `no ethernet cfm mep archive-hold-time`

Режим ввода команд: глобальная конфигурация

ethernet cfm mep level

Используйте данную команду, чтобы настроить уровень MEP на интерфейсе или диапазоне интерфейсов. MEP настраивается для каждой MA.

Формат: `ethernet cfm mep level` *`0-7`* `direction {up|down} mpid` *`1–8191`* `vlan` *`vlan–list`*

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.
direction	Направление для MEP. Возможные значения: • **up** – восходящий • **down** - нисходящий
mpid	Идентификатор MEP. Создает MEP, связанную с данной MA.
vlan–list	Идентификатор VLAN. Диапазон значений: 1–40934. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами Для диапазона используйте дефис (-).

no ethernet cfm mep level

Используйте no-форму команды, чтобы удалить MEP.

Формат: `no ethernet cfm mep level` *`0-7`* `direction {up|down} mpid` *`1–8191`* `vlan` *`vlan–list`*

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.
mpid	Идентификатор MEP. Создает MEP, связанную с данной MA.
vlan–list	Идентификатор VLAN. Диапазон значений: 1–40934. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами Для диапазона используйте дефис (-).

ethernet cfm mep enable

Команда включает административный режим MEP на интерфейсе или диапазоне интерфейсов. По умолчанию MEP выключены. Если они запущены, MEP начинают периодическую отправку сообщений Continuity Check (CC).

Значение по умолчанию: выключено

Формат: `ethernet cfm mep enable level 0-7 vlan vlan-list mpid 1-8191`

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.
mpid	Идентификатор MEP. Создает MEP, связанную с данной MA.
vlan–list	Идентификатор VLAN. Диапазон значений: 1–40934. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).

no ethernet cfm mep enable

Используйте no-форму команды для выключения MEP.

Формат: `no ethernet cfm mep enable level 0-7 vlan vlan-list mpid 1-8191`

Режим ввода команд: конфигурирование интерфейса

ethernet cfm mep active

Используйте эту команду, чтобы установить активный режим MEP на интерфейсе или диапазоне интерфейсов. Активный режим может иметь значения True или False.

Значение по умолчанию: False.

Формат: `ethernet cfm mep active level 0-7 vlan vlan-list mpid 1-8191`

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.
mpid	Идентификатор MEP. Создает MEP, связанную с данной MA.
vlanID	Идентификатор VLAN. Диапазон значений: 1–409. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).

no ethernet cfm mep active

Используйте no-форму команды, чтобы деактивировать MEP.

Формат: `no ethernet cfm mep active level 0-7 vlan vlan-list mpid 1-8191`

Режим ввода команд: конфигурирование интерфейса

ethernet cfm mip level

Используйте эту команду для настройки уровня промежуточной точки обслуживания (MIP). MIP настраиваются для каждого домена и каждого интерфейса или диапазона интерфейсов.

Формат: `ethernet cfm mip level 0-7`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.

ping ethernet cfm mac

Команда генерирует loopback-сообщения от настроенной MEP. Запускается из режима конфигурирования MA.

Формат: `ping ethernet cfm mac mac-address domain domain-name level 0-7 vlan vlan–list mpid 1- 8191 count 1-255`

Режим ввода команд: привилегированный

Параметр	*Описание*
mac-address	MAC-адрес места назначения, для которого необходимо подтвердить непрерывность связи.
domain	Имя домена.
level	Уровень домена обслуживания. Диапазон значений: 0–7. Значение по умолчанию: 0.
mpid	Идентификатор Maintenance End Point (MEP ID), от которой будут передаваться loopback-сообщения. Диапазон значений: 1–8191.
vlanID	Идентификатор VLAN. Диапазон значений: 1–409. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).
count	Количество LBM к передаче. Диапазон значений: 1–255. Значение по умолчанию: 5.

ping ethernet cfm remote–mpid

Команда генерирует loopback-сообщения от настроенной MEP. Запускается из режима конфигурирования MA.

Формат: `ping ethernet cfm remote-mpid 1-8191 domain domain-name level 0-7 vlan vlanID mpid 1- 8191 count 1-255`

Режим ввода команд: привилегированный

Параметр	*Описание*
remote–mpid	Идентификатор MEP, для которой необходимо подтвердить непрерывность связи. Диапазон значений: 1–8191.
domain	Название домена.
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.
vlanID	Идентификатор VLAN. Диапазон значений: 1–409. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).

mpid	Идентификатор MEP, от которой будут передаваться loopback-сообщения. Диапазон значений: 1–8191.
count	Количество LBM к передаче. Диапазон значений: 1–255. Значение по умолчанию: 5.

traceroute ethernet cfm mac

Эта команда генерирует сообщение трассировки линии от настроенной MEP. Запускается из режима конфигурирования MA.

Формат: `traceroute ethernet cfm mac mac-address [domain domain-name | level 0-7] vlan vlanID mpid 1-8191 ttl 1-255`

Режим ввода команд: привилегированный

Параметр	***Описание***
mac-address	MAC-адрес места назначения, для которого необходимо подтвердить непрерывность связи.
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.
mpid	MEP ID, с которой нужно передавать сообщения трассировки линии. Диапазон значений: 1–8191.
vlanID	Идентификатор VLAN. Диапазон значений: 1–40934. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами Для диапазона используйте дефис (-).
ttl	Предполагаемое количество хопов для LTM. Диапазон значений: 1–255. Значение по умолчанию: 64.

traceroute ethernet cfm remote–mpid

Эта команда генерирует сообщение трассировки линии от настроенной MEP. Запускается из режима конфигурирования MA.

Формат: `traceroute ethernet cfm remote-mpid 1-8191 [domain domain-name | level 0-7] vlan vlanID mpid 1-8191 ttl 1-255`

Режим ввода команд: привилегированный

Параметр	***Описание***
remote-mpid	MEP ID, для которого необходимо подтвердить непрерывность связи.
domain	Имя домена.
level	Уровень домена. Диапазон значений: 0–7. Значение по умолчанию: 0.
vlanID	Идентификатор VLAN. Диапазон значений: 1–4094. Отдельные непоследовательные идентификаторы, разделенные запятой (,) без пробелов и нулей между диапазонами. Для диапазона используйте дефис (-).
mpid	Идентификатор MEP, от которой будут передаваться сообщения трассировки линии (LTM). Диапазон значений: 1–8191.
ttl	Количество хопов, оставшихся до LTM. Уменьшается на 1 с каждым ответчиком LinkTrace, который обрабатывает LTM. Диапазон значений: 1–255. Значение по умолчанию: 65. Если LTM TTL равен 0 или 1, LTM не передается на следующий хоп, а при значении 0 LTM не генерируется.

show ethernet cfm domain

Используйте эту команду, чтобы отобразить настроенные параметры домена CFM.

Формат: `show ethernet cfm domain` *`domain-name`*

Режим ввода команд: привилегированный

Параметр	*Описание*
domain-name	Имя домена.
level	Уровень домена
total Services	Количество сервисных экземпляров.
VLAN	Идентификатор VLAN. Диапазон значений: 1–4094
service-name	Строка символов, которая идентифицирует определенную MA в домене.
CC–Interval	Интервал CCM. Временной интервал в секундах между успешными передачами CCM.

show ethernet cfm domain brief

Используйте данную команду, чтобы отобразить сводную информацию о настроенных параметрах домена CFM.

Формат: `show ethernet cfm domain brief`

Режим ввода команд: привилегированный

Параметр	*Описание*
CFM Feature	Указывает, включена ли функция Connectivity Fault Management (CFM).
MEP Archive Hold Time	Период в секундах, в течение которого будут храниться данные от отсутствующей Maintenance End Point (MEP) перед удалением. Допустимые значения: от 1 до 65535 секунд.
domain-name	Имя домена.
level	Уровень домена.
Services	Количество сервисных экземпляров.

show ethernet cfm maintenance-points local domain

Используйте эту команду, чтобы отобразить настроенный домен *domain–name*.

Формат: `show ethernet cfm maintenance-points local domain` *`domain–name`*

Режим ввода команд: привилегированный

Параметр	*Описание*
domain-name	Имя домена обслуживания.
MPID	MEP ID.
Level	Уровень домена.
Type	Тип точки обслуживания: MEP или MIP.
VLAN	MA, определяемая идентификатором VLAN. Диапазон значений: 1–4094.

Port	Индекс интерфейса физического порта или агрегированного канала, к которому присоединена MEP.
Direction	Направление для MEP. Возможные значения: • **up** – восходящий; • **down** – нисходящий.
CC Transmit	Если включено, MEP будет генерировать сообщения CCM.
MEP–Active	Указывает административный статус MEP. **True** указывает, что MEP функционирует нормально. **False** означает, что MEP прекратила функционировать. По умолчанию: **True**.
Operational Status	При значении **True** MEP оперативно включена.
MAC	MAC-адрес MEP.

show ethernet cfm maintenance-points local interface

Используйте эту команду, чтобы отобразить настроенные точки домена на интерфейсе *unit/slot/port*.

Формат: `show ethernet cfm maintenance-points local interface [`*`unit/slot/port`*`]`

Режим ввода команд: привилегированный

Параметр	***Описание***
MPID	MEP ID.
Level	Уровень домена.
Type	Тип точки обслуживания: MEP или MIP.
VLAN	MA, определяемая идентификатором VLAN. Диапазон значений: 1–4094.
Port	Индекс интерфейса физического порта или агрегированного канала, к которому присоединена MEP.
Direction	Направление для MEP. Возможные значения: • **up** – восходящий; • **down** – нисходящий.
CC Transmit	Если включено, MEP будет генерировать сообщения CCM.
MEP–Active	Указывает административный статус MEP. **True** указывает, что MEP функционирует нормально. **False** означает, что MEP прекратила функционировать. По умолчанию: **True**.
Operational Status	При значении **True** MEP оперативно включена.
MAC	MAC-адрес MEP.

show ethernet cfm errors

Используйте данную команду, чтобы отобразить ошибки MEP на определенном домене.

Формат: `show ethernet cfm errors`

Режим ввода команд: привилегированный

Параметр	***Описание***

Level	Уровень домена обслуживания.
SVID	12-битный идентификатор VLAN сервиса.
MPID	MEP ID
DefRDICcm	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.
DefMACStatus	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.
DefRemoteCCM	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.
DefErrorCCM	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.
DefXconCCM	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.

show ethernet cfm errors domain

Используйте данную команду, чтобы отобразить ошибки MEP на определенном домене.

Формат: `show ethernet cfm errors domain` *`domain-name`*

Режим ввода команд: привилегированный

Параметр	***Описание***
domain–name	Имя домена.
Level	Уровень домена.
SVID	12-битный идентификатор VLAN сервиса.
MPID	MEP ID.
DefRDICcm	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.
DefMACStatus	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления
DefRemoteCCM	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.
DefErrorCCM	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.
DefXconCCM	Целочисленное значение, определяющее дефект MEP с самым высоким приоритетом, который генерируется с момента последнего уведомления.

show ethernet cfm errors level

Используйте данную команду, чтобы отобразить ошибки MEP на определенном домене.

Формат: `show ethernet cfm errors level` *`level`*

Режим ввода команд: привилегированный

Параметр	*Описание*
Level	Уровень домена. Диапазон значений: 0–7.
SVID	12-битный VLAN ID сервиса.
MPID	MEP ID.
DefRDICcm	Remote Defect Indication, используемая MEP для передачи соседним MEP информации об обнаруженном дефекте. Такая MEP передает кадры с информацией ETH-RDI. MEP, прежде чем получить такие кадры, определяет, что соседняя MEP находится в дефектном состоянии.
DefMACStatus	Дефект MAC-статуса. Происходит, если порт с транслирующей MEP, не может передавать обычные данные или первичная VLAN MEP выключена. Дефект обнаруживается, когда последнее CCM, полученное локальной MEP от любой удаленной MEP, передает статус ошибки через статус порта TLV или статус интерфейса TLV.
DefRemoteCCM	Удаленный дефект MEP. Если от соседней MEP не поступают CCM-кадры с интервалом равным периоду передачи CCM MEP, умноженным на 3,5, то фиксируется потеря соединения с соседней MEP.
DefErrorCCM	Указывает MEP, которая получила CCM-кадр с неверным значением временного интервала.
DefXconCCM	Дефект кросс-подключения. Фиксируется в случае несовместимости одного из ожидаемых параметров CCM-кадра, например уровня домена, типа имени домена, типа сервисного имени, сервисного идентификатора и пр.

show ethernet cfm maintenance-points remote domain

Используйте эту команду, чтобы отобразить данные удаленных MEP в домене *domain–name*.

Формат: `show ethernet cfm maintenance-points remote domain` *`domain–name`*

Режим ввода команд: привилегированный

Параметр	*Описание*
domain–name	Имя домена.
MEP ID	MEP ID.
RMEP ID	Идентификатор Remote Maintenance Association End Point (RMEP) удаленной MEP.
Level	Уровень домена.
MAC	MAC-адрес удаленной MEP.
VLAN	MA, определяемая идентификатором VLAN. Диапазон значений: 1–4094.
Expiry Timer (sec)	Время истечения для записи последнего сообщения CCM на данной RMEP.
Service ID	Название VLAN ID сервиса.

show ethernet cfm maintenance-points remote level

Используйте эту команду, чтобы отобразить данные удаленных MEP в домене с уровнем *level*.

Формат: `show ethernet cfm maintenance-points remote level` *`level`*

Режим ввода команд: привилегированный

Параметр	*Описание*
domain–name	Имя домена.
MEP ID	MEP ID.
RMEP ID	Идентификатор Remote Maintenance Association End Point (RMEP) удаленной MEP.
Level	Уровень домена.
MAC	MAC-адрес удаленной MEP.
VLAN	MA, определяемая идентификатором VLAN. Диапазон значений: 1–4094
Expiry Timer (sec)	Время истечения для записи последнего сообщения CCM на данной RMEP.
Service ID	Название VLAN ID сервиса.

show ethernet cfm maintenance-points remote detail mac

Используйте эту команду, чтобы отобразить данные удаленной MEP с MAC-адресом *mac–addr*.

Формат: `show ethernet cfm maintenance-points remote detail mac` *`mac–addr`*

Режим ввода команд: привилегированный

Параметр	*Описание*
mac–addr	6-битный MAC-адрес.
MEP ID	MEP ID.
RMEP ID	Идентификатор Remote Maintenance Association End Point (RMEP ID) удаленной MEP.
Level	Уровень домена.
VLAN	MA, определяемая идентификатором VLAN. Диапазон значений: 1–4094
MAC	MAC-адрес удаленной MEP.
Expiry Timer (sec)	Время истечения для записи последнего сообщения CCM на данной RMEP.
Service ID	Идентификатор сервиса.

show ethernet cfm maintenance-points remote detail mpid

Используйте эту команду, чтобы отобразить данные удаленной MEP с идентификатором MEP mpid.

Формат: `show ethernet cfm maintenance-points remote detail mpid` *`1-8191`*

Режим ввода команд: привилегированный

Параметр	*Описание*
mac–addr	6-битный MAC-адрес.
MEP ID	MEP ID.
RMEP ID	Идентификатор Remote Maintenance Association End Point (RMEP ID) удаленной MEP.
Level	Уровень домена.
MAC	MAC-адрес удаленной MEP.
VLAN	MA, определяемая идентификатором VLAN. Диапазон значений: 1–4094.
Expiry Timer (sec)	Время истечения для записи последнего сообщения CCM на данной RMEP.
Service ID	Идентификатор сервиса.

show ethernet cfm traceroute-cache

Трассировка соединения, запущенная для MP, которая может быть просмотрена путем отображения базы данных отслеживания соединения — с помощью идентификатора операции или последовательности возвращенных чисел во время срабатывания.

Формат: `show ethernet cfm traceroute–cache [sequence–num` *`sequence–num`*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
sequence–num	Номер последовательности.

show ethernet cfm statistics

Используйте данную команду, чтобы отобразить статистику, поддерживаемую компонентом CFM для каждой MEP.

Формат: `show ethernet cfm statistics [domain` *`domain-name`* `| level` *`0-7`*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
Out–of–sequence CCMs received	Общее количество полученных неработающих последовательностей CCM-сообщений.
CCMs transmitted	Общее количество переданных CCM.
In–order Loopback Replies received	Общее количество полученных работающих откликов обратных петель (LBR).

Out–of–order Loopback Replies received	Общее количество полученных неработающих LBR.
Bad MSDU Loopback Replies received	Общее количество полученных неверных MSDU LBR.
Loopback Replies transmitted	Общее количество переданных откликов трассировки линии (LTR).
Unexpected LTRs received	Общее количество неожиданных откликов трассировки линии (LTR).

clear ethernet cfm maintenance-points remote

Используйте данную команду, чтобы очистить указанный домен или его уровень удаленной MEP из локальной базы данных.

Формат: clear ethernet cfm maintenance-points remote {domain *domain-name* | level *level*}

Режим ввода команд: привилегированный

clear ethernet cfm traceroute-cache

Используйте данную команду, чтобы очистить кэш трассировки линии Ethernet CFM.

Формат: `clear ethernet cfm traceroute-cache`

Режим ввода команд: привилегированный

9.43 Команды настройки функций Interface Error Disable и Auto Recovery

Функция Interface Error Disable автоматически выключает интерфейс при обнаружении ошибки; трафик не обрабатывается до тех пор, пока интерфейс не будет вновь включен вручную или, если настроена функция Auto Recovery, пока не пройдет настроенный интервал времени автоматического восстановления.

Для выключения интерфейса при ошибке и автоматического восстановления необходимо, чтобы на интерфейсе было обнаружено состояние ошибки, и интерфейс будет помещен в состояние диагностики путем его выключения. Выключенный при ошибке интерфейс не позволяет трафику проходить до того момента, пока интерфейс не будет снова запущен. Выключенный с ошибкой интерфейс можно включить вручную. В качестве альтернативы администратор может включить функцию Auto Recovery. Auto Recovery повторно запускает интерфейс по истечению настроенного интервала времени.

errdisable recovery cause

Используйте данную команду, чтобы включить функцию Auto Recovery для указанного события или всех событий. При включенной функции Auto Recovery порты в выключенном состоянии диагностики восстанавливаются, когда истекает интервал восстановления. Если на интерфейсе продолжают возникать ошибки, интерфейс может быть снова помещен в состояние для диагностики и выключен. Интерфейсы в этом состоянии могут быть включены путем введения команды no shutdown.

Значение по умолчанию: отсутствует

Формат: `errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp- mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service | link-flap}`

Режим ввода команд: глобальная конфигурация

no errdisable recovery cause

Используйте данную команду, чтобы выключить функцию Auto Recovery для указанного события. Интерфейсы в выключенном состоянии Auto Recovery не будут запускаться автоматически.

Формат: `no errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | sfp-mismatch | udld | ucast-storm | bcast-storm | mcast-storm | bpdustorm | keep-alive | mac-locking | denial-of-service service | link-flap}`

Режим ввода команд: глобальная конфигурация

errdisable recovery interval

Используйте эту команду, чтобы настроить временной интервал Auto Recovery. Интервал одинаков для всех событий. Время может быть любым значением от 30 до 86400 секунд. Когда интервал Auto Recovery истекает, система пытается повторно включить (поднять) порты, которые были выключены для диагностики.

Значение по умолчанию: 300

Формат: `errdisable recovery interval` *`30-86400`*

Режим ввода команд: глобальная конфигурация

no errdisable recovery interval

Используйте эту команду, чтобы вернуть временной интервал Auto Recovery в значение по умолчанию (300).

Формат: `no errdisable recovery interval`

Режим ввода команд: глобальная конфигурация

show errdisable recovery

Используйте данную команду, чтобы отобразить статус конфигурации errdisable для всех настроенных случаев.

Формат: `show errdisable recovery`

Режим ввода команд: привилегированный

Отображается информация, представленная ниже.

Параметр	***Описание***
arp-inspection	Состояние (Enable/Disable) ARP-проверки функции Auto Recovery.
bpdguard	Состояние (Enable/Disable) для STP bpduguard функции Auto Recovery.
dhcp-rate-limit	Состояние (Enable/Disable) лимита скорости DHCP функции Auto Recovery.
sfp-mismatch	Состояние (Enable/Disable) несовпадения SFP функции Auto Recovery.
udld	Состояние (Enable/Disable) UDLD функции Auto Recovery.
bpdustorm	Состояние (Enable/Disable) BPDU-шторма функции Auto Recovery.

keepalive	Состояние (Enable/Disable) для LBD функции Auto Recovery.
mac-locking	Состояние (Enable/Disable) MAC-привязки функции Auto Recovery.
denial-of-service	Состояние (Enable/Disable) DoS защиты Auto Recovery.
time interval	Временной интервал автоматического восстановления.

show interfaces status err-disabled

Используйте данную команду, чтобы отобразить интерфейсы, которые были выключены в связи с ошибкой, и время до автоматического восстановления.

Формат: `show interfaces status err-disabled`

Режим ввода команд: привилегированный

Отображается информация, представленная ниже.

Параметр	*Описание*
interface	Интерфейс, который был выключен в связи с ошибкой.
Errdisable Reason	Причина выключения интерфейса
Auto-Recovery Time Left	Оставшееся время до автоматического восстановления.

9.44 Команды настройки UDLD

Задача функции UniDirectional Link Detection (UDLD) — обнаруживать однонаправленные соединения и избегать их. Такие соединения являются аномалиями пересылки на канале коммуникаций 2 уровня, в которых двунаправленные соединения перестают передавать трафик в одном направлении. Используйте команды UDLD, чтобы обнаружить физические порты однонаправленных соединений. Для того чтобы однонаправленное соединение было обнаружено, UDLD необходимо включить на обеих сторонах соединения. Работа UDLD осуществляется путем обмена пакетами, содержащими информацию о соседних устройствах.

udld enable (Global Config)

Эта команда глобально включает UDLD на коммутаторе.

Значение по умолчанию: выключено

Формат: `udld enable`

Режим ввода команд: глобальная конфигурация

no udld enable (Global Config)

Эта команда глобально выключает UDLD на коммутаторе.

Формат: `no udld enable`

Режим ввода команд: глобальная конфигурация

udld message time

Данная команда настраивает интервал между тестовыми сообщениями UDLD-датчика на портах, которые находятся в фазе анонсирования. Диапазон — от 7 до 90 секунд.

Значение по умолчанию: 15 секунд

Формат: `udld message time interval`

Режим ввода команд: глобальная конфигурация

udld timeout interval

Данная команда настраивает интервал времени, после которого UDLD-соединение будет считаться однонаправленным. Диапазон — от 5 до 60 секунд.

Значение по умолчанию: 5 секунд

Формат: `udld timeout interval interval`

Режим ввода команд: глобальная конфигурация

udld reset

Данная команда перезагружает все интерфейсы, которые были выключены при работе UDLD.

Значение по умолчанию: отсутствует

Формат: `udld reset`

Режим ввода команд: привилегированный

udld enable (Interface Config)

Эта команда включает UDLD на определенном интерфейсе.

Значение по умолчанию: выключено

Формат: `udld enable`

Режим ввода команд: конфигурирование интерфейса

no udld enable (Interface Config)

Эта команда выключает UDLD на определенном интерфейсе.

Формат: `no udld enable`

Режим ввода команд: конфигурирование интерфейса

udld port

Данная команда выбирает операционный режим UDLD на данном интерфейсе. Если ключевое слово **aggressive** не введено, порт выполняет действия в обычном режиме.

Значение по умолчанию: normal

Формат: `udld port [aggressive]`

Режим ввода команд: конфигурирование интерфейса

show udld

Данная команда отображает глобальные настройки UDLD.

Формат: `show udld`

Режим ввода команд: пользовательский
привилегированный

Параметр	*Описание*

Admin mode	Глобальный административный режим UDLD.
Message Interval	Период времени в секундах между передачей тестовых пакетов UDLD-датчика.
Timeout Interval	Период времени в секундах перед тем, как принимается решение о том, что соединение однонаправленное.

show udld

Команда отображает настройки UDLD для указанного интерфейса *unit/slot/port*. Если введено ключевое слово all, отображается информация для всех портов.

Формат: `show udld {`*`unit/slot/port`*` | all}`

Режим ввода команд: пользовательский
привилегированный

Параметр	***Описание***
Port	Номер порта.
Admin Mode	Административный режим UDLD, настроенный на данном интерфейсе. Может быть **Enabled** или **Disabled**.
UDLD Mode	Режим UDLD, настроенный на интерфейсе. Может быть **Normal** или **Aggressive.**
UDLD Status	Статус соединения, определенный UDLD. Возможные значения: • **Undetermined**: UDLD не собрал достаточно информации для определения состояния порта. • **Not applicable**: UDLD выключен глобально или на порте. • **Shutdown**: UDLD обнаружил однонаправленное соединение и выключил порт. То есть порт находится в состоянии errDisabled. • **Bidirectional**: UDLD обнаружил двунаправленную линию связи. • **Undetermined (Link Down)**: порт перейдет в это состояние, когда связь порта физически выходит из строя по каким-либо иным причинам, кроме случая, когда он помещен в режим D-Disable протоколом UDLD на коммутаторе.

10 КОМАНДЫ НАСТРОЙКИ ФУНКЦИОНАЛА DATA CENTER

Команды пакета Data Center позволяют сетевым операторам развертывать сети Ethernet с использованием их полного потенциала в поддержку конвергентной сети с данными, поступающими по оптоволоконным каналам и Ethernet в соответствии со спецификацией рабочей группы FC-BB-5 стандарта ANSI T11. Эта возможность позволяет операторам развертывать сети с меньшими расходами и сохранять все операции управления сетью, которые существуют сегодня.

10.1 Команды настройки протокола DCBX

Протокол Data Center Bridging Exchange (DCBX) используется DCB-устройствами для обмена конфигурационной информацией с подключенными напрямую устройствами. Протокол также используется для обнаружения ошибок в конфигурациях партнерских DCB-устройств и, при необходимости, для настройки таких DCB-устройств.

lldp dcbx version

Используйте команду *lldp dcbx version* в режиме глобальной конфигурации чтобы настроить административную версию протокола DCBX. Эта команда позволяет коммутатору поддерживать определенную версию протокола DCBX или определять версию на партнерском устройстве и подстраиваться под нее. DCBX может быть настроен для работы в режиме IEEE, CEE или CIN. В режиме auto определение версии основано на версии партнерского устройства DCBX. Коммутатор работает либо в режиме IEEE, либо в режиме совместимости на каждом интерфейсе.

В режиме *auto* коммутатор пытается быстро начать обмен, посылая кадр IEEE, затем кадр CEE, а затем кадр CIN. При этом коммутатор будет анализировать полученный ответ и по итогам сразу же перейдет на версию партнерского устройства.

CIN — это Cisco Intel Nuova DCBX (версия 1.0). CEE — это объединенный усиленный протокол Ethernet DCBX (версия 1.06).

Значение по умолчанию: auto

Формат: `lldp dcbx version { auto | cin | cee | ieee }`

Режим ввода команд: глобальная конфигурация

Термин	***Значение***
auto	Автоматический выбор версии, основанный на ответе партнерского устройства.
cin	Принудительное включение режима CIN (DCBX 1.0).
cee	Принудительное включение режима CEE (DCBX 1.06).
ieee	Принудительное включение режима IEEE 802.1Qaz (DCBX 1.0).

no lldp dcbx version

Используйте **no**-форму команды, чтобы вернуть версию DCBX в значение по умолчанию **(auto)**.

Формат: `no lldp dcbx version`

Режим ввода команд: глобальная конфигурация

lldp tlv-select dcbxp

Используйте команду *lldp tlv-select dcbxp* в режиме конфигурирования интерфейса или глобальной конфигурации для отправки конкретных DCBX TLV, если LLDP на данном интерфейсе включен для передачи. Если дополнительных параметров нет, все DCBX TLV включаются для передачи. По умолчанию все DCBX TLV включены для передачи. Если настройка выполняется в режиме конфигурирования интерфейса, она перекрывает глобальную конфигурацию на указанном интерфейсе.

Значение по умолчанию: Передача всех TLV по умолчанию включена.

Формат: `lldp tlv-select dcbxp [ ets-config | ets-recommend | pfc | application-priority]`

Режим ввода команд: конфигурирование интерфейса

глобальная конфигурация

Термин	***Значение***
ets-config	Передать TLV конфигурации ETS
ets-recommend	Передать TLV рекомендации ETS.
pfc	Передать TLV конфигурации PFC.
application- priority	Передача TLV приоритета приложения.

no lldp tlv-select dcbxp

Команда **no lldp tlv-select dcbxp** используется, чтобы запретить LLDP отправлять все или некоторые DCBX TLV, даже если LLDP на данном интерфейсе включен для передачи.

Формат: `no lldp tlv-select dcbxp [ ets-config | ets-recommend | pfc | application-priority]`

Режим ввода команд: конфигурирование интерфейса
глобальная конфигурация

lldp dcbx port-role

Команда **lldp dcbx port-role** в режиме конфигурирования интерфейса позволяет настроить роль порта. Возможные значения: manual, auto-upstream, auto-downstream и configuration source. Чтобы сократить нестабильность конфигурации, порты, которые получают информацию о конфигурации из порта-источника конфигурации, будут поддерживать эту конфигурацию в течение двукратного времени жизни записи LLDP, даже если порт исходной конфигурации будет оперативно выключен.

Значение по умолчанию: используется роль порта ***manual***.

Формат: `lldp dcbx port-role {auto-up|auto-down|manual |configuration-source}`

Режим ввода команд: конфигурирование интерфейса

Термин	***Значение***
Manual	При такой настройке роли конфигурация портов не меняется под воздействием партнерских устройств или внутреннего распространения конфигурации. Такие порты будут анонсировать свою конфигурацию на партнерские устройства, если на данном порте включен DCBX. Если роль порта настроена как manual, функция willing bit будет выключена.

Auto-up	Анонсирует конфигурацию, но также готов принять конфигурацию от партнера по соединению и распространять ее внутренне к портам с настройкой auto-down, а также получать внутренне распространяемые конфигурации от портов auto-up. На этих портах функция willing bit включена. Такие порты должны быть подключены к FCF.
Auto-down	Анонсирует конфигурацию, но не настроен принимать ее от партнеров по соединению. При этом порт будет принимать конфигурацию, распространяемую внутренне источником конфигурации. На этих портах функция willing bit выключена. Выбор порта на основе совместимости полученной конфигурации подавляется. Такие порты должны быть подключены к доверенным FCF.
Configuration Source	В этом режиме роль источника конфигурации назначается порту вручную. Полученные через этот порт конфигурации распространяются на другие порты с автоматической конфигурацией. Выбор порта на основе совместимости полученной конфигурации подавляется. Такие порты должны быть подключены к доверенным FCF. На этих портах функция willing bit включена.

no lldp dcbx port-role

Используйте команду *no lldp dcbx port-role* в режиме конфигурирования интерфейса, чтобы настроить порт на ручной режим.

show lldp tlv-select

Команда *show lldp tlv-select* в привилегированном режиме отображает конфигурацию TLV по каждому интерфейсу.

Формат: `show lldp tlv-select {interface all | unit/slot/port }`

Режим ввода команд: привилегированный

Параметр	***Описание***
all	Все интерфейсы.
unit/slot/port	Идентификатор физического интерфейса.

show lldp dcbx interface

Команда *show lldp dcbx interface* в привилегированном режиме отображает локальный контрольный статус DCBX для интерфейса.

Формат: `show lldp dcbx interface all | unit/slot/port <detail>`

Режим ввода команд: привилегированный

Параметр	***Описание***
unit/slot/port	Идентификатор физического интерфейса.
all	Все интерфейсы.
Detail	Отобразить подробную информацию о DCBX.
Status	Вывод сводной информации о статусе.
trafficclass	Класс трафика может находиться в диапазоне от 0 до 6.
traffic class group	Значение Traffic Class Group может находиться в диапазоне от 0 до 2.

no classofservice traffic-class-group

Команда *no classofservice traffic-class-group* в режиме глобальной конфигурации или конфигурирования интерфейса используется для возвращения привязки классов трафика в значения по умолчанию.

Формат: `no classofservice traffic-class-group`

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

traffic-class-group max-bandwidth

Используйте команду *traffic-class-group max-bandwidth* в режиме глобальной конфигурации или конфигурирования интерфейса, чтобы определить максимальный уровень пропускной способности передачи для каждой TCG. Такую операцию также называют ограничением полосы канала, она помогает распределить временные всплески трафика во времени, ограничивая объем передаваемого трафика.

Значение по умолчанию: Max-bandwidth равно нулю для всех TCG.

Формат: `traffic-class-group max-bandwidth` *`bw-0 bw-1 … bw-n`*

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

Эта команда, выполненная в режиме конфигурирования интерфейса, действует только на один интерфейс, в то время как в режиме глобальной конфигурации применяется для всех интерфейсов.

Каждое значение bw-x представляет собой процентный уровень, который находится в диапазоне от 0 до 100 с шагом в 1. Все n значений пропускной способности должны быть заданы с помощью этой команды, их сумма не должна превышать 100%. Число n соответствует количеству поддерживаемых TCG. Максимальное значение пропускной способности для каждой TCG по умолчанию 0, это значит, что никакого верхнего предела не устанавливается, что позволяет очереди TCG потреблять любую доступную негарантированную пропускную способность интерфейса.

Если для любого параметра пропускной способности bw-x задано ненулевое значение, оно должно быть не меньше, чем действующее минимальное значение пропускной способности для соответствующей очереди. Нулевое значение для максимального параметра пропускной способности bw-x может быть задано в любое время без ограничений.

Максимальный предел пропускной способности может быть использован вместе с ограниченной схемой либо со схемой со строгим приоритетом планирования.

Нулевое значение (по умолчанию) означает неограниченный верхний предел передачи, который аналогичен 100%, хотя возможны незначительные эксплуатационные различия в зависимости от того, как устройство воспринимает отсутствие ограничений в сравнении с ограничением на уровне 100%.

no traffic-class-group max-bandwidth

Используйте команду no *traffic-class-group max-bandwidth* в режиме глобальной конфигурации или режиме конфигурирования интерфейса, чтобы восстановить для максимального значения пропускной способности каждой очереди значение по умолчанию.

Формат: `no traffic-class-group max-bandwidth`

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

traffic-class-group min-bandwidth

Команда *traffic-class-group min-bandwidth* в режиме глобальной конфигурации или конфигурирования интерфейса определяет гарантированный минимальный уровень пропускной способности передачи для каждой TCG.

Значение по умолчанию: Min-bandwidth равно нулю для всех TCG.

Формат: `traffic-class-group min-bandwidth bw-0 bw-1 … bw-n`

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

Данная команда, выполненная в режиме конфигурирования интерфейса, действует только на один интерфейс, в то время как в режиме глобальной конфигурации применяется для всех интерфейсов.

Каждое значение bw-x представляет собой процентный уровень, который находится в диапазоне от 0 до 100 с шагом в 1. Все n значений пропускной способности должны быть заданы с помощью этой команды, их общая сумма не должна превышать 100%. Число n зависит от платформы и соответствует количеству поддерживаемых TCG. Минимальное значение пропускной способности для каждой TCG по умолчанию 0, то есть наличие пропускной способности не гарантируется (предоставление по возможности).

Если указанное значение любого параметра bw-x больше, чем текущее максимальное значение пропускной способности для соответствующей TCG, соответствующая максимальная пропускная способность автоматически увеличивает значение на ту же величину.

no traffic-class-group min-bandwidth

Команда *no traffic-class-group min-bandwidth* в режиме глобальной конфигурации или режиме конфигурирования интерфейса восстанавливает для минимального значения пропускной способности каждой очереди значение по умолчанию.

Формат: `no traffic-class-group min-bandwidth`

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

traffic-class-group strict

Используйте команду *traffic-class-group strict* в режиме глобальной конфигурации или режиме конфигурирования интерфейса, чтобы активировать режим планировщика со строгим приоритетом для каждой TCG.

Значение по умолчанию: для всех TCG используется режим взвешенного планировщика.

Формат: `traffic-class-group strict` *`tcg-id-0`* [*`tcg-id-1 … tcg-id-n`*]

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

Данная команда, выполненная в режиме конфигурирования интерфейса, действует только на один интерфейс, в то время как в режиме глобальной конфигурации применяется для всех интерфейсов.

Команда должна задавать как минимум одно, но не более n значений tcg-id. Повторяющиеся значения tcg-id игнорируются. Каждое значение tcg-id находится в диапазоне от 0 до (n-1), где n обозначает общее количество TCG, поддерживаемых интерфейсом. Число n соответствует количеству поддерживаемых TCG.

Когда для TCG назначен строгий приоритет, минимальное значение пропускной способности для TCG игнорируется, пакеты определяются для передачи сразу после поступления. Максимальное значение пропускной способности для очереди, если таковое настроено, служит для ограничения исходящей скорости передачи очереди TCG со строгим приоритетом, чтобы она не потребляла всю пропускную способность интерфейса. Если строгий приоритет назначен нескольким TCG на одном интерфейсе, способ обработки их пакетов для передачи зависит от платформы. Одной из типичных схем является планирование всех TCG со строгим приоритетом перед взвешенными очередями. Приоритет среди TCG со строгим приоритетом остается за группой с наивысшим tcg-id.

no traffic-class-group strict

Используйте команду *no traffic-class-group strict* в режиме глобальной конфигурации или конфигурирования интерфейса, чтобы восстановить режим планировщика по умолчанию для каждой TCG.

Формат: `no traffic-class-group strict` *`tcg-id-0`* [*`tcg-id-1 … tcg-id-n`*]

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

traffic-class-group weight

Команда *traffic-class-group weight* в режиме глобальной конфигурации или конфигурирования интерфейса устанавливает вес для каждой TCG интерфейса.

Значение по умолчанию: для TCG0:TCG1:TCG2 вес установлен в соотношении 100%:0%:0%

Формат: `traffic-class-group weight` *`wp-0 wp-1 … wp-n`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

Данная команда, выполненная в режиме конфигурирования интерфейса, действует только на один интерфейс, в то время как в режиме глобальной конфигурации применяется для всех интерфейсов.

Каждое значение wp-x (weight percentage) представляет собой процентный уровень, который находится в диапазоне от 0 до 100 с шагом в 1. Все n значений пропускной способности должны быть заданы с помощью этой команды, их общая сумма не должна превышать 100%. Число n соответствует количеству поддерживаемых TCG. Значение wp-x по умолчанию находится в соотношении 1:2:3 для TCG0:TCG1:TCG2 и рассчитывается как 100%:0%:0%.

Для TCG, которые настроены со строгим приоритетом, процент веса не учитывается.

no traffic-class-group weight

Команда *no traffic-class-group weight* в режиме глобальной конфигурации или режиме конфигурирования интерфейса восстанавливает вес для каждой TCG интерфейса в значение по умолчанию.

Формат: `no traffic-class-group weight` *`wp-0 wp-1 … wp-n`*

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

show classofservice traffic-class-group

Используйте команду *show classofservice traffic-class-group* в привилегированном режиме, чтобы отобразить привязку классов трафика к Traffic Class Group.

Формат: `show classofservice traffic-class-group [`*`unit/slot/port`*`]`

Режим ввода команд: привилегированный

Расширенный выбор режима передачи и Traffic Class Group

classofservice traffic-class-group

Команда *classofservice traffic-class-group* в режиме глобальной конфигурации или конфигурирования интерфейса используется для привязки внутренних значений Traffic Class Group (TCG).

Значение по умолчанию: все классы трафика привязаны к TCG 0.

Формат: `classofservice traffic-class-group` *`trafficclass traffic class group`*

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейс

Параметр	***Описание***
unit/slot/port	Необязательный параметр, действует только на платформах, которые поддерживают независимое распределение класса сервисов для каждого порта. • Если значение unit/slot/port указано, выводятся таблицы привязки TCG для этого интерфейса. • Если значение unit/slot/port пропущено, отображаются глобальные параметры конфигурации (которые могут быть заменены конфигурацией конкретных портов).

Traffic Class	Идентификатор очереди класса трафика.
Traffic Class Group	Идентификатор TCG.

10.2 Команды настройки FIP Snooping

Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) используется для выполнения функций обнаружения, инициализации и технического обслуживания устройств FC_BB_E. FIP использует отдельный от FCoE EtherType для обнаружения, изолирования, инициализации и обслуживания от прочего трафика, трафика FCoE. FIP-кадры (за одним исключением) имеют стандартный Ethernet-размер (1518 байт для кадра 802.1q), тогда как FCoE-кадры имеют максимум 2240 байт.

В этой части описаны процедуры FIP Snooping, т. е. метода контроля кадров, используемого мостами FIP Snooping для мониторинга FIP-кадров, и применения к ним политик, основанных на данных заголовка L2 в этих кадрах, в соответствии с рекомендациями Приложения C FC_BB_5 ред. 2.00. Возможности FIP Snooping перечислены ниже.

1. Автоматическая настройка Ethernet-списков контроля доступа (ACL) на основе данных в Ethernet-заголовках FIP-кадров.
2. Эмуляция двухточечных FC-соединений внутри сети DCB Ethernet.
3. Повышение безопасности/надежности FCoE за счет предотвращения подмены MAC-адресов FCoE.

Решение моста FIP Snooping поддерживает только конфигурации портов в режиме периметра и подключенных к FCF и предназначено исключительно для использования в периферийной части коммутируемой сети.

Настройки портов коммутатора, где включена функция FIP Snooping, делятся на следующие категории.

1. Порт периметра или периферийный порт (подключен непосредственно к ENode).
2. Порт, подключенный к FCF (который принимает трафик от FCF, направленных на ENode).

По умолчанию режим порта в сети VLAN с включенным FCoE установлен как порт периметра. Порты, подключенные к FCF, должны быть настроены пользователем.

feature fip-snooping

Команда *feature fip-snooping* в режиме глобальной конфигурации глобально включает FIP Snooping на коммутаторе. Когда функция FIP Snooping выключена, полученные FIP-кадры пересылаются или распространяются по обычным правилам многоадресной рассылки.

Когда FIP Snooping включена, на коммутаторе устанавливаются списки контроля доступа FC-BB-5, Приложение D, и FIP-кадры отслеживаются. FIP Snooping не позволяет кадрам FIP или FCoE проходить через порт до тех пор, пока на порте не будет включен PFC. Для передачи значений Dot1p по сети на интерфейсе должно быть включено тегирование трафика.

Значение по умолчанию: выключено

Формат: `feature fip-snooping`

Режим ввода команд: глобальная конфигурация

no feature fip-snooping

Используйте no-форму команды, чтобы вернуть настройки к значениям по умолчанию и глобально выключить FIP Snooping. Когда функция FIP Snooping глобально выключена, полученные FIP-кадры пересылаются или распространяются по обычным правилам многоадресной рассылки. Кроме того, пока не включена функция FIP Snooping, другие команды FIP Snooping недоступны.

Формат: `no feature fip-snooping`

Режим ввода команд: глобальная конфигурация

Пример:

Команда выключает функцию FIP Snooping.

```
s1(config)#no feature fip-snooping
```

fip-snooping enable

Используйте команду *fip-snooping enable* в режиме конфигурирования VLAN, чтобы включить FIP Snooping для пакетов на настроенных VLAN. Функция FIP Snooping в сетях VLAN по умолчанию выключена.

Чтобы FIP Snooping работала на данном интерфейсе, необходимо включить Priority Flow Control (PFC). Для передачи значения Dot1p по сети на интерфейсе должно быть включено тегирование трафика.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Значение по умолчанию: выключено

Формат: `feature fip-snooping`

Режим ввода команд: конфигурирование VLAN

no fip-snooping enable

Используйте ***no***-форму команды, чтобы вернуться в режим по умолчанию (выкл.).

Формат: `no feature fip-snooping`

Режим ввода команд: конфигурирование VLAN

fip-snooping fc-map

Используйте команду *fip-snooping fc-map* в режиме конфигурирования VLAN, чтобы настроить значение FC-MAP на VLAN. Значение FC-MAP используется, чтобы обезопасить коммутатор от неверной конфигурации.

При настройке с использованием заводских MAC-адресов FCoE-устройства передают кадры, содержащие значения FC-MAP в старших 24 битах. Через VLAN передаются только кадры, которые соответствуют настроенному значению FC-MAP. Кадры с MAC-адресов, которые не соответствуют значению FC-MAP, отбрасываются.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Значение по умолчанию: значение FC-MAP по умолчанию — 0x0efc00.

Формат: `fip-snooping fc-map 0x0 – 0xffffff`

Режим ввода команд: конфигурирование VLAN

Параметр	*Описание*
map value	Допустимые значения FC-MAP находятся в диапазоне от 0x0 до 0xffffff.

no fip-snooping fc-map

No-форма команды отмены устанавливает FC-MAP для VLAN в значение по умолчанию.

Формат: `no fip-snooping fc-map`

Режим ввода команд: конфигурирование VLAN

fip-snooping port-mode

Чтобы передать FIP-пакеты, полученные от узлов, на канал FCF, коммутатор должен знать интерфейсы, к которым подключены FCF. Используйте команду *fip-snooping port-mode* в режиме конфигурирования интерфейса, чтобы настроить интерфейс, подключенный к каналу FCF. По умолчанию, если интерфейс не настроен как подключенный к FCF, интерфейс будет настроен как интерфейс узла.

Рекомендуется, чтобы подключенные к FCF порты были настроены в режим auto-upstream, чтобы получать данные DCBX и распространять их далее на CNA-порты (подключенные к узлам).

Интерфейсы должны быть настроены в режиме trunk или general и включены для PFC, прежде чем FCoE-трафик сможет проходить через порт.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Значение по умолчанию: настроен как интерфейс узла.

Формат: `fip-snooping port-mode fcf`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
fcf	Fibre Channel Fabric.

show fip-snooping

Используйте команду *show fip-snooping* в пользовательском или привилегированном режиме, чтобы отобразить информацию о глобальных настройках и статусе FIP Snooping.

Формат: `show fip-snooping`

Режим ввода команд: пользовательский

привилегированный

Отображается информация, представленная ниже.

Параметр	*Описание*
Global Mode	Fibre Channel Fabric.
FCoE VLAN List	Список идентификаторов VLAN, на которых включена FIP Snooping.

FCFs	Количество FCF, обнаруженных на коммутаторе.
ENodes	Количество узлов ENode, обнаруженных на коммутаторе.
Sessions	Общее количество виртуальных сессий на коммутаторе.
Max VLANs	Максимальное количество сетей VLAN, которые могут быть доступны для FIP Snooping на коммутаторе.
Max FCFs in VLAN	Максимальное количество FCF, поддерживаемых одной VLAN.
Max ENodes	Максимальное количество узлов ENode, поддерживаемых коммутатором.
Max Sessions	Максимальное количество сессий, поддерживаемых коммутатором.

show fip-snooping enode

Используйте команду *show fip-snooping enode* в пользовательском или привилегированном режиме, чтобы отобразить информацию об интерфейсах, подключенных к узлам ENode.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Формат: `show fip-snooping enode [ENode-mac]`

Режим ввода команд: пользовательский

привилегированный

Параметр	***Описание***
ENode-mac	MAC-адрес отображаемого узла ENode.

Команда отображает следующую информацию.

Параметр	***Описание***
Interface	Интерфейс, к которому подключен ENode.
VLAN	Идентификатор VLAN, к которой принадлежит ENode.
NameID	Имя ENode.
FIP-MAC	MAC-адрес ENode.
FCID	Идентификационный номер FC-канала виртуального порта, созданный FCF, когда ENode авторизовался в сети.
Sessions Established	Количество успешно установленных виртуальных подключений.

Команда выводит на экран следующую дополнительную информацию, если указан дополнительный аргумент.

Параметр	***Описание***
Sessions Waiting	Количество виртуальных подключений, ожидающих принятия от FCF.
Sessions Failed	Количество неудавшихся сессий.
Max-FCoE-PDU	Максимальный размер PDU FCoE, который MAC-адрес узла ENode будет использовать для трафика FCoE. Это эквивалентно максимальной полезной нагрузке кадра Ethernet, которую ENode намерен отправлять.
Time elapsed	Время с момента первой зафиксированной успешной сессии узла ENode.

show fip-snooping fcf

Используйте команду **show fip-snooping fcf** в пользовательском или привилегированном режиме, чтобы отобразить информацию об интерфейсах, подключенных к FCF.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Формат: `show fip-snooping fcf [fcf-mac]`

Режим ввода команд: пользовательский

привилегированный

Следующая информация отображается, если не прописан mac-аргумент FCF.

Параметр	***Описание***
Interface	Интерфейс, к которому подключен FCF.
VLAN	Идентификаторы VLAN, к которым относится FCF.
No. of ENodes	Общее количество узлов ENode, подключенных к FCF
FPMA/SPMA	Тип MAC-адреса для узла ENode, согласованный с FCF.
FCMAP	FCMAP значение, используемое FCF.
FIP-MAC	MAC-адрес FCF.
Fabric Name	Имя FCF.

Ниже показана дополнительная информация, отображаемая, если аргумент MAC-адреса FCF прописан.

Параметр	***Описание***
Sessions	Общее количество сессий, принятых FCF в связанной VLAN.
D-bit	Отражает значение D-бит, представленное самым последним анонсом обнаружения, полученным от FCF. Когда значение D-бит равно нулю, мост FIP Snooping проверяет периодические KeepAlive-кадры VN_Port FIP, связанные с FCF, и анонсы обнаружения, отправленные FCF. Когда D-бит установлен как 1, коммутатор отбрасывает отслеженные KeepAlive-кадры VN_Port FIP, связанные с FCF, и не прерывает FCoE-сессии, установленные с FCF на основе интервала FKA_VN_PERIOD*5.
Available for Login	Отражает значение A-бита, представленное самым последним анонсом обнаружения, полученным от FCF. Предоставляет информацию о том, что передающий FCF доступен для FIP-кадров FLOGI/FDISC от узлов ENode. Это справочная информация, не имеющая никакого влияния на существующие подключения.
Priority	Приоритет, исходящий от FCF в запрошенном анонсе обнаружения. Указывает приоритет, который был назначен в FCF вручную.
FKA-ADV	FIP keepalive-интервал (FKA_ADV_PERIOD) в секундах, настроенный на FCF и умноженный на пять. Например, если период FKA_ADV, настроенный на FCF, равен 80 секундам, значение этого поля равно 400.
FCF Expiry Time	Значение таймера мониторинга состояния FCF. Запись FCF и все связанные с ней виртуальные сессии будут удалены, когда значение достигает 0. Это значение сбрасывается на Configured FKA- ADV каждый раз, когда от FCF-MAC приходит анонс обнаружения.
Time Elapsed	Время с момента обнаружения FCF.

show fip-snooping sessions

Используйте команду show fip-snooping sessions в пользовательском или привилегированном режиме, чтобы отобразить информацию об активных сессиях FIP Snooping.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Формат: `show fip-snooping sessions [[[vlan` *`vlan-id`*`] | [interface` *`interface-id`*`] | [fcf fcf- mac [enode` *`Enode-mac`*`]]] [detail]]`

Режим ввода команд: пользовательский, привилегированный

Параметр	***Описание***
Interface-id	Идентификатор интерфейса, где включена функция FIP Snooping.
FCF-MAC	MAC-адрес FCF в рамках сессии.
ENode-MAC	MAC-адрес узла ENode в рамках сессии.
VLAN	Идентификатор VLAN, к которой принадлежит сессия.
FCoE MAC	MAC-адрес источника пакетов FCoE, выданные узлом ENode в рамках сессии.
FC-ID	Идентификатор FC-канала виртуального порта, созданного FCF, когда VN_Port узла ENode сделал запрос FLOGI/NPIV/FDISC.

Вывод команды меняется при использовании опции *detail*. В этом случае выводится следующая информация.

Параметр	***Описание***
VLAN	Сеть VLAN, к которой принадлежит сессия.
FC-MAP	FCMAP-значение, используемое FCF.
FCFs	Количество обнаруженных FCF.
ENodes	Количество обнаруженных узлов ENode.
Sessions	Общее количество сессий в FCoE VLAN.
FCF Information	
Interface	Интерфейс, где обнаружен FCF.
MAC	MAC-адрес FCF.
ENodes	Общее количество узлов ENode, подключенных к FCF.
Sessions	Общее количество сессий, принятых FCF в связанной VLAN.
ENode Information	
Interface	Интерфейс, к которому подключен ENode.
MAC	MAC-адрес узла ENode.
Sessions	Общее количество сессий, исходящих из узлов ENode к FCF в сети VLAN.
Waiting	Общее количество подключений, ожидающих принятия FCF в VLAN.
Session Information	
FCoE-MAC	MAC-адрес источника пакетов FCoE, выданных узлом ENode в рамках сессии.

Request (FP, SP)	Тип запроса FIP-сессии, отправленный из ENode. Может быть FLOGI или FDESC (NPIV FDISC). Значения FP и SP являются значения FP-бит и SP-бит в запросах FLOGI или NPIV FDISC соответственно.
Expiry Time	Интервал истечения виртуального подключения/сессии. Используется для отслеживания состояния сессии. Когда значение достигает 0, запись сессии удаляется. Значение устанавливается как 450 секунд (5*90 сек) каждый раз, когда от узла ENode поступает связанный VN_Port FKA. Игнорируется (помечается как NA), если D-бит настроен как единица в анонсе обнаружения FCF.
Mode	Режим адресации, используемый VN_Port на ENode. Другими словами, это тип MAC-адреса, предоставленного (выбранного и возвращенного) FCF. Может быть одним из режимов адресации, т. е. FPMA или SPMA.
State	Состояние виртуальной сессии. Отображается как **Tentative** во время процесса входа ENode в FCF (используя FLOGI или FDESC). Отображает как **Active** после того, как ENode и FCF успешно установили виртуальное соединение.
Session-Time	Время с момента установки успешной виртуальной сессии узлом ENode и FCF. Значение отображается в формате **xd**, **yh**, **zm**, где **x** представляет дни, **y** — часы и **z** — минуты, прошедшие с этой успешной сессии. Для ожидающих сессий поле не предоставляет никакой полезной информации.

show fip-snooping statistics

Используйте команду *show fip-snooping statistics* в пользовательском или привилегированном режиме, чтобы отобразить статистику отслеженных FIP-пакетов в VLAN или на интерфейсе. Если необязательный аргумент (VLAN или интерфейс) не задан, команда отображает статистику для всех VLAN, где включена функция FIP Snooping.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Формат: `show fip-snooping statistics [vlan vlan-id] | [interface interface-id]`

Режим ввода команд: пользовательский

привилегированный

Параметр	***Описание***
vlan-id	VLAN, в которой включена функция FIP Snooping.
interface-id	Интерфейс VLAN, где включена функция FIP Snooping.

В следующей таблице описаны счетчики пакетов на одну FIP-операцию.

Счетчик пакетов	***Описание***
VR	Количество сообщений-запросов VLAN, полученных сетью VLAN.
VN	Количество сообщений-уведомлений VLAN, полученных VLAN.
MDS	Количество сообщений Multicast Discovery Solicitation, обнаруженных в VLAN.
UDS	Количество сообщений Unicast Discovery Solicitation, обнаруженных в VLAN.
FLOGI	Количество событий Fabric Login, обнаруженных в VLAN.
FDISC	Количество событий Fabric Discovery, обнаруженных в VLAN.
LOGO	Количество событий Fabric Logout, обнаруженных в VLAN.
VNPort-keep-alive	Количество сообщений VN_Port Keepalive, обнаруженных в VLAN.

MDA	Количество сообщений Multicast Discovery Advertisement, обнаруженных в VLAN.
UDA	Количество сообщений Unicast Discovery Advertisement, обнаруженных в VLAN.
FLOGI_ACC	Количество событий Fabric Login, принятых VLAN.
FLOGI_RJT	Количество событий Fabric Login, отклоненных VLAN.
FDISC_ACC	Количество событий Fabric Discovery, принятых VLAN.
FDISC_RJT	Количество событий Fabric Discovery, отклоненных VLAN.
LOGO_ACC	Количество событий Fabric Logout, принятых VLAN.
LOGO_RJT	Количество событий Fabric Logout, отклоненных VLAN.
CVL	Количество действий Clear Virtual Link на VLAN.

В следующей таблице описан второй интерфейс или счетчики, связанные с сессией.

Счетчик пакетов	***Описание***
Number of Virtual Session Timeouts	Количество виртуальных сессий, удаленных в связи с истечением таймера сессии.
Number of FCF Session Timeouts	Количество активных сессий с истекшим сроком жизни вследствие истечение срока жизни анонсов обнаружения FCF в сети VLAN
Number of Session configuration failures	Количество сессий в сети VLAN, которые не удалось настроить в аппаратном обеспечении.
Number of Sessions denied with FCF limit	Количество сессий, отклоненных для создания новых FCF, как только количество FCF достигло максимально допустимого в сети VLAN.
Number of Sessions denied with ENode limit	Количество запросов на создание сессий, отклоненных для нового ENode, т. к. количество узлов ENode достигло максимально допустимого в системе.
Number of Sessions denied with System limit	Количество сессий, которые не удалось создать, т. к. количество сессий достигло максимально допустимого в системе.

Когда в качестве аргумента указывается интерфейс, отображаются только применимые к нему статистические данные.

show fip-snooping vlan

Используйте команду *show fip-snooping vlan* в пользовательском или привилегированном режиме, чтобы отобразить информацию по FCoE VLAN и статус FIP Snooping, если указан дополнительный аргумент.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Формат: `show fip-snooping vlan [`*`vlan-id`*`]`

Режим ввода команд: пользовательский

привилегированный

Счетчик пакетов	***Описание***
vlan-id	VLAN, на которой включена функция FIP Snooping.
VLAN	Сеть VLAN, где включена/выполняется функция FIP Snooping.
FC-MAP	Отображаемый FCoE-префикс адреса FCoE переадресации для FCoE VLAN.
FCFs	Количество обнаруженных FCF.

ENodes	Количество обнаруженных узлов ENode.
Sessions	Общее количество сессий в FCoE VLAN.

clear fip-snooping statistics

Используйте команду *clear fip-snooping statistics* в пользовательском или привилегированном режиме, чтобы очистить статистику FIP Snooping в поддерживаемой VLAN или на интерфейсе. Если дополнительный аргумент (VLAN или интерфейс) не задан, команда очищает статистику на всех VLAN, где включена функция FIP Snooping.

Данная команда может использоваться только после включения FIP Snooping с помощью команды *feature fip-snooping*. В противном случае она не отобразится в дереве синтаксиса CLI.

Формат: `clear fip-snooping statistics [vlan vlan-id] | [interface in-terface-id]`

Режим ввода команд: пользовательский

привилегированный

Счетчик пакетов	***Описание***
vlan-id	VLAN, в которой включена функция FIP Snooping.
interface-id	Интерфейс VLAN, где включена функция FIP Snooping.

10.3 Команды настройки управления потоком на основании приоритета

Обычно если управление потоком включено для физического соединения, оно применяется ко всему трафику данного соединения. При возникновении перегрузок на аппаратном уровне выполняется отправка кадров Pause Frame, которые временно приостанавливают поток трафика. Приостановка трафика помогает предотвратить переполнение буфера и сброс кадров.

Управление потоком на основании приоритета (PFC) дает возможность указать, какой трафик приостанавливается на физическом соединении, если происходит перегрузка. Интерфейс может быть настроен на приостановку только трафика с высоким приоритетом (т. е. чувствительного к потере данных), когда необходимо предотвратить сброс кадров, позволяя при этом поступать на интерфейс трафику, который более устойчив к потере данных.

Приоритеты различаются по полю приоритета в заголовке IEEE 802.1Q VLAN, который идентифицирует значение приоритета IEEE 802.1p. Эти значения приоритетов должны быть привязаны к внутренним значениям класса сервиса (CoS).

Для активации управления потоком на основании приоритета для определенного значения CoS на интерфейсе:

1. убедитесь в том, что на интерфейсе включено тегирование трафика, чтобы значения приоритета 802.1p были доставлены по сети;

2. убедитесь в том, что значения приоритета 802.1p привязаны к значениям CoS(см. "classofservice dot1p-mapping").

Когда PFC выключен, интерфейс по умолчанию устанавливается на управление потоком для интерфейса IEEE 802.3x. Когда PFC включен, интерфейс не будет приостанавливать CoS, пока не будет определен хотя бы один приоритет no-drop.

priority-flow-control mode

Используйте команду *priority-flow-control mode* в режиме настройки мостового соединения Datacenter, чтобы включить функцию PFC на данном интерфейсе.

Чтобы FIP Snooping работала на данном интерфейсе, необходимо оперативно включить Priority Flow Control (PFC). Используйте *no*-форму команды, чтобы вернуться в режим по умолчанию (выкл.). Тегирование трафика (магистральный или обычный режим) должно быть включено на интерфейсе, чтобы передавать по сети значение dot1p. Кроме того, dot1mapping к классу обслуживания должен быть установлен как один к одному.

Когда на интерфейсе включен PFC, обычный механизм регулирования PAUSE оперативно выключен.

Значение по умолчанию: режим PFC выключен по умолчанию.

Формат: `priority-flow-control mode { on | off }`

Режим ввода команд: настройка мостового соединения Datacenter

Параметр	***Описание***
on	Включает PFC на интерфейсе.
off	Выключает PFC на интерфейсе.

no priority-flow-control mode

Используйте команду no priority-flow-control mode, чтобы вернуться в режим PFC по умолчанию (выкл.).

Формат: `no priority-flow-control mode`

Режим ввода команд: настройка мостового соединения Datacenter

priority-flow-control priority

Используйте команду *priority-flow-control priority* в режиме настройки мостового соединения Datacenter для настройки приоритетной группы на передачу без потерь (no-drop) или с потерями (drop) на выбранном интерфейсе. На интерфейсе может быть включено до двух приоритетов без потерь. Администратору необходимо настроить аналогичные приоритеты no-drop по всей сети, чтобы обеспечить непрерывную передачу определенного трафика без потерь.

Если PFC на данном интерфейсе не включен, команда не будет выполнена. Для передачи значения dot1p по сети на интерфейсе должно быть включено тегирование трафика. Кроме того, dot1pmapping к классу обслуживания должен быть установлен как один к одному.

Значение по умолчанию: для всех приоритетов — drop.

Формат: `priority-flow-control priority` *`priority-list`* `{drop | no-drop}`

Режим ввода команд: настройка мостового соединения Datacenter

Параметр	***Описание***
no-drop	Включение функционирования без потерь для выбранных приоритетов.
drop	Выключение функционирования без потерь для выбранных приоритетов.

no priority-flow-control priority

Используйте команду *no priority-flow-control priority* в режиме настройки мостового соединения Datacenter для включения функционирования с потерями для всех приоритетов интерфейса. Команда не оказывает влияния на интерфейсы с выключенным PFC или без настроенных приоритетов без потерь.

Формат: `no priority-flow-control priority`

Режим ввода команд: настройка мостового соединения Datacenter

clear priority-flow-control statistics

Команда clear priority-flow-control statistics очищает всю глобальную статистику и статистику интерфейсов PFC.

Формат: `clear priority-flow-control statistics`

Режим ввода команд: привилегированный

show interface priority-flow-control

Используйте команду *show interface priority-flow-control* в привилегированном режиме, чтобы отобразить информацию PFC для одного или всех интерфейсов.

Формат: `show interface [unit/slot/port] priority-flow-control`

Режим ввода команд: привилегированный

Параметр	***Описание***
unit/slot/port	Действительный Ethernet-порт.

Если номер интерфейса отсутствует, для всех интерфейсов отображается следующая информация.

Параметр	***Описание***
Interface Detail	Порт, для которого отображается информация.
PFC Operational Status	Оперативный статус интерфейса.
PFC Configured State	Административный режим PFC на интерфейсе.
Configured Drop Priorities	Значения 802.1p, которые настроены на приоритет с потерями на интерфейсе. Приоритеты с потерями не участвуют в Pause.
Configured No-Drop Priorities	Значения 802.1p, которые настроены на приоритет без потерь. Если приоритет 802.1p, настроенный без потерь, перегружен, то поток с данным приоритетом приостанавливается.
Operational Drop Priorities	Значения 802.1p, которые использует коммутатор с приоритетом потерь. Оперативные приоритеты с потерями могут быть не такими же, как настроенные приоритеты, если интерфейс принял другие приоритеты от похожего устройства через LLDP DCBX.
Configured No-Drop Priorities	Значения 802.1p, которые использует коммутатор с приоритетом без потерь. Оперативные приоритеты без потерь могут быть не такими же, как настроенные приоритеты, если интерфейс принял другие приоритеты от похожего устройства через LLDP DCBX.
Delay Allowance	Оперативный статус интерфейса.
Peer Configuration Compatible	Показывает, принял ли локальный коммутатор совместимую конфигурацию от другого коммутатора через LLDP DCBX.
Compatible Configuration Count	Число полученных конфигураций, принятых и обработанных как действующие. Это число не включает в себя повторяющиеся конфигурации.

Incompatible Configuration Count	Число полученных конфигураций, которые не были приняты от похожего устройства, потому что были несовместимы.
Priority	Значение приоритета 802.1p.
Received PFC Frames	Число PFC-кадров, полученных интерфейсом с соответствующим приоритетом 802.1p.
Transmitted PFC Frames	Число PFC-кадров, отправленных интерфейсом с соответствующим приоритетом 802.1p

10.4 Команды настройки QCN

Функция Quantized Congestion Notification (QCN) входит в состав пакета Data Center.

qcn enable

Используйте команду *qcn enable* в режиме глобальной конфигурации, чтобы включить QCN на всех портах системы. Эта команда общего включения. Когда QCN включена, система распознает CN-тег в принятых кадрах, алгоритм перегрузок работает на настроенных точках Congestion Point (CP) и отправляет сообщения Congestion Notification Messages (CNM) при выявлении перегрузки на CP.

Значение по умолчанию: выключено

Формат: `qcn enable`

Режим ввода команд: глобальная конфигурация

no qcn enable

Команда *no qcn enable* в режиме глобальной конфигурации выключает QCN на всех портах системы. Эта команда общего выключения. Когда QCN выключена, полученные кадры с CN-тегом рассматриваются как обычные кадры данных, CNM не генерируются.

Формат: `no qcn enable`

Режим ввода команд: глобальная конфигурация

qcn cnm-transmit-priority

Используйте команду *qcn cnm-transmit-priority* в режиме глобальной конфигурации, чтобы глобально настроить приоритет Dot1p для сообщений CNM, передающихся системой. Эта команда настраивает значение приоритета Dot1p, с которым передаются CNM. По умолчанию CNM передаются с нулевым приоритетом Dot1p.

Значение по умолчанию: 0

Формат: `qcn cnm-transmit-priority dot1p priority`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
dot1p priority	Диапазон: 0–7.

no qcn cnm-transmit-priority

Команда *no qcn cnm-transmit-priority* в режиме глобальной конфигурации устанавливает приоритет Dot1p для сообщений CNM, передающихся системой, в значение по умолчанию.

Формат: `no qcn cnm-transmit-priority`

Режим ввода команд: глобальная конфигурация

qcn cnpv-priority (datacenter bridging config)

Используйте команду *qcn cnpv-priority* в режиме настройки мостового соединения Datacenter, чтобы глобально настроить CP (очередь портов), которые привязываются к определенным приоритетам Dot1p, когда перегрузка включена (**interior**), выключена (**disable**) или является периферийной точкой перегрузки (**edge**) для всех портов, у которых защитный режим настроен как component.

Значение по умолчанию: все приоритеты для QCN выключены.

Формат: `qcn cnpv-priority priority {interior | edge | disable}`

Режим ввода команд: настройка мостового соединения Datacenter

Счетчик пакетов	***Описание***
cnpv-priority	Диапазон: 0–7.
Interior (ICP)	Используется, когда поток с указанным приоритетом Dot1p должен распознавать перегрузку. Этот параметр позволяет обнаруживать перегрузку выбранного приоритета.
Edge congestion point (ECP)	Используется, когда CP находится на периферии домена уведомления о перегрузке (CND).
Disabled for QCN	Используется, когда требуется, чтобы приоритет не распознавал перегрузку. Этот параметр выключает обнаружение перегрузок на приоритете.

qcn cnpv-priority alternate-priority

Используйте команду *qcn cnpv-priority alternate-priority* в режиме глобальной конфигурации, чтобы настроить альтернативный приоритет для выбранного cnpv-приоритета. Когда получен кадр с приоритетом Dot1p, равной значению приоритета уведомления о перегрузке, значение приоритета кадра заменяется на альтернативный приоритет. Альтернативный приоритет применяется к входящим кадрам, только если приоритет dot1p входящего кадра равен CNPV приоритета CP и CP сконфигурирована как периферийная.

Используйте настройки альтернативного приоритета, чтобы отклонять трафик, поступающий из неосведомленных о CN источников. Трафик из источников, неосведомленных о перегрузке, обнаруживается при входе в домен CND так, чтобы ресурсы, назначенные очередям с поддержкой уведомлений перегрузки, не исчерпывались трафиком из неосведомленных о QCN источников. Так как кадры поступают из источников без QCN и не имеют CN-тега. Если кадры передаются в очереди с включенным информированием перегрузки, то они могут привести к перегрузке и, в свою очередь, вызывают генерацию CNM. Это бесполезно для источников, которые не осведомлены о QCN.

Такая конфигурация применяется ко всем портам, чей режим защиты конфигурирован как component.

Формат: `qcn cnpv-priority cnpv priority alternate-priority non-cnpv priority`

Режим ввода команд: глобальная конфигурация

Счетчик пакетов	***Описание***
cnpv priority	Диапазон: 1–7.
non-cnpv priority	Диапазон альтернативных приоритетов: 0–7.

no qcn cnpv-priority alternate-priority

Команда *no qcn cnpv-priority alternate-priority* в режиме глобальной конфигурации устанавливает альтернативный приоритет в значение по умолчанию.

Формат: `no qcn cnpv-priority cnpv priority alternate-priority`

Режим ввода команд: глобальная конфигурация

qcn cnpv-priority cp-creation

Используйте команду *qcn cnpv-priority cp-creation* в режиме глобальной конфигурации, чтобы настроить охват по умолчанию для режима защиты порта приоритетом, когда CP только создается. По умолчанию областью действия режима защиты каждого порта может иметь значение ***admin*** или ***component***.

Значение по умолчанию: создание CP включено

Формат: `qcn cnpv-priority` *`cnpv-priority`* `cp-creation {enable | disable}`

Режим ввода команд: глобальная конфигурация

Счетчик пакетов	***Описание***
cnpv-priority	Диапазон: 1–7.
admin scope	По приоритету.
component scope	По приоритету уровня конфигурации.
enable	Если создание CP включено, режим защиты порта устанавливается как component.
disable	Если создание CP выключено, режим защиты порта устанавливается как admin.

qcn cnpv-priority defense-mode-choice

Используйте команду *qcn cnpv-priority defense-mode-choice* в режиме конфигурирования интерфейса, чтобы установить режим защиты интерфейса как ***admin*** или ***component***.

Значение по умолчанию: включено

Формат: `qcn cnpv-priority` *`cnpv-priority`* `defense-mode-choice {admin | component}`

Режим ввода команд: конфигурирование интерфейса

Счетчик пакетов	***Описание***
cnpv-priority	Диапазон: 1–7.
admin scope	По приоритету.
component scope	По приоритету уровня конфигурации.

qcn cnpv-priority

Используйте команду *qcn cnpv-priority* в режиме настройки интерфейса, чтобы привязать CP (очередь портов) к определенным приоритетам Dot1p.

Эта конфигурация применяется, если режим защиты настроен как **Admin**.

Значение по умолчанию: по умолчанию QCN выключен для любого приоритета.

Формат: `qcn cnpv-priority priority {interior | edge | disable}`

Режим ввода команд: конфигурирование интерфейса

Счетчик пакетов	*Описание*
cnpv-priority	Диапазон: 0–7.
Возможные варианты для Congestion Point (CP):	
Interior (ICP)	Используется, когда поток с указанным приоритетом Dot1p должен распознавать перегрузку.
Edge congestion point (ECP)	Используется, когда CP находится на периферии домена уведомления о перегрузке (CND).
Disabled for QCN	Используется, когда требуется, чтобы приоритет не распознавал перегрузку. Этот параметр выключает обнаружение перегрузок на приоритете.

qcn cnpv-priority alternate-priority

Используйте команду *qcn cnpv-priority alternate-priority* в режиме конфигурирования интерфейса, чтобы настроить альтернативный приоритет на интерфейсе для приоритета входящих ICP. Значение альтернативного приоритета перекрывает установленный в глобальном режиме альтернативный приоритет для данного входящего ICP на порте. Эта конфигурация применяется, если режим защиты настроен как **Admin**.

Значение по умолчанию: по умолчанию используется альтернативный приоритет, настроенный глобально.

Формат: `qcn alternate-priority incoming priority alternate-priority`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
cnpv-priority	Диапазон: 1–7.
alternate-priority	Диапазон: 0–7.

no qcn cnpv-priority alternate-priority

Используйте команду *no qcn cnpv-priority alternate-priority* в режиме конфигурирования интерфейса, чтобы установить альтернативный приоритет выбранного приоритета порта в значение по умолчанию. Используется, если настроено глобальное значение альтернативного приоритета.

Значение по умолчанию: По умолчанию используется альтернативный приоритет, настроенный глобально.

Формат: `no qcn alternate-priority incoming-priority alternate-priority`

Режим ввода команд: конфигурирование интерфейса

qcn transmit-tlv enable

Используйте команду *qcn transmit-tlv enable* в режиме конфигурирования интерфейса, чтобы включить передачу QNC TLV через LLDP.

Значение по умолчанию: Передача QCN TLV по умолчанию выключена.

Формат: `qcn transmit-tlv enable`

Режим ввода команд: конфигурирование интерфейса

no qcn transmit-tlv enable

Используйте команду *no qcn transmit-tlv enable* в режиме конфигурирования интерфейса, чтобы выключить передачу QNC TLV. QNC TLV распространяются через LLDP.

Формат: `no qcn transmit-tlv enable`

Режим ввода команд: конфигурирование интерфейса

clear qcn statistics

Команда *clear qcn statistics* в привилегированном режиме сбрасывает счетчики переданных CNM в точках CP. Если интерфейс и CP не указаны, эта команда очищает все счетчики CNM для всех CP в системе. Если указан только номер интерфейса, то все счетчики CNM на интерфейсе будут сброшены.

Формат: `clear qcn statistics [interface unit/slot/port] [cp cp-index]`

Режим ввода команд: привилегированный

Параметр	***Описание***
unit/slot/port	Если указан только номер интерфейса, то все счетчики CNM на интерфейсе будут сброшены.
cp-index	Если указан только номер CP, то все счетчики CNM для этого индекса будут сброшены.

show qcn priority

Используйте команду *show qcn priority* в привилегированном режиме, чтобы отобразить конфигурацию QCN.

Формат: `show qcn priority [priority ] [interface unit/slot/port| all]`

Режим ввода команд: привилегированный

Параметр	***Описание***
priority	Если задан только параметр priority, отображается конфигурация по приоритету.
all	Если задан параметр all, отображается конфигурация для всех портов для данного приоритета.
unit/slot/port	Если указан номер интерфейса, команда отображает конфигурацию конкретного порта для данного приоритета.

Приведенные ниже данные отображаются в составе этой команды.

show qcn active priority

Используйте команду *show qcn active priority* в привилегированном режиме, чтобы отобразить оперативную конфигурацию QCN для указанного приоритета Dot1p.

Формат: `show qcn active priority 0–7`

Режим ввода команд: привилегированный

show qcn interface

Команда *show qcn interface* в привилегированном режиме отображает информацию CP для выбранных портов.

Формат `show qcn interface unit/slot/port [cp cpindex]`

Режим ввода команд: привилегированный

show qcn statistics

Используйте команду *show qcn statistics* в привилегированном режиме, чтобы отобразить статистику CNM и кадры с данными для всех портов или указанных CP портов.

Формат `show qcn statistics {interface unit/slot/port cp cp index}`

Режим ввода команд: привилегированный

11 КОМАНДЫ НАСТРОЙКИ МАРШРУТИЗАЦИИ

Данный раздел описывает команды маршрутизации, которые доступны в интерфейсе командной строки. Раздел «Команды маршрутизации» содержит следующие подразделы.

Все команды, приведенные в этом разделе, делятся на три функциональные группы:

- **Команды show выводят информацию о настройках коммутатора, статистику и прочую информацию.**
- **Команды конфигурации настраивают функции коммутатора. Каждой команде конфигурации соответствует команда show, выводящая на дисплей настройки.**
- **Команды очистки, которые возвращают отдельные параметры или все настройки к заводским.**

11.1 Команды настройки протокола ARP

В этом разделе описаны команды, которые используются для настройки Address Resolution Protocol (ARP) и для просмотра ARP-информации на коммутаторе. Протокол ARP связывает IP-адреса с MAC-адресами и хранит информацию в виде ARP-записей в таблице ARP.

arp

Данная команда создает ARP-запись в указанном экземпляре виртуального маршрутизатора (vrf vrf-name). Если виртуальный маршрутизатор не указан, статическая запись ARP создается в маршрутизаторе по умолчанию. Значение параметра ipaddress — это IP-адрес устройства в подсети, подключенной к существующему интерфейсу маршрутизации. Параметр macaddr — это MAC-адрес для этого устройства. Параметр interface указывает интерфейс, на котором доступно данное устройство.

MAC-адрес указывается в формате шести двузначных чисел шестнадцатеричной системы, разделенных двоеточиями, например 00:06:29:32:81:40.

Формат: `arp [vrf vrf-name] ipaddress macaddr interface {unit/slot/port | vlan id}`

Режим ввода команд: глобальная конфигурация

no arp

Эта команда удаляет ARP-запись в указанном виртуальном маршрутизаторе. Значение параметра *ipaddress* — это IP-адрес устройства в подсети, подключенной к существующему интерфейсу маршрутизации. Параметр *macaddr* — это MAC-адрес для этого устройства. Параметр *interface* указывает интерфейс, на котором доступно данное устройство.

Формат: `no arp [vrf vrf-name] ipaddress macaddr interface unit/slot/port`

Режим ввода команд: глобальная конфигурация

ip proxy-arp

Эта команда включает прокси-ARP на интерфейсе маршрутизатора или диапазоне интерфейсов. Без прокси-ARP устройство отвечает только на те ARP-запросы, целевой IP-адрес которых совпадает с адресом, настроенным на получившем запрос интерфейсе. С помощью прокси-ARP устройство может также ответить на запросы, касающиеся других доступных целевых IP-адресов. Устройство отвечает на запросы только в тех случаях, когда целевой IP-адрес места назначения доступен через интерфейсы, отличные от того, на который поступил ARP-запрос.

Значение по умолчанию: включено

Формат: `ip proxy-arp`

Режим ввода команд: конфигурирование интерфейса

no ip proxy-arp

Данная команда выключает прокси-ARP на интерфейсе маршрутизатора.

Формат: `no ip proxy-arp`

Режим ввода команд: конфигурирование интерфейса

ip local-proxy-arp

Эта команда разрешает интерфейсу отвечать на ARP-запросы, предназначенные для IP-адресов внутри данной подсети, и выполнять переадресацию трафика между узлами в подсети.

Значение по умолчанию: выключено

Формат: `ip local-proxy-arp`

Режим ввода команд: конфигурирование интерфейса

no ip local-proxy-arp

Используйте данную команду, чтобы вернуть локальный режим прокси-ARP на интерфейсе в значение по умолчанию.

Формат: `no ip local-proxy-arp`

Режим ввода команд: конфигурирование интерфейса

arp cachesize

Эта команда настраивает размер ARP-таблицы.

Значение по умолчанию: 6144

Формат: `arp cachesize` *`platform specific integer value`*

Режим ввода команд: глобальная конфигурация

no arp cachesize

Данная команда возвращает размер ARP-таблицы в значение по умолчанию.

Формат: `no arp cachesize`

Режим ввода команд: глобальная конфигурация

arp dynamicrenew

Команда позволяет системе автоматически обновлять динамические записи ARP при их устаревании. Когда запись ARP достигает предельного срока хранения, системе требуется принять решение, сохранить или удалить эту запись. Если запись за последнее время использовалась для передачи пакетов данных, система обновит ее, отправив ARP-запрос на соседний интерфейс. Если ответ на запрос будет получен, время хранения записи ARP в таблице обнуляется, удаление записи не происходит. Переадресация трафика к данному узлу на аппаратном уровне продолжится без перерывов. Если запись не используется для пересылки пакетов данных, при выключенной опции автоматического обновления она просто удаляется из ARP-таблицы, и при поступлении новых пакетов данных в адрес соответствующего узла потребуется новый ARP-запрос. Пока маршрутизатор не получит от узла ответ на ARP-запрос, трафик, поступающий в его адрес, может быть потерян. Записи шлюза, то есть записи для соседнего маршрутизатора, обновляются всегда. Динамическая опция обновления применима только для записей узлов.

Использование такой опции имеет один недостаток: однажды созданная запись продолжает оставаться в ARP-таблице и занимать место до тех пор, пока соседний узел отвечает на ARP-запросы, даже если переадресация трафика в его адрес не выполняется. В сети, где число потенциально соседних узлов превышает ресурсы ARP-таблицы, включение динамического обновления может привести к тому, что некоторые узлы не попадут в ARP-таблицу из-за ее переполнения, что затруднит взаимодействие с ними.

Значение по умолчанию: выключено

Формат: `arp dynamicrenew`

Режим ввода команд: привилегированный

no arp dynamicrenew

Эта команда выключает автоматическое обновление динамических записей ARP, когда они устаревают.

Формат: `no arp dynamicrenew`

Режим ввода команд: привилегированный

arp purge

Данная команда удаляет определенные IP-адреса из ARP-таблицы на указанном виртуальном маршрутизаторе. Если маршрутизатор не указан, запись ARP удаляется с маршрутизатора по умолчанию. Команда работает только в отношении динамических записей или записей шлюза.

\

Формат: `arp purge [vrf vrf-name] ipaddress interface {unit/slot/port | vlan id}`

Режим ввода команд: привилегированный

Параметр	*Описание*
ipaddress	IP-адрес для удаления из ARP-таблицы.
vrf-name	Виртуальный маршрутизатор, из таблицы которого будут удаляться IP-адреса..
interface	Интерфейс, из которого будут удаляться IP-адреса.

arp resptime

Эта команда настраивает время ожидания отклика на ARP-запрос.

Значение параметра *seconds* — положительное целое число, которое представляет собой время ожидания отклика IP-адреса на ARP-запрос в секундах. Диапазон значений для *seconds* составляет 1–10 секунд.

Значение по умолчанию: 1

Формат: `arp resptime` *`1-10`*

Режим ввода команд: глобальная конфигурация

no arp resptime

Эта команда настраивает значение времени ожидания отклика на ARP-запрос по умолчанию.

Формат: `no arp resptime`

Режим ввода команд: глобальная конфигурация

arp retries

Команда устанавливает максимальное количество повторных ARP-запросов.

Параметр *retries* — это целое число, которое представляет собой максимальное количество выполняемых повторных запросов. Диапазон значений для retries — 0–10 повторов.

Значение по умолчанию: 4

Формат: `arp retries` *`0-10`*

Режим ввода команд: глобальная конфигурация

no arp retries

Используйте эту команду, чтобы вернуть максимальное количество повторных ARP-запросов в значение по умолчанию.

Формат: `no arp retries`

Режим ввода команд: глобальная конфигурация

arp timeout

Эта команда настраивает время жизни записи ARP.

Значение параметра *seconds* — положительное целое число, которое представляет собой время устаревания записи ARP для IP-адреса в секундах. Диапазон значений для *seconds* составляет 15–21 600 секунд.

Значение по умолчанию: 1200

Формат: `arp timeout` *`15-21600`*

Режим ввода команд: глобальная конфигурация

no arp timeout

Данная команда устанавливает время жизни ARP-записи в значение по умолчанию.

Формат: `no arp timeout`

Режим ввода команд: глобальная конфигурация

clear arp-cache

Эта команда удаляет все динамические записи ARP из ARP-таблицы виртуального маршрутизатора. Если маршрутизатор не указан, очищается ARP-таблица маршрутизатора по умолчанию. Если указано ключевое слово gateway, удалению подлежат и записи шлюза.

Формат: `clear arp-cache [vrf` *`vrf-name`*`] [gateway]`

Режим ввода команд: привилегированный

clear arp-switch

Используйте эту команду, чтобы очистить содержимое ARP-таблицы коммутатора, которая содержит записи, полученные через порт управления. Чтобы оценить, насколько успешно выполнена команда, используйте команду *ping* от удаленной системы в адрес DUT. Чтобы просмотреть записи ARP, используйте команду *show arp switch*. После этого выполните команду *clear arp-switch* и еще раз проверьте записи с помощью *show arp switch*. ARP-записей больше не будет.

Формат: `clear arp-switch`

Режим ввода команд: привилегированный

show arp

Эта команда отображает содержимое ARP-таблицы для указанного экземпляра виртуального маршрутизатора. Если маршрутизатор не указан, отображается ARP-таблица маршрутизатора по умолчанию. Отображаемые записи не являются исчерпывающим перечнем записей ARP. Чтобы увидеть все записи ARP, требуется посмотреть объединенные результаты вывода команд *show arp* и *show arp switch*.

Формат: `show arp [vrf` *`vrf-name`*`]`
Режим ввода команд: привилегированный

Термин	***Значение***
Age Time (секунды)	Время жизни ARP-записи. Значение можно настраивать. Измеряется в секундах.
Response Time (секунды)	Время жизни ARP-запроса. Значение можно настраивать. Измеряется в секундах.
Retries	Максимальное количество повторных ARP-запросов.
Cache Size	Максимальное количество записей в ARP-таблице.
Dynamic Renew Mode	Показывает, пытается ли система автоматически обновлять динамические ARP-записи по мере устаревания.
Total Entry Count Current / Peak	Общее количество записей в ARP-таблице и максимальное количество записей в ARP-таблице.
Static Entry Count Current / Max	Количество статических записей в ARP-таблице и максимальное количество статических записей в ARP-таблице.

Для каждой ARP-записи отображается следующая информация.

Термин	*Значение*
IP Address	IP-адрес устройства в подсети, подключенного к существующему интерфейсу маршрутизации.
MAC Address	Аппаратный MAC-адрес этого устройства.
Interface	Интерфейс маршрутизации, связанный с ARP-записью устройства, в формате *unit/slot/port*.
Type	Настраиваемый тип записи. Возможные значения: Local, Gateway, Dynamic и Static.
Age	Время существования записи ARP с момента последнего обновления (в формате чч:мм:сс).

show arp brief

Команда отображает краткую информацию ARP-таблицы для указанного экземпляра виртуального маршрутизатора. Если маршрутизатор не указан, отображается ARP-таблица маршрутизатора по умолчанию.

Формат: `show arp brief [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

Термин	*Значение*
Age Time (секунды)	Время жизни ARP-записи. Значение можно настраивать. Измеряется в секундах.
Response Time (секунды)	Время жизни ARP-запроса. Значение можно настраивать. Измеряется в секундах.
Retries	Максимальное количество повторных ARP-запросов.
Cache Size	Максимальное количество записей в ARP-таблице.
Dynamic Renew Mode	Показывает, пытается ли система автоматически обновлять динамические ARP-записи по мере устаревания.
Total Entry Count Current / Peak	Общее количество записей в ARP-таблице и максимальное количество записей в ARP-таблице.
Static Entry Count Current / Max	Количество статических записей в ARP-таблице и максимальное количество статических записей в ARP-таблице.

show arp switch

Эта команда отображает содержимое ARP-таблицы коммутатора.

Формат: `show arp switch`

Режим ввода команд: привилегированный

Термин	*Значение*
IP Address	IP-адрес устройства в подсети, подключенного к коммутатору.
MAC Address	Аппаратный MAC-адрес этого устройства.
Interface	Интерфейс маршрутизации, связанный с ARP-записью устройства, в формате *unit/slot/port*.

11.2 Команды настройки IP-маршрутизации

В этой части описаны команды, которые используются для включения и настройки на коммутаторе IP-маршрутизации.

routing

Данная команда включает IPv4- и IPv6-маршрутизацию на интерфейсе или диапазоне интерфейсов. Текущее значение этой функции можно посмотреть с помощью команды show ip brief. Значение будет показано как параметр Routing Mode.

Значение по умолчанию: выключено

Формат: `routing`

Режим ввода команд: конфигурирование интерфейса

no routing

Эта команда выключает маршрутизацию на интерфейсе.

Текущее значение этой функции можно просмотреть с помощью команды show ip brief. Значение будет показано как параметр Routing Mode.

Формат: `no routing`

Режим ввода команд: конфигурирование интерфейса

ip routing

Эта команда включает режим IP-маршрутизатора на коммутаторе.

Формат: `ip routing`

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

no ip routing

Команда выключает режим IP-маршрутизатора на коммутаторе.

Формат: `no ip routing`

Режим ввода команд: глобальная конфигурация

ip address

Данная команда настраивает IP-адрес на интерфейсе или диапазоне интерфейсов. Эту команду также можно использовать для настройки одного или нескольких вторичных IP-адресов на интерфейсе. Команда поддерживает стандарт RFC 3021 и принимает 31-разрядные префиксы для PtP IPv4-соединений.

31-разрядная маска подсети поддерживается только интерфейсами маршрутизации. Эта функция не поддерживается на интерфейсах сетевых портов и сервисных портов, поскольку на таких интерфейсах управления коммутатор выступает в качестве узла, а не маршрутизатора. 32-разрядная маска подсети поддерживается только на loopback-интерфейсах.

Формат: `ip address ipaddr {subnetmask | /masklen} [secondary]`

Режим ввода команд: конфигурирование интерфейса

Термин	*Значение*
ipaddr	IP-адрес интерфейса.
subnetmask	4-значное число в десятичной форме, обозначающее маску подсети интерфейса.
masklen	Реализует стандарт RFC 3021. При использовании в маске подсети выражения с разделителем «/» это целое число, которое указывает длину маски подсети. Диапазон составляет от 5 до 32 бит.

no ip address

Данная команда удаляет IP-адрес интерфейса. Значение ipaddr — это IP-адрес интерфейса в формате a.b.c.d, где диапазон значений a, b, c и d составляет 1–255. Значение subnetmask — это 4-значное число в десятичной форме, обозначающее маску подсети интерфейса. Чтобы удалить все IP-адреса (первичные и вторичные), настроенные на интерфейсе, введите команду no ip address.

Формат: `no ip address [{ipaddr subnetmask [secondary]}]`

Режим ввода команд: конфигурирование интерфейса

ip address dhcp

Данная команда включает DHCPv4-клиент на стандартном (in-band) интерфейсе, позволяя ему получать информацию о сети от DHCP-сервера сети (например, IP-адрес, маску подсети и шлюз по молчанию). Когда на интерфейсе включен DHCP-клиент, система автоматически удаляет все IPv4-адреса, настроенные на интерфейсе вручную.

Чтобы включить DHCPv4-клиент на стандартном интерфейсе и отправлять сообщения DHCP-клиента с опцией идентификатора, используйте команду ip address dhcp client-id в режиме конфигурирования интерфейса.

Значение по умолчанию: выключено

Формат: `ip address dhcp [client-id]`

Режим ввода команд: конфигурирование интерфейса

no ip address dhcp

Команда no *ip address dhcp* освобождает занятый адрес и выключает DHCPv4-клиент на интерфейсе. Используйте no-форму команды *ip address dhcp client-id*, чтобы удалить опцию *client-id* и выключить DHCP-клиент на стандартном интерфейсе.

Формат: `no ip address dhcp [client-id]`

Режим ввода команд: конфигурирование интерфейса

ip default-gateway

Эта команда позволяет вручную настроить шлюз по умолчанию для коммутатора. Настроить можно только один шлюз по умолчанию. При использовании данной команды несколько раз каждая новая команда будет заменять ранее указанные значения.

Когда системе не задан более конкретный маршрут к точке назначения пакета, она направляет пакет на шлюз по умолчанию. Система устанавливает маршрут IPv4 по умолчанию, где адрес этого шлюза указан в качестве соседнего адреса. Приоритетный маршрут — 253. Шлюз по умолчанию, настроенный с помощью данной команды, имеет приоритет над шлюзом по умолчанию, полученным от DHCP-сервера.

Формат: `ip default-gateway` *ipaddr*

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

Параметр	***Описание***
ipaddr	IPv4-адрес подключенного маршрутизатора.

no ip default-gateway

Эта команда удаляет из конфигурации адрес шлюза по умолчанию.

Формат: `no ip default-gateway` *ipaddr*

Режим ввода команд: конфигурирование интерфейса

ip load-sharing

Эта команда настраивает режим балансировки нагрузки IP ECMP.

Значение по умолчанию: src-dst-ip-port

Формат: `ip load-sharing` *mode* `{inner | outer}`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
mode	Настраивает балансировку нагрузки или режим совместного доступа для всех групп ECMP. • src-ip: на основе хэша, используя исходный IP-адрес пакета. • dst-ip: на основе хэша, используя целевой IP-адрес пакета. • src-dst-ip: на основе хэша с использованием исходного и целевого IP-адресов пакета. • src-ip-port: на основе хэша, используя исходный IP-адрес и поле Source TCP/UDP Port пакета. • dst-ip-port: на основе хэша с использованием целевого IP-адреса и поля Destination TCP/UDP Port пакета. • src-dst-ip-port: на основе хэша с использованием исходного и целевого IP-адресов, а также полей Source/Destination TCP/UDP Port пакета.
inner	Включает использование внутреннего IP-заголовка для туннелирования пакетов.
outer	Включает использование внешнего IP-заголовка для туннелирования пакетов.

no ip load-sharing

Формат: `no ip load-sharing`

Режим ввода команд: глобальная конфигурация

ip route

Эта команда настраивает статический маршрут в указанном экземпляре виртуального маршрутизатора (vrf vrf-name). Параметр *ipaddr* — это действительный IP-адрес; *subnetmask* — действительная маска подсети. Параметр *nexthopip* — это действительный IP-адрес ближайшего маршрутизатора. При указании Null0 в качестве значения ближайшего маршрутизатора происходит добавление статического маршрута отказа. Необязательный параметр preference является целым числом (от 1 до 255), который позволяет указать приоритетное значение (называемое также «административная дистанция») для отдельного статического маршрута. Для ввода в таблицу коммутации из существующих маршрутов к одному пункту назначения выбирается маршрут с наименьшей административной дистанцией. Указывая для статического маршрута значение preference, вы определяете, является статический маршрут более или менее приоритетным, чем маршруты протоколов динамической маршрутизации. Параметр *preference* также определяет статический маршрут как более или менее предпочтительный относительно других статических маршрутов к тому же пункту назначения. Маршрут со значением preference 255 нельзя использовать для передачи трафика.

Параметр *description* позволяет ввести описание маршрута.

Чтобы статические маршруты были видимыми, требуется выполнить следующие шаги.

- Включить IP-маршрутизацию глобально.
- Включить IP-маршрутизацию для интерфейса.
- Убедиться, что связанное подключение также доступно.

Значение по умолчанию: preference — 1

Формат: `ip route [vrf vrf-name] ipaddr subnetmask { nexthopip | Null0 | interface {unit/slot/ port| vlan-id}} [preference] [description description]`

Режим ввода команд: глобальная конфигурация

no ip route

Эта команда удаляет один ближайший узел из статического маршрута к целевому адресу. Если использовать параметр *nexthopip*, удаляется ближайший узел. Если указать значение *preference*, приоритет для статического маршрута устанавливается в значение по умолчанию.

Формат: `no ip route ipaddr subnetmask [{nexthopip [preference] | Null0}]`

Режим ввода команд: глобальная конфигурация

ip route default

Данная команда настраивает маршрут по умолчанию. Значение nexthopip — это действительный IP-адрес ближайшего маршрутизатора. Значение preference — целое число от 1 до 255. Маршрут со значением preference 255 нельзя использовать для передачи трафика.

Значение по умолчанию: preference — 1

Формат: `ip route default nexthopip [preference]`

Режим ввода команд: глобальная конфигурация

no ip route default

Данная команда удаляет все настроенные маршруты по умолчанию. Если указан необязательный параметр *nexthopip*, из настроенного маршрута по умолчанию удаляется ближайший узел. Если указано необязательное значение preference, приоритет настроенного маршрута по умолчанию устанавливается в значение по умолчанию.

Формат: `no ip route default [{nexthopip | preference}]`

Режим ввода команд: глобальная конфигурация

ip route distance

Эта команда устанавливает дистанцию (приоритет) по умолчанию для статических маршрутов. При определении оптимального маршрута предпочтение отдается более низким значениям дистанции маршрута. Команды *ip route* и *ip route default* позволяют дополнительно установить дистанцию (приоритет) для конкретных статических маршрутов. Если дистанция не указана с помощью этих команд, используется дистанция по умолчанию. Изменение дистанции по умолчанию не обновляет дистанцию существующих статических маршрутов, даже если изначально они были назначены дистанциями по умолчанию. Новая дистанция по умолчанию будет применяться только к статическим маршрутам, созданным после выполнения команды *ip route distance*.

Значение по умолчанию: 1

Формат: `ip route distance 1-255`

Режим ввода команд: глобальная конфигурация

no ip route distance

Эта команда устанавливает приоритет статического маршрута на маршрутизаторе в значение по умолчанию. При определении оптимального маршрута предпочтение отдается более низким значениям приоритета маршрута.

Формат: `no ip route distance`

Режим ввода команд: глобальная конфигурация

ip route net-prototype

Эта команда добавляет сетевые прототипы IPv4-маршрутов.

Формат: `ip route net-prototype prefix/prefix-length nexthopip num-routes`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
prefix/prefix-length	Целевая сеть и маска маршрута.
nexthopip	Ближайший IP-адрес, который должен принадлежать активному интерфейсу маршрутизации, но не обязательно быть разрешенным.
num-routes	Количество маршрутов, которые необходимо добавить, начиная с указанного аргумента префикса и в пределах длины указанного префикса.

no ip route net-prototype

Команда удаляет все сетевые прототипы IPv4-маршрутов.

Формат: `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*

Режим ввода команд: глобальная конфигурация

ip netdirbcast

Эта команда включает широковещательную переадресацию на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: *`ip netdirbcast`*

Режим ввода команд: конфигурирование интерфейса

no ip netdirbcast

Команда выключает широковещательную переадресацию на интерфейсе или диапазоне интерфейсов.

Формат: *`no ip netdirbcast`*

Режим ввода команд: конфигурирование интерфейса

ip mtu

Эта команда устанавливает значение IP Maximum Transmission Unit (MTU) на интерфейсе маршрутизации или диапазоне интерфейсов. IP MTU — это максимальная размер IP-пакета, который может быть передан на интерфейс без фрагментации.

Если переадресованные пакеты превышают IP MTU на принимающем интерфейсе, они отбрасываются. Пакеты, созданные маршрутизатором, например OSPF-пакеты, могут быть фрагментированы IP-стеком.

OSPF анонсирует IP MTU в пакетах Database Description при их отправке на соседние узлы в процессе обмена базами данных. Если OSPF на двух соседних узлах анонсируют разные значения IP MTU, смежность между ними не образуется (за исключением случаев, когда OSPF даны указания игнорировать различия в IP MTU командой *ip ospf mtu-ignore*).

Размер IP MTU определяет максимальный размер IP-пакета (IP-заголовок плюс полезная нагрузка IP). Он не включает в себя дополнительные байты, которые могут потребоваться для заголовков второго уровня. Чтобы принимать и обрабатывать пакеты, Ethernet MTU (см. mtu) должен учитывать размер Ethernet-заголовка.

Значение по умолчанию: 1500 байт

Формат: `ip mtu` *`68-12270`*

Режим ввода команд: конфигурирование интерфейса

no ip mtu

Данная команда возвращает IP MTU в значение по умолчанию.

Формат: `no ip mtu`

Режим ввода команд: конфигурирование интерфейса

release dhcp

Команда заставляет DHCPv4-клиент освободить занятый IP-адрес на указанном интерфейсе. DHCP-клиент высылает сообщение DHCP Release, сообщая DHCP-серверу, что указанный IP-адрес больше не нужен и может быть назначен другому объекту.

Формат: `release dhcp {unit/slot/port | vlan id}`
Режим ввода команд: привилегированный

renew dhcp

Используйте эту команду, чтобы заставить DHCPv4-клиент немедленно обновить аренду IPv4-адреса на указанном интерфейсе.

Эта команда может быть использована на стандартных (in-band) портах, а также на портах обслуживания или сетевых (out-of-band) портах.

Формат: `renew dhcp {unit/slot/port | vlan id}`

Режим ввода команд: привилегированный

renew dhcp network-port

Команда для обновления IP-адреса на сетевом порте.

Формат: `renew dhcp network-port`

Режим ввода команд: привилегированный

renew dhcp service-port

Используйте данную команду, чтобы обновить IP-адрес на интерфейсе управления.

Формат: `renew dhcp service-port`

Режим ввода команд: привилегированный

encapsulation

Эта команда настраивает тип инкапсуляции уровня соединений для пакета на интерфейсе или диапазоне интерфейсов. Тип инкапсуляции может принимать значения ethernet или snap.

Значение по умолчанию: ethernet

Формат: `encapsulation {ethernet | snap}`

Режим ввода команд: конфигурирование интерфейса

Если маршрутизация кадров выполняется в сеть VLAN, для них всегда используется инкапсуляция Ethernet.

show dhcp lease

Эта команда отображает список IPv4-адресов, которые в настоящее время выделены DHCP-сервером для указанных или всех стандартных интерфейсов. Команда не применима для сетевых или сервисных портов.

Формат: `show dhcp lease [interface {unit/slot/port | vlan id}]`

Режим ввода команд: привилегированный

Параметр	*Описание*
IP address, Subnet mask	IP-адрес и маска подсети, выделенные DHCP-сервером
DHCP Lease server	IPv4-адрес DHCP-сервера, который выделил адрес.
State	Статус DHCPv4-клиента на указанном интерфейсе
DHCP transaction ID	Идентификатор транзакции DHCPv4-клиента.
Lease	Время (в секундах) с момента выделения IP-адреса сервером.
Renewal	Время (в секундах) до отправки DHCPv4-клиентом следующего запроса об обновлении IP-адреса.
Rebind	Время (в секундах) до начала процесса DHCP Rebind.
Retry count	Количество повторов DHCPv4-клиентом сообщения DHCP REQUEST до получения ответа сервера.

show ip brief

Данная команда отображает сводную информацию о глобальной конфигурации IP для указанного виртуального маршрутизатора, включая настройки ограничения скорости ICMP и глобальную конфигурацию ICMP-переадресации. Если маршрутизатор не указан, отображается информация маршрутизатора по умолчанию.

Формат: `show ip brief [vrf vrf-name]`

Режимы ввода команд: привилегированный
пользовательский

Термин	*Значение*
Default Time to Live	Значение TTL для переадресации пакета от локального маршрутизатора к конечному пункту назначения.
Routing Mode	Показывает, включен ли режим маршрутизации.
Maximum Next Hops	Максимальное количество ближайших узлов.
Maximum Routes	Максимальное количество маршрутов.
ICMP Rate Limit Interval	Показывает, как часто происходит инициализация корзины токенов за счет токенов увеличенного размера. Burst-interval устанавливается в диапазоне от 0 до 2 147 483 647 миллисекунд. По умолчанию burst-interval равен 1000 миллисекундам.
ICMP Rate Limit Burst Size	Показывает количество сообщений об ошибках ICMPv4, которые могут быть присланы за один период burst-interval. Диапазон: от 1 до 200 сообщений. Значение по умолчанию — 100 сообщений.
ICMP Echo Replies	Показывает, включены ли ICMP-ответы.
ICMP Redirects	Показывает, включены ли ICMP-перенаправления.

show ip interface

Эта команда отображает всю необходимую информацию об IP-интерфейсе. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово *vlan* используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ip interface {unit/slot/port|vlan 1-4094|loopback 0-7}`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Routing Interface Status	Определяет оперативный статус интерфейса IPv4-маршрутизации. Возможные значения: Up или Down.
Primary IP Address	Основной IP-адрес и маска подсети интерфейса. Значение отображается лишь в том случае, если настроено.
Method	Показывает, настроен IP-адрес вручную или же получен от DHCP-сервера.
Secondary IP Address	Один или несколько вторичных IP-адресов и масок подсети интерфейса. Значение отображается лишь в том случае, если настроено.
Helper IP Address	Вспомогательные IP-адреса, настроенные командой ip helper-address.
Routing Mode	Административный режим участия для маршрутизатора интерфейса. Возможные значения: enable или disable.
Administrative Mode	Административный режим указанного интерфейса. Возможные значения: enable или disable.
Forward Net Directed Broadcasts	Показывает, включена ли широковещательная переадресация.
Proxy ARP	Показывает, включен ли в системе прокси-ARP.
Local Proxy ARP	Показывает, включен ли на интерфейсе локальный прокси-ARP.
Active State	Показывает, активен ли интерфейс. Интерфейс считается активным, если с ним установлена связь и он осуществляет переадресацию.
Link Speed Data Rate	Целое число, представляющее скорость передачи данных физического соединения для указанного интерфейса. Измеряется в мегабитах в секунду (Мбит/с).
MAC Address	Закрепленный физический адрес указанного интерфейса. Формат: 6 двузначных чисел шестнадцатеричной системы, разделенных двоеточиями.
Encapsulation Type	Тип инкапсуляции для указанного интерфейса. Возможные типы: Ethernet или SNAP.
IP MTU	Максимальный размер MTU для кадра в байтах.
Bandwidth	Пропускная способность интерфейса.
Destination Unreachables	Показывает, могут ли быть посланы сообщения ICMP Destination Unreachable (включены или выключены).
ICMP Redirects	Показывает, могут ли быть посланы сообщения ICMP Redirect (включены или выключены).
DHCP Client Identifier	Идентификатор клиента в выводе команды отображается только в тех случаях, если DHCP на стандартном интерфейсе был включен с опцией *client-id*.

show ip interface brief

Эта команда отображает сводную информацию о параметрах IP-конфигурации всех портов маршрутизатора и указывает, каким образом каждый IP-адрес был назначен для заданного экземпляра виртуального маршрутизатора. Если виртуальный маршрутизатор не указан, отображается таблица параметров IP-конфигурации маршрутизатора по умолчанию.

Формат: `show ip interface [vrf vrf-name] brief`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Interface	Действительный слот и номер порта, разделенные косой чертой.
State	Оперативный статус маршрутизации на интерфейсе.
IP Address	IP-адрес интерфейса маршрутизации в 32-битном десятичном формате с точками.
IP Mask	IP-маска интерфейса маршрутизации в 32-битном десятичном формате с точками.
Method	Указывает, как был назначен каждый IP-адрес. Поле содержит одно из следующих значений: • DHCP — адрес предоставлен DHCP-сервером; • Manual — адрес настроен вручную.

show ip load-sharing

Команда отображает текущий настроенный режим балансировки нагрузки IP ECMP.

Формат: `show ip load-sharing`

Режим ввода команд: привилегированный

show ip protocols

Данная команда отображает сводную информацию о конфигурации и статусе для каждого одноадресного протокола маршрутизации, работающего на указанном виртуальном маршрутизаторе. Команда выводит протоколы маршрутизации, которые настроены и включены. Если в командной строке выбран определенный протокол, вывод команды будет ограничен только этим протоколом. Если виртуальный маршрутизатор не указан, отображается конфигурация и статус для маршрутизатора по умолчанию.

Формат: `show ip protocols [vrf` *`vrf-name`*`] [bgp|ospf|rip]`

Режим ввода команд: привилегированный

Термин	*Значение*
Раздел BGP	
Routing Protocol	BGP.
Router ID	Идентификатор маршрутизатора, настроенный для BGP.
Local AS Number	Номер AS, в котором находится локальный маршрутизатор.
BGP Admin Mode	Включен ли BGP глобально.
Maximum Paths	Максимальное количество ближайших узлов на внутреннем или внешнем маршруте BGP.
Always Compare MED	Настроен ли BGP на сравнение MED для маршрутов, полученных от подключенных устройств в других AS.
Maximum AS Path Length	Ограничение длины AS-путей, которые BGP принимает от соседних устройств.
Fast Internal Failover	Будет ли BGP немедленно выключать смежности iBGP, если менеджер таблицы маршрутизации сообщит, что адрес партнерского устройства больше не доступен.
Fast External Failover	Будет ли BGP немедленно выключать смежности eBGP, если соединение с соседним устройством прервется.

Distance	Административная дистанция (или «приоритет маршрута») по умолчанию для внешних, внутренних и локальных маршрутов BGP. В отображаемой следом таблице перечисляются диапазоны соседних адресов, которые были настроены, чтобы переопределить дистанцию по умолчанию на дистанцию указанного соседа. Если адрес соседа попадает в один из этих диапазонов, маршрутам от этого соседа назначаются настроенные дистанции. Если список префиксов сконфигурирован, дистанция назначается только префиксам от соседних устройств, которые разрешены списком префиксов.
Redistribution	Таблица с информацией для каждого протокола источника (connected, static, rip и ospf). Для каждого из этих источников показывается список раздач и карта маршрутов, а также настроенная метрика. Не настроенные поля остаются пустыми. Для OSPF дополнительная линия показывает настроенные параметры соответствия OSPF.
Prefix List In	Глобальный список префиксов, используемых для фильтрации входящих маршрутов от всех соседних устройств.
Prefix List Out	Глобальный список префиксов, используемых для фильтрации исходящих маршрутов для всех соседних устройств.
Networks Originated	Набор сетей, участвующих в работе протокола BGP. Сети, анонсированные соседним устройствам, отмечены как active.
Neighbors	Список настроенных соседних устройств и настроенные для каждого из них входящие и исходящие политики.
Раздел OSPFv2	
Routing Protocol	OSPFv2.
Router ID	Идентификатор маршрутизатора, настроенный для OSPFv2.
OSPF Admin Mode	Включен ли OSPF глобально.
Maximum Paths	Максимальное количество ближайших узлов на внутреннем или внешнем маршруте OSPF.
Routing for Networks	Набор сетей, участвующих в работе протокола OSPF.
Distance	Административная дистанция (или «приоритет маршрута») для внутризональных, внезональных и внешних маршрутов.
Default Route Advertise	Настроен ли OSPF на создание маршрута по умолчанию.
Always	Зависит ли анонсирование по умолчанию от наличия маршрута по умолчанию в общей таблице маршрутизации.
Metric	Метрика, настроенная для анонсирования с маршрутом по умолчанию.
Metric Type	Тип метрики для маршрута по умолчанию.
Redist Source	Тип маршрутов, перераспределяемых протоколом OSPF.
Metric	Метрика, анонсируемая для перераспределяемых маршрутов данного типа.
Metric Type	Тип метрики для перераспределяемых маршрутов данного типа.
Subnets	Перераспределяет OSPF подсети классовых адресов или только классовые префиксы.
Dist List	Список сетей, используемый для фильтрации маршрутов данного типа. Перераспределяются только маршруты, прошедшие список распределения.
Number of Active Areas	Количество OSPF-зон как минимум с одним интерфейсом, работающим на данном маршрутизаторе. Дополнительно приводится разбивка по типу зон.

ABR Status	Является ли маршрутизатор в настоящее время пограничным. Маршрутизатор является пограничным маршрутизатором зоны, если на нем есть интерфейсы, которые работают более чем в одной зоне и одна из которых является магистральной.
ASBR Status	Является ли маршрутизатор пограничным маршрутизатором автономной системы (ASBR). Маршрутизатор является ASBR, если он перераспределяет любые маршруты или является источником маршрута по умолчанию.
Раздел RIP	
RIP Admin Mode	Включен ли RIP глобально.
Split Horizon Mode	Анонсирует ли RIP маршруты на интерфейсы, откуда они были получены.
Default Metric	Метрика, назначенная перераспределенным маршрутам.
Default Route Advertise	Является ли данный маршрутизатор источником маршрута по умолчанию.
Distance	Административная дистанция для маршрутов RIP.
Redistribution	Таблица, отображающая информацию для каждого протокола источника маршрутов(connected, static, bgp и ospf). Для каждого из этих источников отображаются параметры **distribution list** и **metric**. Не настроенные поля остаются пустыми. Для OSPF также отображаются настроенные параметры **ospf match**.
Interface	Интерфейсы, где включен RIP, и версия, отправляемая и принимаемая каждым интерфейсом.

show ip route

Данная команда отображает таблицу маршрутизации для указанного виртуального маршрутизатора (*vrf vrf-name*). Если маршрутизатор не указан, отображается таблица маршрутизации для маршрутизатора по умолчанию. *ip-address* указывает сеть, для которой будет отображаться маршрут, и показывает наиболее подходящий маршрут к адресу. *mask* указывает маску подсети для параметра ip-address. Если использовать ключевое слово *longer-prefixes*, пара *ip-address* и *mask* становится префиксом, и команда отображает маршруты к адресам, которые совпадают с этим префиксом. Используйте параметр *protocol*, чтобы указать протокол, которым установлены маршруты. Значение параметра *protocol* может быть *connected, ospf, rip, static* или *bgp*. Используйте параметр *all*, чтобы отобразить все маршруты, включая наиболее подходящие и прочие. Если параметр *all* не используется, команда отображает только наиболее подходящий маршрут.

Если использовать для *protocol* ключевое слово connected, опция all будет недоступна, потому что наиболее и наименее подходящих подключенных маршрутов не существует.

Если использовать с параметром *protocol* ключевое слово static, становится доступной опция description, например: show ip route *ip-address* static description. Данная команда отображает описание указанного статического маршрута.

Формат: `show ip route [vrf vrf-name] [{ip-address [protocol] | {ip-address mask [longer- prefixes] [protocol] | protocol} [all] | all}]`

Режим ввода команд: привилегированный

пользовательский

Термин	***Значение***

Route Codes	Ключ для кодов протокола маршрутизации, который может появиться при выводе таблицы маршрутизации.

Команда show ip route отображает таблицы маршрутизации в следующем формате:

```
Code IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp, Interface, Truncated
```

Столбцы таблицы маршрутизации отображают следующую информацию.

Термин	***Значение***
Code	Коды для протоколов маршрутизации, создавших маршруты.
Default Gateway	IP-адрес шлюза по умолчанию. Когда в системе нет более точного маршрута до места назначения пакета, пакет отправляется на шлюз по умолчанию.
IP-Address/Mask	IP-адрес и маска целевой сети, соответствующая данному маршруту.
Preference	Административная дистанция, связанная с данным маршрутом. Маршруты с низкими значениями более предпочтительны, чем маршруты с высокими.
Metric	Стоимость, связанная с этим маршрутом.
via Next-Hop	IP-адрес маршрутизатора (если таковой существует), используемый для направления трафика на пути к месту назначения.
Route- Timestamp	Время последнего обновления для динамических маршрутов. Формат для временной метки маршрута будет в виде: • дд:чч:мм, если прошло дней > = 1; • чч:мм:сс если прошло дней < 1.
Interface	Интерфейс маршрутизатора, используемый для направления трафика к следующему целевому узлу. Для отклоненных маршрутов ближайшим будет интерфейс Null0.
T	Флаг, добавляемый к маршруту, чтобы указать, что это ECMP-маршрут, но только один из его ближайших узлов был установлен в таблице переадресации. Таблица переадресации может ограничивать количество ECMP-маршрутов или ECMP-групп. Если ECMP-маршрут не удается установить, потому что достигнуто установленное ограничение, маршрут устанавливается с помощью одного ближайшего узла. Такие сокращенные маршруты обозначаются флагом T после имени интерфейса.

Чтобы административно контролировать трафик, отправляемый на определенную сеть, и предотвратить его передачу через маршрутизатор, можно настроить на маршрутизаторе статический маршрут отказа. Такой трафик будет отброшен, и ICMP-сообщение о недоступности места назначения будет послано обратно к источнику. Обычно такой способ используют для предотвращения маршрутных петель. Маршрут отказа, добавленный в RTO, относится к типу OSPF Inter-Area. Маршруты отказа (маршруты типа REJECT, установленные любым протоколом) не распространяются протоколами OSPF/RIP. Маршруты отказа поддерживаются и в OSPFv2, и в OSPFv3.

show ip route ecmp-groups

Эта команда выдает отчет обо всех ECMP-группах в таблице маршрутизации IPv4. ECMP-группы — это набор из двух или более соседних узлов, используемых в одном или нескольких маршрутах. Группы нумеруются произвольно от 1 до n. Вывод команды показывает количество соседних узлов в группе и количество маршрутов, использующих набор этих соседних узлов. При выводе также указывается IPv4-адрес и исходящий интерфейс для каждого перехода в каждой группе.

Формат: `show ip route ecmp-groups`

Режим ввода команд: привилегированный

show ip route hw-failure

Используйте эту команду для отображения маршрутов, которые не удалось добавить в таблицу из-за ошибок хэша или переполнения таблицы.

Формат: `show ip route hw-failure`

Режим ввода команд: привилегированный

show ip route net-prototype

Данная команда отображает маршруты прототипа сети. Маршруты прототипов сетей отображаются с меткой P.

Формат: `show ip route net-prototype`

Режим ввода команд: привилегированный

show ip route summary

Эта команда показывает сводную информацию о состоянии таблицы маршрутизации. Если введено дополнительное ключевое слово all, некоторая статистика, например количество маршрутов от каждого источника, включает альтернативные маршруты. Альтернативный маршрут — это маршрут, который не является наиболее приоритетным до места назначения и поэтому не попадает в таблицу переадресации. Чтобы включить только количество оптимальных маршрутов, не используйте необязательное ключевое слово.

Формат: `show ip route summary [all]`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Connected Routes	Общее количество маршрутов в таблице маршрутизации.
Static Routes	Общее количество статических маршрутов в таблице маршрутизации.
RIP Routes	Общее количество маршрутов, установленных протоколом RIP.
BGP Routes	Общее количество маршрутов, установленных протоколом BGP.
External	Количество внешних BGP-маршрутов.
Internal	Количество внутренних BGP-маршрутов.
Local	Количество локальных BGP-маршрутов.
OSPF Routes	Общее количество маршрутов, установленных протоколом OSPF.
Intra Area Routes	Общее количество маршрутов между зонами, установленных протоколом OSPF.
External Type-1 Routes	Общее количество маршрутов External Type-1, установленных протоколом OSPF.
External Type-2 Routes	Общее количество маршрутов External Type-2 установленных протоколом OSPF.
Reject Routes	Общее количество отброшенных при установке маршрутов всеми протоколами.
Net Prototype Routes	Количество маршрутов прототипов сети.
Total Routes	Общее количество маршрутов в таблице маршрутизации.

Best Routes (High)	Количество оптимальных маршрутов в таблице маршрутизации на данный момент. Это количество учитывает только наиболее подходящие маршруты к каждому месту назначения. Значение в скобках указывает самое высокое значение количества уникальных оптимальных маршрутов с момента последнего обнуления счетчиков.
Alternate Routes	Количество альтернативных маршрутов в таблице маршрутизации на данный момент. Альтернативный маршрут — это маршрут, который не был определен как оптимальный маршрут к месту назначения.
Route Adds	Количество маршрутов, добавленных в таблицу маршрутизации.
Route Modifies	Количество маршрутов, измененных после того, как они были первоначально добавлены в таблицу маршрутизации.
Route Deletes	Количество маршрутов, удаленных из таблицы маршрутизации.
Unresolved Route Adds	Количество добавлений маршрутов, не удавшихся по причине того, что ни один из ближайших узлов не находился в локальной подсети. Обратите внимание: статические маршруты в начале работы могут не добавиться в таблицу маршрутизации, потому что интерфейсы маршрутизации еще не запущены. В этом случае счетчик работает поэтапно. Статические маршруты добавляются в таблицу маршрутизации по мере включения интерфейсов маршрутизации.
Invalid Route Adds	Количество добавлений маршрутов, не удавшихся по причине того, что маршрут был недействительным. Для каждого из таких сбоев выполняется запись в журнале.
Failed Route Adds	Количество добавлений маршрутов, не удавшихся по причине ограничения ресурсов в таблице маршрутизации.
Hardware Failed Route Adds	Количество маршрутов, не добавленных в таблицу, по причине ошибки хэша или переполнения таблицы.
Reserved Locals	Количество записей в таблице маршрутизации, зарезервированных для локальной подсети на интерфейсе маршрутизации, который выключен. Место для местных маршрутов всегда резервируется, чтобы они могли быть установлены в случае отказа интерфейса маршрутизации.
Unique Next Hops (High)	Количество отдельных соседних узлов, используемых всеми текущими маршрутами в таблице маршрутизации. Сюда относятся локальные интерфейсы для локальных маршрутов и соседи для непрямых маршрутов. Значение в скобках указывает на самый высокий показатель количества отдельных соседних узлов с момента последнего обнуления счетчиков.
Next Hop Groups (High)	Текущее количество групп соседних узлов, используемых одним или несколькими маршрутами. Каждая такая группа включает один или несколько соседних узлов. Значение в скобках указывает на самый высокий показатель количества групп соседних узлов с момента последнего обнуления счетчиков.
ECMP Groups (High)	Количество групп с несколькими соседними узлами. Значение в скобках указывает на самый высокий показатель количества групп с момента последнего обнуления счетчиков.
ECMP Groups	Количество групп с несколькими соседними узлами.
ECMP Routes	Количество маршрутов с несколькими соседними узлами, находящееся в таблице на данный момент.
Truncated ECMP Routes	Количество ECMP-маршрутов с единственным ближайшим узлом, установленных в таблице переадресации на данный момент. Таблица маршрутизации может ограничивать количество ECMP-

	маршрутов или ECMP-групп. Если ECMP-маршрут не удается установить, потому что достигнуто установленное ограничение, маршрут устанавливается с помощью одного ближайшего узла.
ECMP Retries	Количество ECMP-маршрутов, которые были установлены в таблицу маршрутизации после того, как изначально были установлены с единственным ближайшим узлом.
Routes with n Next Hops	Текущее количество маршрутов для каждого количества соседних узлов.

clear ip route counters

Эта команда сбрасывает счетчики таблицы маршрутизации IPv4, указанные в выводе команды show ip route summary, для указанного виртуального маршрутизатора. Если маршрутизатор не указан, команда выполняется для маршрутизатора по умолчанию. Команда сбрасывает только счетчики событий. Счетчики, показывающие текущее состояние таблицы маршрутизации, такие как количество маршрутов каждого типа, не сбрасываются.

Формат: `clear ip route counters [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

show ip route preferences

Эта команда отображает подробную информацию о приоритетах для каждого типа маршрута. Приоритеты маршрута используются для определения лучшего маршрута. Низкие значения приоритета более предпочтительны, чем высокие значения. Маршрут с приоритетом 255 нельзя использовать для передачи трафика.

Формат: `show ip route preferences`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
Local	Значение приоритета для локального маршрута.
Static	Значение приоритета для статического маршрута.
BGP External	Значение приоритета для внешнего BGP-маршрута.
OSPF Intra	Значение приоритета для межзонального OSPF-маршрута.
OSPF Inter	Значение приоритета для внутризонального OSPF-маршрута.
OSPF External	Значение приоритета для внешнего OSPF-маршрута.
RIP	Значение приоритета для RIP-маршрута.
BGP Internal	Значение приоритета для внутреннего BGP-маршрута.
BGP Local	Значение приоритета для локального BGP-маршрута.
Configured Default Gateway	Значение приоритета для маршрута статически настроенного шлюза по умолчанию.
DHCP Default Gateway	Значение приоритета для маршрута шлюза по умолчанию, полученного от DHCP-сервера.

show ip stats

Данная команда отображает статистическую IP-информацию для указанного экземпляра виртуального маршрутизатора. Если виртуальный маршрутизатор не указан, отображается статистика для маршрутизатора по умолчанию.

Формат: `show ip stats [vrf vrf-name]`

Режим ввода команд: привилегированный
пользовательский

show routing heap summary

Эта команда отображает сводную информацию о распределении динамической памяти маршрутизации. Динамическая память маршрутизации — это блок памяти, выделенный при загрузке системы для использования в приложениях маршрутизации.

Формат: `show routing heap summary`

Режим ввода команд: привилегированный

Параметр	*Описание*
Heap Size	Количество памяти в байтах, выделенное при запуске на динамическую память маршрутизации.
Memory In Use	Количество распределенных байтов на данный момент.
Memory on Free List	Количество байтов, находящихся в данный момент в списке доступной памяти. Когда участок динамической памяти освобождается, он попадает в список доступной памяти для дальнейшего использования.
Memory Available in Heap	Количество исходных байтов, которые никогда не были распределены.
In Use High Water Mark	Максимальное количество использованной памяти с последнего перезапуска системы.

11.3 Команды настройки политик маршрутизации

ip policy route-map

Используйте эту команду, чтобы определить *route-map* для применения маршрутизации на основе политики на интерфейсе, указанном в параметре route-map-name. Маршрутизация на основе политики настраивается на интерфейсе, который принимает пакеты, а не отправляет их.

Когда route-map, применяемая к интерфейсу, меняется (например, когда добавляются новые записи или в рамках записей добавляются/удаляются условия для настроек/соответствий), а также при необходимости удалить *route-map* выполняется сначала удаление карты с интерфейса, а затем (при изменениях) — ее обратное добавление, чтобы применить измененную конфигурацию.

Route-map и функционал DiffServ не могут работать на одном интерфейсе.

Формат: `ip policy route-map-name`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
Heap Size	Количество памяти в байтах, выделенное при запуске на динамическую память маршрутизации.

Memory In Use	Количество распределенных байтов на данный момент.
Memory on Free List	Количество байтов, находящихся в данный момент в списке доступной памяти. Когда участок динамической памяти освобождается, он попадает в список доступной памяти для дальнейшего использования.
Memory Available in Heap	Количество исходных байтов, которые никогда не были распределены.
In Use High Water Mark	Максимальное количество использованной памяти с последнего перезапуска системы.

ip prefix-list

Чтобы создать список префиксов или добавить запись в такой список, используйте данную команду в режиме глобальной конфигурации. Списки префиксов позволяют сопоставлять префиксы маршрутов с префиксами, указанными в списке. Каждый список префиксов включает в себя последовательность записей префиксов, упорядоченных в соответствии с порядковыми номерами. Маршрутизатор последовательно проверяет каждый элемент списка префиксов, чтобы определить, совпадает ли префикс маршрута с префиксом записи. Если список префиксов пуст или не существует, разрешены все префиксы. Отказ подразумевается для тех случаев, когда префикс не соответствует ни одной записи из списка. Найдя совпадение или получив отказ, маршрутизатор не проверяет остальную часть списка. Список префиксов можно использовать в route-map.

Настроить можно до 128 списков префиксов. Максимальное количество записей в списке префиксов — 64.

Значение по умолчанию: по умолчанию списки префиксов отсутствуют.

Формат: `ip prefix-list` *`list-name`* {[`seq` *`number`*] {`permit` | `deny`} *`network/length`* [`ge` *`length`*] [`le` *`length`*] | `renumber` *`renumber-interval first-statement-number`*}

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
list-name	Текстовое имя списка префиксов. Длина — до 32 символов.
seq number	(Необязательный параметр.) Порядковый номер данной записи в списке префиксов. Записи в списке префиксов упорядочены от наименьшего порядкового номера к большему и применяются в указанном порядке. Если вы не указываете порядковый номер, система автоматически присваивает записи порядковый номер на пять единиц больше последнего номера в списке. Нельзя настроить две записи с одним и тем же порядковым номером. Значение может быть от 1 до 4294967294.
permit	Разрешить маршруты, префикс места назначения в которых совпадает с записью.
deny	Отклонить маршруты, префикс места назначения в которых совпадает с записью.
network/length	Указывает критерий совпадения для маршрутов, сопоставляемых с записями списка префиксов. Значение network может обозначать любой действительный IP-префикс. Значение length может обозначать любой префикс IPv4 длиной от 0 до 32.
ge length	(Необязательный параметр.) Если эта опция настроена, префикс считается совпадением, если длина маски сети больше либо равна указанному значению. Значение должно быть больше длины сети и меньше либо равно 32.
le length	(Необязательный параметр.) Если эта опция настроена, префикс считается совпадением, если длина маски сети меньше либо равна указанному значению. Значение должно быть больше длины ge и меньше либо равно 32.

renumber	(Необязательный параметр.) Предоставляет возможность изменить порядковую нумерацию заявлений записей в списке IP-префиксов с заданным интервалом, начиная с указанного порядкового номера. Диапазон значений для *renumber-interval* — 1–100, диапазон значений для *first-statement-number* — 1–1000.

no ip prefix-list

Чтобы удалить список префиксов или запись в списке префиксов, используйте **no**-форму данной команды. Команда **no ip prefixlist list-name** удаляет весь список префиксов. Чтобы удалить отдельную запись в списке префиксов, необходимо точно указать эту запись со всеми опциями.

Формат: `no ip prefix-list` *`list-name`* `[seq` *`number`*`] { permit | deny }` *`network/length`* `[ge` *`length`*`] [le` *`length`*`]`

Режим ввода команд: глобальная конфигурация

ip prefix-list description

Используйте команду **ip prefix-list description** в режиме глобальной конфигурации, чтобы применить текстовое описание к списку префиксов.

Значение по умолчанию: описания отсутствуют.

Формат: `ip prefix-list` *`list-name`* `description` *`text`*

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
list-name	Текстовое имя списка префиксов.
description text	Текст описания для списка префиксов. Длина — до 80 символов.

no ip prefix-list description

Используйте **no**-форму команды, чтобы удалить текст описания.

Формат: `no ip prefix-list list-name description`

Режим ввода команд: глобальная конфигурация

ipv6 prefix-list

Используйте эту команду, чтобы создать списки IPv6-префиксов. Список префиксов IPv6 может включать только IPv6-адреса. Списки префиксов позволяют сопоставлять префиксы маршрутов с префиксами, указанными в списке. Каждый список префиксов включает в себя последовательность записей префиксов, упорядоченных в соответствии с порядковыми номерами. Маршрутизатор последовательно проверяет каждый элемент списка префиксов, чтобы определить, совпадает ли префикс маршрута с префиксом записи. Для сопоставления маршрутов IPv6 используются только списки IPv6-префиксов. Если список префиксов пуст или не существует, разрешены все префиксы. Отказ подразумевается для тех случаев, когда префикс не соответствует ни одной записи из списка. Найдя совпадение или получив отказ, маршрутизатор не проверяет остальную часть списка. Список префиксов IPv6 можно использовать route-map для сопоставления префикса маршрута при использовании команды match ipv6 address. Route-map может содержать списки IPv4-префиксов и

IPv6-префиксов. Если сопоставляемый маршрут является маршрутом IPv6, используются только списки IPv6-префиксов.

Настроить можно до 128 списков префиксов. Максимальное количество заявлений в списке префиксов — 64. Указанные числа относятся только к спискам IPv6-префиксов. Списки IPv4-префиксов учитываются в аналогичных рамках отдельно.

Значение по умолчанию: по умолчанию списки префиксов отсутствуют.

Формат: `ipv6 prefix-list` *`list-name`* `[seq` *`seq-number`*`] { {permit/deny}` *`ipv6-prefix/prefix-length`*`[ge` *`ge-value`*`] [le` *`le-value`*`] | description` *`text`* `| renumber` *`renumber-interval first-statement-number`*`}`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
list-name	Текстовое имя списка префиксов. Длина — до 32 символов.
seq number	(Необязательный параметр.) Порядковый номер данной записи в списке префиксов. Записи в списке префиксов упорядочены от наименьшего порядкового номера к большему и применяются в указанном порядке. Если вы не указываете порядковый номер, система автоматически присваивает записи порядковый номер на пять единиц больше последнего номера в списке. Нельзя настроить две записи с одним и тем же порядковым номером. Значение может быть от 1 до 4294967294.
permit	Разрешить маршруты, префикс места назначения в которых совпадает с записью.
deny	Отклонить маршруты, префикс места назначения в которых совпадает с записью.
ipv6-prefix/ prefix-length	Указывает критерий совпадения для маршрутов, сопоставляемых с записями списка префиксов. Значение ipv6-prefix подразумевает любой действующий IPv6-префикс, где адрес указан в шестнадцатеричном формате с использованием 16-битных значений, разделенных двоеточиями. Значение prefix-length — это длина IPv6-префикса в формате десятичного значения, указывающая, сколько из смежных битов высокого порядка адреса содержат префикс (сетевую часть адреса). Десятичное значение необходимо отделять косой чертой.
ge length	(Необязательный параметр.) Если эта опция настроена, длина префикса должна быть больше либо равна значению ipv6-prefix/prefix-length. Это показатель минимального значения в диапазоне длины.
le length	(Необязательный параметр.) Если эта опция настроена, длина префикса должна быть меньше либо равна значению ipv6-prefix/prefix-length. Это показатель максимального значения в диапазоне длины.
Description	Описание списка префиксов. Может содержать до 80 символов.
renumber	(Необязательный параметр.) Предоставляет возможность изменить порядковую нумерацию записей в списке IPv6-префиксов с заданным интервалом, начиная с указанного порядкового номера.

no ipv6 prefix-list

Используйте эту команду, чтобы удалить весь список IPv6-префиксов или отдельную запись из списка.

Формат: `ipv6 prefix-list list-name`

Режим ввода команд: глобальная конфигурация

Прежде чем использовать данную команду для удаления списка IPv6-префиксов, требуется удалить его описание с помощью команды no ip prefix-list description.

route-map

Используйте команду *route-map* в режиме глобальной конфигурации, чтобы создать route-map и перейти в режим его конфигурирования. Route-map предназначена для ограничения распределения маршрутов определенным диапазоном префиксов. Команда распределения указывает route-map, которая относится к списку префиксов. Список префиксов определяет префиксы, которые могут быть распределены. ПО позволяет создавать до 64 route-map.

Значение по умолчанию: по умолчанию настроенные карты маршрутов отсутствуют. Если нет специальных тегов для отклонения или разрешения маршрутов, по умолчанию они разрешены.

Формат: `route-map map-tag [permit|deny] [sequence-number]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
map-tag	Текстовое имя *route-map*. *Route-map* с одинаковыми именами группируются с учетом их порядковых номеров. Имя может содержать до 32 символов.
permit	(Необязательный параметр.) Маршруты, соответствующие всем условиям в route-map, разрешены.
deny	(Необязательный параметр.) Маршруты, соответствующие всем условиям в route-map, отклоняются.
sequence-number	(Необязательный параметр.) Целое число, используемое для упорядочения наборов *route-map* с одинаковыми именами. *Route-map* упорядочиваются от наименьшего к наибольшему порядковому номеру, более низкие порядковые номера применяются в первую очередь. Если порядковый номер не указан, система присваивает значение на 10 единиц больше последнего использованного порядкового номера. Диапазон — от 0 до 65 535.

no route-map

Чтобы удалить *route-map* или одну из ее записей, используйте no-форму команды.

Формат: `no route-map map-tag [permit|deny] [sequence-number]`

Режим ввода команд: глобальная конфигурация

match as-path

Команда устанавливает условие сравнения *route-map*, при котором BGP-пути автономной системы сравниваются со списком контроля доступа AS-пути. При вводе нового условия *match as-path* в запись *route-map*, в котором уже есть условие *match as-path*, к существующему условию сравнения будут добавлены числа нового списка доступов AS-пути до достижения максимально допустимого количества списков. Маршрут считается совпадающим, если он совпадает с одним или несколькими списками контроля доступа AS-пути, на которые ссылается условие сравнения.

Формат: `match as-path as-path-list-number`

Режим ввода команд: конфигурирование route-map

Параметр	*Описание*
as-path-list-number	Целое число от 1 до 500, определяющее список контроля доступа AS-пути, используемый как критерий для сравнения.

no match as-path

Данная команда удаляет условие сравнения route-map, при котором BGP-пути автономной системы сравниваются со списком контроля доступа AS-пути.

Формат: `no match as-path as-path-list-number`

Режим ввода команд: конфигурирование route-map

match community

Команда *match community* в режиме конфигурирования route-map используется, чтобы настроить *route-map* для сопоставления со списком BGP-сообщества. Если список сообщества возвращает действие *permit*, маршрут считается совпадающим. Если запись сопоставления ссылается на список сообщества, который не настроен, ни один маршрут не будет считаться совпадающим с записью.

Формат: `match community community-list [community-list...] [exact-match]`

Режим ввода команд: конфигурирование route-map

Параметр	*Описание*
community-list	Имя стандартного списка сообщества. В одно условие сравнения может быть включено до 8 имен.
exact-match	(Необязательный параметр.) Если указана эта опция, маршрут считается совпадающим, если набор сообществ на маршруте точно совпадает с набором сообществ в одной из записей списка сообщества.

no match community

Используйте **no**-форму отмены команды, чтобы удалить условие сравнения из route-map. Команда *no match community list exact-match* удаляет запись сравнения из *route-map*. (Она не просто удаляет опцию exact-match.) Команда *no match community* удаляет условие сравнения и все его списки сообществ.

Формат: `no match community community-list [community-list...] [exact-match]`

Режим ввода команд: конфигурирование route-map

match ip address

Чтобы настроить route-map на основе префикса места назначения, используйте команду *match ip address* в режиме конфигурирования route-map. Если указать в одной записи несколько списков префиксов, совпадение будет засчитано, если префикс совпадет с любым значением из списка префиксов. Если настроить запись match ip address внутри части route-map, которая уже имеет записи match ip address, новые списки префиксов будут добавлены к существующим наборам списков префиксов.

Значение по умолчанию: критерии сравнения не заданы.

Формат: `match ip address prefix-list prefix-list-name [prefix-list-name...]`

Режим ввода команд: конфигурирование route-map

Параметр	*Описание*
prefix-list-name	Имя списка префиксов, используемого для определения набора совпадающих маршрутов. Можно указать до 8 списков префиксов.

no match ip address

Чтобы удалить запись сравнения из карты маршрута, используйте **no**-форму команды.

Формат: `no match ip address [prefix-list prefix-list-name [prefix-list-name...]]`

Режим ввода команд: конфигурирование route-map

match ip address <access-list-number | access-list-name>

Данная команды настраивает route-map так, чтобы совпадение определялось на основе критериев соответствия, указанных в списке контроля доступа IP (IP ACL). Имейте в виду, что IP ACL необходимо настроить, прежде чем связывать с route-map. Действия, присутствующие в настройках IP ACL, применяются наряду с другими действиями в route-map. Если IP ACL, на который ссылается карта маршрутов, удаляется или в этом ACL происходит добавление/удаление правил, конфигурация отклоняется.

Если существует набор IP ACL, указанных в этой команде, и пакет совпадает хотя бы с одним критерием этих списков, к пакету применяется соответствующий набор действий в этой route-map.

Если при выполнении команды обнаруживаются дублирующие номера/имена в списках контроля IP-доступа, настройки дубликатов игнорируются.

Значение по умолчанию: критерии сравнения не заданы.

Формат: `match ip address access-list-number | access-list-name [...access-list-number| name ]`

Режим ввода команд: конфигурирование route-map

Параметр	*Описание*
Access-list-number	Номер ACL, определяющий список контроля доступа, настройка которого выполняется в рамках команды. Для стандартных списков контроля доступа это число от 1 до 99. Для расширенных списков контроля доступа это число от 100 до 199.
Access-list-name	Имя списка контроля доступа, определяющее обозначенный IP ACL. Может содержать до 31 символа. При выполнении этой команды match можно указать не более 16 ACL.

no match ip address

Чтобы удалить запись сравнения из route-map, используйте **no**-форму команды.

Формат: `no match ip address [access-list-number | access-list-name]`

Режим ввода команд: конфигурирование route-map

match ipv6 address

Используйте эту команду, чтобы настроить route-map для сопоставления на основе префикса места назначения. Параметр **prefix-list *prefix-list-name*** указывает на имя списка IPv6-префиксов, используемых для определения набора совпадающих маршрутов. Можно указать до 8 списков префиксов. Если в одной записи указать несколько списков префиксов, совпадение будет засчитано, если префикс совпадет с любым из списков префиксов. Если настроить запись match ipv6 address внутри части route-map, которая уже имеет запись match ipv6 address, новые списки префиксов будут добавлены к существующим наборам списков префиксов.

Значение по умолчанию: критерии сравнения не заданы.

Формат: `match ipv6 address prefix-list` *`prefix-list-name`* [*`prefix-list-name...`*]

Режим ввода команд: конфигурирование route-map

no match ipv6 address

Чтобы удалить запись сравнения из route-map, используйте no-форму команды.

Формат: `no match ipv6 address prefix-list` *`prefix-list-name`* [*`prefix-list-name...`*]]

Режим ввода команд: конфигурирование route-map

match length

Используйте эту команду, чтобы настроить карту маршрута на сопоставление по длине пакета 3 уровня между указанными минимальными и максимальными значениями. *min* определяет минимальную длину пакета 3 уровня (включительно), разрешенную для сопоставления. *max* определяет максимальную длину пакета 3 уровня (включительно), разрешенную для сопоставления. Каждая *route-map* может содержать одну запись сопоставления по диапазону длины пакета.

Значение по умолчанию: критерии сравнения не заданы.

Формат: `match length` *`min max`*

Режим ввода команд: конфигурирование route-map

no match length

Команда для удаления записи сопоставления длинна пакета из route-map.

Формат: `no match length`

Режим ввода команд: конфигурирование route-map

match mac-list

Данная команды настраивает route-map так, чтобы совпадение определялось на основе критериев соответствия, указанных в списке контроля доступа MAC (MAC ACL).

MAC ACL необходимо настроить, прежде чем связывать с route-map. Действия, присутствующие в настройках MAC ACL, применяются наряду с другими действиями в route-map. Если MAC ACL, на который ссылается route-map, удаляется или в этом ACL происходит добавление/удаление правил, конфигурация отклоняется.

Значение по умолчанию: критерии сравнения не заданы.

Формат: `match mac-list mac-list-name [mac-list-name]`

Режим ввода команд: конфигурирование route-map

Параметр	*Описание*
mac-list-name	Имя MAC-списка, которое определяет настраиваемый MAC ACL. Имя MAC ACL может быть длиной до 31 символа.

no match mac-list

Чтобы удалить запись сравнения из route-map, используйте **no**-форму команды.

Формат: `no match mac-list [...mac-list-name]`

Режим ввода команд: конфигурирование route-map

set as-path

Используйте команду *set as-path* в режиме конфигурирования *route-map*, чтобы добавить одно или несколько AS в AS-путь в BGP-маршрута. Эта команда обычно используется для вставки одного или более экземпляров локального AS в начале атрибута AS_PATH BGP-маршрута. Это увеличивает длину AS-пути в маршруте. Длина AS-пути оказывает сильное влияние на выбор BGP-маршрута. Изменение длины AS-пути может повлиять на выбор маршрута на локальном маршрутизаторе или на маршрутизаторах, на которых анонсируется этот маршрут.

Если при подготовке входящего маршрута первый сегмент в AS_PATH принятого маршрута является AS_SEQUENCE, в начало последовательности вставляется значение *as-path-string*. Если первый сегмент является AS_SET, значение *as-path-string* добавляется в начало AS-пути в качестве нового сегмента типа AS_SEQUENCE. При подготовке исходящего маршрута для внешнего партнерского устройства *as-path-string* следует за локальным номером AS, которое всегда является первым ASN.

Формат: `set as-path prepend as-path-string`

Режим ввода команд: конфигурирование route-map

Параметр	*Описание*
as-path-string	Список количества AS-путей, добавляемых в начало атрибута AS_PATH для совпадающих BGP маршрутов. Чтобы добавить несколько AS, разделите ASN пробелами и заключите строку в кавычки. Можно добавить до 10 номеров AS.

no set as-path

Используйте **no**-форму команды, чтобы удалить команду *set* из *route-map*.

Формат: `no set as-path prepend as-path-string`

Режим ввода команд: конфигурирование route-map

set comm-list delete

Используйте команду *set comm-list delete* в режиме конфигурирования *route-map*, чтобы удалить сообщества BGP из входящего или исходящего сообщения UPDATE. *Route-mapc* этой set-командой может быть использована для удаления выбранных сообществ из входящих или

исходящих маршрутов. Когда список сообществ применяется к маршруту с такой целью, каждое сообщество маршрута заносится в список сообществ поочередно (по одному за раз). Сообщества, разрешенные списком, удаляются из маршрута. Из-за того, что сообщества обрабатываются индивидуально, списки сообществ, используемые для удаления записей с несколькими сообществами, не должны включать опцию *exact-match*. В противном случае записи никогда не будут совпадать с индивидуальным сообществом.

Если запись route-map одновременно включает в себя условия *set community* и *set comm-list delete*, в первую очередь обрабатывается условие *set comm-list delete*, а затем условие *set community* (то есть сообщества сначала удаляются, а потом добавляются).

Формат: `set comm-list` *`community-list-name`* `delete`

Режим ввода команд: конфигурирование route-map

Параметр	***Описание***
community-list-name	Имя стандартного списка сообществ.

no set comm-list

Чтобы удалить команду *set* из *route-map*, используйте **no**-форму команды.

Формат: `no set comm-list`

Режим ввода команд: конфигурирование route-map

set community

Используйте команду *set community* в режиме конфигурирования *route-map*, чтобы изменить атрибут сообществ для соответствующих маршрутов. Команда *set community* может быть использована для назначения сообществ маршрутам, созданным через сеть BGP и команды распределения, а также установить сообщества на маршруты, полученные от конкретного соседа или анонсируемые конкретному соседу. Она также может быть использована для удаления всех сообществ из маршрута.

Формат: `set community {`*`community-number`* `[additive] | none}`

Режим ввода команд: конфигурирование route-map

Параметр	***Описание***
community-number	От 1 до 16 номеров сообществ в виде целых 32-битных чисел или в формате AA:NN. Разделяются пробелами. Привычные значения сообществ no advertise и no-export также можно использовать.
additive	(Необязательный параметр.) Добавление сообщества к тем, что уже прикреплены к маршруту.
none	(Необязательный параметр.) Удаляет все сообщества из соответствующих маршрутов.

no set community

Используйте **no**-форму команды, чтобы удалить условия *set* из *route-map*.

Формат: `no set community`

Режим ввода команд: конфигурирование route-map

set interface

Если администратор сети не хочет возвращаться к нормальной переадресации, а решает отбрасывать пакеты, не соответствующие указанным критериям, в качестве последней записи в карте маршрута требуется настроить запись set для маршрутизации пакетов на интерфейс *null 0. set interface null0* необходимо настраивать в отдельном правиле. Не следует добавлять его вместе с другим утверждением, имеющим другие условия *match/set*.

Формат: `set interface null0`

Режим ввода команд: конфигурирование route-map

set ip next-hop

Используйте эту команду, чтобы указать ближайший смежный маршрутизатор на пути к месту назначения, к которому требуется переадресовывать пакеты. Если указано несколько IP-адресов, для маршрутизации пакетов используется первый IP-адрес, связанный с текущим подключенным интерфейсом.

Эта команда влияет на все входящие типы пакетов и всегда используется, если настроена. Если настроенный ближайший узел не присутствует в таблице маршрутизации, маршрутизатор присылает соответствующий ARP-запрос.

В записи *route-map* условия *set ip next-hop* и *set ip default next-hop* являются взаимоисключающими. Однако set ip default next-hop может быть настроен в отдельной записи *route-map*.

Формат: `set ip next-hop ip-address [...ip-address]`

Режим ввода команд: конфигурирование route-map

Параметр	***Описание***
ip-address	IP-адрес соседнего узла, к которому направляются пакеты, должен быть адресом смежного маршрутизатора. В одном условии может быть указано до 16 IP-адресов.

no set ip next-hop

Данная команда удаляет соответствующую команду *set* из *route-map*.

Формат: `no set ip next-hop ip-address [...ip-address]`

Режим ввода команд: конфигурирование route-map

set ip default next-hop

Используйте эту команду, чтобы настроить список IP-адресов ближайших узлов по умолчанию. Если указано несколько IP-адресов, используется первый ближайший узел, который является смежным с используемым маршрутизатором. Попытки использования дополнительно указанных IP-адресов выполняются по очереди.

Пакет направляется к ближайшему узлу указанному данной командой, только в случае если в таблице маршрутизации не существует явно заданного маршрута для места назначения пакета. Маршрут по умолчанию в таблице маршрутизации не считается заданным маршрутом для неизвестного адреса места назначения.

В записи *route-map* условия *set ip next-hop* и *set ip default next-hop* являются взаимоисключающими. Однако *set ip default next-hop* может быть настроен в отдельной записи *route-map*.

Формат: `set ip default next-hop ip-address [...ip-address]`

Режим ввода команд: конфигурирование route-map

Параметр	***Описание***
ip-address	IP-адрес соседнего узла, к которому направляются пакеты, должен быть адресом смежного маршрутизатора. В одном условии может быть указано до 16 IP-адресов.

no set ip default next-hop

Данная команда удаляет соответствующую команду *set* из *route-map*.

Формат: `no set ip default next-hop ip-address [...ip-address]`

Режим ввода команд: конфигурирование route-map

set ip precedence

Команда используется для установки трехбитного IP-приоритета в IP-заголовке пакета. Три бита позволяют использовать 8 вариантов значений IP-приоритета: от 0 до 7. Эта команда применяется при реализации QoS и может использоваться другими сервисами QoS, такими как Weighted Fair Queuing (WFQ) и Weighted Random Early Detection (WRED).

Формат: `set ip precedence 0-7`

Режим ввода команд: конфигурирование route-map

Параметр	***Описание***
0	Устанавливает приоритет распорядка
1	Устанавливает приоритет очередности
2	Устанавливает немедленный приоритет
3	Устанавливает Flash-приоритет
4	Устанавливает приоритет Flash-переопределения
5	Устанавливает критический приоритет
6	Устанавливает приоритет межсетевого управления
7	Устанавливает приоритет управления сетью

no set ip precedence

Используйте эту команду, чтобы установить трехбитный IP-приоритет в IP-заголовке пакета в значение по умолчанию.

Формат: `no set ip precedence`

Режим ввода команд: конфигурирование route-map

set ipv6 next-hop (BGP)

Используйте команду *set ipv6 next-hop* в режиме конфигурирования *route-map*, чтобы установить ближайший IPv6-узел на маршруте. Если команда используется в *route-map*, которая

применяется к UPDATE-сообщениям, принятым от соседа, она устанавливает ближайший адрес для соответствующих IPv6-маршрутов, полученных от соседа.

Если команда используется в *route-map*, которая применяется к UPDATE-сообщениям, отправленным соседу, то она устанавливает ближайший адрес для соответствующих IPv6-маршрутов, отправленных соседу. Если адрес является локальным адресом подключения, предполагается, что адрес соответствует интерфейсу, где UPDATE-сообщение будет отправлено или получено. Если команда указывает глобальный IPv6-адрес, он не обязательно должен находиться в локальной подсети.

Формат: `set ipv6 next-hop ipv6-address`

Режим ввода команд: конфигурирование route-map

Параметр	***Описание***
ipv6-address	Набор IPv6-адресов в качестве сетевого адреса для поля «Next Hop» в атрибуте MP_NLRI UPDATE-сообщения.

no set ipv6 next-hop (BGP)

Используйте **no**-форму команды, чтобы удалить команду **set** из route-map.

Формат: `no set ipv6 next-hop`

Режим ввода команд: конфигурирование route-map

set local-preference

Чтобы установить локальный приоритет определенных BGP-маршрутов, используйте команду *set local-preference* в режиме конфигурирования карты маршрута. Локальный приоритет — это первый атрибут, используемый для сравнения BGP-маршрутов. Установка локального приоритета может повлиять на то, какой BGP-маршрут будет выбран в качестве оптимального. При использовании вместе с командой *match as-path* или *match ip address* данная команда может применяться для выбора в качестве приоритетных тех маршрутов, которые направляют определенные AS, или же для выбора локального маршрутизатора как более приоритетной точки выхода для определенных целевых адресов.

Формат: `set local-preference value`
Режим ввода команд: конфигурирование карты маршрута

Параметр	***Описание***
value	Значение локального приоритета, от 0 до 4 294 967 295 (любое целое 32-битное число).

no set local-preference

Используйте **no**-форму команды, чтобы удалить команду *set* из карты маршрута.

Формат: `no set local-preference value`

Режим ввода команд: конфигурирование карты маршрута

set metric (BGP)

Чтобы задать метрику маршрута, используйте команду *set metric* в режиме конфигурирования *route-map*. При использовании в контексте BGP эта команда устанавливает атрибут Multi Exit

Discriminator (MED). Когда между двумя автономными системами (AS) используются несколько точек пиринга, установка MED на маршрутах, анонсируемых одним маршрутизатором, может влиять на другую AS так, что передача трафика будет выполняться через конкретного партнера.

Формат: `set metric value`
Режим ввода команд: конфигурирование route-map

Параметр	***Описание***
value	Значение метрики, от 0 до 4294967295 (любое целое 32-битное число).

no set metric (BGP)

Используйте **no**-форму команды, чтобы удалить команду *set* из *route-map*.

Формат: `no set metric value`

Режим ввода команд: конфигурирование route-map

show ip policy

Эта команда отображает *route-map*, связанные с каждым интерфейсом.

Формат: `show ip policy`

Режим ввода команд: привилегированный

Параметр	***Описание***
Interface	Интерфейс.
Route-map	Route-map.

show ip prefix-list

Эта команда отображает конфигурацию и статус списка префиксов.

Формат: `show ip prefix-list [detail | summary] prefix-list-name [network/length] [seq sequence-number] [longer] [first-match]`

Режим ввода команд: привилегированный

Параметр	***Описание***
detail | summary	Интерфейс.
prefix-list-name	(Необязательный параметр.) Имя конкретного списка префиксов.
network/length	(Необязательный параметр.) Номер сети и длина маски сети (в битах).
seq	(Необязательный параметр.) Порядковый номер записи списка префиксов.
sequence-number	(Необязательный параметр.) Порядковый номер записи в списке префиксов.
longer	(Необязательный параметр.) Отображает все записи списка префиксов, которые уточняют заданную сеть/длину маски.
first-match	(Необязательный параметр.) Отображает все записи списка префиксов, которые совпадают с заданной сетью/длиной маски.

Ниже перечислены допустимые формы данной команды.

- `show ip prefix-list prefix-list-name network/length first-match`

- show ip prefix-list prefix-list-name network/length longer show ip prefix-list prefix-list-name network/length
- show ip prefix-list prefix-list-name seq sequence-number show ip prefix-list prefix-list-name
- show ip prefix-list summary
- show ip prefix-list summary prefix-list-name show ip prefix-list detail
- show ip prefix-list detail prefix-list-name

show ipv6 prefix-list

Эта команда отображает настройку и статус выбранного списка префиксов.

Формат: show ipv6 prefix-list [detail | summary] *listname* [*ipv6-prefix/prefix-length*] [seq *sequence- number*] [longer] [first-match]

Режим ввода команд: привилегированный

Параметр	*Описание*
detail | summary	(Необязательный параметр.) Позволяет отобразить подробную или сводную информацию о списке префиксов.
list-name	(Необязательный параметр.) Имя конкретного списка префиксов.
ipv6-prefix/prefix- length	(Необязательный параметр.) Номер сети и длина маски сети (в битах).
seq	(Необязательный параметр.) Порядковый номер записи списка префиксов.
sequence-number	(Необязательный параметр.) Порядковый номер записи в списке префиксов.
longer	(Необязательный параметр.) Отображает все записи списка префиксов, которые уточняют заданную сеть/длину маски.
first-match	(Необязательный параметр.) Отображает все записи списка префиксов, которые совпадают с заданной сетью/длиной маски.

Ниже перечислены допустимые формы данной команды:

- show ipv6 prefix-list listname ipv6-prefix/prefix-length first-match
- show ipv6 prefix-list listname ipv6-prefix/prefix-length longer show ipv6 prefix-list listname ipv6-prefix/prefix-length
- show ipv6 prefix-list listname seq sequence-number show ipv6 prefix-list listname
- show ipv6 prefix-list summary
- show ipv6 prefix-list summary prefix-list-name show ipv6 prefix-list detail
- show ipv6 prefix-list detail prefix-list-name

Команда отображает следующую информацию.

Параметр	*Описание*
count	Количество записей в списке префиксов.
range entries	Количество записей, совпадающих с введенным диапазоном.
ref count	Количество записей, ссылающихся на данный список префиксов.
seq	Порядковый номер записи в списке.
permit/deny	Указанное действие.
sequences	Диапазон порядковых номеров для записей в списке.
hit count	Количество совпадений для данной записи префикса.

show route-map

Используйте команду *show route-map* в привилегированном режиме, чтобы отобразить route-map.

Формат: `show route-map [`*`map-name`*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
map-name	(Необязательный параметр.) Имя заданной route-map.

clear ip prefix-list

Чтобы сбросить счетчики списка IP-префиксов, используйте команду *clear ip prefix-list* в привилегированном режиме. Эта команда используется, чтобы очистить счетчики совпадений для списка префиксов. Число совпадений указывается для определенной записи списка префиксов.

Формат: `clear ip prefix-list [[`*`prefix-list-name`*`] [`*`network/length`*`]]`

Режим ввода команд: привилегированный

Параметр	*Описание*
prefix-list-name	(Необязательный параметр) Имя списка префиксов, для которого будут сброшены счетчики.
network/length	(Необязательный параметр.) Номер сети и длина маски сети (в битах). Если эта опция указана, счетчики совпадений сбрасываются только для совпадающей записи.

clear ipv6 prefix-list

Используйте эту команду, чтобы сбросить счетчики совпадений для списка IPv6 префиксов. Число совпадений указывается для определенной записи списка префиксов.

Формат: `clear ipv6 prefix-list [`*`prefix-list-name`*`] [ipv6-prefix/`*`prefix-length`*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
list-name	(Необязательный параметр) Имя списка префиксов, для которого будут сброшены счетчики.
ipv6-prefix/prefix-length	(Необязательный параметр.) Номер IPv6-префикса и длина маски сети (в битах). Если эта опция указана, счетчики совпадений сбрасываются только для совпадающего заявления.

11.4 Команды Router Discovery Protocol

В этой части приведены команды, которые используются для просмотра и настройки параметров Internet Router Discovery Protocol (IRDP) на коммутаторе. Протокол IRDP позволяет узлу обнаружить IP-адреса маршрутизаторов в подсети.

ip irdp

Эта команда включает протокол IRDP на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `ip irdp`

Режим ввода команд: конфигурирование интерфейса

no ip irdp

Команда выключает протокол IRDP на интерфейсе.

Формат: `no ip irdp`

Режим ввода команд: конфигурирование интерфейса

ip irdp address

Данная команда настраивает адрес, используемый интерфейсом для отправления анонсов обнаружения маршрутизатора. Действительные значения для *ipaddr* — 224.0.0.1, IP-адрес многоадресной рассылки для всех узлов, и 255.255.255.255, ограниченный широковещательный адрес.

Значение по умолчанию: 224.0.0.1

Формат: `ip irdp address` *ipaddr*

Режим ввода команд: конфигурирование интерфейса

no ip irdp address

Эта команда устанавливает адрес, используемый интерфейсом для отправления анонсов обнаружения маршрутизатора, в значение по умолчанию.

Формат: `no ip irdp address`

Режим ввода команд: конфигурирование интерфейса

ip irdp holdtime

Эта команда настраивает значение поля holdtime (в секундах) для анонсов обнаружения маршрутизатора, отправляемых с данного интерфейса. Диапазон значений — от 4 до 9000 секунд.

Значение по умолчанию: утроенное значение максимального интервала

Формат: `ip irdp holdtime` *4-9000*

Режим ввода команд: конфигурирование интерфейса

no ip irdp holdtime

Команда устанавливает значение в поле holdtime (в секундах) для анонсов обнаружения маршрутизатора, отправляемых с данного интерфейса, по умолчанию.

Формат: `no ip irdp holdtime`

Режим ввода команд: конфигурирование интерфейса

ip irdp maxadvertinterval

Эта команда настраивает максимальное разрешенное время (в секундах) между отправкой анонсов обнаружения маршрутизатора с данного интерфейса. Диапазон значений для maxadvertinterval — от 4 до 9000 секунд.

Значение по умолчанию: 600

Формат: `ip irdp maxadvertinterval` *`4-1800`*

Режим ввода команд: конфигурирование интерфейса

no ip irdp maxadvertinterval

Данная команда устанавливает параметр maxadvertinterval в значение по умолчанию (в секундах).

Формат: `no ip irdp maxadvertinterval`

Режим ввода команд: конфигурирование интерфейса

ip irdp minadvertinterval

Эта команда настраивает минимальное разрешенное время (в секундах) между отправкой анонсов обнаружения маршрутизатора с данного интерфейса. Диапазон значений для minadvertinterval — от 3 до 1800 секунд.

Значение по умолчанию: 0.75 * maxadvertinterval

Формат: `ip irdp minadvertinterval` *`3-1800`*

Режим ввода команд: конфигурирование интерфейса

no ip irdp minadvertinterval

Данная команда устанавливает параметр minadvertinterval в значение по умолчанию.

Формат: `no ip irdp minadvertinterval`

Режим ввода команд: конфигурирование интерфейса

ip irdp multicast

Эта команда настраивает IP-адрес места назначения для анонсов обнаружения маршрутизатора как 224.0.0.1, то есть как адрес по умолчанию. no-форма данной команды настраивает IP-адрес как 255.255.255.255, чтобы анонсы обнаружения отправлялись на ограниченный широковещательный адрес.

Формат: `ip irdp multicast` *`ip address`*

Режим ввода команд: конфигурирование интерфейса

no ip irdp multicast

По умолчанию анонсы обнаружения маршрутизатора отправляются на адрес 224.0.0.1. Чтобы они отправлялись на ограниченный широковещательный адрес (255.255.255.255), используйте no-форму команды.

Формат: `no ip irdp multicast`

Режим ввода команд: конфигурирование интерфейса

ip irdp preference

Данная команда настраивает приоритет конкретного адреса в качестве адреса маршрутизатора по умолчанию по отношению к другим адресам маршрутизатора в той же подсети.

Значение по умолчанию: 0

Формат: `ip irdp preference -2147483648 to 2147483647`

Режим ввода команд: конфигурирование интерфейса

no ip irdp preference

Данная команда устанавливает в значение по умолчанию приоритет конкретного адреса в качестве адреса маршрутизатора по умолчанию по отношению к другим адресам маршрутизатора в той же подсети.

Формат: `no ip irdp preference`

Режим ввода команд: конфигурирование интерфейса

show ip irdp

Команда отображает информацию протокола IPRDP для всех интерфейсов, конкретного интерфейса или конкретной VLAN. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ip irdp {unit/slot/port|vlan 1-4093|all}`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
Interface	Значение unit/slot/port, которое соответствует физическому или виртуальному интерфейсу маршрутизации.
vlan	Используйте это ключевое слово, чтобы непосредственно указать идентификатор VLAN для маршрутизирующего VLAN-интерфейса вместо формата *unit/slot/port*.
Ad Mode	Режим анонсирования, который показывает, включено ли обнаружение маршрутизатора на данном интерфейсе.
Dest Address	Целевой IP-адрес анонсов обнаружения маршрутизатора.
Max Int	Максимальный интервал анонсов: максимально допустимое время в секундах между отправкой анонсов обнаружения маршрутизатора с данного интерфейса.

Min Int	Минимальный интервал анонсов: минимально допустимое время в секундах между отправкой анонсов обнаружения маршрутизатора с данного интерфейса.
Hold Time	Период времени в секундах, в течение которого система должна сохранять анонс маршрутизатора, прежде чем удалить его.
Preference	Приоритет конкретного адреса в качестве адреса маршрутизатора по умолчанию по отношению к другим адресам маршрутизатора в той же подсети.

11.5 Команды настройки виртуального маршрутизатора

ip vrf

Данная команда создает виртуальный маршрутизатор с указанным именем и выполняет вход в режим конфигурирования виртуального маршрутизатора.

Значение по умолчанию: виртуальные маршрутизаторы не заданы

Формат: `ip vrf` *`vrf-name`*

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
vrf-name	Имя виртуального маршрутизатора. Строка длиной до 64 символов ASCII.

no ip vrf

Удаляет виртуальный маршрутизатор с указанным названием.

Формат: `no ip vrf` *`vrf-name`*

Режим ввода команд: глобальная конфигурация

maximum routes

Эта команда резервирует количество разрешенных маршрутов и устанавливает максимальное ограничение на количество маршрутов для экземпляра виртуального маршрутизатора в объеме сводной таблицы маршрутизации для данного маршрутизатора (при условии наличия достаточного свободного места в сводной таблице маршрутизации).

Значение по умолчанию: ограничено количеством доступных свободных маршрутов.

Формат: `maximum routes {`*`limit`*` | warn `*`threshold`*`}`

Режим ввода команд: конфигурирование виртуального маршрутизатора

Параметр	***Описание***
limit	Количество маршрутов для экземпляра виртуального маршрутизатора в сводной таблице маршрутизации. Диапазон значений — от 1 до 4 294 967 295. Если указанное ограничение превышает размер сводной таблицы маршрутизатора, применяется ограничение по действительному размеру.
warn threshold	Значение порога (от 1 до 100) обозначает процент от предельного значения, при котором будет создано соответствующее предупреждение. Если предельное значение не задано, в качестве предельного значения принимается общий объем платформы.

no maximum routes

Эта команда удаляет резервирование для разрешенных маршрутов экземпляра виртуального маршрутизатора и значение порога предупреждений.

Формат: `no maximum routes`

Режим ввода команд: конфигурирование виртуального маршрутизатора

description

Данная команда позволяет настроить текст описания для виртуального маршрутизатора.

Значение по умолчанию: отсутствует

Формат: `description` *`text`*

Режим ввода команд: конфигурирование виртуального маршрутизатора

Параметр	***Описание***
text	Текст описания для виртуального маршрутизатора. Длина текста — до 512 ASCII-символов.

no description

Эта команда удаляет текст описания виртуального маршрутизатора.

Формат: `no description`

Режим ввода команд: конфигурирование виртуального маршрутизатора

ip vrf forwarding

Эта команда связывает IP-интерфейс с виртуальным маршрутизатором.

Значение по умолчанию: маршрутизатор по умолчанию

Формат: `ip vrf forwarding` *`vrf-name`*

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
vrf-name	Имя виртуального маршрутизатора.

no ip vrf forwarding

Эта команда удаляет привязку IP-интерфейса к настроенному виртуальному маршрутизатору и опять связывает его с маршрутизатором по умолчанию.

Формат: `no ip vrf forwarding`

Режим ввода команд: конфигурирование интерфейса

show ip vrf

Данная команда отображает информацию об экземплярах виртуального маршрутизатора.

Значение по умолчанию: отсутствует

Формат: `show ip vrf [{`*`vrf-name`*` | detail `*`vrf-name`*` | interfaces | memory [`*`vrf-name`*`]}]`

Режим ввода команд: привилегированный

Параметр	*Описание*
vrf-name	Название экземпляра виртуального маршрутизатора.
detail	Отображает конфигурацию и статус виртуального маршрутизатора.
interfaces	Отображает список интерфейсов и виртуальные маршрутизаторы, с которыми они связаны.
memory	Отображает текущее использование памяти процессами, запущенными на виртуальном маршрутизаторе.

11.6 Команды настройки маршрутизации сети VLAN

В этой части описаны команды, которые используются для просмотра и настройки маршрутизации VLAN, а также для просмотра информации о состоянии виртуальной маршрутизации.

vlan routing

Данная команда включает маршрутизацию в сети VLAN. Параметр *vlanid* имеет диапазон от 1 до 4094. Параметр [interface ID] имеет диапазон от 1 до 256. Обычно аргумент идентификатора интерфейса не указывается, и система выбирает идентификатор интерфейса автоматически. Однако если указать идентификатор интерфейса, он станет номером порта в *unit/slot/port* для виртуального интерфейса маршрутизации. Если будет выбран идентификатор интерфейса, который уже используется, CLI выведет сообщение об ошибке и не создаст интерфейс VLAN. При использовании продуктов с конфигурацией на основе текста включение в команду vlan routing идентификатора интерфейса в текстовой конфигурации гарантирует, что значение *unit/slot/port* для интерфейса VLAN после перезагрузки останется прежним. Сохранение значения *unit/slot/port* одинаковым гарантирует, что после перезагрузки системы для каждого интерфейса будет применена правильная конфигурация.

Формат: `vlan routing` *`vlanid`* [*`interface ID`*]

Режим ввода команд: конфигурация VLAN

no vlan routing

Эта команда выключает маршрутизацию в сети VLAN.

Формат: `no vlan routing` *`vlanid`*

Режим ввода команд: конфигурация VLAN

Обычно клавишу **<ввода>** нажимают без указания идентификатора интерфейса, и система выбирает идентификатор интерфейса автоматически.

interface vlan

Используйте эту команду, чтобы войти в режим конфигурирования интерфейса для указанной VLAN. Диапазон значений vlan-id — от 1 до 4094.

Формат: `interface vlan` *`vlan-id`*

Режим ввода команд: глобальная конфигурация

show ip vlan

Эта команда отображает информацию о маршрутной информации VLAN для всех VLAN с включенной маршрутизацией.

Формат: `show ip vlan`

Режим ввода команд: привилегированный
пользовательский

Параметр	*Описание*
MAC Address used by Routing VLANs	MAC-адрес, связанный с Internal Bridge-Router Interface (IBRI). Этот же MAC-адрес используется всеми виртуальными интерфейсами маршрутизации. Он отображается над информацией по каждой VLAN.
VLAN ID	Идентификатор VLAN.
Logical Interface	Логический интерфейс, связанный с виртуальным интерфейсом маршрутизации, в формате unit/slot/port.
IP Address	IP-адрес, связанный с данной VLAN.
Subnet Mask	Маска подсети, связанная с данной VLAN.

11.7 Команды настройки протокола VRRP

В этой части приведены команды, которые используются для настройки Virtual Router Redundancy Protocol (VRRP) и для просмотра информации о состоянии VRRP. VRRP помогает обеспечить аварийное переключение и балансировку нагрузки при настройке двух устройств в качестве VRRP-пары.

ip vrrp (режим глобальной конфигурации)

Используйте эту команду в режиме глобальной конфигурации, чтобы включить на маршрутизаторе административный режим VRRP.

Значение по умолчанию: отсутствует

Формат: `ip vrrp`

Режим ввода команд: глобальная конфигурация

no ip vrrp

В режиме глобальной конфигурации команда выключает административный режим VRRP по умолчанию на маршрутизаторе.

Формат: `no ip vrrp`

Режим ввода команд: глобальная конфигурация

ip vrrp (режим конфигурирования интерфейса)

Используйте эту команду в режиме конфигурирования интерфейса, чтобы создать виртуальный маршрутизатор, связанный с интерфейсом или диапазоном интерфейсов. Параметр vrid — это идентификатор виртуального маршрутизатора, который является целым числом от 1 до 255.

Формат: `ip vrrp vrid`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp

В режиме конфигурирования интерфейса данная команда удаляет виртуальный маршрутизатор, связанный с интерфейсом. Идентификатор виртуального маршрутизатора, *vrid* — это целое число от 1 до 255.

Формат: `no ip vrrp vrid`

Режим ввода команд: конфигурирование интерфейса

ip vrrp mode

Эта команда включает виртуальный маршрутизатор, настроенный на указанном интерфейсе. Включение поля статуса запускает виртуальный маршрутизатор. Параметр vrid — это идентификатор виртуального маршрутизатора, который является целым числом от 1 до 255.

Значение по умолчанию: выключено

Формат: `ip vrrp vrid mode`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp mode

Данная команда выключает виртуальный маршрутизатор, настроенный на указанном интерфейсе. Выключение поля статуса останавливает виртуальный маршрутизатор.

Формат: `no ip vrrp vrid mode`

Режим ввода команд: конфигурирование интерфейса

ip vrrp ip

Эта команда устанавливает значение IP-адреса виртуального маршрутизатора для интерфейса или диапазона интерфейсов. Значение *ipaddr* — это IP-адрес, который будет настроен на интерфейсе для VRRP. Параметр *vrid* — это идентификатор виртуального маршрутизатора, который является целым числом в диапазоне от 1 до 255. Необязательный параметр *[secondary]* может быть использован для назначения IP-адреса в качестве вторичного.

Значение по умолчанию: отсутствует

Формат: `ip vrrp vrid ip ipaddr [secondary]`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp ip

Используйте эту команду в режиме конфигурирования интерфейса, чтобы удалить с интерфейса значение вторичного IP-адреса. Чтобы удалить первичный IP-адрес, на интерфейсе требуется удалить виртуальный маршрутизатор.

Формат: `no ip vrrp vrid ipaddress secondary`

Режим ввода команд: конфигурирование интерфейса

ip vrrp accept-mode

Используйте эту команду, чтобы позволить основному VRRP-узлу принимать пакеты ping, отправленные по одному из IP-адресов виртуального маршрутизатора.

Значение по умолчанию: выключено

Формат: `ip vrrp vrid accept-mode`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp accept-mode

Используйте эту команду, чтобы запретить основному VRRP-узлу принимать пакеты ping, отправленные по одному из IP-адресов виртуального маршрутизатора.

Формат: `no ip vrrp vrid accept-mode`

Режим ввода команд: конфигурирование интерфейса

ip vrrp authentication

Эта команда устанавливает значение для подробных данных авторизации на виртуальном маршрутизаторе, настроенном на указанном интерфейсе или диапазоне интерфейсов. Параметр *{none | simple}* указывает тип авторизации для виртуального маршрутизатора, настроенный на указанном интерфейсе. Параметр *[key]* не является обязательным, он необходим только для авторизации с использованием простого текстового пароля. Параметр *vrid* — это идентификатор виртуального маршрутизатора, который является целым числом от 1 до 255.

Значение по умолчанию: без авторизации

Формат: `ip vrrp vrid authentication {none | simple key}`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp authentication

Команда устанавливает значение по умолчанию для подробных данных авторизации на виртуальном маршрутизаторе, настроенном на указанном интерфейсе или диапазоне интерфейсов.

Формат: `no ip vrrp vrid authentication`

Режим ввода команд: конфигурирование интерфейса

ip vrrp preempt

Эта команда устанавливает режим preemption на настраиваем виртуальном маршрутизаторе указанного интерфейса или диапазона интерфейсов. Параметр *vrid* — это идентификатор виртуального маршрутизатора, целое число от 1 до 255.

Значение по умолчанию: включено

Формат: `ip vrrp vrid preempt`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp preempt

Команда возвращает режим preemption на настраиваем виртуальном маршрутизаторе указанного интерфейса или диапазона интерфейсов в значение по умолчанию.

Формат: `no ip vrrp vrid preempt`

Режим ввода команд: конфигурирование интерфейса

ip vrrp priority

Эта команда устанавливает приоритет маршрутизатора в рамках VRRP-группы. Может использоваться для настройки интерфейса или диапазона интерфейсов. Чем больше значения, тем выше приоритет. Диапазон — от 1 до 254. Параметр vrid — это идентификатор виртуального маршрутизатора в диапазоне от 1 до 255.

Маршрутизатор с более высоким приоритетом назначается главным. Если маршрутизатор настроен с адресом, который используется как адрес виртуального маршрутизатора, он называется «владельцем адреса». Приоритет владельца адреса всегда 255, поэтому владелец адреса всегда является главным маршрутизатором. Если приоритет главного маршрутизатора менее 255 (то есть это не владелец адреса), а приоритет другого маршрутизатора в группе имеет более высокое значение, другой маршрутизатор станет главным только в том случае, если включен режим preemption.

Значение по умолчанию: 100; для владельца адреса значение автоматически устанавливается как 255.

Формат: `ip vrrp` *`vrid`* `priority` *`1-254`*

Режим ввода команд: конфигурирование интерфейса

no ip vrrp priority

Команда устанавливает приоритет виртуального маршрутизатора, настроенного на указанном интерфейсе или диапазоне интерфейсов, в значение по умолчанию.

Формат: `no ip vrrp` *`vrid`* `priority`

Режим ввода команд: конфигурирование интерфейса

ip vrrp timers advertise

Эта команда устанавливает частоту (в секундах), с которой интерфейс или диапазон интерфейсов на указанном виртуальном маршрутизаторе отправляет анонсы виртуального маршрутизатора.

Значение по умолчанию: 1

Формат: `ip vrrp` *`vrid`* `timers advertise` *`1-255`*

Режим ввода команд: конфигурирование интерфейса

no ip vrrp timers advertise

Эта команда устанавливает частоту анонсов виртуального маршрутизатора для интерфейса или диапазона интерфейсов в значение по умолчанию.

Формат: `no ip vrrp` *`vrid`* `timers advertise`

Режим ввода команд: конфигурирование интерфейса

ip vrrp track interface

Используйте эту команду, чтобы менять приоритет VRRP-маршрутизатора на основе доступности его интерфейсов. Команда применяется для отслеживания интерфейсов, которые не настроены для VRRP. Отслеживаются только IP-интерфейсы. Отслеживаемый интерфейс работает, если доступен IP-адрес этого интерфейса. В противном случае отслеживаемый интерфейс считается выключенным. Данную команду можно использовать, чтобы настроить один интерфейс или диапазон интерфейсов. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Когда отслеживаемый интерфейс выключен или удален с маршрутизатора, приоритет VRRP-маршрутизатора будет уменьшен на величину, указанную в аргументе *priority*. Когда интерфейс снова станет доступен для IP-протокола, приоритет будет повышен на величину аргумента *priority*.

Настроенный VRRP-интерфейс может отслеживать несколько интерфейсов. Если отслеживаемый интерфейс выключается, приоритет маршрутизатора понижается на 10 единиц (шаг по умолчанию) за каждый выключенный интерфейс. Шаг изменения приоритета по умолчанию изменяется с помощью аргумента *priority*. Приоритет виртуального маршрутизатора по умолчанию — 100, а шаг изменения приоритета по умолчанию — 10. По умолчанию интерфейсы не отслеживаются. Если указать только интерфейс для отслеживания, не указывая необязательное значение приоритета, для интерфейса устанавливается приоритет по умолчанию. Шаг изменения приоритета по умолчанию — 10.

Значение по умолчанию: приоритет: 10

Формат: `ip vrrp` *`vrid`* `track interface {`*`unit/slot/port`*`|vlan` *`1-4093`*`} [decrement` *`priority`*`]`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp track interface

Используйте эту команду, чтобы удалить интерфейс или диапазон интерфейсов из списка отслеживаемых или восстановить шаг изменения приоритета в значение по умолчанию.

Формат: `no ip vrrp` *`vrid`* `track interface {`*`unit/slot/port`*`|vlan` *`1-4093`*`} [decrement]`

Режим ввода команд: конфигурирование интерфейса

ip vrrp track ip route

Данная команда позволяет отслеживать доступность маршрута на интерфейсе или диапазоне интерфейсов. Если отслеживаемый маршрут удален, VRRP-маршрутизатора будет уменьшен на величину, указанную в аргументе priority. Если маршрут добавляется, приоритет будет увеличен согласно значению того же аргумента.

Настроенный VRRP интерфейс может отслеживать несколько маршрутов. Если отслеживаемый маршрут оказывается недоступным, приоритет маршрутизатора понижается на 10 единиц (шаг по умолчанию) за каждый недоступный маршрут. По умолчанию маршруты не отслеживаются. Если указать только маршрут для отслеживания, не указывая необязательное значение приоритета, устанавливается приоритет по умолчанию. Шаг изменения приоритета по умолчанию — 10. Шаг изменения приоритета по умолчанию изменяется с помощью аргумента priority.

Значение по умолчанию: приоритет: 10

Формат: `ip vrrp vrid track ip route ip-address/prefix-length [decrement priority]`

Режим ввода команд: конфигурирование интерфейса

no ip vrrp track ip route

Используйте эту команду, чтобы удалить маршрут из списка отслеживаемых или восстановить шаг изменения приоритета в значение по умолчанию. При удалении недоступного IP-маршрута из списка отслеживаемых приоритет должен быть увеличен на соответствующее значение.

Формат: `no ip vrrp vrid track interface unit/slot/port [decrement]`

Режим ввода команд: конфигурирование интерфейса

show ip vrrp interface stats

Данная команда отображает статистику каждого виртуального маршрутизатора, настроенного на коммутаторе. Аргумент *unit/slot/p*ort относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ip vrrp interface stats {unit/slot/port|vlan 1-4093} vrid`

Режим ввода команд: привилегированный

пользовательский

Параметр	***Описание***
Uptime	Время работы виртуального маршрутизатора с момента включения в днях, часах, минутах и секундах.
Protocol	Протокол, настроенный на интерфейсе.
State Transitioned to Master	Общее количество случаев, когда статус виртуального маршрутизатора был изменен на MASTER.
Advertisment Received	Общее количество VRRP-анонсов, полученных этим виртуальным маршрутизатором.
Advertisment Interval Errors	Общее количество полученных VRRP-анонсов, для которых интервал анонсирования отличался от значения, настроенного для этого виртуального маршрутизатора.
Authentication Failure	Общее количество полученных VRRP-пакетов, которые не прошли проверку аутентификации.
IP TTL errors	Общее количество VRRP-пакетов, полученных виртуальным маршрутизатором, в которых IP TTL не было равно 255.
Zero Priority Packets Received	Общее количество VRRP-пакетов, полученных виртуальным маршрутизатором с приоритетом 0.
Zero Priority Packets Sent	Общее количество VRRP-пакетов, отправленных виртуальным маршрутизатором с приоритетом 0.
Invalid Type Packets Received	Общее количество VRRP-пакетов, полученных виртуальным маршрутизатором с недействительным значением поля type.
Address List Errors	Общее количество полученных VRRP-пакетов, для которых список адресов не соответствует локально настроенному списку данного виртуального маршрутизатора.

Invalid Authentication Type	Общее количество полученных VRRP-пакетов с неизвестным типом аутентификации.
Authentication Type Mismatch	Общее количество полученных VRRP-анонсов с параметром auth type, не равным локально настроенному типу аутентификации виртуального маршрутизатора.
Packet Length Errors	Общее количество полученных VRRP-пакетов с длиной пакета менее длины VRRP-заголовка.

show ip vrrp

Эта команда отображает, включены ли на коммутаторе функции VRRP. Она также выводит некоторые глобальные параметры, необходимые для мониторинга. Дополнительных опций у команды нет.

Формат: `show ip vrrp`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
VRRP Admin Mode	Административный режим VRRP-функционала на коммутаторе.
Router Checksum Errors	Общее количество VRRP-пакетов, полученных с неверным значением контрольной суммы VRRP.
Router Version Errors	Общее количество полученных VRRP-пакетов с неизвестным или не поддерживаемым номером версии.
Router VRID Errors	Общее количество полученных VRRP-пакетов с неверным значением VRID для этого виртуального маршрутизатора.

show ip vrrp interface

Эта команда отображает всю конфигурационную информацию и статистику VRRP-маршрутизатора для виртуального маршрутизатора, настроенного на указанном интерфейсе. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Используйте вывод команды, чтобы проверить настройки отслеживаемого интерфейса или IP-маршрута.

Формат: `show ip vrrp interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`} `*`vrid`*

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
IP Address	Настроенный IP-адрес виртуального маршрутизатора.
VMAC address	VMAC-адрес указанного маршрутизатора.
Authentication type	Тип аутентификации указанного виртуального маршрутизатора.
Priority	Значение приоритета указанного виртуального маршрутизатора с учетом всех снижений приоритета на основании отслеживаемых интерфейсов или маршрутов.
Configured Priority	Приоритет, настроенный с помощью команды ip vrrp vrid priority 1-254.

Advertisement interval	Интервал анонсирования в секундах для указанного виртуального маршрутизатора.
Pre-Empt Mode	Режим preemption, настроенный на указанном маршрутизаторе.
Administrative Mode	Статус указанного маршрутизатора (Enable или Disable).
Accept Mode	Если включен, основной узел VRRP может принимать пакеты ping, отправленные по одному из IP-адресов виртуального маршрутизатора.
State	Статус виртуального маршрутизатора (Master/backup).

show ip vrrp interface brief

Эта команда отображает информацию о каждом виртуальном маршрутизаторе, настроенном на коммутаторе. Дополнительных опций у команды нет. Она отображает информацию для каждого виртуального маршрутизатора.

Формат: `show ip vrrp interface brief`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
Interface	Интерфейс в формате unit/slot/port
VRID	Идентификатор виртуального маршрутизатора.
IP Address	IP-адрес виртуального маршрутизатора.
Mode	Указывает, включен или выключен виртуальный маршрутизатор.
State	Статус виртуального маршрутизатора (Master/backup).

11.8 Команды настройки протокола VRRPv3

Протокол VRRPv3 обеспечивает резервирование адресов маршрутизатора (как для IPv4, так и для IPv6). Поддержка VRRPv3 аналогична поддержке VRRP. Основные различия между версиями протокола представлены в следующей таблице.

VRRPv2	***VRRPv3***
Поддержка резервирования IPv4-адресов	Поддержка резервирования IPv4- и IPv6-адресов
Поддержка аутентификации	Без поддержки аутентификации
Не работает с link-local адресами	Поддерживается работа с link-local IPv6-адресами
Интервал отправки VRRP задается в секундах	Интервал отправки VRRP-анонсов задается в сантисекундах(0,01 секунды).
Формат MAC-адреса VRRP — 00-00-5E-00-01-{VRID}	Формат MAC-адреса для IP-адресов IPv6 VR — 00-00-5E-00-02-{VRID}
Реализация SNMP MIB основана на RFC 2787. Используются 32-битные счетчики.	Реализация SNMP MIB основана на RFC 6527. Используются 64-битные счетчики

fhrp version vrrp v3

Чтобы включить на устройстве поддержку конфигурации протокола VRRP версии 3 (VRRPv3), выполните команду fhrp version vrrp v3 в режиме глобальной конфигурации.

При включении VRRPv3 протокол VRRP версии 2 (VRRPv2) становится недоступным. После выполнения команды no fhrp version vrrp v3 поддержка VRRPv3 выключается, включается версия VRRPv2. Кроме того, эта команда выполняет сброс оперативных данных и применяет конфигурацию VRRPv2. Аналогичные процессы происходят при выполнении команды no ip vrrp во время использования VRRPv2.

Значение по умолчанию: выключено

Формат: `fhrp version vrrp v3`

Режим ввода команд: глобальная конфигурация

no fhrp version vrrp v3

Данная команда отключает на устройстве протокол VRRPv3 и включает VRRPv2.

Формат: `no fhrp version vrrp v3`

Режим ввода команд: глобальная конфигурация

snmp-server enable traps vrrp

Эта команда включает отправку SNMP-трапов, определенных в стандартах для VRRPv2 и VRRPv3.

Значение по умолчанию: включено

Формат: `snmp-server enable traps vrrp`

Режим ввода команд: глобальная конфигурация

no snmp-server enable traps vrrp

Данная команда выключает отправку SNMP-трапов, определенных в стандартах для VRRPv2 и VRRPv3.

Значение по умолчанию: включено

Формат: `no snmp-server enable traps vrrp`

Режим ввода команд: глобальная конфигурация

vrrp

Команда vrrp позволяет создать группу виртуальных маршрутизаторов VRRPv3 и войти в режим конфигурирования группы VRRPv3.

Формат: `vrrp group-id address-family {ipv4 | ipv6}`

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
group-id	Номер группы виртуальных маршрутизаторов. Диапазон — от 1 до 255.
address-family	Семейство адресов для данной группы VRRP.
ipv4	(Необязательно.) Семейство адресов IPv4.
ipv6	(Необязательно.) Семейство адресов IPv6.

no vrrp

Команда no vrrp удаляет указанную группу виртуальных маршрутизаторов VRRPv3. Перед использованием этой команды необходимо выключить виртуальный маршрутизатор, выполнив команду shutdown в соответствующем режиме конфигурирования VRRP.

Формат: `no vrrp group-id address-family {ipv4 | ipv6}`

Режим ввода команд: конфигурирование интерфейса

preempt

Данная команда позволяет настроить устройство в качестве главного виртуального маршрутизатора для группы VRRP, если его приоритет выше приоритета текущего главного виртуального маршрутизатора.

Значение по умолчанию: включено, значение задержки по умолчанию — 0

Формат: `preempt [delay minimum centiseconds]`

Режим ввода команд: конфигурирование VRRPv3

Параметр	***Описание***
delay minimum	Длительность задержки (в сантисекундах), прежде чем устройство отправит анонс о получении статуса главного устройства. Время задержки по умолчанию — 0 сантисекунд. Диапазон: 0–3600 сантисекунд.

no preempt

Данная команда запрещает устройству, приоритет которого выше приоритета текущего главного виртуального маршрутизатора, становиться главным виртуальным маршрутизатором.

Формат: `no preempt [delay minimum` *`centiseconds`*`]`

Режим ввода команд: конфигурирование VRRPv3

accept-mode

Данная команда устанавливает режим, в котором главный маршрутизатор будет принимать пакеты, отправленные на виртуальные IP-адреса других владельцев (не принадлежащие ему), как свои пакеты.

Значение по умолчанию: выключено

Формат: `accept-mode`

Режим ввода команд: конфигурирование VRRPv3

no accept-mode

Команда возвращает режим приема пакетов на виртуальные IP-адреса в значение по умолчанию.

Формат: `no accept-mode`

Режим ввода команд: конфигурирование VRRPv3

priority

Эта команда задает приоритет устройства в группе VRRPv3. Значение приоритета определяет, какое устройство становится главным виртуальным маршрутизатором.

Значение по умолчанию: 100

Формат: `priority level`

Режим ввода команд: конфигурирование VRRPv3

Параметр	*Описание*
level	Приоритет устройства в группе VRRPv3. Диапазон — от 1 до 254. Значение по умолчанию: 100.

no priority

Команда устанавливает приоритет устройства в значение по умолчанию.

Формат: `priority`

Режим ввода команд: конфигурирование VRRPv3

timers advertise

Используйте эту команду, чтобы установить интервал между последовательными анонсами, отправляемыми главным виртуальным маршрутизатором в группе VRRP. Чтобы восстановить значение по умолчанию, применяется no-форма этой команды.

Анонсы, отправляемые главным виртуальным маршрутизатором, содержат интервал анонсирования, состояние и приоритет текущего главного виртуального маршрутизатора. Интервал между последовательными анонсами - это время, по истечении которого другие маршрутизаторы будут считать главный маршрутизатор недоступным. Резервные VRRP-маршрутизаторы изучают соответствующие значения из анонсов главного маршрутизатора. Значения интервалов, настроенные на главном маршрутизаторе, всегда переопределяют любые другие интервалы оценки работоспособности, определенные на резервных VRRP-маршрутизаторах.

Значение по умолчанию: 100

Формат: `timers advertise centiseconds`

Режим ввода команд: конфигурирование VRRPv3

Параметр	*Описание*
centiseconds	Интервал между последовательными анонсами главного виртуального маршрутизатора. Значение устанавливается в сантисекундах. Диапазон допустимых значений: 1–4095 сантисекунд .

no timers advertise

Данная команда устанавливает интервал между анонсами в значение по умолчанию.

Формат: `no timers advertise`

Режим ввода команд: конфигурирование VRRPv3

shutdown

Команда shutdown выключает конфигурацию VRRP-группы на данном маршрутизаторе.

Формат: `shutdown`

Режим ввода команд: конфигурирование VRRPv3

no shutdown

Выполните команду no shutdown, чтобы обновить состояние виртуального маршрутизатора после завершения конфигурирования.

Формат: `no shutdown`

Режим ввода команд: конфигурирование VRRPv3

address

Эта команда устанавливает первичный или вторичный IP-адрес устройства внутри группы VRRPv3. Чтобы удалить вторичный адрес, используйте no-форму этой команды.

Если параметр primary или secondary не указан, указанный IP-адрес будет установлен как первичный. Первичный виртуальный IPv6-адрес должен быть только адресом link-local. Если в качестве первичного IP-адреса VRRP указывается глобальный IPv6-адрес, возвращается ошибка со следующим текстом: «Error! Primary virtual IPv6 address should be a link-local address only». Удаление первичного виртуального IP-адреса (как IPv4, так и IPv6) не разрешается. Первичный виртуальный IP-адрес виртуального маршрутизатора можно только изменить. Вторичный виртуальный IP-адрес можно удалить с помощью no-формы данной команды. В силу требований протокола VRRPv3 для IPv6 для функционирования группы необходимо настроить первичный виртуальный IPv6-адрес link-local. После добавления в группу первичного link-local IPv6-адреса можно добавить глобальные адреса в качестве вторичных.

Формат: `address ip-address [primary | secondary]`

Режим ввода команд: конфигурирование VRRPv3

Параметр	***Описание***
ip-address	IPv4- или IPv6-адрес, может быть указан в одном из следующих форматов: *ipv4-address*, *ipv6-link-local-address*, *ipv6-address>/<prefix-len>.*
primary	(Необязательно.) Устанавливает первичный IP-адрес группы VRRPv3.
secondary	(Необязательно.) Устанавливает вторичный IP-адрес группы VRRPv3.

no address

Данная команда удаляет настроенный вторичный IPv4- или IPv6-адрес. Первичный адрес нельзя удалить, его можно только изменить.

Формат: `no address ip-address secondary`

Режим ввода команд: конфигурирование VRRPv3

track interface

С помощью данной команды можно настроить отслеживание интерфейса устройства в группе VRRPv3. После настройки отслеживания, система будет выводить уведомления при изменении состояния интерфейса. С помощью параметра decrement можно задать значение, на которое будет уменьшен приоритет устройства в группе VRRPv3, если интерфейс выключится.

Значение по умолчанию: включено

Формат: `track interface {unit/slot/port | vlan vlan-id} [decrement number]`

Режим ввода команд: конфигурирование VRRPv3

Параметр	***Описание***
unit/slot/port	Интерфейс для отслеживания.
vlan-id	VLAN для отслеживания.
decrement number	(Необязательно.) Шаг уменьшения приоритета VRRP для отслеживаемого объекта. Число, на которое будет уменьшен приоритет. Диапазон — 1–254.

no track interface

Команда выключает отслеживание интерфейса устройства в группе VRRPv3.

Значение по умолчанию: включено.

Формат: `track interface {unit/slot/port | vlan vlan-id} [decrement number]`

Режим ввода команд: конфигурирование VRRPv3

track ip route

С помощью данной команды можно настроить отслеживание IP-маршрута для устройства в группе VRRPv3. После настройки отслеживания, система будет выводить уведомления при изменении состояния IP-маршрута. С помощью параметра decrement можно задать значение, на которое будет уменьшен приоритет устройства в группе VRRPv3, если маршрут станет недоступным.

Значение по умолчанию: выключено

Формат: `track ip route ip-address/prefix-len [decrement number]`

Режим ввода команд: конфигурирование VRRPv3

Параметр	***Описание***
ip-address/prefix-len	Префикс и длина префикса маршрута для отслеживания.
decrement number	(Необязательно.) Шаг уменьшения приоритета VRRP для отслеживаемого объекта. Число, на которое будет уменьшен приоритет. Диапазон — 1–254.

no track ip route

Эта команда выключает отслеживание отслеживание IP-маршрута.

Формат: `no track ip route ip-address/prefix-len [decrement number]`

Режим ввода команд: конфигурирование VRRPv3

clear vrrp statistics

Данная команда удаляет статистические данные VRRP для указанного интерфейса устройства в группе VRRPv3 и соответствующего семейства IP-адресов. Если выполнить эту команду без дополнительных параметров, будет удалена глобальная статистика и выполнена перезагрузка всех виртуальных маршрутизаторов (как IPv4, так и IPv6).

Если указаны дополнительные параметры, статистика будет удалена только для виртуальных маршрутизаторов, соответствующих указанным значениям (таким как семейство IP-адресов, интерфейс и идентификатор группы виртуальных маршрутизаторов).

Формат: `clear vrrp statistics [{ipv4| ipv6} {unit/slot/port | vlan vlan-id} vr-id]`

Режим ввода команд: привилегированный

Параметр	*Описание*
ipv4	(Необязательно.) Указывает на то, что группа виртуальных маршрутизаторов принадлежит к семейству адресов IPv4.
ipv6	(Необязательно.) Указывает на то, что группа виртуальных маршрутизаторов принадлежит к семейству адресов IPv6.
unit/slot/port	(Необязательно.) Номер интерфейса, к которой принадлежит виртуальный маршрутизатор.
vlan-id	(Необязательно.) Номер VLAN, к которой принадлежит виртуальный маршрутизатор
vr-id	(Необязательно.) Номер группы виртуальных маршрутизаторов. Диапазон — от 1 до 255.

show vrrp

Используйте эту команду для вывода информации по всем активным группам VRRPv3 (без параметров), всем активным группам VRRPv3, настроенным в семействе адресов IPv4 или IPv6, или активным группам VRRPv3, настроенным в семействе адресов IPv4 или IPv6 для указанного интерфейса.

Формат: `show vrrp [{ipv4 | ipv6}] [{unit/slot/port | vlan vlan-id} vr-id]`

Режим ввода команд: привилегированный

Параметр	*Описание*
ipv4	(Необязательно.) Указывает на то, что группа виртуальных маршрутизаторов принадлежит к семейству адресов IPv4.
ipv6	(Необязательно.) Указывает на то, что группа виртуальных маршрутизаторов принадлежит к семейству адресов IPv6.
unit/slot/port	(Необязательно.) Номер интерфейса, к которой принадлежит виртуальный маршрутизатор.
vlan-id	(Необязательно.) Номер VLAN, к которой принадлежит виртуальный маршрутизатор.
vr-id	(Необязательно.) Номер группы виртуальных маршрутизаторов. Диапазон — от 1 до 255.

show vrrp brief

Данная команда выводит краткую информацию обо всех активных группах VRRPv3.

Формат: `show vrrp brief`

Режим ввода команд: привилегированный

Параметр	*Описание*
Interface	Интерфейс, на котором настроен VRRPv3.
VR	Идентификатор виртуального маршрутизатора.
A-F	Тип семейства IP-адресов (IPv4 или IPv6), к которому принадлежит данный виртуальный маршрутизатор.
Pri	Приоритет виртуального маршрутизатора.
AdvIntvl	Интервал отправки анонсов, настроенный для данного виртуального маршрутизатора.
Pre	Режим приоритетного прерывания виртуального маршрутизатора.
Acc	Режим приема данного виртуального маршрутизатора.
State	Состояние виртуального маршрутизатора в группе VRRPv3. Может иметь одно из следующих значений: Init (идет инициализация), Backup (резервный), Master (главный).
VR IP address	Виртуальный IP-адрес группы VRRPv3.

show vrrp statistics

Данная команда выводит статистические данные для указанной группы VRRPv3 или глобальную статистику. Если выполнить данную команду без параметров, будет показана глобальная статистика.

Если параметры заданы, будет показана статистика только для виртуальных маршрутизаторов, соответствующих значениям параметров (таким как семейство IP-адресов, интерфейс и идентификатор группы виртуальных маршрутизаторов).

Формат: `show vrrp statistics [{ipv4| ipv6} {unit/slot/port | vlan vlan-id} vrid]`

Режим ввода команд: привилегированный

Параметр	*Описание*
ipv4	(Необязательно.) Указывает на то, что группа виртуальных маршрутизаторов принадлежит к семейству адресов IPv4.
ipv6	(Необязательно.) Указывает на то, что группа виртуальных маршрутизаторов принадлежит к семейству адресов IPv6.
unit/slot/port	(Необязательно.) Номер интерфейса, к которой принадлежит виртуальный маршрутизатор.
vlan-id	(Необязательно.) Номер VLAN, к которой принадлежит виртуальный маршрутизатор.
vr-id	(Необязательно.) Номер группы виртуальных маршрутизаторов. Диапазон — от 1 до 255.

11.9 Команды настройки DHCP- и BOOTP-ретрансляторов

В этой части описываются команды для настройки BootP/DHCP-ретрансляторов на коммутаторе. Агент DHCP-ретранслятора работает на уровне 3 и переадресует DHCP-запросы и ответы между клиентами и серверами, которые находятся в разных физических подсетях.

bootpdhcprelay cidoptmode

Эта команда включает опцию Circuit ID для BOOTP/DHCP-ретранслятора в системе.

Значение по умолчанию: выключено

Формат: `bootpdhcprelay cidoptmode`

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

no bootpdhcprelay cidoptmode

Эта команда выключает опцию Circuit ID для BOOTP/DHCP-ретранслятора в системе.

Формат: `no bootpdhcprelay cidoptmode`

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

bootpdhcprelay maxhopcount

Данная команда настраивает максимальное разрешённое число ретрансляций BootP/DHCP-запросов. Значение hops находится в диапазоне от 1 до 16.

Значение по умолчанию: 4

Формат: `bootpdhcprelay maxhopcount` *`1-16`*

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

no bootpdhcprelay maxhopcount

Эта команда устанавливает максимальное разрешённое число ретрансляций BootP/DHCP-запросов в значение по умолчанию.

Формат: `no bootpdhcprelay maxhopcount`

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

bootpdhcprelay minwaittime

Команда настраивает минимальное время ожидания (в секундах) для BootP/DHCP-ретранслятора в системе. Если агент BOOTP-ретранслятора получает BOOTREQUEST-сообщение, он МОЖЕТ использовать значение поля seconds-since-client-began-booting в запросе как аргумент при решении, следует ли транслировать этот запрос. Значение параметра — от 0 до 100 секунд.

Значение по умолчанию: 0

Формат: `bootpdhcprelay minwaittime` *`0-100`*

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

no bootpdhcprelay minwaittime

Эта команда устанавливает минимальное время ожидания (в секундах) для BootP/DHCP-ретранслятора в системе в значение по умолчанию.

Формат: `no bootpdhcprelay minwaittime`

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

bootpdhcprelay serverip

Для настройки IP-адреса сервера для BootP/DHCP-ретранслятора в системе используется команда функционала *ip helper*. Параметр *ipaddr* — это IP-адрес сервера.

Значение по умолчанию: 0.0.0.0

Формат: `ip helper-address ipaddr dhcp`

Режим ввода команд: глобальная конфигурация

no bootpdhcprelay serverip

Эта команда устанавливает IP-адрес сервера для BootP/DHCP-ретранслятора в системе в значение по умолчанию: 0.0.0.0.

Формат: `no ip helper-address ipaddr dhcp`

Режим ввода команд: глобальная конфигурация

bootpdhcprelay enable

Для включения ретрансляции DHCP-пакетов используется команда функционала ip helper.

Значение по умолчанию: выключено

Формат: `ip helper enable`

Режим ввода команд: глобальная конфигурация

no bootpdhcprelay enable

Используйте эту команду, чтобы выключить ретрансляцию DHCP-пакетов.

Значение по умолчанию: выключено

Формат: `no ip helper enable`

Режим ввода команд: глобальная конфигурация

show bootpdhcprelay

Эта команда отображает информацию BootP/DHCP-ретранслятора для виртуального маршрутизатора. Если маршрутизатор не указан, отображается информация маршрутизатора по умолчанию.

Формат: `show bootpdhcprelay [vrf vrf-name]`

Режим ввода команд: привилегированный
пользовательский

Параметр	*Значение*
Maximum Hop Count	Максимальное разрешённое число ретрансляций BootP/DHCP запросов.
Minimum Wait Time (Seconds)	Минимальное время ожидания.
Admin Mode	Показывает, включена или выключена ретрансляция DHCP-запросов.
Circuit Id Option Mode	Режим опции DHCP Circuit ID (enabled или disabled).

show ip bootpdhcprelay

Данная команда отображает информацию BootP/DHCP-ретранслятора.

Формат: `show ip bootpdhcprelay`

Режим ввода команд: привилегированный
пользовательский

Параметр	*Значение*
Maximum Hop Count	Максимальное разрешённое число ретрансляций BootP/DHCP запросов.
Minimum Wait Time (Seconds)	Минимальное время ожидания.
Admin Mode	Показывает, включена или выключена ретрансляция DHCP-запросов.
Circuit Id Option Mode	Режим опции DHCP Circuit ID (enabled или disabled).

11.10 Команды настройки IP Helper

В этой части приводятся команды для настройки и мониторинга агента IP Helper. IP Helper выполняет ретрансляцию DHCP и других широковещательных UDP-пакетов от локального клиента к одному или нескольким серверам, которые находятся за пределами сети клиента.

Функция IP Helper представляет собой механизм, позволяющий маршрутизатору направлять определенные широковещательные UDP-пакеты по определенному IP-адресу. Это дает возможность различным приложениям обращаться к серверам в нелокальных подсетях, даже если приложение было разработано в расчете на то, что сервер всегда находится в локальной подсети. Функция также позволяет использовать для доступа к серверу широковещательные пакеты (либо с ограниченным широковещательным адресом 255.255.255.255, либо направленные на сетевой широковещательный адрес).

Администратор сети может настроить записи ретрансляции как на глобальном уровне, так и на интерфейсах маршрутизации. Каждая запись ретрансляции привязывает интерфейс входа и номер UDP-порта места назначения к одному IPv4-адресу (адресу IP Helper). Администратор сети может настроить несколько записей ретрансляции для одного интерфейса и UDP-порта, и в этом случае агент ретранслирует соответствующие пакеты на каждый адрес сервера. Конфигурация интерфейса имеет приоритет над глобальной конфигурацией. Т. е. если UDP-порт места назначения пакета соответствует любой записи на принимающем интерфейсе, пакет обрабатывается в соответствии с конфигурацией интерфейса. Если пакет не совпадает ни с одной записью на

принимающем интерфейсе, он обрабатывается в соответствии с глобальной конфигурацией IP Helper.

Администратор сети может настроить записи ретрансляции со значением discard, чтобы система отбрасывала соответствующие пакеты. Discard-записи используются для отбрасывания пакетов, полученных на определенном интерфейсе, когда в соответствии с глобальной записью ретрансляции они были бы переданы. Discard-записи ретрансляции могут быть настроены на интерфейсах, но не на глобальном уровне.

Помимо настройки адреса сервера администратор сети также настраивает, какие UDP-порты можно переадресовывать. Некоторые номера UDP-портов для удобства пользователей могут быть указаны по названию в интерфейсе пользователя, но администратор сети может настроить запись ретрансляции с любым номером UDP-порта. Администратор сети может настроить записи ретрансляции, в которых не указан UDP-порт места назначения. Агент ретрансляции при передаче считает, что эти записи соотносят пакеты с UDP-портами назначения, перечисленными в таблице ниже. Это список портов по умолчанию.

Порты по умолчанию: номера UDP-портов, указанные в виде масок

Протокол	*Номер UDP-порта*
IEN-116 Name Service	42
DNS	53
NetBIOS Name Server	137
NetBIOS Datagram Server	138
TACACS Server	49
Time Service	37
DHCP	67
Trivial File Transfer Protocol (TFTP)	69

Система ограничивает количество записей ретрансляции значением, в четыре раза превышающим максимальное количество интерфейсов маршрутизации. Администратор сети может распределять записи ретрансляции по своему усмотрению. Ограничений на количество записей ретрансляции на отдельном интерфейсе и ограничений на количество серверов для отдельной пары {interface, UDP port} не существует.

Агент ретрансляции направляет DHCP-пакеты в обоих направлениях. Он ретранслирует широковещательные пакеты от клиента к одному или нескольким DHCP-серверам, а также пакеты, которые DHCP-сервер одноадресным образом передает обратно к агенту ретрансляции, — к клиентам.

Для остальных протоколов агент ретрансляции передает только широковещательные пакеты от клиента к серверу. Предполагается, что обратные пакеты с сервера в адрес клиента передаются одноадресно и непосредственно клиенту. Поскольку в обратном направлении для других протоколов, кроме DHCP, ретрансляции нет, агент ретрансляции сохраняет IP-адрес источника из исходного пакета клиента. Агент ретрансляции использует локальный IP-адрес в качестве IP-адреса источника для передаваемых клиентских DHCP-пакетов.

Когда коммутатор получает широковещательный UDP-пакет на интерфейс маршрутизации, агент ретрансляции проверяет, настроен ли интерфейс для ретрансляции UDP-порта назначения. Если да, агент ретрансляции одноадресно передает пакет на настроенные IP-адреса сервера. В противном случае агент ретрансляции проверяет, есть ли глобальная конфигурация для UDP-порта

назначения. Если да, агент ретрансляции одноадресно передает пакет на настроенные IP-адреса сервера. В противном случае пакет не передается. Обратите внимание, что, если пакет соответствует DISCARD-записи ретрансляции на принимающем интерфейсе, такой пакет отбрасывается вне зависимости от глобальной конфигурации.

Агент ретрансляции передает пакеты, только если они соответствуют следующим условиям.

- MAC-адрес места назначения должен быть единым широковещательным адресом (FF:FF:FF:FF:FF:FF).
- IP-адрес места назначения должен быть ограниченным широковещательным адресом (255.255.255.255) или направленным широковещательный адресом для интерфейса-получателя.
- Время жизни записи (TTL) IP должно быть более 1.
- В поле протокола в IP-заголовке должен быть указан UDP (17).
- UDP-порт места назначения должен совпадать с настроенной записью ретрансляции.

clear ip helper statistics

Используйте эту команду, чтобы обнулить статистику, отображаемую командой show ip helper statistics для указанного виртуального маршрутизатора. Если маршрутизатор не указан, команда выполняется для маршрутизатора по умолчанию.

Формат: `clear ip helper statistics [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

ip helper-address (глобальная конфигурация)

Используйте эту команду, чтобы настроить ретрансляцию определенных широковещательных UDP-пакетов, получаемых любым интерфейсом. Эта команда может быть выполнена несколько раз для указания нескольких адресов серверов для заданного количества UDP-портов или же для уточнения количества UDP-портов, обрабатываемых определенным сервером.

Значение по умолчанию: адреса IP Helper не настроены.

Формат: `ip helper-address server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip| nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Режим ввода команд: глобальная конфигурация

конфигурирование виртуального маршрутизатора

Параметр	***Описание***
server-address	Одноадресный или направленный IPv4-адрес, на который отправляются ретранслируемые широковещательные UDP-пакеты. Адресом сервера не может быть IP-адрес, настроенный на каком-либо интерфейсе локального маршрутизатора
dest-udp-port	Номер UDP-порта места назначения, от 0 до 65 535.
port-name	UDP-порт места назначения может быть дополнительно определен по названию. Указан порт по номеру или по названию, значения не имеет. Имена портов распознаются следующим образом: • dhcp (порт 67) • domain (порт 53)

	• isakmp (порт 500) • mobile-ip (порт 434) • nameserver (порт 42) • netbios-dgm (порт 138) • netbios-ns (порт 137) • ntp (порт 123) • pim-auto-rp (порт 496) • rip (порт 520) • tacacs (порт 49) • tftp (порт 69) • time (порт 37) Прочие порты нужно указывать по номеру.

no ip helper-address (глобальная конфигурация)

Используйте **no**-форму команды, чтобы удалить запись IP Helper. Команда *no ip helper-address* без указанных аргументов очищает все глобальные адреса IP Helper.

Формат: `no ip helper-address [server-address [dest-udp-port | dhcp | domain | isakmp | mobile-ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs | tftp | time]`

Режим ввода команд: глобальная конфигурация

ip helper-address (конфигурирование интерфейса)

Используйте эту команду, чтобы настроить ретрансляцию определенных широковещательных UDP-пакетов, получаемых определенным интерфейсом или диапазоном интерфейсов. Эта команда может быть выполнена на интерфейсе маршрутизации несколько раз для указания нескольких адресов серверов для заданного количества портов или же для уточнения количества портов, обрабатываемых определенным сервером.

Значение по умолчанию: адреса IP Helper не настроены.

Формат: `ip helper-address {server-address | discard} [dest-udp-port | dhcp | domain | isakmp| mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip | tacacs| tftp | time]`

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
server-address	Одноадресный или направленный IPv4-адрес, на который отправляются ретранслируемые широковещательные UDP-пакеты. Адресом сервера не может быть IP-адрес, настроенный на каком-либо интерфейсе локального маршрутизатора
dest-udp-port	Номер UDP-порта места назначения, от 0 до 65 535.
port-name	UDP-порт места назначения может быть дополнительно определен по названию. Указан порт по номеру или по названию, значения не имеет. Имена портов распознаются следующим образом: • dhcp (порт 67) • domain (порт 53)

	• isakmp (порт 500) • mobile-ip (порт 434) • nameserver (порт 42) • netbios-dgm (порт 138) • netbios-ns (порт 137) • ntp (порт 123) • pim-auto-rp (порт 496) • rip (порт 520) • tacacs (порт 49) • tftp (порт 69) • time (порт 37) Прочие порты нужно указывать по номеру.

no ip helper-address (режим конфигурирования интерфейса)

Используйте данную команду, чтобы удалить запись ретрансляции на интерфейсе. Команда в no-форме без указанных аргументов очищает все адреса IP Helper на интерфейсе.

Формат: `no ip helper-address [server-address | discard ][dest-udp-port | dhcp | domain | isakmp | mobile ip | nameserver | netbios-dgm | netbios-ns | ntp | pim-auto-rp | rip| tacacs | tftp | time]`

Режим ввода команд: конфигурирование интерфейса

ip helper enable

Используйте данную команду, чтобы включить ретрансляцию UDP-пакетов. Эта команда может быть использована для временного выключения IP Helper без удаления всех его адресов. Эта команда заменяет команду *bootpdhcprelay enable*, но влияет не только на DHCP-пакеты — она также ретранслирует любые другие протоколы, для которых был настроен адрес IP Helper.

Значение по умолчанию: выключено

Формат: `ip helper enable`

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

no ip helper enable

Используйте **no**-форму команды, чтобы выключить ретрансляцию всех UDP-пакетов.

Формат: `no ip helper enable`

Режим ввода команд: глобальная конфигурация

show ip helper-address

Команда отображает конфигурацию адреса IP Helper на указанном виртуальном маршрутизаторе. Если виртуальный маршрутизатор не указан, отображается конфигурация для маршрутизатора по умолчанию. Аргумент *unit/slot/port* соответствует физическому или

виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата unit/slot/port).

Формат: `show ip helper-address [vrf` *`vrf-name`*`] [{`*`unit/slot/port`*`|vlan` *`1-4093`*`}]`

Режим ввода команд: привилегированный

Параметр	*Описание*
interface	Конфигурация ретрансляции применяется к пакетам, поступающим на этот интерфейс. Это поле устанавливается в значение any для глобальных записей IP Helper.
UDP Port	Конфигурация ретрансляции применяется для пакетов с UDP-портами назначения, совпадающими с данным портом. Записи с UDP-портами, идентифицированными как any, применяются к пакетам с целевыми UDP-портами, перечисленными в таблице 4.
Discard	При значении Yes пакеты, прибывающие на данный интерфейс с данным UDP-портом назначения, отбрасываются, а не ретранслируются. Discard-записи используются, чтобы перекрывать глобальные записи адреса IP Helper, которые в противном случае были бы применены к пакету.
Hit Count	Количество случаев, когда запись IP Helper была использована для ретрансляции или отбрасывания пакета.
Server Address	IPv4-адрес сервера, на который ретранслируются пакеты.

show ip helper statistics

Используйте эту команду, чтобы отобразить количество DHCP- и других UDP-пакетов, обрабатываемых и ретранслируемых агентом UDP-ретранслятора на указанном виртуальном маршрутизаторе. Если виртуальный маршрутизатор не указан, отображается конфигурация маршрутизатора по умолчанию.

Формат: `show ip helper statistics [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
DHCP client messages received	Число действительных сообщений, полученных от DHCP-клиента. Счетчик увеличивается только тогда, когда IP-helper глобально включен, входящий интерфейс маршрутизации доступен и пакет проходит ряд проверок пригодности, например на наличие TTL>1 и действительных адресов источника и адресата.
DHCP client messages relayed	Количество сообщений DHCP-клиента, ретранслированных на сервер. Если сообщение ретранслируется на несколько серверов, счетчик увеличивается на единицу для каждого сервера.
DHCP server messages received	Количество DHCP-ответов, полученных от DHCP-сервера. Этот счетчик включает только те сообщения, которые DHCP-сервер одноадресным образом передает агенту ретрансляции для ретрансляции клиенту.
DHCP server messages relayed	Количество сообщений DHCP-сервера, переданных клиенту.
UDP clients messages received	Количество полученных действительных UDP-пакетов. Это значение включает DHCP-сообщения и все другие ретранслируемые протоколы. Условия аналогичны тем, которые были указаны для первой статистики в этой таблице.

UDP clients messages relayed	Количество ретранслированных UDP-пакетов. Это значение включает в себя ретранслируемые DHCP-сообщения, а также все другие протоколы. Счет увеличивается с каждым сервером, к которому посылается пакет.
DHCP message hop count exceeded max	Количество полученных сообщений DHCP-клиента, в которых счетчики хопов превышали максимально допустимое значение. Максимальное количество хопов является настраиваемым значением, указанным в show bootpdhcprelay. Для каждого из таких отказов выполняется запись в журнале. Агент DHCP-ретранслятора не перенаправляет такие пакеты.
DHCP message with secs field below min	Количество полученных сообщений DHCP-клиента с полями secs меньше минимально допустимого значения. Минимально допустимое значение является настраиваемым значением и отображается в show bootpdhcprelay. Для каждого из таких отказов выполняется запись в журнале. Агент DHCP-ретранслятора не перенаправляет такие пакеты.
DHCP message with giaddr set to local address	Количество полученных сообщений DHCP-клиента, чьи адреса шлюза, giaddr, уже установлены в значение IP-адреса, настроенного как один из собственных адресов агента ретрансляции. В этом случае другое устройство пытается перехватить адрес агента ретрансляции. Агент ретрансляции не перенаправляет такие пакеты. Подробности каждого такого случая фиксируются в журнале.
Packets with expired TTL	Число пакетов, полученных с TTL, равным 0 или 1, которые в иной ситуации могли бы ретранслированы.
Packets that matched a discard entry	Число пакетов, отброшенных агентом ретрансляции, поскольку они совпали с discard-записью ретрансляции.

11.11 Команды настройки протокола OSPF

В этом разделе описаны команды, используемые для просмотра и настройки протокола Open Shortest Path First (OSPF). OSPF — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути Алгоритм Дейкстры. Протокол OSPF представляет собой протокол внутреннего шлюза (IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

Общие команды настройки OSPF

router ospf

Используйте эту команду, чтобы включить OSPF-маршрутизацию на указанном виртуальном маршрутизаторе и перейти в режим конфигурирования OSPF-маршрутизатора. Если виртуальный маршрутизатор не указан, OSPF-маршрутизация включается на маршрутизаторе по умолчанию.

Формат: `router ospf [vrf vrf-name]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
vrf vrf-name	Виртуальный маршрутизатор, на котором будет включена OSPF-маршрутизация.

enable

Эта команда устанавливает административный режим OSPF-маршрутизатора в значение по умолчанию (активен).

Значение по умолчанию: включено

Формат: `enable`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no enable

Эта команда устанавливает административный режим OSPF-маршрутизатора как неактивный.

Формат: `no enable`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

network area

Используйте эту команду, чтобы включить OSPFv2 на интерфейсе и установить для него идентификатор зоны, если IP-адрес интерфейса покрывается указанным префиксом.

Значение по умолчанию: выключено

Формат: `network` *`ip-address wildcard-mask`* `area` *`area-id`*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no network area

Используйте эту команду, чтобы выключить OSPFv2 на интерфейсе, если ранее IP-адрес интерфейса покрывался указанным префиксом.

Формат: `no network` *`ip-address wildcard-mask`* `area` *`area-id`*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

1583compatibility

Эта команда включает совместимость с OSPF 1583.

Режим совместимости 1583 включен по умолчанию. Если все OSPF-маршрутизаторы в домене маршрутизации могут работать в соответствии с RFC 2328, режим совместимости с OSPF 1583 рекомендуется выключить.

Значение по умолчанию: включено

Формат: `1583compatibility`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no 1583compatibility

Эта команда выключает совместимость с OSPF 1583.

Формат: `no 1583compatibility`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area default-cost

Эта команда настраивает стоимость по умолчанию для stub-зоны. Необходимо указать идентификатор зоны и целое значение от 1 до 16 777 215.

Формат: `area areaid default-cost 1-16777215`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area nssa

Эта команда настраивает зону с указанным идентификатором в качестве NSSA.

Формат: `area areaid nssa`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area nssa

Эта команда выключает NSSA для указанного идентификатора зоны.

Формат: `no area areaid nssa`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area nssa default-info-originate

Эта команда настраивает значение метрики и тип маршрута по умолчанию, анонсируемый в NSSA. Необязательный параметр metric определяет метрику маршрута по умолчанию и должен быть в диапазоне от 1 до 16 777 214. Если метрика не указана, значение по умолчанию — ****. Тип метрики может быть сопоставимым (nssa-external 1) или несопоставимым (nssa-external 2).

Формат: `area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area nssa default-info-originate

Команда возвращает тип маршрут по умолчанию, анонсируемый в NSSA, в значение по умолчанию.

Формат: `no area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area nssa no-redistribute

Эта команда настраивает NSSA Area Border router (ABR) так, чтобы полученные внешние маршруты не были перераспределены в NSSA.

Формат: `area areaid nssa no-redistribute`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area nssa no-redistribute

Эта команда настраивает NSSA Area Border router (ABR) так, чтобы полученные внешние маршруты перераспределялись в NSSA.

Формат: no area *areaid* nssa no-redistribute

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area nssa no-summary

Эта команда настраивает NSSA так, что суммированные LSA не анонсируются в NSSA.

Формат: *area areaid nssa no-summary*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area nssa no-summary

Эта команда настраивает NSSA так, что суммированные LSA анонсируются в NSSA.

Формат: no area *areaid* nssa no-summary
Режим ввода команд: конфигурирование OSPF-маршрутизатора

area nssa translator-role

Данная команда настраивает NSSA в роли транслятора. Значение always заставляет маршрутизатор принять роль транслятора, как только он станет пограничным маршрутизатором, а значение *candidate* вынуждает маршрутизатор участвовать в процессе выборов, когда он достигает статуса пограничного маршрутизатора.

Формат: area *areaid* nssa translator-role {always | candidate}

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area nssa translator-role

Эта команда выключает роль транслятора для NSSA из указанного идентификатора зоны.

Формат: no area *areaid* nssa translator-role {always | candidate}

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area nssa translator-stab-intv

Эта команда настраивает *stabilityinterval* для транслятора NSSA. *Stabilityinterval* — это период времени, в течение которого выбранный транслятор продолжает выполнять свои обязанности после определения факта, что его статус транслятора был замещен другим маршрутизатором.

Значение по умолчанию: 40
Формат: area *areaid* nssa translator-stab-intv *stabilityinterval*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area nssa translator-stab-intv

Эта команда вовращает *stabilityinterva*l для транслятора NSSA в значение по умолчанию.

Формат: no area *areaid* nssa translator-stab-intv *stabilityinterval*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area range

Используйте команду area range в режиме конфигурирования OSPF-маршрутизатора, чтобы настроить общий префикс, который пограничный маршрутизатор зоны будет анонсировать в определенной зоне.

Значение по умолчанию: диапазоны маршрутов не настроены; стоимости не настроены.

Формат: `area areaid range ip-address netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost cost]`

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

Параметр	*Описание*
area-id	Идентификатор зоны для зоны, сети которой будут суммироваться маршруты.
prefix netmask	Анонсируемый суммированный префикс, когда ABR вычисляет маршрут к одной или нескольким сетям в пределах этого префикса в данной зоне.
summarylink	Если указано это ключевое слово, суммированные префиксы анонсируются в LSA типа 3.
nssaexternallink	Если указано это ключевое слово, суммирование маршрутов используется при трансляции LSA типа 7 в LSA типа 5.
advertise	(Необязательный параметр.) Если указано это ключевое слово, суммированный префикс анонсируется, если указанный диапазон маршрутов в зоне активен. Это значение используется по умолчанию.
not-advertise	(Необязательный параметр.) Если указано это ключевое слово, ни суммированные, ни содержащиеся префиксы не анонсируются, если указанный диапазон маршрутов в зоне активен. Если указана опция not-advertise, любые статические значения стоимости, настроенные ранее, удаляются из конфигурации системы.
cost	(Необязательный параметр.) Если указана стоимость, OSPF устанавливает поле метрики суммированных LSA в настроенное значение вместо установки метрики на наибольшую стоимость среди сетей в диапазоне содержащихся префиксов. Статическая стоимость может быть настроена, только если настроено анонсирование суммированых маршрутов. Диапазон — от 0 до 16 777 215. Если стоимость установлена как 16 777 215 для суммирования типа 3, суммированый LSA типа 3 и содержащиеся префиксы не анонсируется. Такое поведение равносильно указанию опции **not-advertise.** Если суммирование настроено для трансляции LSA типа 7 в LSA типа 5, суммированный LSA типа 5 отправляется, если метрика установлена в значение 16 777 215; однако другие маршрутизаторы не будут рассчитывать маршруты от LSA типа 5 с этой метрикой.

no area range

no-форма команды удаляет указанный диапазон суммирования маршрутов или возвращает параметр в значение по умолчанию.

Формат: `no area areaid range prefix netmask {summarylink | nssaexternallink} [advertise | not- advertise] [cost]`

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

no-форма команды может использоваться, чтобы вернуть опцию [advertise | not-advertise] в значение по умолчанию без удаления диапазона префиксов. Удаление и восстановление может побудить OSPF временно анонсировать префиксы, содержащиеся внутри диапазона. Обратите

внимание, что использование ключевого слова advertise или not-advertise возвращает конфигурацию в значение по умолчанию.

Также **no**-форма команды может использоваться, чтобы удалить статические значения стоимости для суммированного префикса, чтобы OSPF установил стоимость в наибольшее значение среди содержащихся маршрутов.

area stub

Эта команда создает stub-зону для указанного идентификатора зоны. Stub-зона характеризуется тем, что внешние AS LSA в ней не распространяются. Удаление внешних AS LSA и сводной LSA может существенно ухудшить состояние связи для базы данных маршрутизаторов в stub-зоне.

Формат: `area areaid stub`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area stub

Эта команда удаляет stub-зону для указанного идентификатора зоны.

Формат: `no area areaid stub`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area stub no-summary

Эта команда настраивает режим stub-зоны, заданной параметром areaid, в котором запрещена рассылка LSA типа 3.

Значение по умолчанию: выключено

Формат: `area areaid stub no-summary`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area stub no-summary

Команда возвращает режим stub-зоны, заданной параметром areaid, в значение по умолчанию.

Формат: `no area areaid stub no-summary`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area virtual-link

Данная команда создает виртуальный интерфейс OSPF для указанного *areaid* и *neighbor.* Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `area areaid virtual-link neighbor`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area virtual-link

Эта команда удаляет виртуальный интерфейс OSPF для указанного интерфейса *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `no area areaid virtual-link neighbor`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area virtual-link authentication

Эта команда настраивает тип аутентификации и ключ для виртуального интерфейса OSPF, указанный как *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Значение *type* может быть *none*, *simple* или *encrypt*. Значение *key* составляется из стандартных символов. Ключ аутентификации должен содержать 8 байт или меньше, если тип аутентификации простой. Если используется тип *encrypt*, ключ может быть до 16 байт. Неаутентифицированные интерфейсы не нуждаются в ключе аутентификации. Если используется тип encrypt, должен быть указан идентификатор ключа в диапазоне от 0 до 255. Значение по умолчанию для типа аутентификации — отсутствует. Как следствие, по умолчанию не настроены ни ключ-пароль, ни идентификатор ключа.

Значение по умолчанию: отсутствует

Формат: `area areaid virtual-link neighbor authentication {none | {simple key} | {encrypt key keyid}}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area virtual-link authentication

Команда устанавливает тип аутентификации и ключ для виртуального интерфейса OSPF, указанный как *areaid* и *neighbor*, в значение по умолчанию. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `no area areaid virtual-link neighbor authentication`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area virtual-link dead-interval

Эта команда настраивает «dead interval» для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — то идентификатор маршрутизатора соседнего устройства. Диапазон значений для seconds составляет 1–65 535 секунд.

Значение по умолчанию: 40

Формат: `area areaid virtual-link neighbor dead-interval seconds`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area virtual-link dead-interval

Команда устанавливает значение «dead interval» по умолчанию для виртуального интерфейса OSPF.

Формат: `no area areaid virtual-link neighbor dead-interval`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area virtual-link hello-interval

Эта команда настраивает интервал «hello» для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Диапазон значений для seconds — от 1 до 65 535.

Значение по умолчанию: 10

Формат: `area areaid virtual-link neighbor hello-interval 1-65535`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area virtual-link hello-interval

Команда устанавливает интервал «hello» для виртуального интерфейса OSPF в значение по умолчанию.

Формат: `no area areaid virtual-link neighbor hello-interval`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area virtual-link retransmit-interval

Данная команда настраивает интервал повторной передачи для виртуального интерфейса OSPF, определяемом *areaid* или *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Диапазон значений для *seconds* — от 0 до 3600.

Значение по умолчанию: 5

Формат: `area areaid virtual-link neighbor retransmit-interval seconds`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area virtual-link retransmit-interval

Эта команда устанавливает интервал повторной передачи для виртуального интерфейса OSPF на виртуальном интерфейсе в значение по умолчанию.

Формат: `no area areaid virtual-link neighbor retransmit-interval`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

area virtual-link transmit-delay

Данная команда настраивает задержку передачи для виртуального интерфейса OSPF, определяемом *areaid* или *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Диапазон значений для seconds — от 0 до 3600 (1 час).

Значение по умолчанию: 1

Формат: `area areaid virtual-link neighbor transmit-delay seconds`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no area virtual-link transmit-delay

Эта команда устанавливает задержку передачи для виртуального интерфейса OSPF в значение по умолчанию.

Формат: `no area` *areaid* `virtual-link` *neighbor* `transmit-delay`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

auto-cost

По умолчанию OSPF рассчитывает стоимость соединения для каждого интерфейса на основании пропускной способности интерфейса. Быстрые соединения имеют более низкие метрики, что повышает их приоритет при выборе маршрута. Параметры настройки в командах *auto-cost reference-bandwidth* и *bandwidth* предоставляют возможность управлять стоимостью соединения по умолчанию. Можно настроить для OSPF пропускную способность интерфейса независимо от фактической скорости соединения. Второй параметр настройки позволяет контролировать соотношение пропускной способности интерфейса к стоимости соединения. Стоимость соединения рассчитывается как соотношение эталонной пропускной способности к пропускной способности интерфейса (*ref_bw / interface bandwidth*), при этом пропускная способность интерфейса устанавливается командой *bandwidth*. Поскольку по умолчанию эталонная пропускная способность составляет 100 Мбит/с, OSPF использует одинаковую стоимость соединения по умолчанию для всех интерфейсов, пропускная способность которых равна или более 100 Мбит/с. Команда *auto-cost* позволяет изменить эталонную пропускную способность, указав ее значение в Мбит/с. Значение эталонной пропускной способности может быть от 1 до 4 294 967 Мбит/с.

Значение по умолчанию: 100 Мбит/с

Формат: `auto-cost reference-bandwidth` *1-4294967*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no auto-cost reference-bandwidth

Используйте эту команду, чтобы установить эталонную пропускную способность в значение по умолчанию.

Формат: `no auto-cost reference-bandwidth`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

capability opaque

Используйте эту команду для включения на маршрутизаторе функционала Opaque Capability. Информация, содержащаяся в Opaque LSA, может быть использована непосредственно протоколом OSPF или косвенно приложением, которое будет распространять информацию по всему домену OSPF. Система поддерживает хранение и распространение Opaque LSA различных диапазонов действия. Значение по умолчанию enabled обозначает, что по умолчанию OSPF будет переадресовывать Opaque LSA.

Значение по умолчанию: включено

Формат: `capability opaque`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no capability opaque

Используйте эту команду для выключения на маршрутизаторе функционала Opaque Capability.

Формат: `no capability opaque`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

clear ip ospf

Используйте данную команду, чтобы выключить и перезапустить OSPF для указанного виртуального маршрутизатора. Если виртуальный маршрутизатор не указан, OSPF выключается и перезапускается на маршрутизаторе по умолчанию.

Формат: `clear ip ospf [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

clear ip ospf configuration

Используйте данную команду, чтобы сбросить конфигурацию OSPF для указанного виртуального маршрутизатора до заводских настроек. Если виртуальный маршрутизатор не указан, сброс выполняется на маршрутизаторе по умолчанию.

Формат: `clear ip ospf configuration [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

clear ip ospf counters

Данная команда позволяет сбросить глобальную статистику и статистику интерфейса для указанного виртуального маршрутизатора. Если виртуальный маршрутизатор не указан, сброс статистики выполняется для маршрутизатора по умолчанию.

Формат: `clear ip ospf counters`

Режим ввода команд: привилегированный

clear ip ospf neighbor

Используйте эту команду, чтобы сбросить настройки смежности со всеми OSPF-соседями для указанного виртуального маршрутизатора. На каждый соседний интерфейс отправляется одностороннее сообщение «Hello». После этого настройки смежности можно переустановить. Если маршрутизатор не указан, смежность со всеми OSPF-соседями сбрасывается для маршрутизатора по умолчанию. Чтобы сбросить смежность с определенным маршрутизатором, необходимо указать идентификатор соседнего маршрутизатора, используя необязательный параметр [*neighbor-id*].

Формат: `clear ip ospf neighbor [ vrf` *`vrf-name`*`] [`*`neighbor-id`*`]`

Режим ввода команд: привилегированный

clear ip ospf neighbor interface

Чтобы сбросить настройки смежности со всеми соседями для указанного интерфейса, используйте необязательный параметр [unit/slot/port]. Чтобы сбросить настройки смежности с определенным идентификатором маршрутизатора на указанном интерфейсе, используйте необязательный параметр [neighbor-id].

Формат: `clear ip ospf neighbor interface` *`[unit/slot/port] [`*`neighbor-id`*`]`*

Режим ввода команд: привилегированный

clear ip ospf redistribution

Команда позволяет очистить все самостоятельно сгенерированные внешние LSA для указанного виртуального маршрутизатора. Если маршрутизатор не указан, команда выполняется для маршрутизатора по умолчанию. По мере необходимости можно повторно применить настройки перераспределения и создать префиксы.

Формат: `clear ip ospf redistribution [vrf vrf-name]`

Режим ввода команд: привилегированный

default-information originate

Эта команда используется, чтобы управлять анонсами маршрутов по умолчанию.

Значение по умолчанию: метрика — не определена;
тип — 2

Формат: `default-information originate [always] [metric 0-16777214] [metric-type {1 | 2}]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no default-information originate

Эта команда используется, чтобы управлять анонсами маршрутов по умолчанию.

Формат: `no default-information originate [metric] [metric-type]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

default-metric

Данная команда используется, чтобы установить значения для метрик по умолчанию анонсируемых маршрутов.

Формат: `default-metric 1-16777214`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no default-metric

Данная команда используется, чтобы установить значения по умолчанию для метрик по умолчанию анонсируемых маршрутов.

Формат: `no default-metric`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

distance ospf

Эта команда устанавливает значение приоритета OSPF-маршрута на маршрутизаторе. При определении оптимального маршрута предпочтение отдается более низким значениям приоритета маршрута. Тип OSPF-маршрута может обозначаться как *intra, inter* или *external*. Всем маршрутам типа *external* присваивается одинаковое значение приоритета. Диапазон значений для *preference* — от 1 до 255.

Значение по умолчанию: 110

Формат: `distance ospf {intra-area 1-255 | inter-area 1-255 | external 1-255}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no distance ospf

Эта команда устанавливает приоритет OSPF-маршрута на маршрутизаторе в значение по умолчанию. Тип OSPF-маршрута может обозначаться как *intra*, *inter* или *external*. Всем маршрутам типа external присваивается одинаковое значение приоритета.

Формат: `no distance ospf {intra-area | inter-area | external}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

distribute-list out

Используйте эту команду, чтобы указать список контроля доступа для фильтрации маршрутов, принятых от указанного протокола источника.

Формат: `distribute-list 1-199 out {rip | bgp | static | connected}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no distribute-list out

Используйте эту команду, чтобы удалить список контроля доступа для фильтрации маршрутов, принятых от указанного протокола источника.

Формат: `no distribute-list 1-199 out {rip | bgp | static | connected}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

exit-overflow-interval

Данная команда настраивает интервал выхода из режима переполнения для OSPF. Он обозначает время в секундах после входа в состояние переполнения, в течение которого маршрутизатор выжидает и не пытается выходить из этого состояния. Это позволяет маршрутизатору снова создать AS-external-LSA не по умолчанию. Если интервал установлен как 0, маршрутизатор не пытается самостоятельно выходить из состояния переполнения и требует перезапуска. Диапазон значений для seconds — от 0 до 2 147 483 647 секунд.

Значение по умолчанию: 0

Формат: `exit-overflow-interval seconds`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no exit-overflow-interval

Эта команда устанавливает интервал выхода из режима переполнения для OSPF в значение по умолчанию.

Формат: `no exit-overflow-interval`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

external-lsdb-limit

Эта команда настраивает ограничение внешних LSDB для OSPF. Если значение установлено как -1, ограничений не существует. Если количество AS-external-LSA не по умолчанию в базе данных состояния соединения маршрутизатора достигает ограничения LSDB, маршрутизатор входит в состояние переполнения. Маршрутизатор никогда не хранит в базе данных AS-external-LSA, превышающие по количеству установленное LSDB-ограничение. Ограничение для внешних LSDB должно быть установлено на одном уровне на всех маршрутизаторах, подключенных к OSPF-магистрали и/или любой обычной OSPF-зоне. Диапазон значений для ограничения — от -1 до 2 147 483 647.

Значение по умолчанию: -1

Формат: `external-lsdb-limit` *`limit`*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no external-lsdb-limit

Эта команда устанавливает ограничение внешних LSDB для OSPF в значение по умолчанию.

Формат: `no external-lsdb-limit`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

log-adjacency-changes

Чтобы включить ведение журнала изменений состояния OSPFv2-соседей, используйте команду log-adjacency-changes в режиме настройки OSPF-маршрутизатора. Изменения состояния регистрируются с уровнем опасности INFORMATIONAL.

Значение по умолчанию: изменения состояния смежности регистрируются, но без детализации.

Формат: `log-adjacency-changes [detail]`
Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

Параметр	***Описание***
detail	(Необязательный параметр.) Когда указано это ключевое слово, регистрируются все изменения состояния смежности. В противном случае OSPF записывает только переходы в FULL-состояние и обратный переход.

no log-adjacency-changes

Используйте no-форму команды, чтобы выключить ведение журнала изменений.

Формат: `no log-adjacency-changes [detail]`

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

prefix-suppression

Эта команда подавляет в анонсах от OSPFv2-маршрутизатора анонсирование всех IPv4-префиксов, кроме префиксов, связанных с вторичными IPv4-адресами, loopback и пассивными интерфейсами.

Чтобы включить в число подавляемых анонсы, связанные с loopback или пассивным интерфейсом, используйте команду ip ospf prefix-suppression в режиме конфигурирования интерфейса. Префиксы, связанные с вторичными IPv4-адресами, не могут быть подавлены.

Значение по умолчанию: подавление префиксов выключено.

Формат: `prefix-suppression`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no prefix-suppression

Эта команда выключает подавление префиксов. Все префиксы анонсируются свободно.

Формат: `no prefix-suppression`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

prefix-suppression

Эта команда подавляет в анонсах от OSPFv3-маршрутизатора анонсирование всех IPv6-префиксов, кроме префиксов, связанных с вторичными IPv6-адресами, loopback и пассивными интерфейсами.

Чтобы включить в число подавляемых анонсы, связанные с loopback или пассивным интерфейсом, используйте команду ipv ospf prefix-suppression в режиме конфигурирования интерфейса. Префиксы, связанные с вторичными IPv6-адресами, не могут быть подавлены.

Значение по умолчанию: подавление префиксов выключено.

Формат: `prefix-suppression`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no prefix-suppression

Эта команда выключает подавление префиксов. Все префиксы анонсируются свободно.

Формат: `no prefix-suppression`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

router-id

Эта команда устанавливает уникальный идентификатор OSPF-маршрутизатора.

Формат: `router-id` *`ipaddress`*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

redistribute

Эта команда настраивает OSPF-протокол на разрешение перераспределения маршрутов от указанных передающих протоколов/маршрутизаторов.

Значение по умолчанию: метрика — не определена;
тип — 2;
тег — 0.

Формат: `redistribute {rip | bgp | static | connected} [metric 0-16777214] [metric-type {1 | 2}] [tag 0-4294967295] [subnets]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no redistribute

Эта команда настраивает OSPF-протокол на запрет перераспределения маршрутов от указанных передающих протоколов/маршрутизаторов.

Формат: `no redistribute {rip | bgp | static | connected} [metric] [metric-type] [tag] [subnets]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

maximum-paths

Эта команда устанавливает максимальное количество путей для заданного места назначения, о которых OSPF может сообщать.

Значение по умолчанию: 4

Формат: `maximum-paths maxpaths`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no maximum-paths

Данная команда устанавливает максимальное количество путей для заданного места назначения, о которых OSPF может сообщать, в значение по умолчанию.

Формат: `no maximum-paths`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

passive-interface default

Используйте эту команду, чтобы включить глобальный пассивный режим по умолчанию для всех интерфейсов. Команда перезаписывает любой уровень пассивного режима интерфейса. OSPF не будет формировать смежности через пассивные интерфейсы.

Значение по умолчанию: выключено

Формат: `passive-interface default`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no passive-interface default

Эта команда выключает глобальный пассивный режим по умолчанию для всех интерфейсов. Любой интерфейс, ранее настроенный на пассивный режим, по исполнению команды выходит из него.

Формат: `no passive-interface default`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

passive-interface

Используйте эту команду, чтобы настроить интерфейс как пассивный. Команда перезаписывает глобальный пассивный режим, который уже действует на интерфейсе. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово *vlan* используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Значение по умолчанию: выключено

Формат: `passive-interface {`*`unit/slot/port`*`|vlan `*`1-4094`*`}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no passive-interface

Используйте эту команду, чтобы настроить интерфейс как непассивный. Команда перезаписывает глобальный пассивный режим, который уже действует на интерфейсе.

Формат: `no passive-interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

timers pacing flood

Используйте команду *timers pacing flood* в режиме глобального конфигурирования OSPFv2-маршрутизатора, чтобы настроить скорость, с которой OSPFv2 отправляет пакеты LS Update. Протокол OSPF распространяет маршрутную информацию в виде анонсов Link State Advertisements (LSA), которые содержатся в пакетах Link State Update (LS Update). Чтобы уменьшить вероятность отправки соседу больше пакетов, чем он может принять, OSPF ограничивает скорость передачи пакетов LS Update. По умолчанию OSPF отправляет до 30 обновлений в секунду на каждом интерфейсе (1 / интервал шага). Используйте данную команду, чтобы настроить скорость отправки пакетов.

Значение по умолчанию: 33 миллисекунды

Формат: `timers pacing flood `*`milliseconds`*

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

Параметр	***Описание***
milliseconds	Среднее время между отправкой пакетов LS Update. Диапазон — от 5 до 100 мс. По умолчанию — 33 мс.

no timers pacing flood

Используйте команду *no timers pacing flood*, чтобы вернуть интервал отправки LSA в значение по умолчанию.

Формат: `no timers pacing flood`

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

timers pacing lsa-group

Для того, чтобы отрегулировать, как OSPF группирует LSA для периодического обновления, используйте команду *timers pacing lsa-group* в режиме конфигурирования OSPFv2-маршрутизатора. OSPF обновляет автоматически сгенерированные LSA приблизительно раз в 30 минут. Когда OSPF обновляет LSA, он учитывает все автоматически сгенерированные LSA, период существования

которых составляет от 1800 до 1800 плюс размер интервала группы. Группировка LSA для обновления позволяет OSPF объединять обновленные LSA в минимальное количество пакетов LS Update. Сокращение количества пакетов LS Update делает распространение LSA более эффективным.

Если OSPF производит новый или измененный LSA, он выбирает для него случайную задержку обновления. По истечении задержки обновления OSPF обновляет LSA. Выбирая случайную задержку обновления, OSPF избегает обновления большого количества LSA за один раз, даже если таковые возникли в одно время.

Значение по умолчанию: 60 секунд

Формат: `timers pacing lsa-group` *`seconds`*

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

Параметр	***Описание***
seconds	Продолжительность окна, за которое обновляются LSA. Диапазон — от 10 до 1800 секунд.

timers spf

Используйте данную команду, чтобы настроить время задержки и удержания SPF. Действительный диапазон для обоих параметров — от 0 до 65 535 секунд.

Значение по умолчанию: задержка — 5
удержание — 10

Формат: `timers spf` *`delay-time hold-time`*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

trapflags

Используйте данную команду, чтобы включить индивидуальные OSPF-трапы, одновременно включить группу флагов для трапов или одновременно включить все флаги для трапов. Различные группы флагов для трапов и отдельные флаги для трапов каждой группы перечислены в таблице ниже.

Группа	***Флаги***
errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow
retransmit	• packets • virt-packets
state-change	• if-state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

- Чтобы включить отдельный флаг, введите group name и затем выбранный флаг.
- Чтобы включить все флаги группы, введите имя группы и ключевое слово all.
- Чтобы включить все флаги, введите команду *trapflags all*.

Значение по умолчанию: выключено

Формат: `trapflags {all | errors {all | authentication-failure | bad-packet | config-error | virt- authentication-failure | virt-bad-packet | virt-config-error} |lsa {all | lsa-maxage | lsa-originate} |overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} |state-change {all | if-state-change | neighbor-state-change | vir-tif-state-change | virtneighbor-state-change}
}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no trapflags

Команда устанавливает настройки OSPF-трапов и соответствующих флагов в значение по умолчанию.

- Чтобы выключить отдельный флаг, введите group name и затем выбранный флаг.
- Чтобы выключить все флаги группы, введите имя группы и ключевое слово all.
- Чтобы выключить все флаги, введите команду с указанием trapflags all.

Формат: `no trapflags { all |errors {all | authentication-failure | bad-packet | config-error | virt- authentication-failure | virt-bad-packet | virt-config-error} |lsa {all | lsa-maxage | lsa-originate} |overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} |state-change {all | if-state-change | neighbor-state-change | virtif-state- change | virtneighbor-state-change}
}`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

Команды настройки протокола на OSPF-интерфейсе

ip ospf area

Используйте эту команду, чтобы включить OSPFv2 и установить идентификатор зоны интерфейса или диапазона интерфейсов. Параметр *area-id* — это IP-адрес, представленный 4-значным десятичным числом с точкой или десятичным значением в диапазоне от 0 до 4294967295. Эта команда замещает выполнение команды *network area*. Она также может использоваться, чтобы настроить на интерфейсе анонсирование вторичных адресов в адрес OSPFv2-домена.

Значение по умолчанию: выключено

Формат: `ip ospf area area-id [secondaries none]`

Режим ввода команд: конфигурирование интерфейса

no ip ospf area

Команда выключает OSPF на интерфейсе.

Формат: `no ip ospf area [secondaries none]`

Режим ввода команд: конфигурирование интерфейса

bandwidth

По умолчанию OSPF вычисляет стоимость соединения интерфейса как соотношение эталонной пропускной способности к пропускной способности интерфейса. Эталонная пропускная способность устанавливается с помощью команды *auto-cost*. В целях расчета стоимости соединения OSPF используйте команду bandwidth для определения пропускной способности интерфейса. Пропускная способность указывается в килобитах в секунду. Если значение пропускной способности не настроено, пропускная способность устанавливается в значение фактической пропускной способности интерфейса для интерфейсов маршрутизации на основе портов и на 10 Мбит/с для виртуальных интерфейсов маршрутизации. Команда не влияет на фактическую скорость интерфейса. Эту команду можно использовать, чтобы настроить один или несколько интерфейсов.

Значение по умолчанию: фактическая пропускная способность интерфейса

Формат: `bandwidth` *`1-10000000`*

Режим ввода команд: конфигурирование интерфейса

no bandwidth

Используйте данную команду, чтобы установить пропускную способность интерфейса в значение по умолчанию.

Формат: `no bandwidth`

Режим ввода команд: конфигурирование интерфейса

ip ospf authentication

Эта команда устанавливает тип OSPF-аутентификации и ключ для указанного интерфейса или диапазона интерфейсов. Значение *type* может быть определено как *none*, *simple* или *encrypt*. Значение *key* составляется из стандартных символов. Ключ аутентификации должен содержать 8 байт или меньше, если тип аутентификации простой. Если используется тип encrypt, ключ может быть до 16 байт. Если используется тип *encrypt*, должен быть указан *keyid* в диапазоне от 0 до 255. Не идентифицированные интерфейсы не нуждаются в ключе аутентификации и идентификаторе ключа. Значение по умолчанию для типа аутентификации отсутствует.

Формат: `ip ospf authentication {none | {simple` *`key`*`} | {encrypt` *`key keyid`*`}}`

Режим ввода команд: конфигурирование интерфейса

no ip ospf authentication

Эта команда устанавливает тип аутентификации OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ip ospf authentication`

Режим ввода команд: конфигурирование интерфейса

ip ospf cost

Данная команда настраивает стоимость на OSPF-интерфейсе или диапазоне интерфейсов. Параметр *cost* имеет диапазон от 1 до 65 535.

Значение по умолчанию: 10

Формат: `ip ospf cost` *1-65535*

Режим ввода команд: конфигурирование интерфейса

no ip ospf cost

Эта команда устанавливает стоимость на OSPF-интерфейсе в значение по умолчанию.

Формат: `no ip ospf cost`

Режим ввода команд: конфигурирование интерфейса

ip ospf database-filter all out

Используйте команду *ip ospf database-filter all out* в режиме настройки интерфейса, чтобы выключить на интерфейсе распространение OSPFv2 LSA.

Значение по умолчанию: выключено

Формат: `ip ospf database-filter all out`

Режим ввода команд: конфигурирование интерфейса

no ip ospf database-filter all out

Используйте команду no ip ospf database-filter all out в режиме настройки интерфейса, чтобы включить на интерфейсе распространение OSPFv2 LSA.

Значение по умолчанию: выключено

Формат: `ip ospf database-filter all out`

Режим ввода команд: конфигурирование интерфейса

ip ospf dead-interval

Эта команда настраивает Dead-interval OSPF для указанного интерфейса или диапазона интерфейсов. Значение для seconds (диапазон: 1–65535) — это действительное положительное целое число, время в секундах, в течение которого пакеты Hello не отправляются с маршрутизатора до того момента, пока соседние маршрутизаторы не объявляют, что маршрутизатор выключен. Значение Dead-interval должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Это значение должно быть кратно Hello-интервалу (т. е. 4). Диапазон допустимых значений в секундах — от 1 до 65535.

Значение по умолчанию: 40

Формат: `ip ospf dead-interval` *seconds*

Режим ввода команд: конфигурирование интерфейса

no ip ospf dead-interval

Эта команда устанавливает «dead-interval» OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ip ospf dead-interval`

Режим ввода команд: конфигурирование интерфейса

ip ospf hello-interval

Данная команда устанавливает Hello-интервал OSPF для указанного интерфейса или диапазона интерфейсов. Значение для seconds — это действительное положительное целое число, время в секундах. Значение Hello-интервала должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Диапазон допустимых значений — от 1 до 65535.

Значение по умолчанию: 10

Формат: `ip ospf hello-interval` *`seconds`*

Режим ввода команд: конфигурирование интерфейса

no ip ospf hello-interval

Эта команда устанавливает Hello-интервал OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ip ospf hello-interval`

Режим ввода команд: конфигурирование интерфейса

ip ospf network

Команда настраивает OSPF рассматривать интерфейс или диапазон интерфейсов как PtP соединение, а не широковещательный интерфейс. Опция broadcast устанавливает широковещательный тип сети OSPF. Опция point-to-point устанавливает PtP тип сети OSPF. OSPF по умолчанию рассматривает интерфейсы как широковещательные (интерфейсы loopback имеют специальный тип loopback, который не может быть изменен). Если в сети присутствуют только два маршрутизатора, OSPF может работать более эффективно путем обозначения сети как PtP. Для таких сетей OSPF не избирает назначенный маршрутизатор и не генерирует LSA-анонсы. Обе конечные точки соединения должны быть настроены на работу в PtP режиме.

Значение по умолчанию: broadcast

Формат: `ip ospf network {broadcast | point-to-point}`

Режим ввода команд: конфигурирование интерфейса

no ip ospf network

Используйте эту команду, чтобы вернуть тип OSPF-сети в значение по умолчанию.

Формат: `no ip ospf network`
Режим ввода команд: конфигурирование интерфейса

ip ospf prefix-suppression

Эта команда подавляет анонсирование всех IPv4-префиксов, связанных с интерфейсом, кроме префиксов, связанных с вторичными IPv4-адресами. Данная команда перекрывает глобальную конфигурацию. Если данная конфигурация не определена, применяется конфигурация глобального подавления префиксов.

Подавление префиксов может быть выключено на уровне интерфейса с использованием опции *disable*. Опция *disable* полезна тем, что выделяет отдельные интерфейсы из выполнения подавления префиксов, если функция включена глобально.

Следует отметить, что функция disable не эквивалентна отсутствию настроек подавления префиксов на отдельных интерфейсах. Если подавление префиксов не настроено на уровне интерфейса, для IPv4-префиксов, связанных с интерфейсом, применяется глобальная конфигурация подавления префиксов.

Значение по умолчанию: подавление префиксов не настроено.

Формат: `ip ospf prefix-suppression [disable]`

Режим ввода команд: конфигурирование интерфейса

no ip ospf prefix-suppression

Данная команда удаляет настройки подавления префиксов на уровне интерфейса. После выполнения команды *no ip ospf prefix-suppression* к интерфейсу применяется глобальная конфигурация подавления префиксов. Отсутствие настройки команды не эквивалентно выключению подавления префиксов на уровне интерфейса.

Формат: `no ip ospf prefix-suppression`

Режим ввода команд: конфигурирование интерфейса

ip ospf priority

Эта команда устанавливает OSPF-приоритет для указанного интерфейса маршрутизатора или диапазона интерфейсов. Приоритет интерфейса — это целое число от 0 до 255. Нулевое значение обозначает, что маршрутизатор не подходит на роль назначенного маршрутизатора в данной сети.

Значение по умолчанию: 1, наивысший приоритет маршрутизатора.

Формат: `ip ospf priority` *`0-255`*

Режим ввода команд: конфигурирование интерфейса

no ip ospf priority

Эта команда устанавливает OSPF-приоритет для указанного интерфейса маршрутизатора в значение по умолчанию.

Формат: `no ip ospf priority`

Режим ввода команд: конфигурирование интерфейса

ip ospf retransmit-interval

Эта команда настраивает интервал повторной передачи OSPF для указанного интерфейса или диапазона интерфейсов. Интервал повторной передачи указывается в секундах. Значение seconds — это число секунд между повторной отправкой LSA для соседей, принадлежащих интерфейсу данного маршрутизатора. Это значение также используется при повторной передаче описания базы данных и пакетов с запросами состояния канала. Диапазон — от 0 до 3600 секунд (1 час).

Значение по умолчанию: 5

Формат: `ip ospf retransmit-interval` *`0-3600`*

Режим ввода команд: конфигурирование интерфейса

no ip ospf retransmit-interval

Команда устанавливает интервал повторной передачи OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ip ospf retransmit-interval`

Режим ввода команд: конфигурирование интерфейса

ip ospf transmit-delay

Данная команда устанавливает задержку передачи OSPF для указанного интерфейса или диапазона интерфейсов. Задержка передачи указывается в секундах. Кроме того, она устанавливает ожидаемое количество секунд, которое требуется для передачи пакета с обновлением состояния соединения через этот интерфейс. Интервал действительных значений для seconds — от 1 до 3600 (1 час).

Значение по умолчанию: 1

Формат: `ip ospf transmit-delay` *`1-3600`*

Режим ввода команд: конфигурирование интерфейса

no ip ospf transmit-delay

Команда устанавливает задержку передачи OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ip ospf transmit-delay`

Режим ввода команд: конфигурирование интерфейса

ip ospf mtu-ignore

Эта команда выключает OSPF-обнаружение несоответствия MTU на интерфейсе или диапазоне интерфейсов. Пакеты OSPF Database Description задают размер наибольшего IP-пакета, который может быть отправлен на интерфейсе без фрагментации. Если маршрутизатор получает пакет Database Description, он проверяет значение MTU, анонсируемое соседом. По умолчанию, если MTU больше, чем маршрутизатор может принять, пакет Database Description отбрасывается и OSPF-соседство не устанавливается.

Значение по умолчанию: включено

Формат: `ip ospf mtu-ignore`

Режим ввода команд: конфигурирование интерфейса

no ip ospf mtu-ignore

Эта команда включает OSPF-обнаружение несоответствия MTU.

Формат: `no ip ospf mtu-ignore`

Режим ввода команд: конфигурирование интерфейса

Команды настройки функции IP Event Dampening

dampening

Используйте данную команду, чтобы включить IP Event Dampening на интерфейсе маршрутизации.

Формат: `dampening [half-life period] [reuse-threshold suppress-threshold max-suppress-time[restart restart-penalty]]`

Режим ввода команд: конфигурирование интерфейса

Параметр	*Описание*
Half-life period	Время в секундах, за которое штраф сокращается вдвое. Настраиваемый диапазон составляет 1–30 секунд. Значение по умолчанию — 5 секунд.
Reuse Threshold	Значение штрафа, за который восстанавливается смягченный интерфейс. Настраиваемый диапазон составляет от 1 до 20 000. Значение по умолчанию — 1000.
Suppress Threshold	Значение штрафа, за который на интерфейсе включается функция смягчения. Настраиваемый диапазон составляет от 1 до 20 000. Значение по умолчанию — 2000.
Max Suppress Time	Максимальное количество времени (в секундах), которое интерфейс может находится в состоянии подавления после окончания нестабильного поведения. Настраиваемый диапазон составляет 1–255 секунд. Значение по умолчанию в 4 раза больше периода сокращения штрафа. Если значение установлено по умолчанию, максимальное время сдерживания по умолчанию составит 20 секунд.
Restart Penalty	Штраф, применяемый к интерфейсу после перезагрузки устройства. Настраиваемый диапазон составляет от 1 до 20 000. Значение по умолчанию — 2000.

no dampening

Эта команда выключает функцию IP Event Dampening на интерфейсе маршрутизации.

Формат: `no dampening`

Режим ввода команд: конфигурирование интерфейса

show dampening interface

Эта команда показывает количество интерфейсов, настроенных с функцией IP Event Dampening, и количество подавляемых интерфейсов.

Формат: `show dampening interface`

Режим ввода команд: привилегированный

show interface dampening

Эта команда отображает состояние и настроенные параметры интерфейсов, на которых активна функция IP Event Dampening.

Формат: `show interface dampening`

Режим ввода команд: привилегированный

Параметр	*Описание*
Flaps	Количество случаев, когда состояние соединения интерфейса менялось с UP на DOWN.
Penalty	Накопленный штраф.
Supp	Обозначает, подавляется ли интерфейс.
ReuseTm	Период в секундах, по истечении которого интерфейсу разрешено снова включиться.
HalfL	Настроенный период сокращения штрафа.
ReuseV	Настроенный порог повторного использования.
SuppV	Настроенный порог подавления.
MaxSTm	Настроенное максимальное время подавления.
MaxP	Максимальный возможный штраф.
Restart	Настроенный штраф перезагрузки.

1. **Команда clear counters устанавливает счетчик ошибок неустойчивости соединения на ноль.**
2. **Команда конфигурирования интерфейса no shutdown устанавливает значение режима подавления в False.**
3. **Любое изменение в конфигурации сервиса смягчения сбрасывает текущий штраф, время повторного использования и статус подавления в значения по умолчанию, т. е. 0, 0 и FALSE соответственно.**

Команды настройки OSPF Graceful Restart

Использование функционала Graceful Restart позволяет производить «щадящую перезагрузку» маршрутизаторов, при которой смежные маршрутизаторы продолжают пересылать IPv4 пакеты с использование OSPF-маршрутов анонсированных перезагружаемым коммутатором.

Смежный маршрутизатор входит в режим помощника, если он получает от перезагружающегося маршрутизатора LSA-graceful, обозначающий его намерение выполнить щадящую перезагрузку. В режиме помощника коммутатор продолжает отправлять анонсы остальной сети, что они имеют полную смежность с перезагружающимся маршрутизатором, тем самым избегая перестроения OSPF-топологии и потенциального переполнения LSA и SPF (которые определяют маршруты OSPF). Соседи-помощники продолжают направлять пакеты через перезагружающийся маршрутизатор. Перезагружающийся маршрутизатор заново узнает топологию сети от своих соседей-помощников.

Функция Graceful Restart может быть включена для плановых, внеплановых или для обоих типов перезагрузки. Плановая перезагрузка выполняется оператором через управляющую команду initiate failover.

nsf

Используйте эту команду, чтобы включить функцию OSPF Graceful Restart на интерфейсе.

Значение по умолчанию: выключено

Формат: `nsf [ietf] [planned-only]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

Параметр	*Описание*
ietf	Это ключевое слово принимается, но не является обязательным.
planned-only	Это необязательное ключевое слово обозначает, что OSPF должен выполнить щадящую перезагрузку, только если перезагрузка плановая (например, если перезагрузка — результат команды initiate failover).

no nsf

Используйте эту команду, чтобы выключить Graceful Restart для любых перезагрузок.

Формат: `no nsf`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

nsf restart-interval

Команда настраивает интервал в секундах, в течение которого перезагружающийся маршрутизатор будет просить своих соседей ожидать, прежде чем входить в режим помощника. Этот интервал называют «щадящим периодом». Перезагружающийся маршрутизатор включает щадящий период в свои анонсы LSA. Для плановых перезагрузок (используя команду initiate failover) щадящие LSA отсылаются до перезагрузки блока управления, а в случае внеплановых — отсылаются после начала перезагрузки.

Щадящий период должен быть достаточно долгим, чтобы позволить перезагружающемуся маршрутизатору восстановить все свои смежности и выполнить полный обмен базы данных с каждым из соседей.

Значение по умолчанию: 120 секунд

Формат: `nsf [ietf] restart-interval` *`1-1800`*

Режим ввода команд: конфигурирование OSPF-маршрутизатора

Параметр	*Описание*
ietf	Это ключевое слово принимается, но не является обязательным.
seconds	Количество секунд, которое перезагружающийся маршрутизатор запрашивает на ожидание у своих соседей перед тем, как они войдут в режим помощника. Диапазон — от 1 до 1800 секунд.

no nsfrestart-interval

Используйте эту команду, чтобы вернуть значение щадящего периода в значение по умолчанию.

Формат: `no [ietf] nsf restart-interval`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

nsf helper

Команда включает функцию соседей-помощников для протокола OSPF. Данную функцию можно включить для плановых, внеплановых или обоих типов перезагрузок.

Значение по умолчанию: OSPF может выступать как сосед-помощник для плановых и внеплановых перезагрузок

Формат: `nsf helper [planned-only]`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

Параметр	*Описание*
planned-only	Это необязательное ключевое слово указывает, что OSPF следует назначать помощников только маршрутизатору, выполняющему плановую перезагрузку.

no nsf helper

Используйте эту команду, чтобы выключить функцию соседей-помощников для протокола OSPF.

Формат: `no nsf helper`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

nsf ietf helper disable

Используйте эту команду, чтобы выключить функцию соседей-помощников для протокола OSPF.

Команды no nsf helper и nsf ietf helper disable функционально равнозначны. Команда nsf ietf helper disable поддерживается исключительно для совместимости с CLI других вариантов программного обеспечения сети.

Формат: `nsf ietf helper disable`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

nsf helper strict-lsa-checking

Используйте данную команду, чтобы потребовать от соседа-помощника OSPF выходить из режима помощника при изменении топологии.

Значение по умолчанию: включено

Формат: `nsf [ietf] helper strict-lsa-checking`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

Параметр	*Описание*
ietf	Это ключевое слово принимается, но не является обязательным.

no nsf [ietf] helper strict-lsa-checking

Данная команда позволяет OSPF продолжать использовать соседа-помощника, несмотря на изменение топологии.

Значение по умолчанию: включено

Формат: `nsf [ietf] helper strict-lsa-checking`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

Команды настройки функции OSPFv2 Stub Router

max-metric router-lsa

Чтобы настроить OSPF-маршрутизатор на вход в режим Stub Router, используйте данную команду в режиме глобальной конфигурации OSPF-маршрутизатора. Когда OSPF находится в режиме Stub Router, как это определено в RFC 3137, протокол OSPF устанавливает метрику для nonstub маршрутов в анонсах LSA своего маршрутизатора как LsInfinity. Из-за большой длины пути через Stub Router и соседние маршрутизаторы предпочитают любой альтернативный путь. Это позволяет полностью перенаправить транзитный трафик не на Stub Router, если доступны альтернативные маршруты. Режим Stub Router полезен при добавлении или удалении маршрутизатора из сети или для избежания транзитных маршрутов, когда маршрутизатор перезагружается.

Можно принудительно ввести OSPF в режим Stub Router. OSPF останется в этом режиме до тех пор, пока его не выведут из него. Аналогичным образом можно настроить OSPF войти в данный режим на настраиваемое количество времени после того, как маршрутизатор загрузится.

Если настроить маршрутизатор на вход в режим Stub Router во время запуска (max-metric router-lsa on-startup) и затем ввести команду max-metric router-lsa, ничего не произойдет. Если OSPF административно находится в режиме Stub Router (была задана команда max-metric router-lsa), а вы настроите OSPF входить в режим Stub Router во время запуска (max-metric router-lsa on-startup), OSPF выйдет из данного режима (предположив, что период запуска истек), и конфигурация обновится.

Значение по умолчанию: OSPF не находится в режиме Stub Router

Формат: `max-metric router-lsa [on-startup seconds] [summary-lsa {metric}]`

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

Параметр	*Описание*
on-startup	(Необязательный параметр.) OSPF войдет в режим Stub Router после перезагрузки.
seconds	(Обязателен при использовании on-startup.) Время в секундах, которое OSPF будет находится в режиме Stub Router после перезагрузки. Диапазон — от 5 до 86 400 секунд. Значение по умолчанию отсутствует.
summary-lsa	(Необязательный параметр.) Устанавливает значения метрики в LSA типа 3 и 4 как LsInfinity (0xFFFFFF).
metric	(Необязательный параметр.) Значение, посылаемые в суммарных LSA, когда маршрутизатор находится в режиме Stub Router. Диапазон — от 1 до 16 777 215. Значение по умолчанию: 16 711 680 (0xFF0000).

no max-metric router-lsa

Используйте данную команду в режиме конфигурирования OSPFv2-маршрутизатора, чтобы выключить режим Stub Router. Команда очищает любой тип режима (always или on-startup) и отключает опцию *summary-lsa*.

Формат: `no max-metric router-lsa [on-startup] [summary-lsa]`

Режим ввода команд: конфигурирование OSPFv2-маршрутизатора

clear ip ospf stub-router

Используйте команду clear ip ospf stub-router в привилегированном режиме, чтобы заставить OSPF выйти из режима Stub Router для конкретного маршрутизатора, если он автоматически вошел в этот режим по причине ограничения ресурсов. OSPF выходит из режима Stub Router только по причине ограничения ресурсов или если маршрутизатор находится в нем с момента запуска. Если виртуальный маршрутизатор не указан, команда выполняется для маршрутизатора по умолчанию. Эта команда не действует, если режим Stub Router постоянно активен.

Формат: `clear ip ospf stub-router [vrf vrf-name]`

Режим ввода команд: привилегированный

Команды просмотра оперативного состояния устройства для протокола OSPF

show ip ospf

Эта команда отображает информацию о глобальных настройках OSPF для указанного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию.

Формат: `show ip ospf [vrf vrf-name]`

Режим ввода команд: привилегированный

Некоторые поля из представленных ниже отображаются, только если включен протокол OSPF и настроен определенный функционал.

Термин	*Значение*
Router ID	Идентификатор маршрутизатора, для которого отображается информация.
OSPF Admin Mode	Показывает, включен или выключен административный режим OSPF на маршрутизаторе.
RFC 1583 Compatibility	Показывает, включена совместимость с RFC 1583.
External LSDB Limit	Максимальное количество записей AS-external-LSA, которые могут быть помещены в базу данных состояния соединения.
Exit Overflow Interval	Время в секундах после входа в состояние переполнения, по истечении которого маршрутизатор будет пытаться выйти из этого состояния.
Spf Delay Time	Количество секунд между двумя последовательными изменениями LSA, во время которых откладывается время расчета таблицы маршрутизации.
Spf Hold Time	Количество секунд между двумя последовательными расчетами spf.
Flood Pacing Interval	Среднее время в миллисекундах между передачами пакетов LS Update на интерфейс.
LSA Refresh Group Pacing Time	Размер группового окна обновления LSA в секундах.
Opaque Capability	Показывает, может ли маршрутизатор посылать Opaque LSA.
Autocost Ref BW	Показывает значение эталонной пропускной способности, настроенное на маршрутизаторе, для автоматического расчёта стоимости.
Default Passive Setting	Показывает, является ли интерфейс пассивным по умолчанию.
Maximum Paths	Максимальное количество маршрутов, которые OSPF может установить для одного места назначения.

Default Metric	Значение стоимости по умолчанию для распространяемых маршрутов.
Stub Router Configuration	Показывает, может ли маршрутизатор входить в режим Stub Router.
Stub Router Startup Time	Показывает время, в течение которого маршрутизатор будет находится в режиме Stub Router после загрузки. Это поле выводится, только если OSPF настроен входить в режим Stub Router при запуске.
Summary LSA Metric Override	**Enabled** (*met*) или **Disabled**, где *met* — это значения, которые посылаются в сводных LSA в режиме Stub Router.
BFD Enabled	Отображает статус BFD.
Default Route Advertise	Указывает, анонсируются ли маршруты по умолчанию, полученные от других протоколов-источников.
Always	Показывает, всегда ли анонсируются маршруты по умолчанию.
Metric	Метрики распространяемых маршрутов. Если метрики не настроены, это поле остается пустым.
Metric Type	Показывает тип анонсируемых маршрутов других протоколов: External Type 1 или External Type 2.
Number of Active Areas	Количество активных зон OSPF. Активная зона OSPF — это зона с хотя бы одним работающим интерфейсом.
ABR Status	Показывает, является ли маршрутизатор пограничным маршрутизатором зоны OSPF.
ASBR Status	Показывает, включен ли режим ASBR. Маршрутизатор автоматически становится ASBR, когда он настроен распространять маршруты, полученные другими протоколами. Возможные значения для статуса ASBR: enabled (если маршрутизатор настроен распространять маршруты, полученные другими протоколами) или disabled (если он не настроен на это). Enabled подразумевает то, что маршрутизатор является пограничным маршрутизатором автономной системы (ASBR).
Stub Router Status	Состояние режима Router **Active** или **Inactive.**
Stub Router Reason	Показывает причину, по которой маршрутизатор находится в режиме Stub Router **Configured**, **Startup** или **Resource Limitation**. Это поле отображается, только если режим Stub Router активен.
Stub Router Startup Time Remaining	Время в секундах до того, как OSPF выйдет из режима Stub Router. Это поле отображается, только если OSPF находится в режиме Stub Router после загрузки.
Stub Router Duration	Время, прошедшее с момента последнего входа маршрутизатора в режим Stub Router. Эта строка отображается, только если Stub Router активен и маршрутизатор вошел в режим Stub Router по причине ограничения ресурсов. Продолжительность отображается в формате дд:чч:мм:сс.
External LSDB Overflow	Если количество полученных внешних LSA превышает настроенный лимит, External LSDB Limit, OSPF входит в состояние переполнения. В этом состоянии OSPF отзывает все свои сгенерированные внешние LSA. После истечении установленного времени Exit Overflow Interval OSPF выходит из состояния переполнения, если количество внешних LSA было уменьшено.
External LSA Count	Количество внешних LSA типа 5 в базе данных состояния соединения.
External LSA Checksum	Количество контрольных сумм LS внешних LSA, содержащихся в базе данных состояния соединения.
AS_OPAQUE LSA Count	Показывает количество AS Opaque LSA в базе данных OSPF.
AS_OPAQUE LSA Checksum	Показывает количество контрольных сумм LS-анонсов состояния соединения AS Opaque, содержащихся в базе данных состояния соединения.
New LSAs Originated	Количество новых сгенерированных LSA.

LSAs Received	Количество полученных LSA, определенных как новые.
LSA Count	Общее количество LSA, находящихся в данный момент в базе данных состояния соединения.
Maximum Number of LSAs	Максимальное количество LSA, которые OSPF может хранить.
LSA High Water Mark	Максимальный размер базы данных состояния соединения с момента запуска системы.
AS Scope LSA Flood List Length	Количество LSA, в данный момент находящихся в очереди глобального режима переполнения и ждущих перенаправления через домен OSPF.
Retransmit List Entries	Общее количество LSA, ждущих подтверждения всеми соседями. Любые LSA могут ожидать подтверждения более чем одним соседним устройством.
Maximum Number of Retransmit Entries	Максимальное количество LSA, которые могут ожидать подтверждения в любое время.
Retransmit Entries High Water Mark	Максимальное количество LSA в списках повторной передачи всех соседей в любое время.
NSF Support	Указывает, включено ли nonstop-маршрутизация (NSF) протокола OSPF для плановых или внеплановых перезагрузок или для обоих типов (Always).
NSF Restart Interval	Настраиваемый пользователем интервал, во время которого соседний маршрутизатор будет находится в режиме помощника после получения уведомления о том, что маршрутизатор выполняет щадящую перезагрузку.
NSF Restart Status	Действующий статус щадящей перезагрузки маршрутизатора. • Not Restarting (не перезагружается); • Planned Restart (плановая перезагрузка). Unplanned Restart (внеплановая перезагрузка).
NSF Restart Age	Количество секунд до того, как закончится интервал щадящей перезагрузки.
NSF Restart Exit Reason	Показывает, по какой причине маршрутизатор последний раз выходил из последней перезагрузки: • None — щадящая перезагрузка не проводилась; • In Progress — перезагрузка в процессе; • Completed — предыдущая щадящая перезагрузка выполнена успешно; • Timed Out — время предыдущей щадящей перезагрузки истекло; • Topology Changed — предыдущая щадящая перезагрузка досрочно прекращена из-за изменения топологии.
NSF Help Support	Показывает, включена ли функция соседа-помощника OSPF для плановых или внеплановых перезагрузок либо для обоих типов (Always).
NSF help Strict LSA checking	Показывает, включена ли строгая проверка LSA. Если включена, то сосед-помощник OSPF выйдет из режима помощника, как только произойдет изменение топологии. Если выключена, сосед-помощник OSPF продолжит работать в этом режиме, несмотря на изменение топологии.
Prefix- suppression	Отображает, включено ли подавление префиксов.

show ip ospf abr

Данная команда отображает записи внутренней таблицы OSPF для маршрутизаторов Area Border Routers (ABR) для указанного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию.

Формат: `show ip ospf abr [vrf vrf-name]`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Type	Тип маршрута к месту назначения. Может быть: • intra — маршрут внутри зоны; • inter — маршрут между зонами.
Router ID	Идентификатор маршрутизатора места назначения.
Cost	Стоимость использования пути.
Area ID	Идентификатор зоны, из которой получены данные о маршруте.
Next Hop	Ближайший узел по направлению к месту назначения.
Next Hop Intf	Исходящий интерфейс маршрутизатора, используемый при перенаправлении трафика на ближайший узел.

show ip ospf area

Эта команда отображает информацию о зоне для указанного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию. Параметр *areaid* указывает OSPF-зону, которая будет отображаться.

Формат: `show ip ospf area areaid [vrf vrf-name]`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
AreaID	Идентификатор запрошенной OSPF-зоны.
External Routing	Число, представляющее возможности внешней маршрутизации для этой зоны.
Spf Runs	Количество случаев, когда таблица маршрутизации внутри зоны была рассчитана с использованием базы данных состояния соединения этой зоны.
Area Border Router Count	Общее количество пограничных маршрутизаторов в данной зоне.
Area LSA Count	Общее количество LSA в базе данных состояния соединения этой зоны, исключая внешние AS LSA.
Area LSA Checksum	Число, представляющее контрольную сумму LSA зоны для указанного AreaID, исключая внешние LSA (LS типа 5).
Flood List Length	Количество LSA, ждущих распространения внутри зоны.
Import Summary LSAs	Показывает, импортируются ли суммированные LSA.
OSPF Stub Metric Value	Значение метрики stub-зоны. Это поле отображается, только если зона сконфигурирована как stub-зона.

Следующая информация OSPF NSSA отображается только в том случае, если зона настроена как NSSA:

Термин	*Значение*
Import Summary LSAs	Показывает, импортируются ли LSA типа 3 в NSSA.
Redistribute into NSSA	Показывает, распространяется ли информация в NSSA.
Default Information Originate	Показывает, анонсируется ли NSSA маршрут по умолчанию.
Default Metric	Значения стоимости для маршрута по умолчанию, анонсируемого NSSA.
Default Metric Type	Тип значений для маршрута по умолчанию, анонсируемого NSSA.
Translator Role	Роль транслятора NSSA для ABR: always или candidate.
Translator Stability Interval	Период времени, в течение которого выбранный транслятор продолжает выполнять свои обязанности после определения факта, что его статус транслятора был замещен другим маршрутизатором.
Translator State	Показывает статус маршрутизатора ABR: disabled, always или elected.

show ip ospf asbr

Эта команда отображает записи внутренней таблицы OSPF-маршрутизации для ASBR указанного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию.

Формат: `show ip ospf asbr [vrf vrf-name]`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Type	Тип маршрута к месту назначения. Может быть: • intra — маршрут внутри зоны; • inter — маршрут между зонами.
Router ID	Идентификатор маршрутизатора места назначения.
Cost	Стоимость использования пути.
Area ID	Идентификатор зоны, из которой получены данные о маршруте.
Next Hop	Ближайший узел по направлению к месту назначения.
Next Hop Intf	Исходящий интерфейс маршрутизатора, используемый при перенаправлении трафика на ближайший узел.

show ip ospf database

Данная команда отображает информацию о базе данных OSPF, когда OSPF включен для определенного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию. Если не указывать дополнительных параметров, команда отобразит заголовки LSA для всех зон. Используйте необязательный параметр areaid, чтобы отобразить информацию базы данных для определенной зоны. Используйте необязательные параметры, чтобы указать тип отображаемых LSA

Термин	*Значение*
vrf-name	Виртуальный маршрутизатор, для которого будет отображаться информация.

asbr-summary	Используйте *asbr-summary*, чтобы показать сводные LSA для ASBR.
external	Используйте *external*, чтобы отобразить внешние LSA.
network	Используйте *network*, чтобы отобразить LSA сети.
nssa-external	Используйте *nssa-external*, чтобы отобразить внешние LSA NSSA.
opaque-area	Используйте *opaque-area*, чтобы отобразить opaque LSA для зоны.
opaque-as	Используйте *opaque-as*, чтобы отобразить AS opaque LSA.
opaque-link	Используйте *opaque-link*, чтобы отобразить opaque LSA соединения.
router	Используйте *router*, чтобы отобразить LSA маршрутизатора.
summary	Используйте *summary*, чтобы показать суммарные LSA базы данных LSA.
lsid	Используйте *lsid*, чтобы указать идентификатор состояния соединения (LSID). Значение *lsid* может быть IP-адресом или числом в диапазоне от 0 до 4 294 967 295.
adv-router	Используйте *adv-router*, чтобы показать LSA, ограниченные анонсирующим маршрутизатором
self-originate	Используйте *self-originate*, чтобы отобразить LSA, сгенерированные самим маршрутизатором.

Информация ниже отображается только в том случае, если включен OSPF.

Формат: `show ip ospf [areaid] database [vrf vrf-name] [{database-summary | [{asbr-summary | external | network | nssa-external | opaque-area | opaque-as | opaque-link | router| summary}] [lsid] [{adv-router [ipaddr] | self-originate}]}]`

Режим ввода команд: привилегированный

пользовательский

Для каждого типа соединения и зоны отображается следующая информация:

Термин	***Значение***
Link Id	Число, обозначающее LSA, создаваемый маршрутизатором из всех остальных сгенерированных LSA того же типа LS.
Adv Router	Идентификатор анонсирующего маршрутизатора.
Age	Число, представляющее время существования LSA в секундах.
Sequence	Число, представляющее версию LSA.
Checksum	Итоговая контрольная сумма LSA.
Options	Целое число, обозначающее, что LSA получает особый режим обработки во время расчета маршрутизации.
Rtr Opt	Опции маршрутизатора, действительные только для соединений этого маршрутизатора.

show ip ospf database database-summary

Используйте данную команду, чтобы отобразить количество каждого типа LSA в базе данных каждой зоны и для маршрутизатора. Команда также отображает общее количество LSA в базе данных.

Формат: `show ip ospf database database-summary`

Режим ввода команд: привилегированный

пользовательский

Термин	***Значение***

Router	Общее количество LSA маршрутизатора в базе данных состояния соединения OSPF.
Network	Общее количество LSA сети в базе данных состояния соединения OSPF.
Summary Net	Общее количество сводных LSA сети в базе данных.
Summary ASBR	Количество сводных LSA маршрутизатора ASBR в базе данных.
Type-7 Ext	Общее количество внешних LSA типа 7 в базе данных.
Self-Originated Type-7	Общее количество автоматически возникших внешних AS LSA в базе данных состояния соединения OSPF.
Opaque Link	Количество LSA opaque-соединения в базе данных.
Opaque Area	Количество LSA opaque-зоны в базе данных.
Subtotal	Количество записей в указанной зоне.
Opaque AS	Количество AS LSA в базе данных.
Total	Количество записей для всех зон.

show ip ospf interface

Эта команда отображает информацию для объекта IFO или таблицы виртуального интерфейса. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ip ospf interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`| loopback `*`loopback-id`*`}`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
IP Address	IP-адрес для указанного интерфейса.
Subnet Mask	Маска сети.
Secondary IP Address(es)	Вторичные IP-адреса, если они настроены на интерфейсе.
OSPF Admin Mode	Указывает, включен ли OSPF на интерфейсе маршрутизатора.
OSPF Area ID	Идентификатор OSPF-зоны для указанного интерфейса.
OSPF Network Type	Тип сети на данном интерфейсе, где запущен OSPF.
Router Priority	Приоритет OSPF для указанного интерфейса.
Retransmit Interval	Retransmit-интервал OSPF для указанного интерфейса.
Hello Interval	Hello-интервал OSPF для указанного интерфейса.
Dead Interval	Dead-интервал OSPF для указанного интерфейса.
LSA Ack Interval	Интервал ожидания подтверждения LSA OSPF для указанного интерфейса.
Transmit Delay	Интервал задержки передачи OSPF для указанного интерфейса.
Authentication Type	Тип аутентификации OSPF для указанного интерфейса: none, simple или encrypt.
Metric Cost	Стоимость OSPF-интерфейса.
Passive Status	Статус пассивного интерфейса.
OSPF MTU-ignore	Указывает, игнорируются ли несовпадения MTU в пакетах DBD, присланных соседними маршрутизаторами.
Flood Blocking	Показывает, включена ли блокировка рассылки на интерфейсе.
OSPF Interface Type	Тип OSPF-интерфейса будет broadcast или ptp.
State	Состояния OSPF-интерфейса могут обозначаться как down, loopback, waiting, point-to-point, designated router и backup designated router.
Designated Router	Идентификатор назначенного маршрутизатора (DR).

Backup Designated Router	Идентификатор резервного назначенного маршрутизатора (BDR).
Number of Link Events	Количество событий соединения.
Local Link LSAs	Количество LSA локальных соединений opaque в базе данных состояния соединения.
Local Link LSA Checksum	Сумма контрольных сумм LS-анонсов LS локальных соединений opaque в базе данных состояния соединения.
Prefix-suppression	Отображает статус подавления префиксов на данном интерфейсе: enabled, disabled или unconfigured.

show ip ospf interface brief

Данная команда отображает краткую информацию для объекта IFO или таблицы виртуального интерфейса. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию.

Формат: `show ip ospf interface brief [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
Interface	*unit/slot/port*
OSPF Admin Mode	Указывает, включен ли OSPF на интерфейсе маршрутизатора.
OSPF Area ID	Идентификатор OSPF-зоны для указанного интерфейса.
Router Priority	Приоритет OSPF для указанного интерфейса.
Cost	Стоимость для OSPF-интерфейса.
Hello Interval	Hello-интервал OSPF для указанного интерфейса.
Dead Interval	Dead-интервал OSPF для указанного интерфейса
Retransmit Interval	Retransmit-интервал OSPF для указанного интерфейса.
Interface Transmit Delay	Интервал задержки передачи OSPF для указанного интерфейса.
LSA Ack Interval	Интервал ожидания подтверждения LSA OSPF для указанного интерфейса.

show ip ospf interface stats

Команда отображает статистику для указанного интерфейса. Информация ниже отображается, если включен OSPF. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ip ospf interface stats {`*`unit/slot/port`*`|vlan` *`1-4093`*`}`

Режим ввода команд: привилегированный
пользовательский

Термин	***Значение***
OSPF Area ID	Идентификатор OSPF-зоны для указанного интерфейса.
Area Border Router Count	Общее количество пограничных маршрутизаторов в данной зоне. Изначальное значение — 0, которое пересчитывается в каждом проходе SPF.
AS Border Router Count	Общее количество пограничных маршрутизаторов AS в данной зоне.
Area LSA Count	Общее количество LSA в базе данных состояния соединения этой зоны, исключая внешние AS LSA.
IP Address	IP-адрес, связанный с данным OSPF-интерфейсом.
OSPF Interface Events	Количество случаев, когда указанный OSPF-интерфейс менял свой статус

	или когда происходили ошибки.
Virtual Events	Количество изменений статуса или ошибок, зафиксированных на данном виртуальном соединении.
Neighbor Events	Количество случаев, когда соседнее устройство меняло свой статус или происходила ошибка.
Sent Packets	Количество OSPF-пакетов, переданных интерфейсом.
Received Packets	Количество действительных OSPF-пакетов, принятых интерфейсом.
Discards	Количество принятых OSPF-пакетов, отброшенных по причине ошибки в пакете или при его обработке.
Bad Version	Количество принятых OSPF-пакетов, чье поле версии в заголовке OSPF не совпадало с версией OSPF-процесса, который обрабатывал пакет.
Source Not On Local Subnet	Количество принятых пакетов, отброшенных из-за того, что IP-адрес источника не находится в подсети, настроенной на данном интерфейсе. **Примечание:** Это поле относится только к OSPFv2.
Virtual Link Not Found	Количество принятых пакетов, отброшенных из-за того, что входной интерфейс находится не в магистральной зоне, а заголовок OSPF идентифицировал пакет как принадлежащий к магистрали, но у OSPF не было виртуального канала для отправителя пакета.
Area Mismatch	Количество OSPF-пакетов, отброшенных из-за того, что идентификатор зоны в OSPF-заголовке не совпадает с идентификатором, настроенным на входном интерфейсе.
Invalid Destination Address	Количество OSPF-пакетов, отброшенных из-за того, что IP-адрес не является адресом входного интерфейса и адресом многоадресной рассылки AllDrRouters или AllSpfRouters.
Wrong Authentication Type	Количество пакетов, отброшенных из-за того, что тип аутентификации, указанный в OSPF-заголовке, не совпадал с типом аутентификации, настроенным на входном интерфейсе. **Примечание:** Это поле относится только к OSPFv2.
Authentication Failure	Количество OSPF-пакетов, отброшенных из-за того, что отправитель — несуществующий сосед или IP-адрес отправителя не совпадает с предыдущим записанным IP-адресом для этого соседа. **Примечание:** Это поле относится только к OSPFv2.
No Neighbor at Source Address	Количество OSPF-пакетов, отброшенных из-за того, что отправитель — несуществующий сосед или IP-адрес отправителя не совпадает с предыдущим записанным IP-адресом для этого соседа. **Примечание:** Не относится к hello-пакетам
Invalid OSPF Packet Type	Количество OSPF-пакетов, отброшенных из-за того, что поле packet type в OSPF-заголовке является неизвестным типом.
Hellos Ignored	Количество принятых hello-пакетов, которые игнорируются данным маршрутизатором от новых соседей после того, как было достигнуто предельное количество соседей на данном интерфейсе или в системе в целом.

show ip ospf lsa-group

Эта команда отображает количество сгенерированных LSA для каждой группы LSA для указанного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию.

Формат: `show ip ospf lsa-group [vrf vrf-name]`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Total self-originated LSAs	Количество LSA, которые маршрутизатор создает в настоящее время.
Average LSAs per group	Количество сгенерированных LSA, разделенное на количество групп LSA. Количество групп LSA — это интервал обновления (1800 секунд), разделенный на интервал шага (настроенный командой timers pacing lsa-group) плюс 2.
Pacing group limit	Максимальное количество сгенированных LSA в одной группе LSA. Если количество LSA в группе превышает предельное количество, OSPF раздает LSA через интервал обновления, чтобы достичь лучшего соотношения.
Groups	Для каждого шага LSA-группы отображается диапазон времени существования LSA в группе и количество LSA в группе.

show ip ospf neighbor

Эта команда отображает информацию о соседях OSPF для указанного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию. Если не указать IP-адрес соседа, команда отобразит общую информацию в таблице. Если указать интерфейс или туннель, отобразится только информация для данного интерфейса или туннеля, если интерфейс является физическим интерфейсом маршрутизации, и VLAN-формат — если интерфейс является маршрутизирующим VLAN-интерфейсом. Параметр ip-address — IP-адрес соседа, и если его указать, отобразится детальная информация об этом соседе. Информация ниже отображается только в том случае, если включен OSPF и у интерфейса есть соседи.

Формат: `show ip ospf neighbor [vrf` *`vrf-name`*`][interface {`*`unit/slot/port`*`|vlan` *`1-4093`*`}] [ip- address]`

Режим ввода команд: привилегированный
пользовательский

Если не указать IP-адрес, таблица с данными столбцами отобразится для всех соседей или для соседа, связанного с интерфейсом, который вы укажете:

Термин	*Значение*
Router ID	Идентификатор соседнего маршрутизатора.
Priority	OSPF-приоритет указанного интерфейса. Приоритет интерфейса — это целое число от 0 до 255. Нулевое значение обозначает, что маршрутизатор не подходит на роль назначенного маршрутизатора в данной сети.
IP Address	IP-адрес соседа.
Interface	Интерфейс локального маршрутизатора в формате unit/slot/port.
State	Статус соседних маршрутизаторов. Возможные значения: • Down — исходное состояние соседа; от соседа не было получено свежей информации. • Attempt — от соседа не было получено свежей информации, но более согласованные усилия должны быть приложены, чтобы связаться с соседом. • Init — от соседа недавно был замечен Hello-пакет, но двунаправленное соединение пока еще не установлено. • way — между двумя маршрутизаторами установлено

	двунаправленное соединение. • Exchange start — первый шаг в создании смежности между двумя соседними маршрутизаторами, цель состоит в том, чтобы решить, какой маршрутизатор является главным, и принять решение относительно начального номера последовательности DD. • Exchange — маршрутизатор описывает всю свою базу данных состояния соединения путем отправки пакетов Database Description соседу. • Loading — соседу посылаются пакеты Link State Request с запросом более недавних LSA, которые были обнаружены (но еще не получены) в статусе Exchange. • Full — соседние маршрутизаторы полностью смежны и теперь они будут появляться в LSA маршрутизаторов и LSA сети.
Dead Time	Время в секундах, которое маршрутизатор ожидает перед тем, как посчитать соседа недоступным.

Если указать IP-адрес соседнего маршрутизатора, отобразится следующая информация:

Термин	***Значение***
Interface	unit/slot/port
Neighbor IP Address	IP-адрес соседнего маршрутизатора.
Interface Index	Идентификатор интерфейса соседнего маршрутизатора.
Area ID	Идентификатор зоны OSPF, связанной с данным интерфейсом.
Options	Целое число, обозначающее необязательные OSPF-возможности, поддерживающиеся соседним устройством. Необязательные OSPF-возможности соседа также перечислены в hello-пакетах. Это позволяет hello-пакетам быть отклоненными (например, если с соседом еще не было установлено соединения), если происходит несоответствие в некоторых ключевых OSPF-возможностях.
Router Priority	OSPF-приоритет указанного интерфейса. Приоритет интерфейса — это целое число от 0 до 255. Нулевое значение обозначает, что маршрутизатор не подходит на роль назначенного маршрутизатора в данной сети.
Dead Timer Due	Время в секундах, которое маршрутизатор ожидает перед тем, как посчитать соседа недоступным.
Up Time	Время работы соседнего устройства; сколько времени прошло с последнего момента, как соседство перешло в состояние Full.
State	Статус соседних маршрутизаторов.
Events	Количество случаев, когда соседнее устройство меняло свой статус или происходила ошибка.
Retransmitted LSAs	Количество LSA, переданных соседу.
Retransmission Queue Length	Целое число, обозначающее текущую длину очереди повторной передачи для указанного идентификатора соседнего маршрутизатора на указанном интерфейсе.
Restart Helper Status	Указывает статус данного маршрутизатора как помощника во время щадящей перезагрузки маршрутизатора, указанного в командной строке. • Helping — данный маршрутизатор является соседом-помощником для указанного соседа. Сосед-помощник не уведомляет об изменениях соседства во время щадящей перезагрузки и продолжает анонсировать перезагружающийся маршрутизатор как FULL-соседство. Сосед-помощник продолжает передавать пакеты данных перезагружающемуся маршрутизатору, полагая, что таблица пересылки перезапускающегося маршрутизатора

	поддерживается во время перезагрузки. • Not Helping — данный маршрутизатор не является соседом-помощником в данный момент.
Restart Reason	Если маршрутизатор находится в режиме соседа-помощника, это отображает причину перезапуска, данную перезапускающимся маршрутизатором. • Unknown (0) — неизвестна • Software restart (1) — перезапуск программного обеспечения • Software reload/upgrade (2) — перезагрузка/обновление программного обеспечения • Switch to redundant control processor (3) — переключение на резервный управляющий процессор • Unrecognized — значение, не указанное в RFC 3623. Когда OSPF посылает LSA Graseful, он устанавливает причину перезапуска как Software restart для плановой программной перезагрузки (при использовании команды initiate failover) и статус Unknown при внеплановой программной перезагрузке.
Remaining Grace Time	Количество секунд, оставшихся от интервала текущей щадящей перезагрузки. Отображается, только когда данный маршрутизатор в настоящее время находится в режиме соседа-помощника для указанного в команде маршрутизатора.
Restart Helper Exit Reason	Указывает причину, по которой указанный маршрутизатор вышел из щадящей перезагрузки в последний раз. • None — щадящая перезагрузка не проводилась • In Progress — перезагрузка в процессе • Completed — предыдущая щадящая перезагрузка выполнена успешно • Timed Out — время предыдущей щадящей перезагрузки истекло • Topology Changed — предыдущая щадящая перезагрузка досрочно прекращена из-за изменения топологии.

show ip ospf range

Эта команда отображает набор диапазонов маршрутов зоны OSPFv2, настроенных для суммирования для данной зоны виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию.

Формат: `show ip ospf range` *`areaid`* `[vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

Термин	***Значение***
Prefix	Суммарный префикс.
Subnet Mask	Маска подсети суммарного префикса.
Type	**S** (суммарное соединение) или **E** (внешнее соединение).
Action	**Advertise** или **Suppress.**
Cost	Метрики, которые анонсируются, если диапазон активен. Если статическая стоимость не настроена, поле отображает значение **Auto**. Если поле Action имеет значение **Suppress,** в данном поле отображается **N/A**.
Active	Активен ли диапазон в текущий момент. Значение: **Y** или **N**.

show ip ospf statistics

Эта команда отображает информацию о недавних подсчетах Shortest Path First (SPF) для указанного виртуального маршрутизатора. Если маршрутизатор не указан, информация отображается для маршрутизатора по умолчанию. SPF — это расчеты таблицы маршрутизации OSPF. Вывод команды перечисляет количество случаев, когда SPF выполнялся для каждой OSPF-зоны. Таблица следует данной информации. Для каждого из 15 последних запусков SPF команда показывает статистику: как давно был проведен SPF; сколько времени это заняло; причины, по которым SPF был запланирован; отдельные компоненты времени вычислений таблицы маршрутизации и время обновления Routing Information Base (RIB). Самые свежие статистические данные отображаются в конце таблицы.

Формат: `show ip ospf statistics [vrf vrf-name]`

Режим ввода команд: привилегированный

Термин	*Значение*
Delta T	Время с момента расчета таблицы маршрутизации. Указывается в формате часов, минут и секунд (чч:мм:сс).
Intra	Время, ушедшее на подсчет маршрутов внутри зоны, в миллисекундах.
Summ	Время, ушедшее на подсчет маршрутов между зонами, в миллисекундах.
Ext	Время, ушедшее на подсчет внешних маршрутов, в миллисекундах.
SPF Total	Общее время, ушедшее на подсчет маршрутов, в миллисекундах. Может превышать сумму соответствующих полей для внешних, внутренних и межзональных маршрутов.
RIB Update	Время, прошедшее с последнего выполненного подсчета таблицы маршрутизации, до момента, пока все изменения не были выполнены в общей таблице маршрутизации (RIB), в миллисекундах.
Reason	События, запустившие SPF. Коды причин перечислены ниже: • R — LSA нового маршрутизатора • N — LSA новой сети • SN — суммарный LSA новой сети • SA — суммарный LSA нового ASBR-маршрутизатора • X — новый внешний LSA.

show ip ospf stub table

Эта команда отображает OSPF Stub Table для виртуального маршрутизатора. Если маршрутизатор не указан, будет показана информация маршрутизатора по умолчанию. Информация ниже отображается только в том случае, если на коммутаторе инициализирован OSPF.

Формат: `show ip ospf stub table [vrf vrf-name]`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Area ID	32-битный идентификатор созданной stub-зоны.
Type of Service	Тип сервиса, связанного со stub-метриками. Коммутатор

	поддерживает только тип Normal TOS.
Metric Val	Значения метрик, применяемые на основе TOS. По умолчанию устанавливаются наименьшие значения вида обслуживания среди интерфейсов других зон. OSPF-стоимость маршрута является функцией от значения этой метрики.
Import Summary LSA	Управляет импортом суммарных LSA в stub-зоны.

show ip ospf traffic

Эта команда отображает статистику OSPFv2-пакетов, статистику LSA и статистику очереди сообщений OSPFv2 для виртуального маршрутизатора. Если маршрутизатор не указан, будет показана информация маршрутизатора по умолчанию. Статистика пакетов считает пакеты и LSA с момента последнего сброса OSPFv2-счетчиков (с помощью команды clear ip ospf counters).

Команда clear ip ospf counters не очищает метки high water mark (HWM) для очереди сообщений.

Формат: `show ip ospf traffic [vrf` *`vrf-name`*`]`

Режим ввода команд: привилегированный

Параметр	***Описание***
OSPFv2 Packet Statistics	Количество пакетов каждого типа, принятых и отправленных с момента последнего сброса OSPF-счетчиков.
LSAs Retransmitted	Количество LSA, переданных данным маршрутизатором с момента последнего сброса OSPF-счетчиков.
LS Update Max Receive Rate	Максимальная скорость полученных пакетов LS Update во время любого 5-секундного интервала с момента последнего сброса OSPF-счетчиков. Скорость указывается в пакетах в секунду.
LS Update Max Send Rate	Максимальная скорость переданных пакетов LS Update во время любого 5-секундного интервала с момента последнего сброса OSPF-счетчиков. Скорость указывается в пакетах в секунду.
Number of LSAs	Количество LSA каждого типа, полученных с момента последнего сброса OSPF-счетчиков.
OSPFv2 Queue Statistics	Для каждой очереди сообщений OSPFv2: текущий счетчик, текущий маркер HWM, количество пакетов, которые не удалось поставить в очередь, и ограничение очереди. Маркеры HWM не очищаются во время сброса OSPF-счетчиков.

show ip ospf virtual-link

Эта команда отображает информацию виртуального интерфейса OSPF для указанной зоны и соседнего узла для виртуального маршрутизатора. Если маршрутизатор не указан, будет показана информация маршрутизатора по умолчанию. Параметр areaid определяет зону, а параметр neighbor — идентификатор соседнего маршрутизатора.

Формат: `show ip ospf virtual-link [vrf` *`vrf-name`*`]` *`areaid neighbor`*

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
Area ID	Идентификатор запрошенной OSPF-зоны.
Neighbor Router ID	Идентификатор соседнего маршрутизатора.
Hello Interval	Настроенный hello-интервал для указанного OSPF-интерфейса.
Dead Interval	Настроенный dead-интервал для указанного OSPF-интерфейса.
Interface Transmit Delay	Настроенная задержка передачи для указанного OSPF-интерфейса.

Retransmit Interval	Настроенный интервал ретрансляции для указанного OSPF-интерфейса.
Authentication Type	Настроенный тип аутентификации для указанного OSPF-интерфейса.
State	Состояния OSPF-интерфейса могут обозначаться как own, loopback, waiting, point-to-point, designated router и backup designated router. Этот параметр показывает статус OSPF-интерфейса.
Neighbor State	Статус соседнего узла.

show ip ospf virtual-link brief

Настроенная задержка передачи для указанного OSPF-интерфейса.

Эта команда отображает краткую информацию виртуального интерфейса OSPF для всех зон в системе.

Формат: `show ip ospf virtual-link brief`

Режим ввода команд: привилегированный
пользовательский

Параметр	***Описание***
Area ID	Идентификатор запрошенной OSPF-зоны.
Neighbor	Соседний интерфейс виртуального OSPF-интерфейса.
Hello Interval	Настроенный hello-интервал для указанного OSPF-интерфейса.
Dead Interval	Настроенный dead-интервал для указанного OSPF-интерфейса.
Retransmit Interval	Настроенный интервал ретрансляции для указанного OSPF-интерфейса.
Transmit Delay	Настроенная задержка передачи для указанного OSPF-интерфейса.

11.12 Команды настройки протокола RIP

В этой части описаны команды, используемые для просмотра и настройки Routing Information Protocol (RIP), который представляет собой протокол дистанционно-векторной маршрутизации, используемый для маршрутизации трафика в пределах небольшой сети.

router rip

Используйте эту команду, чтобы войти в режим RIP на маршрутизаторе.

Формат: `router rip`

Режим ввода команд: глобальная конфигурация

enable (RIP)

Эта команда устанавливает административный режим RIP-маршрутизатора в значение по умолчанию (активен).

Значение по умолчанию: включено

Формат: `enable`

Режим ввода команд: конфигурирование RIP-маршрутизатора

no enable (RIP)

Эта команда устанавливает административный режим RIP-маршрутизатора как неактивный.

Формат: `no enable`

Режим ввода команд: конфигурирование RIP-маршрутизатора

ip rip

Эта команда включает RIP на интерфейсе маршрутизатора или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `ip rip`

Режим ввода команд: конфигурирование интерфейса

no ip rip

Команда выключает RIP на интерфейсе маршрутизатора.

Формат: `no ip rip`

Режим ввода команд: конфигурирование интерфейса

auto-summary

Эта команда включает режим автоматического суммирования RIP.

Значение по умолчанию: выключено

Формат: `auto-summary`

Режим ввода команд: конфигурирование RIP-маршрутизатора

no auto-summary

Команда выключает режим автоматического суммирования RIP.

Формат: `no auto-summary`

Режим ввода команд: конфигурирование RIP-маршрутизатора

default-information originate (RIP)

Эта команда используется, чтобы управлять анонсами маршрутов по умолчанию.

Формат: `default-information originate`

Режим ввода команд: конфигурирование RIP-маршрутизатора

no default-information originate (RIP)

Эта команда используется, чтобы управлять анонсами маршрутов по умолчанию.

Формат: `no default-information originate`

Режим ввода команд: конфигурирование RIP-маршрутизатора

default-metric (RIP)

Данная команда используется, чтобы установить значения метрик по умолчанию анонсируемых маршрутов.

Формат: `default-metric` *`0-15`*

Режим ввода команд: конфигурирование RIP-маршрутизатора

no default-metric (RIP)

Команда используется для сброса значения метрик по умолчанию анонсируемых маршрутов.

Формат: `no default-metric`

Режим ввода команд: конфигурирование RIP-маршрутизатора

distance rip

Эта команда устанавливает значение приоритета RIP-маршрута на маршрутизаторе. При определении оптимального маршрута предпочтение отдается более низким значениям приоритета маршрута. Маршрут со значением preference 255 нельзя использовать для передачи трафика.

Значение по умолчанию: 15

Формат: `distance rip` *`1-255`*

Режим ввода команд: конфигурирование RIP-маршрутизатора

no distance rip

Эта команда возвращает приоритет RIP-маршрута на маршрутизаторе в значение по умолчанию.

Формат: `no distance rip`

Режим ввода команд: конфигурирование RIP-маршрутизатора

distribute-list out (RIP)

Используйте эту команду, чтобы настроить фильтр для анонсируемых маршрутов от протокола-источника.

Значение по умолчанию: 0

Формат: `distribute-list` *`1-199`* `out {ospf | bgp | static | connected}`

Режим ввода команд: конфигурирование RIP-маршрутизатора

no distribute-list out

Используйте эту команду, чтобы удалить фильтр для анонсируемых маршрутов от протокола-источника.

Формат: `no distribute-list` *`1-199`* `out {ospf | bgp | static | connected}`

Режим ввода команд: конфигурирование RIP-маршрутизатора

ip rip authentication

Эта команда устанавливает тип RIP-аутентификации версии 2 и ключ для указанного интерфейса или диапазона интерфейсов. Значение *type* может быть определено как *none*, *simple* или *encrypt*. Значение ключа аутентификации *[key]* должно быть в пределах 16 байт. Значение *[key]* составляется из стандартных символов. Если используется тип *encrypt*, должен быть указан keyid в диапазоне от 0 до 255.

Не идентифицированные интерфейсы не нуждаются в ключе аутентификации и идентификаторе ключа.

Значение по умолчанию: отсутствует

Формат: `ip rip authentication {none | {simple key} | {encrypt key keyid}}`

Режим ввода команд: конфигурирование интерфейса

no ip rip authentication

Эта команда возвращает тип RIP-аутентификации версии 2 и ключ для указанного интерфейса в значение по умолчанию.

Формат: `no ip rip authentication`

Режим ввода команд: конфигурирование интерфейса

ip rip receive version

Данная команда настраивает интерфейс или диапазон интерфейсов разрешать получение контрольных пакетов RIP указанной версии (или нескольких версий).

Значение mode может быть: *rip1* — чтобы получать только пакеты RIP версии 1, *rip2* — чтобы получать только пакеты RIP версии 2, *both* —чтобы получать пакеты обоих форматов, или none — чтобы запретить принимать контрольные пакеты любых форматов RIP.

Значение по умолчанию: both

Формат: `ip rip receive version {rip1 | rip2 | both | none}`

Режим ввода команд: конфигурирование интерфейса

no ip rip receive version

Эта команда настраивает интерфейс разрешать получение контрольных пакетов RIP версии по умолчанию.

Формат: `no ip rip receive version`

Режим ввода команд: конфигурирование интерфейса

ip rip send version

Эта команда настраивает интерфейс или диапазон интерфейсов разрешать отправление контрольных пакетов RIP указанной версии. Значение mode может быть: *rip1* — чтобы передавать пакеты RIP версии 1, *rip1c* (RIP версия 1 в режиме совместимости) — чтобы магистрально передавать пакеты RIP версии 2, *rip2* — чтобы отправлять пакеты RIP версии 2 с помощью многоадресной рассылки, или none — чтобы запретить передавать контрольные пакеты любых форматов RIP.

Значение по умолчанию: rip2

Формат: `ip rip send version {rip1 | rip1c | rip2 | none}`

Режим ввода команд: конфигурирование интерфейса

no ip rip send version

Эта команда настраивает интерфейс или диапазон интерфейсов разрешать отправление контрольных пакетов RIP указанной версии по умолчанию.

Формат: `no ip rip send version`

Режим ввода команд: конфигурирование интерфейса

hostroutesaccept

Эта команда включает для RIP режим hostroutesaccept.

Значение по умолчанию: включено

Формат: `hostroutesaccept`

Режим ввода команд: конфигурирование RIP-маршрутизатора

no hostroutesaccept

Команда выключает для RIP режим hostroutesaccept.

Формат: `no hostroutesaccept`

Режим ввода команд: конфигурирование RIP-маршрутизатора

split-horizon

Эта команда устанавливает RIP в режим *split horizon*. Split horizon — это техника обхода проблем, которые могут возникнуть при включении маршрутов в обновления, посылаемые маршрутизатору, который изначально распространял данные маршруты. Можно использовать следующие опции. None — специальная обработка не требуется. *Simple* — маршрут не будет включаться в обновления, посылаемые маршрутизатору, который изначально распространял данные маршруты. *Poisoned reverse* — маршрут будет включаться в обновления, посылаемые маршрутизатору, который изначально распространял данные маршруты, но связанные метрики будут установлены в бесконечное значение.

Значение по умолчанию: simple

Формат: `split-horizon {none | simple | poison}`

Режим ввода команд: конфигурирование RIP-маршрутизатора

no split-horizon

Эта команда возвращает настройки RIP-режима split horizon в значение по умолчанию.

Формат: `no split-horizon`

Режим ввода команд: конфигурирование RIP-маршрутизатора

redistribute (RIP)

Эта команда настраивает RIP-протокол на распространение маршрутов из указанных протоколов/маршрутизаторов. Внутренние маршруты RIP распространяются по умолчанию.

Значение по умолчанию: метрика — не настроена;
соответствие — внутреннее.

Режим ввода команд: Конфигурирование RIP-маршрутизатора

Формат для OSPF в качестве протокола источника: `redistribute ospf [metric 0-15] [match[internal] [external 1] [external 2] [nssa- external 1] [nssa-external-2]]`

Формат для другого протокола-источника: `redistribute {bgp | static | connected} [metric 0-15]`

no redistribute

Эта команда удаляет настройку RIP-протокола на распространение маршрутов из указанных протоколов/маршрутизаторов.

Формат: `no redistribute {ospf | bgp | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`

Режим ввода команд: конфигурирование RIP-маршрутизатора

show ip rip

Данная команда отображает информацию, относящуюся к RIP-маршрутизатору.

Формат: `show ip rip`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
RIP Admin Mode	Включен или выключен.
Split Horizon Mode	None, simple или poison reverse.
Auto Summary Mode	Enable или disable. При значении enable группы смежных маршрутов объединяются в единую запись, чтобы уменьшить общее количество записей. По умолчанию: enable.
Host Routes Accept Mode	Enable или disable. При значении enable маршрутизатор принимает маршруты узлов. По умолчанию: enable.
Global Route Changes	Количество изменений маршрутов, произведенных RIP в базе данных IP-маршрутов. Не включает в себя обновления времени существования маршрута.
Global queries	Количество откликов, посланных RIP-запросам от других систем.
Default Metric	Значения метрик по умолчанию для распространяемых маршрутов, если таковые уже были установлены, или пустое значение, если таковые не были настроены. Действительные значения: от 1 до 15.
Default Route Advertise	Маршрут по умолчанию.

show ip rip interface brief

Эта команда отображает общую информацию для каждого RIP-интерфейса. Для отображения результатов для каждого интерфейса должна быть включена соответствующая маршрутизация (например, командой ip rip).

Формат: `show ip rip interface brief`

Режим ввода команд: привилегированный
пользовательский

Термин	*Значение*
Interface	*unit/slot/port*
IP Address	IP-адрес источника, используемый указанным RIP-интерфейсом.
Send Version	RIP-версия (версии), используемая, когда указанному интерфейсу отсылаются обновления. Используемые типы: none, RIP-1, RIP-1c и RIP-2.
Receive Version	RIP версия (версии), разрешенная, когда на указанный интерфейс приходят обновления. Используемые типы: none, RIP-1, RIP-2 и Both.
RIP Mode	Административный режим маршрутизатора с RIP (enabled или disabled).
Link State	Режим интерфейса (enabled или disabled).

show ip rip interface

Данная команда отображает информацию, относящуюся к определенному RIP-интерфейсу. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ip rip interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`}`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
Interface	Количество ответных пакетов RIP, полученных RIP-процессом и впоследствии отброшенных по какой-либо причине.
IP Address	IP-адрес источника, используемый указанным RIP-интерфейсом.
Send Version	RIP-версия (версии), используемая, когда указанному интерфейсу отсылаются обновления. Используемые типы: none, RIP-1, RIP-1c и RIP-2. Это значение можно настраивать.
Receive Version	RIP версия (версии), разрешенная, когда на указанный интерфейс приходят обновления. Используемые типы: none, RIP-1, RIP-2 и Both. Это значение можно настраивать.
RIP Admin Mode	Административный режим маршрутизатора, где запущен RIP.
Link State	Указывает, включен или выключен RIP-интерфейс.
Authentication Type	Тип RIP-аутентификации для указанного интерфейса. Возможные значения: none, simple и encrypt.

Следующая информация будет недействительна, если соединение не поднято.

Термин	*Значение*
Bad Packets Received	Количество ответных пакетов RIP, полученных RIP-процессом и впоследствии отброшенных по какой-либо причине.
Bad Routes Received	Количество маршрутов, содержащихся в действительных RIP-пакетах, которые по какой-либо причине игнорировались.
Updates Sent	Количество запущенных обновлений RIP, которые фактически поступали на данный интерфейс.

11.13 Команды регулирования ICMP-сообщений

В этой части описаны команды, используемые для настройки опций передачи различных типов ICMP-сообщений.

ip unreachables

Данная команда включает генерацию сообщений ICMP Destination Unreachable на интерфейсе или диапазоне интерфейсов. По умолчанию генерация сообщений ICMP Destination Unreachable включена.

Значение по умолчанию: включено

Формат: `ip unreachables`

Режим ввода команд: конфигурирование интерфейса

no ip unreachables

Используйте данную команду, чтобы выключить генерацию сообщений ICMP Destination Unreachable.

Формат: `no ip unreachables`

Режим ввода команд: конфигурирование интерфейса

ip redirects

Данная команда включает генерацию маршрутизатором сообщений ICMP Redirect. По умолчанию генерация сообщений ICMP Redirect включена. Эту команду можно использовать для настройки интерфейса, диапазона интерфейсов или же всех интерфейсов.

Значение по умолчанию: включено

Формат: `ip redirects`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса
конфигурирование виртуального маршрутизатора

no ip redirects

Используйте данную команду, чтобы выключить генерацию маршрутизатором сообщений ICMP Redirect.

Формат: `no ip redirects`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

ipv6 redirects

Данная команда включает генерацию маршрутизатором сообщений ICMPv6 Redirect. По умолчанию генерация сообщений ICMPv6 Redirect включена. Эту команду можно использовать для настройки интерфейса, диапазона интерфейсов или же всех интерфейсов.

Значение по умолчанию: включено

Формат: `ipv6 redirects`

Режим ввода команд: конфигурирование интерфейса

no ipv6 redirects

Используйте данную команду, чтобы выключить генерацию маршрутизатором сообщений ICMPv6 Redirect.

Формат: `no ipv6 redirects`

Режим ввода команд: конфигурирование интерфейса

ip icmp echo-reply

Используйте данную команду, чтобы включить генерацию маршрутизатором сообщений ICMP Echo Reply. По умолчанию генерация сообщений ICMP Echo Reply включена.

Значение по умолчанию: включено

Формат: `ip icmp echo-reply`

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

no ip icmp echo-reply

Эта команда выключает генерацию маршрутизатором сообщений ICMP Echo Reply.

Формат: `no ip icmp echo-reply`

Режим ввода команд: глобальная конфигурация

ip icmp error-interval

Используйте данную команду, чтобы ограничить скорость, с которой отсылаются сообщения об ошибке ICMP IPv4. Ограничение скорости настраивается как совокупность параметров *burst-size* и *burst-interval*.

Параметр burst-interval определяет, как часто инициализируется ограничение с параметром burst-size. Значение burst-interval — от 0 до 2 147 483 647 миллисекунд (мс). Параметр burst-size — это количество ICMP-сообщений об ошибке, которые могут быть посланы за время burst-interval. Диапазон: от 1 до 200 сообщений. Чтобы выключить ограничение скорости ICMP, необходимо установить параметр burst-interval на ноль (0).

Значение по умолчанию: *burst-interval* — 1000 мс.
burst-size — 100 сообщений

Формат: `ip icmp error-interval` *`burst-interval [burst-size]`*

Режим ввода команд: глобальная конфигурация
конфигурирование виртуального маршрутизатора

no ip icmp error-interval

Используйте no-форму команды, чтобы вернуть burst-interval и burst-size в значения по умолчанию.

Формат: `no ip icmp error-interval`

Режим ввода команд: глобальная конфигурация

11.14 Команды настройки BFD

Протокол Bidirectional Forwarding Detection (BFD) проверяет двусторонние соединения между маршрутизаторами, которые могут находиться на расстоянии одного или нескольких хопов друг от друга. Протокол работает с любым базовым механизмом передачи и уровнем протокола с широким диапазоном периодов обнаружения, особенно в сценариях, когда требуется быстрое обнаружение сбоев в уровне передачи данных для множества одновременных сессий.

Используйте приведенные ниже команды, чтобы настроить протокол BFD.

feature bfd

Эта команда включает BFD на устройстве. Следует отметить, что для настройки других параметров протокола и интерфейса BFD должен быть включен.

Значение по умолчанию: выключено

Формат: `feature bfd`

Режим ввода команд: глобальная конфигурация

no feature bfd

Команда выключает BFD глобально и удаляет данные текущей сессии. Статические настройки сохраняются.

Формат: `no feature bfd`

Режим ввода команд: глобальная конфигурация

bfd

Данная команда включает BFD на всех интерфейсах, связанных с OSPF-процессом. BFD должен быть включен на отдельном интерфейсе, чтобы запустить включение BFD с этого интерфейса.

Значение по умолчанию: выключено

Формат: `bfd`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

no bfd

Данная команда выключает BFD на всех интерфейсах, связанных с OSPF-процессом.

Формат: `no bfd`

Режим ввода команд: конфигурирование OSPF-маршрутизатора

bfd echo

Эта команда включает эхо-режим BFD на IP-интерфейсе.

Значение по умолчанию: выключено

Формат: `bfd echo`

Режим ввода команд: конфигурирование интерфейса

no bfd echo

Команда выключает эхо-режим BFD на IP-интерфейсе.

Формат: `no bfd echo`

Режим ввода команд: конфигурирование интерфейса

bfd interval

Эта команда настраивает параметры BFD-сессии для всех доступных интерфейсов на устройстве (режим глобальной конфигурации) или для IP-интерфейса (режим конфигурирования интерфейса). Она перекрывает любые текущие настройки BFD на отдельных интерфейсах (в режиме глобальной конфигурации) или глобально настроенные параметры BFD-сессии (в режиме конфигурирования интерфейса).

Значение по умолчанию: отсутствует

Формат: `bfd interval` *`transmit-interval`* `min_rx` *`minimum-receive-interval`* `multiplier` *`detection- time-multiplier`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

Термин	***Значение***
transmit-interval	Желаемый минимальный интервал передачи, т. е. минимальный интервал, который пользователь хочет использовать при отправке контрольных BFD-пакетов. Выражается в миллисекундах. Диапазон: от 100 до 1000 мс (с шагом изменения в 100), значение по умолчанию — 100 мс.
minimum-receive-interval	Необходимый минимальный интервал получения, т. е. минимальный интервал, с которым система может получать контрольные BFD-пакеты. Выражается в миллисекундах. Диапазон: от 100 до 1000 мс (с шагом в 100), значение по умолчанию — 100 мс.
detection-time-multiplier	Количество контрольных BFD-пакетов, которые должны быть пропущены подряд для того, чтобы объявить сессию завершенной. Диапазон составляет от 1 до 50, значение по умолчанию — 3.

no bfd interval

В режиме глобальной конфигурации эта команда возвращает параметры BFD-сессии для всех доступных интерфейсов на устройстве в значения по умолчанию. В режиме конфигурирования интерфейса эта команда возвращает параметры BFD-сессии для всех сессий IP-интерфейса в значения по умолчанию.

Формат: `no bfd interval`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

bfd slow-timer

Эта команда устанавливает обязательное значение приоритета для интервала получения echo. Это значение определяет интервал, которые используют асинхронные сеансы для контрольных BFD-пакетов, когда функция echo включена. Значение slow-timer используется как новый интервал для контрольных пакетов, в то время как echo-пакеты используют настроенные интервалы BFD.

Значение по умолчанию: 2000

Формат: `bfd slow-timer` *`echo-receive-interval`*

Режим ввода команд: глобальная конфигурация

Термин	*Значение*
echo-receive-interval	Значение интервала, представленное в миллисекундах. Диапазон — от 1000 до 30000 мс (с шагом в 100), значение по умолчанию — 2000 мс.

no bfd slow-timer

Эта команда устанавливает значение приоритета для BFD slow-timer в значение по умолчанию.

Формат: `no bfd slow-timer`

Режим ввода команд: глобальная конфигурация

ip ospf bfd

Эта команда включает BFD на интерфейсах, связанных с процессом OSPF.

Значение по умолчанию: выключено

Формат: `ip ospf bfd`

Режим ввода команд: конфигурирование интерфейса

ip ospf bfd

Команда выключает BFD на интерфейсах, связанных с процессом OSPF.

Значение по умолчанию: выключено

Формат: `no ip ospf bfd`

Режим ввода команд: конфигурирование интерфейса

neighbor fall-over bfd

Эта команда включает в BFD поддержку быстрого аварийного переключения на BGP-соседа.

Значение по умолчанию: выключено

Формат: `neighbor` *`ipaddress`* `fall-over bfd`

Режим ввода команд: конфигурирование BGP-маршрутизатора

no neighbor fall-over bfd

Команда выключает поддержку аварийного переключения BGP-соседа посредством протокола BFD.

Формат: `no neighbor ipaddress fall-over bfd`

Режим ввода команд: конфигурирование BGP-маршрутизатора

show bfd neighbors

Эта команда отображает список BFD-смежностей, перечисляющий активных BFD-соседей.

Формат: `show bfd neighbors [details]`

Режим ввода команд: привилегированный

Параметр	*Описание*
details	Предоставляет дополнительные подробности, зарегистрированные BFD, и отображает статус административного режима: Enabled или Disabled.

Отображается информация, представленная ниже.

Параметр	*Описание*
Our IP address	Текущий IP-адрес.
Neighbor IP address	IP-адрес активного BFD-соседа
State	Текущий статус: Up или Down.
Interface	Текущий интерфейс.
Uptime	Период активности интерфейса.
Registered Protocol	Протокол, с которого была запущена сессия BFD и который зарегистрирован на прием событий от BFD (например, BGP).
Local Diag	Состояние диагностики, указывающее причину недавних изменений в статусе локальной сессии.
Demand mode	Указывает, намерена ли система использовать режим Demand. Примечание. Режим Demand не поддерживается в текущей версии ПО.
Minimum transmit interval	Минимальный интервал, используемый при передаче контрольных BFD-пакетов.
Actual TX Interval	Интервал передачи, используемый при передаче контрольных пакетов.
Actual TX Echo interval	Интервал передачи, используемый при передаче echo-пакетов.
Minimum receive interval	Минимальный интервал, с которым система может принимать контрольные BFD-пакеты.
Detection interval multiplier	Количество контрольных BFD-пакетов, которые должны быть пропущены подряд для того, чтобы объявить сессию завершенной.
My discriminator	Уникальный идентификатор для локальной BFD-сессии.
Your discriminator	Уникальный идентификатор для удаленной BFD-сессии.
Tx Count	Количество переданных BFD-пакетов.
Rx Count	Количество принятых BFD-пакетов.
Drop Count	Количество отброшенных пакетов.

debug bfd event

Данная команда отображает информацию о BFD-статусе передачи.

Формат: `debug bfd event`

Режим ввода команд: привилегированный

debug bfd packet

Эта команда отображает информацию об отладке контрольных BFD-пакетов.

Формат: `debug bfd packet`

Режим ввода команд: привилегированный

12 КОМАНДЫ НАСТРОЙКИ IP SLA

Функция IP service-level agreement (SLA – соглашение об уровне предоставления услуги) позволяет пользователям контролировать производительность сети между маршрутизаторами или от маршрутизатора до удаленного IP-устройства. Программное обеспечение поддерживает следующие возможности измерения:

- Удаленное отслеживание IP-доступности;
- Контроль порогового значения Round-trip-time.

Данные собираются измерением времени отклика ICMP и доступности. В основном, эта функция используется в корпоративных сетях на пограничных устройствах клиентов с множественной адресацией, в которых необходимо автоматическое переключение на следующего приоритетного интернет-провайдера в случае проблем с доступностью текущего провайдера.

Ip sla

Используйте данную команду, чтобы начать настройку операций IP SLA и войти в режим конфигурирования IP SLA.

Значение по умолчанию: не настроено ни одной операции IP SLA

Формат: `ip sla` *`operation-number`*

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
operation-number	Определяет настраиваемую операцию IP SLA. Может принимать значения от 1 до 128.

Рекомендации по использованию

Конфигурирование операции IP SLA начинается при помощи команды `ip sla`. Эта команда задает идентификационный номер для настраиваемой операции. После ввода этой команды маршрутизатор входит в режим конфигурации IP SLA.

Данная команда поддерживается как в IPv4-сетях, так и в IPv6-сетях, в которых поддерживаются адреса IPv6. Максимальное число поддерживаемых IP SLA – 128 (IPv4 и IPv6 совместно).

После того, как операция настроена, необходимо запланировать ее запуск. Для более подробной информации о планировании операций см. команду `ip sla schedule`.

После планирования операции вы не сможете изменить ее конфигурацию. Чтобы изменить конфигурацию операции после ее планирования, она должна быть либо остановлена, либо сначала удалена (с помощью команды `no ip sla`), а затем перенастроена с новыми параметрами операции.

Чтобы отобразить текущее состояние операции IP SLA, используется команда `show ip sla configuration` в пользовательском или привилегированном режиме.

Пример: показана операция 55, настроенная как операция ICMP Echo в IPv4-сети и запланированная на запуск. Приведена команда `ip sla`, используемая в IPv4-сети.

```
(Routing)(config)# ip sla 55
(Routing)(config-ip-sla)#icmp-echo 172.16.1.175
(Routing)(config-ip-sla-echo)#exit
(Routing)(config-ip-sla)#exit
(Routing)(config)# ip sla schedule 55
```

В случае если операция 55 уже сконфигурирована и не была запланирована, интерфейс командной строки перейдет в режим конфигурации IP SLA для операции 55. Если операция уже существует и была запланирована, эта команда не будет выполнена.

no ip sla

Данная команда удалит всю информацию о конфигурации операции IP SLA и ее расписание.

Формат: `no ip sla` *`operation-number`*

Режим ввода команд: глобальная конфигурация

Ip sla schedule

После настройки операции IP SLA находится в состоянии ожидания и должен быть запущен с помощью команды `ip sla schedule`. Используйте no-форму команды, чтобы остановить операцию и перевести ее в состояние по умолчанию (ожидание).

Значение по умолчанию: по умолчанию операция находится в состоянии ожидания. В состоянии ожидания операция включена, но не выполняет активный поиск и сбор информации.

Формат: `ip sla schedule` *`operation-number`*

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
operation-number	Определяет настраиваемую операцию IP SLA. Может принимать значения от 1 до 128.

Рекомендации по использованию

По умолчанию IP SLA не запланированы на запуск. После создания объекта IP SLA с помощью команды `ip sla` его необходимо запустить (с бесконечным временем жизни) с помощью команды `ip sla schedule` (режим конфигурации CLI). Когда передается команда `ip sla schedule`, операция `ip sla` переходит из ожидающего состояния в активное и немедленно начинает отслеживание и сбор информации. Отслеживание IP SLA можно остановить, отключив конфигурацию расписания IP SLA с помощью команды `no ip sla schedule`.

Данная команда поддерживается как в IPv4-сетях, так и в IPv6-сетях, в которых поддерживаются адреса IPv6.

После планирования операции вы не сможете изменить ее конфигурацию. Чтобы изменить конфигурацию операции после ее планирования, она должна быть либо остановлена при помощи команды no ip schedule, либо сначала удалена (с помощью команды no ip sla), а затем перенастроена с новыми параметрами операции.

Чтобы отобразить текущие настройки операции, используйте команду show ip sla configuration в пользовательском или привилегированном режиме.

Пример: операция 55 настроена как операция ICMP Echo в IPv4-сети и запланирована на запуск. Пример показывает использование команды ip sla schedule в IPv4-сети.

```
(Routing)(config)# ip sla 55
(Routing)(config-ip-sla)# icmp-echo 172.16.1.175
(Routing) (config-ip-sla-echo)#exit
(Routing)(config-ip-sla)#exit
(Routing)(config)# ip sla schedule 55
```

no ip sla schedule

Данная команда используется для того чтобы остановить операцию и вернуть ее в состояние по умолчанию (ожидание).

Формат: no ip sla schedule *operation-number*

Режим ввода команд: глобальная конфигурация

track ip sla

Эта команда используется для отслеживания состояния операции соглашений об уровне обслуживания (SLA) и для входа в режим настройки отслеживания.

Значение по умолчанию: выключено

Формат: track *object-number* ip sla *operation-number*
[reachability | state]

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
object-number	Определяет объект для отслеживания. Может принимать значения от 1 до 128.
operation-number	Определяет операцию IP SLA для отслеживания.
reachability	Отслеживает, доступен ли маршрут.
state	Отслеживает код возврата операции.

Рекомендации по использованию

Значение return-code операции поддерживается каждой операцией IP SLA. Код возврата интерпретируется процессом отслеживания. Код возврата может вернуть значения OK, OverThreshold и Timeout.

Можно отслеживать два аспекта работы IP SLA: Reachability (достижимость) и State (состояние). Принятие кода возврата OverThreshold является разницей между этими аспектами. В приведенной ниже таблице показано сравнение между аспектами Reachability и State операций IP SLA, которое можно отслеживать.

Отслеживание	*Код возврата*	*Состояние Track*
Reachability	OK или OverThreshold	Up Down
State	OK Timeout, OverThreshold	Up Down

Максимальное количество отслеживаемых объектов — 128 (IPv4 и IPv6 совместно). Если ни одно из необязательных ключевых слов (Reachability или State) не указано в настроенной команде CLI `track ip sla`, тогда настраивается тип отслеживания по умолчанию со значением Reachability.

Пример: процесс отслеживания сконфигурирован для отслеживания состояния (State) операции IP SLA 5:

```
(Routing)(config)# track 2 ip sla 5 state
```

В следующем примере процесс отслеживания сконфигурирован для отслеживания достижимости (Reachability) операции IP SLA 6:

```
(Routing)(config)# track 3 ip sla 6 reachability
```

no track ip sla

Данная команда отключает отслеживание.

Формат: `no track` *`object-number`*

Режим ввода команд: глобальная конфигурация

12.1 Команды режима конфигурации Track

delay

Чтобы настроить задержку для действий при изменении состояния достижимости объекта отслеживания, используйте команду delay в режиме конфигурации Track.

Значение по умолчанию: отсутствует

Формат: `delay {up` *`seconds`* `[down` *`seconds`*`] | [down` *`seconds`*`]`
`up` *`seconds`*`}`

Режим ввода команд: Режим конфигурации Track

Параметр	*Описание*
up ***seconds***	Время задержки уведомления о событии up. Значение задержки, в секундах. Может принимать значения от 0 до 180. Значение по умолчанию – 0.

down *seconds*	Время задержки уведомления о событии down. Значение задержки, в секундах. Может принимать значения от 0 до 180. Значение по умолчанию – 0.

Рекомендации по использованию

Чтобы свести к минимуму флаппинг состояния достижимости (Up/Down), используйте команду `delay`. Это введет ненулевую задержку в секундах между переходами состояний UP и Down для объекта Track.

Время задержки определяет интервал удержания для состояния (UP/DOWN) перед выполнением действий на связанных статических маршрутах.

Пример: объект Track 10 создается и связывается с операцией IP SLA 11, а затем настраивается задержка 5 секунд для `up` и 3 секунды для `down`:

```
(Routing)(config)#track 10 ip sla 11
(Routing)(config-track)#delay up 5 down 3
```

no delay

Используйте эту команду чтобы сбросить задержку при изменении состояния достижимости объекта отслеживания на значение по умолчанию.

Формат: `no delay`

Режим ввода команд: режим конфигурации Track

12.2 Команды режима конфигурации IP SLA

icmp-echo

Используйте эту команду в режиме конфигурации IP SLA, чтобы настроить операцию ICMP Echo по соглашениям об уровне предоставления услуги IP (IP SLA).

Значение по умолчанию: для настраиваемой операции не настроен тип операции IP SLA.

Формат: `icmp-echo` *`destination-ip-address`* `[source-interface {`*`interface-name`* `|` `vlan` *`vlan-id`*`}]`

Режим ввода команд: режим конфигурации IP SLA

Параметр	*Описание*
destination-ip-address	IPv4 или IPv6-адрес назначения.
source-interface *{interface-name* | vlan *vlan-id}*	Используется для указания исходного интерфейса для операции.

Рекомендации по использованию

В первую очередь необходимо настроить тип операции IP SLA (ICMP echo). Чтобы изменить значения (`destination-ip-address` или `source-interface-name`) существующей запланированной операции IP SLA ICMP Echo, необходимо остановить операцию IP SLA, используя команду `no ip sla schedule operation-number`. Или же вы должны сначала удалить операцию IP SLA (используя команду `no ip sla global configuration`), а затем перенастроить ее с новыми параметрами.

Операции IP SLA ICMP Echo поддерживают адреса IPv4 и IPv6.

Пример: операция IP SLA 12 создается и настраивается как эхо-операция с использованием протокола ICMP и целевого IPv4-адреса 143.1.16.125:

```
(Routing)(config)#ip sla 12
(Routing)(config-ip-sla)#icmp-echo 143.1.16.125
```

В следующем примере операция IP SLA 13 создается и настраивается как эхо-операция с использованием протокола ICMP и целевого IPv6-адреса 3001:CD6:200::1:

```
(Routing)(config)#ip sla 13
(Routing)(config-ip-sla)#icmp-echo 3001:CD6:200::1
```

12.3 Команды режима конфигурации IP SLA ICMP ECHO

frequency

Используйте эту команду для установки скорости, с которой указанная операция IP SLA повторяется в подрежиме конфигурации ICMP echo режима конфигурации IP SLA.

Значение по умолчанию: 60 секунд

Формат: `frequency` *`seconds`*

Режим ввода команд: режим конфигурации IP SLA ICMP ECHO

Параметр	*Описание*
seconds	Количество секунд между операциями IP SLA. Принимает значения в диапазоне 1 – 3600.

Рекомендации по использованию

Одиночная операция IP SLA будет повторяться с заданной частотой в течение всего срока действия операции. Например, операция эхо-сигнала ICMP с частотой 60 отправляет пакет ICMP Echo Request один раз каждые 60 секунд в течение срока действия операции. Этот пакет отправляется при запуске операции, а затем снова отправляется через 60 секунд.

Если выполнение отдельной операции IP SLA занимает больше времени, чем указанное значение частоты, статистический счетчик «busy», увеличивается, а не сразу повторяет операцию.

Ниже приведены рекомендуемые рекомендации по настройке команд `frequency`, `timeout` и `threshold` для операции IP SLA ICMP Echo:

(`frequency` *`seconds`*) → (`timeout` *`milliseconds`*) → (`threshold` *`milliseconds`*)

Рекомендуется не устанавливать значение частоты менее 60 секунд, поскольку потенциальные издержки от многочисленных активных операций могут существенно повлиять на производительность сети.

Данная команда поддерживается как в IPv4-сетях, так и в IPv6-сетях, в которых поддерживаются адреса IPv6.

Пример: в примере показано, как настроить операцию IP SLA ICMP Echo (операция 11), чтобы она повторялась каждые 80 секунд. Показана команда frequency (IP SLA), используемая в сети IPv4 в подрежиме конфигурации ICMP Echo режима конфигурации IP SLA:

```
(Routing)(config)#ip sla 11
(Routing)(config-ip-sla)#icmp-echo 152.15.10.145
```

```
(Routing)(config-ip-sla-echo)#frequency 80
```

no frequency

Используйте эту команду для возврата частоты к значению по умолчанию.

Формат: `no frequency`

Режим ввода команд: режим конфигурации IP SLA ICMP ECHO

timeout

Используйте эту команду, чтобы установить время, в течение которого операция IP SLA ожидает ответа от своего пакета запроса. Эта команда доступна в подрежиме конфигурации ICMP Echo режима конфигурации IP SLA.

Значение по умолчанию: 5000 миллисекунд

Формат: `timeout` *`milliseconds`*

Режим ввода команд: Режим конфигурации IP SLA ICMP ECHO

Параметр	*Описание*
milliseconds	Время, в течение которого операция ожидает получения ответа от своего пакета запроса, в миллисекундах (мс). Может принимать значения от 50 до 300000. Значение аргумента в миллисекундах должно основываться на сумме как максимального значения времени возврата (RTT – round-trip time) для пакетов, так и времени обработки операции IP SLA.

Рекомендации по использованию

Рекомендуется, чтобы значение аргумента в миллисекундах основывалось на сумме как максимального значения времени возврата (RTT – round-trip time) для пакетов, так и времени обработки операции IP SLA.

Используйте команду `timeout` (IP SLA), чтобы установить, как долго операция ожидает получения ответа от своего пакета запроса, и используйте команду `frequency` (IP SLA), чтобы установить скорость, с которой возобновляется операция IP SLA. Значение, указанное для команды `timeout` (IP SLA), не может быть больше значения, указанного для команды `frequency` (IP SLA).

Ниже приведены рекомендуемые рекомендации по настройке команд `frequency`, `timeout` и `threshold` для операции IP SLA ICMP Echo:

`(frequency` *`seconds`*`)` → `(timeout` *`milliseconds`*`)` → `(threshold` *`milliseconds`*`)`

Данная команда поддерживается как в IPv4-сетях, так и в IPv6-сетях, в которых поддерживаются адреса IPv6.

Пример: значение `timeout` для операции IP SLA 11 установлено на 2500 мс:

```
(Routing)(config)#ip sla 11
(Routing)(config-ip-sla)#icmp-echo 152.17.10.145
(Routing)(config-ip-sla-echo)#timeout 2500
```

no timeout

Используйте эту команду для возврата timeout к значению по умолчанию.

Формат: `timeout` *`milliseconds`*

Режим ввода команд: режим конфигурации IP SLA ICMP ECHO

threshold

Используйте эту команду в подрежиме конфигурации ICMP Echo конфигурации IP SLA, чтобы установить верхнее пороговое значение для расчета статистики мониторинга сети, созданной операцией IP SLA.

Значение по умолчанию: 5000 миллисекунд

Формат: `threshold` *`milliseconds`*

Режим ввода команд: режим конфигурации IP SLA ICMP ECHO

Параметр	*Описание*
milliseconds	Продолжительность времени в миллисекундах, необходимая для объявления возрастающего порога. Принимает значения в диапазоне 50 – 60000. Значение по умолчанию – 5000.

Рекомендации по использованию

Значение, указанное для этой команды, не должно превышать значение, указанное для команды `timeout`. Значение `threshold`, настроенное этой командой, используется только для вычисления статистики мониторинга сети, созданной операцией IP SLA.

Для операции IP SLA ICMP Echo команда `threshold` (IP SLA) устанавливает верхнее пороговое значение для измерения времени прохождения сигнала (RTT).

Ниже приведены рекомендуемые рекомендации по настройке команд `frequency`, `timeout` и `threshold` для операции IP SLA ICMP Echo:

`(frequency` *`seconds`*`)` → `(timeout` *`milliseconds`*`)` → `(threshold` *`milliseconds`*`)`

Данная команда поддерживается как в IPv4-сетях, так и в IPv6-сетях, в которых поддерживаются адреса IPv6.

Пример: в примере показано, как настроить порог срабатывания IP SLA ICMP Echo на 3500. В этом примере показана команда `threshold` (IP SLA), используемая в сети IPv4 в подрежиме конфигурации ICMP Echo режима конфигурации IP SLA:

```
(Routing)(config)#ip sla 11
(Routing)(config-ip-sla)#icmp-echo 152.17.10.145
(Routing)(config-ip-sla-echo)#threshold 3500
```

no threshold

Используйте эту команду для сброса threshold к значению по умолчанию.

Формат: `no threshold`

Режим ввода команд: режим конфигурации IP SLA ICMP ECHO

vrf (IP SLA)

Используйте эту команду в подрежиме конфигурации ICMP Echo режима конфигурации IP SLA, чтобы разрешить мониторинг достижимости в виртуальных частных сетях (VPN) с использованием операций IP SLA.

Значение по умолчанию: каждая операция IP SLA используется для мониторинга в Default VRF

Формат: `vrf` *`vrf-name`*

Режим ввода команд: режим конфигурации IP SLA ICMP ECHO

Параметр	*Описание*
vrf-name	Имя VPN-маршрутизации и переадресации (VRF).

Рекомендации по использованию

Эта команда определяет VPN для настраиваемой операции. Используйте эту команду, только если необходимо измерить время отклика через VPN-туннель.

Команда `vrf` (IP SLA) поддерживается только в сетях IPv4. Эта команда **не** поддерживается в сетях IPv6 для настройки операции IP SLA, поддерживающей адреса IPv6.

Пример: в примере показано как настроить работу IP SLA для VPN. В этом примере показано, как тестовый трафик может передаваться в уже существующем VPN-туннеле между двумя конечными точками.

```
(Routing)(config)#ip sla 11
(Routing)(config-ip-sla)#icmp-echo 35.1.10.2
(Routing)(config-ip-sla-echo)#vrf vpn1
```

no vrf (IP SLA)

Используйте эту команду для отмены настройки ранее настроенного соответствия VRF.

Формат: `no vrf`

Режим ввода команд: режим конфигурации IP SLA ICMP ECHO

12.4 Команды очистки

clear ip sla statistics

Используйте эту команду для очистки статистической информации IP SLA для определенной операции IP SLA или всех IP SLA.

Формат: `clear ip sla statistics [operation-number]`

Режим ввода команд: привилегированный

Параметр	*Описание*
operation-number	Номер IP SLA конкретной операции, статистику которой необходимо очистить.

12.5 Команды show

show ip sla configuration

Используйте эту команду в пользовательском или привилегированном режиме, чтобы просмотреть значения конфигурации (включая все значения по умолчанию) для указанной операции IP SLA или для всех операций.

Формат: `show ip sla configuration [operation-number]`

Режим ввода команд: привилегированный

Параметр	*Описание*
operation-number	IP SLA номер конкретной операции, связанной с отображаемой статистикой.

Пример: операции IP SLA ICMP Echo поддерживают адреса IPv4 и IPv6. Пример выходных данных из команды `show ip sla configuration` для различных операций IP SLA в сетях IPv4 и IPv6 показан ниже.

```
(Routing)#show ip sla configura-

tion 3 Entry number: 3
Type of operation: echo
Target       address/Source       address:
1.1.1.1/0.0.0.0 Operation timeout (milli-
seconds): 5000
Vrf     Name:
Schedule:
    Next Scheduled Start Time: Start Time already passed
    Operation frequency (seconds): 60
    Life: Forever
Threshold (milliseconds): 5000
```

В следующем примере показаны выходные данные команды `show ip sla configuration`, когда указанная операция является операцией ICMP Echo в сети IPv6:

```
(Routing)#show ip sla configura-

tion 5 Entry number: 3
Type of operation: echo
Target                  address/Source                  address:
2001:DB8:100::1/2001:0DB8:200::FFFE  Operation  timeout  (milli-
seconds): 5000
Vrf     Name:
Schedule:
    Next Scheduled Start Time: Pending Trigger
    Operation   frequency   (sec-
    onds): 60 Life: Forever
Threshold (milliseconds): 5000
```

show ip sla statistics

Используйте эту команду в пользовательском или привилегированном режиме для просмотра статистики и текущего рабочего состояния указанной операции IP SLA или всех операций.

Формат: `show ip sla statistics [operation-number] [details]`

Режим ввода команд: привилегированный

Параметр	*Описание*
operation-number	Номер операции IP SLA, для которого отображается статистика и рабочее состояние.
details	Включите эту опцию, чтобы отобразить статистику и рабочее состояние более подробно.

Рекомендации по использованию

Эта команда показывает текущее состояние операций IP SLA, в том числе, является ли операция активной, а также данные мониторинга, возвращенные для последней (самой последней выполненной) операции.

Пример:

```
(Routing)# show ip sla statistics details
 Round Trip Time (RTT) for
 Index 1 Type of operation: icmp-
 echo
      Latest RTT: 1 ms
```

```
Latest operation start time: 47 millisec-
onds Latest operation return code: OK
Over thresholds occurred:
FALSE Number of successes:
14
Number of failures: 0  Op-
eration time to live: For-
ever
Operational state of entry: Active
```

show ip route track-table

Эта команда отображает информацию для всех отслеживаемых статических IPv4-маршрутов для данного VRF или VRF по умолчанию.

Формат: `show ip route [vrf vrf-name] track-table`

Режим ввода команд: привилегированный

Параметр	*Описание*
vrf *vrf-name*	Отображает все отслеженные статические маршруты, связанные с конкретным VRF.

Пример:

```
(Routing)#show ip route track-table

ip route 0.0.0.0 0.0.0.0 10.130.167.129 track 10 state is [up]
```

show ipv6 route track-table

Эта команда отображает информацию обо всех отслеживаемых статических IPv6-маршрутах.

Формат: `show ipv6 route track-table`

Режим ввода команд: привилегированный

Пример:

```
(Routing)#show ipv6 route track-table

ipv6 route 2001:B66::/32 4001::1 track 15 state is [up]
```

show ipv6 route track-table

Эта команда отображает информацию обо всех отслеживаемых статических IPv6-маршрутах.

Формат: `show ipv6 route track-table`

Режим ввода команд: привилегированный

show track

Эта команда используется для отображения подробной информации для всех или для конкретного объекта слежения. Также она используется для отображения краткой информации для всех объектов отслеживания или объектов отслеживания, связанных с данной операцией IP SLA.

Формат: `show track [brief | track-number | {ip sla operation-number}]`

Режим ввода команд: привилегированный

Параметр	*Описание*
brief	Отображает краткую информацию для всех отслеживаемых объектов.
track-number	Номер отслеживаемого объекта с подробной информацией для отображения.

ip sla ***operation-number***	Номер операции IP SLA, для которой должна отображаться краткая информация, связанная с объектами отслеживания.

Пример: В следующем примере показана подробная информация для всех отслеживаемых объектов.

```
(Routing)#show track

Track 10
  IP   SLA   1   reachability
  Reachability is Up
    1   change,   last   change
  01:12:36 Delay up 5 secs,
  down 5 secs Latest operation
  return code: OK Latest RTT
  (millisecs) 1500

Track 11
  IP SLA 2 state
  State is Up
    1   change,   last   change
   00:41:55 Delay up 10 secs,
   down 10 secs Latest opera-
   tion return code: OK Latest
   RTT (millisecs) 1000

 Track 13
   IP  SLA  1
   state
   State   is
   Up
     1   change,   last   change
   00:34:08 Delay up 5 secs,
   down 5 secs Latest opera-
   tion return code: OK Latest
   RTT (millisecs) 1500
```

В следующем примере показана подробная информация для отслеживаемого объекта 10.

```
(Routing)#show track 10

Track 10
  IP SLA 1 reacha-
  bility   Reacha-
  bility is Up
    1   change,   last   change
  01:12:36 Delay up 5 secs,
  down 5 secs Latest opera-
  tion return code: OK Latest
  RTT (millisecs) 1500
```

В следующем примере показана краткая информация для всех объектов отслеживания, связанных с операцией IP SLA 1.

```
(Routing)#show track ip sla 1

Track  Object                Parameter      Valu  Last
10     ip sla     1          reachability   Up    01:12:36
```

```
13      ip sla     1            state           Up    00:34:08
```

В следующем примере показана краткая информация для всех отслеживаемых объектов.

```
(Routing)#show track brief

Track  Object                 Parameter      Valu  Last
10     ip sla     1           reachability   Up    01:12:36
11     ip sla     2           state          Up    00:41:55

13     ip sla     1           state          Up    00:34:08
```

13 КОМАНДЫ BGP

В этом разделе описаны команды, используемые для просмотра и настройки протокола BGP, который является протоколом маршрутизации трафика между автономными системами.

Команды в этом разделе делятся на три функциональные группы:

- **Команды просмотра оперативного состояния устройства, которые отображают настройки коммутатора, статистику и другую информацию.**
- **Команды настройки, которые задают характеристики и настройки коммутатора. Для каждой команды настройки существует команда просмотра оперативного состояния устройства, отображающая текущие параметры конфигурации.**
- **Команды очистки частично сбрасывают состояние протокола.**

Параметр	***Описание***
as-number	Номер автономной системы маршрутизатора (ASN). Указывается в диапазоне 1–429496729.

no router bgp

При выполнении команды no router bgp BGP выключается, при этом все конфигурации BGP возвращаются в значения по умолчанию. Можно также использовать команду no enable (BGP) в режиме конфигурирования BGP-маршрутизатора, чтобы глобально выключить BGP без сброса конфигурации.

Значение по умолчанию: BGP неактивен.
Формат: `no router bgp as-number`
Режим ввода команд: глобальная конфигурация

address-family ipv4

Для входа в режим конфигурирования семейства адресов IPv4 VRF и настройки параметров BGR VRF используется команда address-family ipv4 vrf в режиме конфигурирования BGP-маршрутизатора. Команды, вводимые в этом режиме, дают возможность установления соединения с соседними узлами BGP в рамках данного экземпляра VRF. Все команды для настройки соединения с соседним узлом также приведены в этом режиме.

Значение по умолчанию: конфигурация VRF выключена.
Формат: `address-family ipv4 vrf vrf-name`
Режим ввода команд: конфигурирование BGP-маршрутизатора

no address-family ipv4

Используйте no-форму команды, чтобы удалить конфигурацию IPv4 VRF.

Формат: `no address-family ipv4 vrf vrf-name`
Режим ввода команд: конфигурирование BGP-маршрутизатора

address-family ipv6

Для входа в режим конфигурирования семейства адресов IPv6 и указания специальных параметров конфигурации для IPv6 используйте команду address-family ipv6 в режиме конфигурирования BGP-маршрутизатора Команды, введенные в этом режиме, используются для обеспечения обмена IPv6-маршрутами, настройки генерируемых IPv6-префиксов и настройки входящих и исходящих политик, применяемых к IPv6-маршрутам.

Значение по умолчанию: обмен IPv6-маршрутами выключен.

Формат: `address-family ipv6`

Режим ввода команд: конфигурирование BGP-маршрутизатора

no address-family ipv6

Используйте no-форму команды, чтобы удалить конфигурацию семейства адресов IPv6.

Формат: `no address-family ipv6`

Режим ввода команд: конфигурирование BGP-маршрутизатора

address-family vpnv4 unicast

Эта команда входит в режим конфигурирования семейства адресов VPN4 и устанавливает сессию маршрутизации для распространения адресов VPN IPv4 (VPNv4) через магистральную сеть. Если соседний узел iBGP находится в этом режиме, каждый префикс VPNv4 генерируется как глобально уникальный путем добавления 8-байтового параметра Route Distinguisher (RD). В адрес соседнего узла отправляются только одноадресные префиксы.

В режиме конфигурирования семейства адресов VPNv4 доступны следующие команды:

- `neighbor` *`ip-address`* `activate`
- `neighbor` *`ip-address`* `send-community extended`

Для выхода из режима конфигурирования семейства адресов VPNv4 используйте команду exit.

Значение по умолчанию: режим конфигурирования семейства адресов VPNv4 выключен.

Формат: `address-family vpnv4 unicast`

Режим ввода команд: конфигурирование BGP-маршрутизатора

no address-family vpnv4 unicast

Используйте no-форму команды, чтобы удалить конфигурацию, настроенную в этом режиме.

Формат: `no address-family vpnv4 unicast`

Режим ввода команд: конфигурирование BGP-маршрутизатора

aggregate-address

Чтобы настроить агрегированный адрес для BGP, используйте команду aggregate-address в режиме конфигурирования маршрутизатора. По умолчанию агрегированные адреса не настроены. Если дополнительные параметры не указаны, агрегированный адрес анонсируется с атрибутом

ATOMIC_AGGREGATE и пустым значением AS Path. Параллельно с агрегированным адресом анонсируются более конкретные маршруты.

Соответствующими агрегированному адресу считаются более точные префиксы (т. е. префиксы с большей длиной, чем агрегированный адрес). Префикс, равный по длине агрегированному адресу, не считается соответствующим.

Когда BGP формирует агрегированный адрес, одновременно в общей таблице маршрутизации устанавливается маршрут отказа для агрегированного префикса. Любые принятые пакеты, которые соответствуют агрегированному префиксу (и не соответствуют более конкретному маршруту), считаются соответствующими маршруту отказа и отбрасываются.

BGP поддерживает до 128 агрегированных адресов для каждого семейства адресов.

Значение по умолчанию: По умолчанию агрегированные адреса не настроены. Если дополнительные параметры не указаны, агрегированный адрес анонсируется с атрибутом ATOMIC_AGGREGATE и пустым значением AS Path. Параллельно с агрегированным адресом анонсируются более конкретные маршруты.

Формат: `aggregate-address {address mask|`*`ipv6-prefix/pfx-len`*`} [as-set] [summary-only]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
address mask	Агрегированный IPv4-префикс и маска. Маршрут по умолчанию (0.0.0.0 0.0.0.0) не может быть настроен как агрегированный адрес. Маска не может быть 32-битной (255.255.255.255). Сочетание префикса и маски должно являться допустимым одноадресным префиксом адреса назначения.
ipv6-prefix/pfx	Агрегированный IPv6-префикс и длина префикса. Диапазон длины префикса составляет от 1 до 127.
as-set	(Необязательный параметр.) Обычно агрегированный маршрут анонсируется с пустым полем AS Path и атрибутом ATOMIC_AGGREGATE. Если настроен параметр as-set, агрегированный маршрут анонсируется с указанием AS_PATH. Если значение AS_PATH всех объединяемых маршрутов одно и то же, AS_PATH агрегированного маршрута с ним совпадает. Если же объединяемые маршруты имеют различные значения AS_PATH, AS_PATH агрегированного маршрута включает в себя AS_SET с перечислением всех номеров AS, упомянутых в AS_PATH объединяемых маршрутов. Если параметр as-set не задан, агрегированный маршрут анонсируется с пустым полем AS_PATH.
summary-only	(Необязательный параметр.) Когда указан параметр summary-only, более конкретные маршруты в пределах агрегированного адреса не анонсируются соседним узлам.

no aggregate-address

Используйте эту команду, чтобы удалить агрегированный адрес BGP. Параметр address mask представляет собой агрегированный префикс и маску.

Формат: `no aggregate-address address mask`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

bgp aggregate-different-meds

Используйте команду bgp aggregate-different meds, чтобы разрешить объединение маршрутов с различными атрибутами MED. По умолчанию в BGP разрешено объединять только те маршруты, которые имеют одинаковое значение MED, как предписывается стандартом RFC 4271.

При использовании этой команды для активного агрегированного адреса можно анонсировать путь без атрибута MED. Если данная команда не используется и несколько маршрутов объединяются в агрегированный адрес, имея при этом разные атрибуты MED, в агрегированном адресе будет использован MED первого соответствующего маршрута. Любой другой соответствующий префикс с тем же MED включается в агрегированный маршрут. Соответствующие префиксы с другими MED не считаются частью агрегированного маршрута и продолжают анонсироваться в качестве индивидуальных маршрутов.

Значение по умолчанию: все маршруты, объединенные в данном агрегированном адресе, должны иметь одинаковое значение MED.

Формат: bgp aggregate-different-meds

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

no bgp aggregate-different-meds

Используйте команду no bgp aggregate-different meds в режиме конфигурирования BGP-маршрутизатора, чтобы вернуть соответствующие настройки в значение по умолчанию.

Формат: `no bgp aggregate-different-meds`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

bgp always-compare-med

Данная команда используется для настройки сравнения значений MED в процессе принятия решения по маршрутам, полученным из разных AS. MED представляет собой 32-битное целое число, которое обычно устанавливается внешним узлом и указывает внутреннюю дистанцию до целевого узла. В процессе принятия решения значения MED сравниваются, и приоритет отдается маршрутам с более короткой внутренней дистанцией. Поскольку разные AS могут использовать различные метрики внутренней дистанции или иметь различные политики настройки MED, процесс принятия решений обычно не сравнивает значения MED в маршрутах, полученных от узлов из других автономных систем. Эта команда позволяет принудительно включить в BGP сравнение атрибутов MED для маршрутов, полученных из любых AS.

Значение по умолчанию: значения MED сравниваются только для маршрутов, полученных от узлов в той же AS.

Формат: `bgp always-compare-med`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

no bgp always-compare-med

Используйте no-форму команды, чтобы вернуться к режиму по умолчанию, когда значения MED сравниваются только для путей, полученных от соседей в той же AS.

Формат: `no bgp always-compare-med`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

bgp bestpath as-path ignore

Команда bgp bestpath as-path ignore в режиме конфигурирования маршрутизатора позволяет включить игнорирование длины AS-PATH в процессе принятия решения по расчету оптимального пути. Для IPv6-маршрутов эта команда настраивается в режиме конфигурирования семейства адресов IPv6. Чтобы повлиять на вычисление ECMP-маршрутов, требуется настроить параметр AS-PATH.

Значение по умолчанию: длина AS-PATH учитывается в протоколе BGP при расчете оптимального пути.

Формат: `bgp bestpath as-path ignore`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

no bgp bestpath as-path ignore

Используйте no-форму команды, чтобы вернуться к режиму по умолчанию, при котором длина AS-PATH в протоколе BGP не игнорируется.

Формат: `no bgp bestpath as-path ignore`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

bgp client-to-client reflection

По умолчанию Route Reflector отражает маршруты, полученные от одних клиентов, по направлению к другим клиентам. Однако если клиенты Route Reflector обладают полносвязной BGP-топологией (full mesh), отражение маршрутов таким клиентам не выполняется. Команда bgp client-to-client reflection, в зависимости от режима выполнения, включает отражение между клиентами маршрутов IPv4, IPv6 или IPv4 VRF.

Отражение маршрута может повлиять на выбор маршрутов клиентами. Route Reflector отражает только те маршруты, которые были выбраны в качестве оптимальных. На выбор оптимального маршрута к ближайшему BGP-узлу может влиять IGP-метрика маршрута. Поскольку

IGP-дистанция до конкретного ближайшего узла на клиенте может отличаться от IGP-дистанции, переданной Route Reflector, Route Reflector может не выполнять дальнейшее анонсирование маршрута, выбранного клиентом в качестве оптимального в отсутствие сигналов от Route Reflector. Избежать такого эффекта можно, в частности, путем обеспечения полносвязной BGP-топологии на всех клиентах внутри кластера. При наличии полносвязной BGP-топологии у Route Reflector пропадает необходимость отражать маршруты одних клиентов в адрес других клиентов того же кластера. Когда отражение от клиента к клиенту выключено, Route Reflector продолжает отражать маршруты неклиентских узлов клиентам и в обратном направлении.

Значение по умолчанию: если маршрутизатор настроен в качестве Route Reflector, отражение от клиента к клиенту включено.

Формат: `bgp client-to-client reflection`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

no bgp client-to-client reflection

Формат: `no bgp client-to-client reflection`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv6
конфигурирование семейства адресов IPv4 VRF

bgp cluster-id

Используйте команду bgp cluster-id в режиме конфигурирования BGP-маршрутизатора, чтобы указать идентификатор кластера для Route Reflector. Чтобы вернуть идентификатор кластера в значение по умолчанию, используйте no-форму этой команды.

Route Reflector и его клиенты образуют кластер. Поскольку кластер с одним Route Reflector имеет единственную точку отказа, можно настроить кластер с несколькими Route Reflector. Чтобы избежать отправки клиенту нескольких копий маршрута, каждый Route Reflector нужно настроить с указанием одного и того же идентификатора кластера. Используемые Route Reflector с одинаковым идентификатором кластера должны иметь одинаковый набор клиентов, иначе некоторые маршруты могут быть не отражены в адрес отдельных клиентов. Для отражения IPv4- и IPv6-маршрутов используется один и тот же идентификатор кластера.

Значение по умолчанию: Route Reflector без настроенного идентификатора кластера использует вместо него свой идентификатор BGP-маршрутизатора (настроенный командой bgp router-id).

Формат: **`bgp cluster-id`** *`cluster-id`*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
cluster-id	Отличный от нуля 32-битный идентификатор, который идентифицирует кластер Route Reflector и связанных клиентов. Идентификатор кластера может быть введен в формате с точками, как IPv4-адрес, или как целое число.

no bgp cluster-id

Формат: **no bgp cluster-id** *cluster-id*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

bgp default local-preference

Используйте эту команду для указания локального приоритета по умолчанию. Локальный приоритет является атрибутом, отправляемым внутренним узлам для указания уровня приоритета маршрута. Маршрут с более высоким численным значением локального приоритета является предпочтительным.

BGP назначает локальный приоритет по умолчанию для каждого пути, полученного от внешнего узла. (Значения LOCAL_PREF для путей, полученных от внутренних узлов, не меняются.) BGP также назначает локальный приоритет по умолчанию для локально созданных путей. При изменении значения локального приоритета по умолчанию BGP автоматически инициирует программную внутреннюю перезагрузку для всех узлов, чтобы применить новое значение локального приоритета.

Значение по умолчанию: если эта команда не использована, BGP анонсирует внутренним узлам локальный приоритет 100 в сообщениях UPDATE.

Формат: bgp default local-preference *number*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
number	Значение для использования в качестве локального приоритета, анонсируемого на внутренние узлы. Диапазон — от 0 до 4294967295.

no bgp default local-preference

Эта команда устанавливает локальный приоритет BGP-маршрутизатора в значение по умолчанию.

Формат: no bgp default local-preference

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

bgp fast-external-failover

Данная команда настраивает BGP на выполнение немедленного сброса смежности с внешним узлом в случае отказа интерфейса маршрутизации. Когда в BGP поступает событие отказа интерфейса маршрутизации, BGP сбрасывает смежность со всеми внешними узлами, IPv4-адреса которых принадлежат к подсетям неисправного интерфейса. Для определенных интерфейсов такой режим можно перенастроить с помощью команды ip-bgp fast-external-failover.

Значение по умолчанию: режим fast external failover включен.

Формат: bgp fast-external-failover

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

no bgp fast-external-failover

Используйте эту команду, чтобы выключить режим fast-external-failover в BGP.

Формат: `no bgp fast-external-failover`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

bgp fast-internal-failover

Эта команда настраивает BGP на выполнение немедленного сброса смежности с внутренним узлом, если таковой оказывается недоступным. BGP отслеживает доступность каждого внутреннего узла по IP-адресу. Если узел становится недоступным (т. е. в RIB больше не находится путей к IP-адресу узла, отличных от пути по умолчанию), протокол BGP сбрасывает смежность.

Значение по умолчанию: режим fast internal failover включен.

Формат: `bgp fast-internal-failover`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

no bgp fast-internal-failover

Используйте эту команду, чтобы вернуть настройки команды bgp fast-internal-failover в значения по умолчанию.

Формат: `no bgp fast-internal-failover`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

bgp listen

Используйте эту команду, чтобы активировать в IPv4 BGP функцию динамического обнаружения соседей, создать диапазон IPv4- или IPv6-адресов для прослушивания и связать его с указанным шаблоном узла сети.

Используйте значение max-number, чтобы задать глобальное максимальное количество создаваемых динамических соседей IPv4 BGP.

Динамические соседние BGP-узлы настраиваются с использованием диапазона IP-адресов и групп BGP-узлов. Каждый диапазон может быть настроен как IP-адрес подсети. После того как для группы BGP-узлов настроен диапазон подсети и инициирована TCP-сессия для IP-адреса в диапазоне подсети, новый соседний BGP-узел создается динамическим.

Динамически создаваемые соседи не отображаются в текущей конфигурации.

Если имя шаблона узла сети не указано, все создаваемые динамические соседние узлы наследуют параметры по умолчанию. Имя шаблона узла сети для диапазона прослушивания может быть назначено/изменено в любое время.

Максимальное совокупное количество групп для диапазона прослушивания IPv4 и IPv6 равно 10.

Значение по умолчанию: с диапазоном BGP-подсетей прослушивания не связана ни одна подсеть, функция динамического обнаружения BGP-соседей не активна.

Формат: `bgp listen { limit` *`max-number`* `| range` *`network / length`* `[ inherit peer` *`peer-template- name`* `] }`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv6

Параметр	***Описание***
limit ***max-number***	Устанавливает предельное количество BGP-соседей для динамического диапазона подсети IPv4. Выражается числом от 1 до 100. По умолчанию — 20.
range ***network / length***	Указывает диапазон подсетей прослушивания, который должен быть создан. Параметр length — это IP-префикс, который представляет подсеть. Длина маски подсети обозначается в битах. Параметр network — это действительный IPv4-префикс.
inherit peer ***peer-template-name***	(Необязательный параметр.) Указывает имя BGP-шаблона узла сети, который требуется связать с указанным диапазоном подсетей прослушивания, чтобы его параметры наследовались динамически создаваемыми соседями. Шаблон будет наследоваться динамически создаваемыми соседями.

no bgp listen

Используйте эту команду, чтобы выключить в IPv4 BGP функцию динамического обнаружения соседей, удалить диапазон IPv4-адресов для прослушивания и удалить его связь с указанным шаблоном узла сети.

Формат: `no bgp listen { limit | range` *`network / length`* `[ inherit peer` *`peer-template-name`* `] }`

Режим ввода команд: конфигурирование BGP-маршрутизатора

bgp log-neighbor-changes

Используйте эту команду, чтобы включить ведение журнала изменений состояний смежности. В журнале регистрируются прямые и обратные изменения состояний смежности. Прямые изменения состояния, за исключением переходов в состояние Established, регистрируются с уровнем критичности Informational. Обратные изменения и переход в состояние Established регистрируются с уровнем критичности Notice.

Значение по умолчанию: изменения состояний смежности не регистрируются.

Формат: `bgp log-neighbor-changes`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

no bgp log-neighbor-changes

Используйте эту команду, чтобы вернуть настройки команды bgp log-neighbor-changes в значение по умолчанию.

Формат: `no bgp log-neighbor-changes`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

bgp maxas-limit

Команда *bgp maxas-limit* в режиме конфигурирования маршрутизатора позволяет указать ограничение длины для значений AS Path, которые BGP принимает от соседних узлов. Если BGP получает путь, в котором атрибут AS Path длиннее установленного ограничения, BGP отправляет сообщение NOTIFICATION и сбрасывает смежность.

Значение по умолчанию: BGP принимает атрибуты AS Path длиной до 75 номеров AS.

Формат: `bgp maxas-limit` *`number`*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
number	Максимальная длина атрибута AS Path, который может быть принят BGP от любого из соседей. Длина — это количество номеров AS, перечисленных в данном пути. Ограничение может быть установлено как любое число от 1 до 100.

no bgp maxas-limit

Чтобы вернуться в значение по умолчанию, используйте no-форму этой команды.

Формат: `no bgp maxas-limit`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

bgp router-id

Используйте эту команду, чтобы установить идентификатор BGP-маршрутизатора. Значения по умолчанию для идентификатора BGP-маршрутизатора нет. Система не может выбрать идентификатор маршрутизатора автоматически. Его необходимо настроить вручную.

Идентификатор BGP-маршрутизатора должен быть действительным одноадресным IPv4-адресом, не обязательно назначенным данному маршрутизатору. Идентификатор маршрутизатора указывается в формате IP-адреса, разделенном точками. Установка идентификатора маршрутизатора в значение 0.0.0.0 выключает BGP. Изменение существующего идентификатора маршрутизатора приводит к выключению и повторному включению BGP, в результате чего все смежности создаются заново.

Значение по умолчанию: 0.0.0.0

Формат: `bgp router-id router-id`

Режим ввода команд: конфигурирование BGP-маршрутизатора

Параметр	***Описание***
router-id	IPv4-адрес для использования в качестве идентификатора BGP-маршрутизатора.

no bgp router-id

Данная команда сбрасывает идентификатор BGP-маршрутизатора и выключает протокол BGP.

Формат: `no bgp router-id router-id`

Режим ввода команд: конфигурирование BGP-маршрутизатора

default-information originate

Эта команда разрешает BGP создать маршрут по умолчанию (для BGP, IPv4 VRF или IPv6, в зависимости от режима). По умолчанию BGP не создает маршрут по умолчанию. Если маршрут по умолчанию перераспределен в BGP, BGP не анонсирует такой маршрут по умолчанию, пока не будет выполнена команда default-information originate. Опция always по умолчанию выключена.

Значение по умолчанию: BGP не создает маршрут по умолчанию. Опция **always** по умолчанию выключена.

Формат: `default-information originate [always]`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	*Описание*
always	(Необязательный параметр.) Ключевое слово, которое позволяет BGP создавать маршрут по умолчанию, даже если таковой отсутствует в общей таблице маршрутизации.

no default-information originate

Используйте эту команду, чтобы выключить в BGP создание маршрута по умолчанию.

Формат: `no default-information originate`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

default metric

Используйте эту команду, чтобы установить значение атрибута Multi Exit Discriminator (MED) для перераспределенных маршрутов (BGP, IPv4 VRF или IPv6, в зависимости от режима), если в команде redistribute (конфигурирование BGP-маршрутизатора) метрики заданы не были.

Значение по умолчанию: метрики не установлены, в перераспределенные маршруты не включается значение MED.

Формат: `default-metric` *`value`*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	*Описание*
value	Значение для установки в качестве MED. Диапазон — от 1 до 4294967295.

no default metric

Используйте эту команду, чтобы удалить значение по умолчанию для метрики перераспределенных маршрутов.

Формат: `no default-metric`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

distance (конфигурирование BGP-маршрутизатора)

Используйте эту команду для установки приоритета (также называемого «административной дистанцией») для BGP-маршрутов указанных направлений. Можно использовать до 128 экземпляров этой команды. Каждый экземпляр команды должен иметь собственный префикс и маску. Если команда distance выполняется с настройками префикса и маски ранее выполненной аналогичной команды, настройки новой команды заменяют ранее выполненные настройки. Значения префикса и маски из конфигурации различных команд могут перекрываться. Если возникло такое наложение, к маршрутам соседнего узла применяются команды, в которых значения префикса и маски наиболее полно совпадают с адресом данного узла.

Дистанция для ECMP-маршрутов определяется путем применения команды distance к соседнему узлу, который обеспечивает наилучший маршрут.

Команда distance не применяется к существующим маршрутам. Чтобы применить изменения конфигурации к самой команде distance или к используемому в команде списку префиксов, придется выполнить жесткую перезагрузку всех затрагиваемых соседей.

Значение по умолчанию: BGP устанавливает значения приоритета в соответствии с командой distance bgp, пока они не переопределены для конкретных соседей или префиксов данной командой.

Формат: `distance` *`distance`* [*`prefix wildcard-mask`* [*`prefix-list`*]]

Режим ввода команд: конфигурирование BGP-маршрутизатора

Параметр	*Описание*
distance	Значение приоритета для совпадающих маршрутов. Диапазон — от 1 до 255.
prefix wildcard-mask	(Необязательный параметр.) Указанное значение distance присваивается маршрутам, изученным BGP от узлов, адреса которых находятся в пределах этого префикса. Параметр wildcard-mask представляет собой перевернутую маску сети, где 1 бит указывает на незначимую часть префикса.
prefix-list	(Необязательный параметр.) Можно дополнительно определить prefix-list, чтобы ограничить значение дистанции определенным набором префиксов, изученных от соответствующих соседей.

no distance (конфигурирование BGP-маршрутизатора)

Используйте эту команду, чтобы установить предпочтение для BGP-маршрутов в значение по умолчанию.

Формат: `no distance` *`distance`* [*`prefix wildcard-mask`* [*`prefix-list`*]]

Режим ввода команд: конфигурирование BGP-маршрутизатора

distance BGP

Используйте эту команду для установки приоритета (также называемого «административной дистанцией») для BGP-маршрутов. Различные значения дистанции можно настроить для маршрутов, изученных от внешних узлов, изученных от внутренних узлов и локально созданных BGP-маршрутов. Маршрут с более низким значением приоритета будет предпочтительней маршрута к тому же пункту значения с более высоким значением приоритета. Маршруты с приоритетом 255 не могут быть выбраны в качестве оптимальных маршрутов и использованы для переадресации.

Изменение дистанций BGP по умолчанию не влияет на существующие маршруты. Чтобы применить изменение дистанции к существующим маршрутам, необходимо выполнить их принудительное удаление из RIB и повторное изучение. Это можно выполнить за счет перезагрузки узлов, от которых были изучены маршруты, или за счет выключения и повторного включения протокола BGP.

Значение по умолчанию: внешний — 20
внутренний — 200
локальный — 200

Формат: `distance bgp` *`external-distance internal-distance local-distance`*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	***Описание***
external-distance	Значение приоритета для маршрутов, изученных от внешних узлов. Диапазон — от 1 до 255.
internal-distance	Значение приоритета для маршрутов, изученных от внутренних узлов. Диапазон — от 1 до 255.
local-distance	Значение приоритета для локально созданных маршрутов. Диапазон — от 1 до 255.

no distance BGP

Используйте эту команду, чтобы установить в значение по умолчанию приоритеты BGP-маршрутов на маршрутизаторе.

Формат: `no distance bgp`

Режим ввода команд: конфигурирование BGP-маршрутизатора

distribute-list prefix in

Используйте эту команду, чтобы настроить фильтр на основе префикса места назначения для BGP-маршрутов, принимаемых от всех соседних устройств. Список анонсирования применяется ко всем маршрутам, полученным от всех соседей. Однако принимаются только маршруты, разрешенные списком префиксов. Если команда ссылается на несуществующий список префиксов, она принимается, при этом все маршруты считаются разрешенными.

Значение по умолчанию: списки анонсирования не заданы

Формат: `distribute-list prefix` *`list-name`* `in`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
list-name	Список префиксов, используемый для фильтрации всех принимаемых маршрутов на основе префикса места назначения.

no distribute-list prefix in

Эта команда выключает фильтр на основе префикса места назначения для BGP-маршрутов, принимаемых от всех соседних устройств.

Формат: `no distribute-list prefix` *`list-name`* `in`
Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

distribute-list prefix out

Используйте эту команду, чтобы настроить фильтр для анонсируемых маршрутов на основе префикса места назначения. Для каждого источника маршрута (RIP, OSPF, статического, подключенного) может быть выполнен только один экземпляр этой команды. Одним из экземпляров этой команды также может стать глобальный фильтр для исходящих префиксов.

Если команда ссылается на несуществующий список префиксов, она принимается, при этом все маршруты считаются разрешенными.

Если список анонсирования добавляется, изменяется или удаляется для перераспределения маршрутов, BGP автоматически переоценивает все оптимальные маршруты.

Значение по умолчанию: списки анонсирования не заданы

Формат: `distribute-list prefix` *`list-name`* `out [` *`protocol`* `| connected | static ]`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
prefix list-name	Список префиксов, используемых для фильтрации маршрутов, анонсируемых на соседние узлы.
protocol|connected|static	(Необязательный параметр.) При указании источника маршрута список анонсирования применяется к перераспределяемым маршрутам из этого источника. Перераспределяются только маршруты, прошедшие

	список анонсирования. Значение параметра protocol может быть rip или ospf.

no distribute-list prefix out

Используйте эту команду, чтобы сбросить настройки команды distribute-list prefix out в значение по умолчанию.

Формат: `no distribute-list prefix list-name out [ protocol | connected | static]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

enable (BGP)

Эта команда глобально включает BGP, сохраняя при этом конфигурацию. BGP включен по умолчанию, если был указан номер AS с помощью команды router bgp и настроен идентификатор маршрутизатора с помощью команды bgp router-id.

Формат: `enable`

Режим ввода команд: конфигурирование BGP-маршрутизатора

no enable

Данная команда глобально выключает административный режим BGP в системе, сохраняя при этом конфигурацию. При выключении протокола BGP его конфигурация сохраняется. Если выполнить команду *no router bgp*, вся конфигурация BGP сбрасывается к значению по умолчанию.

Если протокол BGP выключен административно, BGP отправляет на каждый узел сообщение Notification с кодом ошибки Cease.

Формат: `no enable`

Режим ввода команд: конфигурирование BGP-маршрутизатора

ip bgp fast-external-failover

Эта команда обеспечивает возможность «щадащей перезагрузки».

Значение по умолчанию: Выключен.

Формат: `bgp graceful-restart [restart-time` *`restart-time`* `|stalepath-time` *`stalepath-time`*`]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

Параметр	***Описание***
Restart-time	Максимальное время в секундах, перед которым должна быть завершена «щадащая перезагрузка» устройства. Период задается в диапазоне от 1 до 3600 секунд. Значение по умолчанию составляет 120 секунд.
Stalepath-time	Максимальное время, в течение которого вспомогательный маршрутизатор сохраняет устаревшие маршруты от перезапуска узла BGP. Период задается в диапазоне от 1 до 3600 секунд. Значение по умолчанию составляет 300 секунд.

no ip bgp fast-external-failover

Эта команда возвращает настройки «щадящей перезагрузки» к значению по умолчанию.

Формат: `no bgp graceful-restart [restart-time` *`restart-time`* `|stalepath-time` *`stalepath-time`*`]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

ip bgp fast-external-failover

Эта команда настраивает режим Fast External Failover для указанного интерфейса маршрутизации.

С помощью этой команды режим Fast External Failover, настроенный глобально, переопределяется для указанного интерфейса маршрутизации. При указании ключевого слова *permit* данный режим включается на указанном интерфейсе независимо от текущей глобальной конфигурации. При указании *deny* данный режим на указанном интерфейсе выключается независимо от текущей глобальной конфигурации.

Значение по умолчанию: Fast External Failover включен глобально. Конфигурация для конкретных интерфейсов отсутствует

Формат: `ip bgp fast-external-failover {permit | deny}`

Режим ввода команд: конфигурирование интерфейса

Параметр	***Описание***
permit	Это ключевое слово включает Fast External Failover на интерфейсе независимо от глобальной конфигурации.
deny	Это ключевое слово выключает Fast External Failover на интерфейсе независимо от глобальной конфигурации.

no ip bgp fast-external-failover

Данная команда выполняет сброс соответствующих настроек на интерфейсе, после чего интерфейс использует глобальные настройки.

Формат: `no ip bgp fast-external-failover`

Режим ввода команд: конфигурирование интерфейса

maximum-paths

Данная команда указывает максимальное количество ближайших узлов, которое BGP может включить в маршруты Equal Cost Multipath (ECMP), выведенные из путей от соседей за пределами локальной автономной системы.

Пути могут учитываться в ECMP, если они обладают одинаковыми атрибутами (такими как локальный приоритет, AS Path, источник, MED, тип узла и IGP-дистанция). Когда BGP использует несколько путей в маршруте ECMP, он все равно выбирает только один путь в качестве оптимального и анонсирует только его на соседние узлы.

Значение по умолчанию: BGP использует один ближайший узел.

Формат: `maximum-paths` *`number-of-paths`*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	*Описание*
number-of-paths	Максимальное количество ближайших узлов в маршруте BGP. Значение — от 1 до 32, если платформа или SDM-шаблон не накладывают дополнительных ограничений на этот диапазон.

no maximum-paths

Команда возвращает максимальное количество ближайших узлов, которое BGP может включить в ECMP-маршруты, в значение по умолчанию.

Формат: `no maximum-paths`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

maximum-paths igbp

Данная команда указывает максимальное количество ближайших узлов, которое BGP может включить в маршруты Equal Cost Multipath (ECMP), выведенные из путей от соседей в пределах локальной автономной системы.

Пути могут учитываться в ECMP, если они обладают одинаковыми атрибутами (такими как локальный приоритет, AS Path, источник, MED, тип узла и IGP-дистанция). Когда BGP использует несколько путей в маршруте ECMP, он все равно выбирает только один путь в качестве оптимального и анонсирует только его на соседние узлы.

Значение по умолчанию: BGP использует один ближайший узел.

Формат: `maximum-paths igbp` *`number-of-paths`*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	*Описание*
number-of-paths	Максимальное количество ближайших узлов в маршруте BGP. Значение — от 1 до 32, если платформа или SDM-шаблон не накладывают дополнительных ограничений на этот диапазон.

no maximum-paths igbp

Данная команда сбрасывает к значению по умолчанию максимальное количество ближайших узлов, которое BGP может включить в маршруты ECMP, выведенные из путей от соседей в пределах локальной автономной системы.

Формат: `no maximum-paths igbp`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

neighbor activate (конфигурирование семейства адресов IPv4 VRF)

Используйте команду neighbor activate, чтобы включить обмен префиксов IPv4 VRF с соседним узлом.

С помощью этой команды в режиме одноадресного вещания семейства адресов vpnv4 локальному BGP-маршрутизатору разрешается отправка префиксов IPv4 VRF в адрес BGP-узла по магистральной сети. В каждый адрес, передаваемый в NLRI, добавляется префикс с 8-байтовым параметром Route Distinguisher (RD).

Если IPv4 VRF включается для соседнего узла, соответствующая смежность сбрасывается и перезапускается, чтобы передать изменения на соседний узел. Рекомендуется полностью настраивать все необходимые политики IPv4-маршрутизации для узла, прежде чем активировать его.

Значение по умолчанию: префиксы VPNv4 на соседний узел не посылаются.

Формат: `neighbor` *`prefix`* `activate`

Режим ввода команд: конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
prefix	IPv4-адрес.

no neighbor activate (конфигурирование семейства адресов IPv4 VRF)

Используйте no-форму команды, чтобы выключить обмен префиксами IPv4 VRF с соседом и отключить карты экспорта для указанного экземпляра VRF.

Формат: `no neighbor` *`prefix`* `activate`

Режим ввода команд: конфигурирование семейства адресов IPv4 VRF

neighbor activate (конфигурирование семейства адресов IPv6)

Чтобы включить обмен IPv6-маршрутами с соседним узлом, используйте команду neighbor activate. В качестве адреса соседнего узла требуется указать тот же IP-адрес, что был использован командой neighbor remote-as при создании узла.

Если IPv6 включается или выключается для соседнего узла, соответствующая смежность сбрасывается и перезапускается, чтобы передать изменения на соседний узел. Рекомендуется полностью настраивать все необходимые политики IPv6-маршрутизации для узла, прежде чем активировать его.

Значение по умолчанию: обмен IPv6-маршрутами выключен.

Формат: `neighbor {`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`*`} activate`

Режим ввода команд: конфигурирование семейства адресов IPv6

Параметр	***Описание***
ipv4-address	IPv4-адрес соседнего узла.
ipv6-address	IPv6-адрес соседнего узла.
interface	Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.

autodetect interface	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.

no neighbor activate

Используйте no-форму команды, чтобы выключить обмен маршрутами IPv6.

Формат: `no neighbor {`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`*`} activate`

Режим ввода команд: конфигурирование семейства адресов IPv6

Параметр	***Описание***
ipv4-address	IPv4-адрес соседнего узла.
ipv6-address	IPv6-адрес соседнего узла.
interface	Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.
autodetect interface	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.

neighbor advertisement-interval

Используйте эту команду, чтобы настроить минимальное время, которое должно пройти между анонсами одного и того же маршрута в адрес указанного соседнего узла. RFC 4271 рекомендует устанавливать для внутренних узлов более короткий интервал, чем для внешних узлов, чтобы включить внутри автономной системы ускоренную конвергенцию. Это значение не ограничивает скорость выбора маршрута и касается только скорости его анонсирования. Если за время ожидания анонсирования BGP изменяет маршрут к месту назначения несколько раз, соседнему узлу анонсируется только последний вариант.

BGP принудительно обеспечивает соблюдение интервала анонсирования путем ограничения того, как часто фаза 3 процесса принятия решения может работать для каждой группы обновлений. Интервал применяется к анонсам удаления в той же степени, как и к активным анонсам.

Значение по умолчанию: 30 секунд для внешних узлов;
5 секунд для внутренних узлов.

Формат: `neighbor` *`ip-address`* `advertisement-interval` *`seconds`*

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	***Описание***
ip-address	IPv4-адрес соседнего узла.
seconds	Минимальное время между анонсами маршрута в секундах. Диапазон — от 0 до 600 секунд.

no neighbor advertisement-interval

Используйте эту команду, чтобы вернуть минимальное время, которое должно пройти между анонсами одного и того же маршрута в адрес указанного соседнего узла, в значение по умолчанию.

Формат: `no neighbor` *`ip-address`* `advertisement-interval`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

neighbor connect-retry-interval

Эта команда настраивает интервал для выполнения попытки повторного подключения к указанному соседнему узлу. Если соседний узел не реагирует на начальную попытку TCP-подключения, коммутатор выполняет три повторных попытки. Первая повторная попытка следует по истечении интервала, настроенного командой neighbor connect-retry-interval. Каждая последующая повторная попытка выполняется после удвоенного предыдущего интервала. Таким образом, по умолчанию TCP-подключение повторяется через 2, 4 и 8 секунд. Если ни одна из попыток не будет успешной, смежность сбрасывается в состояние IDLE и запускается таймер продолжительности этого состояния. Протокол BGP пропускает повторные попытки и сразу переходит в состояние IDLE, если TCP при попытке подключения возвращает ошибку «destination unreachable».

Выполнение этой команды в режиме конфигурирования шаблона узла сети (Peer Template) добавляет эту настройку в шаблон.

Значение по умолчанию: 2 секунды

Формат: `neighbor {ip-address | ipv6-address [interface interface-name] | autodetect interface interface-name} connect-retry-interval retry-time`

Режим ввода команд: конфигурирование BGP-маршрутизатора

Параметр	***Описание***
ip-address	IP-адрес соседнего узла.
ipv6-address [interface *interface-name*]	IPv6-адрес соседнего узла. Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.
autodetect interface interface-name	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
retry-time	Интервал ожидания в секундах для выполнения попытки повторного TCP-подключения к указанному соседнему узлу после сбоя прошлой попытки.

no neighbor connect-retry-interval

Эта команда сбрасывает к значению по умолчанию интервал для выполнения попытки повторного подключения к указанному соседнему узлу.

Формат: `no neighbor ip-address connect-retry-interval`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

neighbor default-originate

Данная команда позволяет настроить протокол BGP так, чтобы он создавал маршрут по умолчанию к соседнему узлу. Используйте необязательный параметр if-default-present, чтобы создавать маршрут по умолчанию к соседнему узлу, только если такой маршрут существует в таблице маршрутизации.

По умолчанию маршрут к конкретному соседнему узлу не имеет MED, а в качестве источника указывается IGP. Атрибуты можно настроить с помощью дополнительной карты маршрута. Соседний узел, настроенный с использованием команды default-originate, помещается в специальную группу обновлений отдельно от соседних узлов, которые не были настроены с использованием этой команды. Как следствие, команда global default-originate не оказывает воздействия на соседние узлы, настроенные с помощью этой команды. Настройки default-originate для определенного соседнего узла, если таковые применены, перезаписывают конфигурацию, созданную командой global default-originate. В результате выполнения этой команды соседнему узлу в анонсе маршрута по умолчанию отправляется значение AS PATH, включающее только AS происхождения маршрута. Использование необязательного параметра if-default-present позволяет создавать маршрут по умолчанию к соседнему узлу, только если такой маршрут существует в таблице маршрутизации. Такая форма команды не устанавливает маршрут по умолчанию в Adj-RIB-Out для настроенной группы узлов (маршрут не будет отражаться в выводе команды show ip bgp neighbor advertised-routes).

Создание маршрута по умолчанию не зависит от фильтрации по префиксу, настроенной с помощью команды distribute-list prefix out.

Карту маршрута можно настроить так, чтобы установленные атрибуты маршрута по умолчанию передавались соседнему узлу. Если карта маршрута включает в себя условие match ip-address, это условие игнорируется. Если карта маршрута включает в себя условия match community или match as-path, маршрут по умолчанию не анонсируется. Если для указанного имени карты маршрута не существует, маршрут по умолчанию не анонсируется.

Значение по умолчанию: маршруты по умолчанию не создаются

Формат: `neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	***Описание***
ip-address	IPv4-адрес соседнего узла.
map-name	(Необязательный параметр.) Карту маршрута можно настроить так, чтобы установленные атрибуты маршрута по умолчанию анонсировали соседнему узлу.

no neighbor default-originate

Используйте эту команду, чтобы выключить в BGP создание маршрута по умолчанию для указанного соседнего узла.

Формат: `no neighbor` *`ip-address`* `default-originate [if-default-present][route-map` *`map-name`*`]`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

neighbor description

Данная команда позволяет создать текстовое описание соседнего узла Описание является информационным и не имеет никакого функционального влияния.

Выполнение этой команды в режиме конфигурирования шаблона узла сети (Peer Template) добавляет эту настройку в шаблон.

Значение по умолчанию: описание не задано

Формат: `neighbor ip-address autodetect interface interface-name description text`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование шаблона узла сети

Параметр	***Описание***
ip-address	IP-адрес соседнего узла.
autodetect interface *interface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
text	Текстовое описание соседнего узла. Допустимая длина — до 80 символов.

no neighbor description

Используйте эту команду, чтобы удалить текстовое описание соседнего узла.

Формат: `no neighbor ip-address autodetect interface interface-name description`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование шаблона узла сети

neighbor ebgp-multihop

Используйте эту команду, чтобы настроить протокол BGP на установление соседства с внешними узлами, не имеющими прямого подключения.

Эта команда действует только для внешних BGP-соседей. Для внутренних BGP-соседей значение TTL остается равно 64 и не может быть изменено. Соседний узел может унаследовать эту конфигурацию из шаблона узла сети. Чтобы конфигурация update-source работала для внешних соседних узлов BGP, параметр ebgp-multihop hop-count должен быть настроен на увеличение значения TTL относительно TTL по умолчанию (1).

Выполнение этой команды в режиме конфигурирования шаблона узла сети (Peer Template) добавляет эту настройку в шаблон.

Значение по умолчанию: 1

Формат: `neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } ebgp-multihop hop-count`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование шаблона узла сети

Параметр	***Описание***
ip-address	IPv4-адрес соседнего узла.
ipv6-address [interface *interface-name*]	IPv6-адрес соседнего узла. Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.
autodetect interface *interface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
ebgp-multihop hop-count	Максимальное количество хопов до соседнего узла. Допустимый диапазон — 1–255.

no neighbor ebgp-multihop

Используйте эту команду для удаления настроенного соседства.

Формат: `no neighbor { ip-address | ipv6-address [ interface interface-name ] | autodetect interface interface-name } ebgp-multihop`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование шаблона узла сети

neighbor filter-list

Данная команда фильтрует входящие и исходящие анонсы указанного соседнего узла на основании их параметра AS Path. Для каждого направления анонсов указанного соседнего узла можно настроить только один список AS Path. Если команда запускается повторно для настроенного узла, новый номер списка AS Path заменяет предыдущий.

Если список фильтров для соседнего узла настроен с указанием несуществующего списка контроля доступа AS Path, фильтруются все маршруты.

Значение по умолчанию: списки фильтрации соседних узлов не настроены.

Формат: `neighbor ip-address filter-list as-path-list-number {in | out}`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
ip-address	IPv4-адрес соседнего узла.
as-path-list-number	Идентификатор списка AS Path.
in	Список AS Path применяется для фильтрации анонсов, принятых от соседнего узла.
out	Список AS Path применяется для фильтрации анонсов, отправляемых в адрес соседнего узла.

no neighbor filter-list

Данная команда удаляет настройки фильтров для соседних узлов.

Формат: `no neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

neighbor filter-list (конфигурирование семейства адресов IPv6)

Эта команда настраивает BGP-фильтр, чтобы применить ACL AS Path к сообщениям UPDATE, полученным от указанного соседнего узла или направленным в его адрес. Фильтрация для IPv6 не зависит от фильтрации, настроенной для IPv4. Если сообщение UPDATE включает в себя как IPv4, так и IPv6 NLRI, оно может быть отфильтровано для IPv4, но принято для IPv6 или наоборот.

Если список фильтров для соседнего узла настроен с указанием несуществующего списка контроля доступа AS Path, фильтруются все маршруты.

Значение по умолчанию: списки фильтрации соседних узлов не настроены.

Формат: `neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Режим ввода команд: конфигурирование семейства адресов IPv6

Параметр	***Описание***
ip-address	IPv6-адрес соседнего узла.
as-path-list-number	Идентификатор списка AS Path.
in	Список AS Path применяется для фильтрации анонсов, принятых от соседнего узла.
out	Список AS Path применяется для фильтрации анонсов, отправляемых в адрес соседнего узла.

no neighbor filter-list (конфигурирование семейства адресов IPv6)

Данная команда удаляет настройки фильтров IPv6 для соседних узлов.

Формат: `no neighbor` *`ip-address`* `filter-list` *`as-path-list-number`* `{in | out}`

Режим ввода команд: конфигурирование семейства адресов IPv6

neighbor inherit peer

Данная команда используется, чтобы настроить на узле BGP наследование конфигурационных параметров из шаблона узла сети. Параметры сессий и политики узла могут быть настроены один раз в шаблоне для наследования несколькими соседними узлами, что устраняет необходимость установки повторяющихся параметров для каждого соседнего узла.

Параметры наследуются из указанного шаблона узла сети, а также из других шаблонов, настройки которых наследует указанный шаблон. Прямое наследование настроек соседнего узла может происходить только из одного шаблона узла сети.

Значение по умолчанию: параметры конфигурации не наследуются.

Формат: neighbor {*ip-address*| *ipv6-address* [interface *interface-name*] autodetect interface *interface-name*} inherit peer *template-name*

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
ip-address	IP-адрес соседнего узла, параметры конфигурации которого наследуются из шаблона.
ipv6-address [interface *interface-name*]	IPv6-адрес соседнего узла. Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.
autodetect interface *interface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
template-name	Имя шаблона узла сети, параметры конфигурации которого должен унаследовать указанный соседний узел.

no neighbor inherit peer

Используйте эту команду, чтобы удалить настройки наследования.

Формат: no neighbor *ip-address* inherit peer *template-name*

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

neighbor local-as

Эта команда позволяет настроить BGP так, чтобы вместо собственной AS маршрутизатора при анонсировании маршрутов в адрес соседних узлов передавалось значение локальной AS. Эта команда разрешена только для внешних BGP-соседей. Соседний узел может унаследовать эту конфигурацию из шаблона узла сети.

Значение по умолчанию: локальная AS на узле не настроена.

Формат: neighbor { *ip-address* | *ipv6-address* [interface *interface-name*] | autodetect interface *interface-name* } local-as *as-number* no-prepend replace-as

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
ip-address	IPv4-адрес соседнего узла.
ipv6-address [interface *interface-name*]	IPv6-адрес соседнего узла. Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.
autodetect interface *interface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
local-as *as-number*	Номер AS для анонсирования в качестве локальной AS в AS PATH, отправляемых соседнему узлу.
no-prepend	Не использовать для локальной AS в AS PATH префикс, полученный в сообщениях UPDATE от соседнего узла.
replace-as	Заменяет собственную AS маршрутизатора номером локальной AS в AS PATH, отправляемых соседнему узлу.

neighbor maximum-prefix (конфигурирование BGP-маршрутизатора)

Эта команда настраивает максимальное количество префиксов, которое BGP может принимать от указанного соседнего узла. Указанное ограничение сравнивается с количеством префиксов, полученных от соседнего узла, включая префиксы, отброшенные на основании политик для входящего трафика. Если сессия между узлами закрыта, смежность не включается до тех пор, пока для соседнего узла не будет выполнена команда clear ip bgp. Соседний узел можно также восстановить с помощью последовательного выполнения команд neighbor shutdown и no neighbor shutdown.

Значение по умолчанию: ограничение префиксов совпадает с максимальным количеством маршрутов, которое можно установить в таблице маршрутизации. Порог предупреждения по умолчанию составляет 75%. Если не настроена опция warning-only, соседний узел, превышающий ограничение, выключается

Формат: `neighbor` *`ip-address`* `maximum-prefix { `*`maximum`*` | unlimited } [`*`threshold`*`] [warning-only]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

Параметр	***Описание***
ip-address	IPv4-адрес соседнего узла.
maximum	Максимальное количество префиксов, которые BGP может принять от указанного соседнего узла. Диапазон значений — от 0 до максимального количества маршрутов, поддерживаемых данным маршрутизатором.
unlimited	Ограничений по количеству префиксов нет.
threshold	(Необязательный параметр.) Когда количество префиксов, получаемых от соседнего узла, превышает этот процент от максимального значения, BGP отправляет системное сообщение. Диапазон составляет от 1 до 100 процентов. Значение по умолчанию составляет 75%.
warning-only	(Необязательный параметр.) При превышении максимального количества префиксов BGP принимает избыточные префиксы и записывает системное сообщение, но не сбрасывает смежность.

no neighbor maximum-prefix

Команда возвращает максимальное количество префиксов, которые BGP принимает от указанного соседнего узла, в значение по умолчанию.

Формат: `no neighbor` *`ip-address`* `maximum-prefix`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

neighbor next-hop-self

Эта команда настраивает BGP так, чтобы при анонсировании маршрутов внутренним узлам атрибут next-hop представлял собой локальный IP-адрес. В общем случае BGP сохраняет атрибут next-hop, полученный от внешнего узла.

Когда атрибут *next-hop* в маршрутах, полученных от внешних узлов, сохраняется, внутренним узлам требуется маршрут к IP-адресу внешнего узла. Обычно это решается путем настройки IGP на пограничном маршрутизаторе для анонсирования внешней (или DMZ) подсети. Опция *next-hop-self* устраняет необходимость анонсировать внешнюю подсеть в IGP.

Значение по умолчанию: не включено

Формат: `neighbor` *`ip-address`* `next-hop-self`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

Параметр	***Описание***
ip-address	IP-адрес соседнего узла.

no neighbor next-hop-self

Эта команда выключает узлы, настроенные в качестве ближайших для локально созданных путей. После выполнения этой команды требуется перезагрузить BGP-узел, чтобы изменения вступили в силу.

Формат: `no neighbor` *`ip-address`* `next-hop-self`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

neighbor password

Используйте эту команду для включения аутентификации MD5 для TCP-сегментов, получаемых от соседних узлов и отправляемых в их адрес, а также настройки ключа аутентификации.

Аутентификация MD5 должна быть включена или выключена на обоих узлах. Для обоих узлов также требуется настроить одинаковый пароль. Когда TCP-соединение установлено, если изменяется пароль на одном конце, пароль на другом конце должен быть изменен соответственно до истечения времени удержания соединения. При значении времени удержания по умолчанию оба пароля должны быть изменены в течение 120 секунд, чтобы соединение не было отброшено.

Выполнение этой команды в режиме конфигурирования шаблона узла сети (Peer Template) добавляет эту настройку в шаблон.

Значение по умолчанию: аутентификация MD5 выключена

Формат: `neighbor {`*`ip-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] |autodetect interface` *`interface-name`*`} password` *`string`*

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

конфигурирование шаблона узла сети

Параметр	*Описание*
ip-address	IP-адрес соседнего узла.
ipv6-address [interface *interface-name*]	IPv6-адрес соседнего узла. Если IPv6-адрес соседнего узла является локальным адресом, то локальный интерфейс также должен быть указан.
autodetect interface i*nterface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
string	Пароль, от 1 до 25 символов с учетом регистра.

no neighbor password

Эта команда выключает проверку аутентификации MD5 для TCP-сегментов, получаемых от соседнего узла и отправляемых в его адрес.

Формат: `neighbor {`*`ip-address`*` | `*`ipv6-address`*` [interface `*`interface-name`*`] |autodetect interface `*`interface-name`*`} password`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

конфигурирование шаблона узла сети

neighbor prefix-list

Данная команда включает фильтрацию анонсов в адрес указанного соседнего узла на основании префикса места назначения каждого маршрута. Для каждого направления анонсов и каждого соседнего узла можно настроить только один список префиксов. При использовании несуществующего списка префиксов все префиксы считаются разрешенными.

Значение по умолчанию: списки префиксов не настроены.

Формат: `neighbor `*`ip-address`*` prefix-list `*`prefix-list-name`*` { in | out }`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

конфигурирование шаблона узла сети

Параметр	*Описание*
ip-address	IP-адрес соседнего узла.
prefix-list-name	Имя списка префиксов.
in	Список префиксов применяется для фильтрации анонсов, принятых от соседнего узла.
out	Список префиксов применяется для фильтрации анонсов, отправленных на соседний узел.

no neighbor prefix-list

Эта команда выключает фильтрацию анонсов в адрес указанного соседнего узла на основании префикса места назначения каждого маршрута.

Формат: `no neighbor` *`ip-address`* `prefix-list` *`prefix-list-name`* `{ in | out }`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

конфигурирование шаблона узла сети

neighbor remote-as

Эта команда настраивает соседний узел и идентифицирует его автономную систему. Номер AS соседнего устройства требуется указать при создании соседнего узла. Настроить можно до 256 соседних узлов. При наследовании шаблона с параметром remote-as происходит автоматическое создание соседнего узла, если тот еще не существует.

Значение по умолчанию: соседние узлы не настроены.

Формат: `neighbor {ip-address | ipv6-address [interface interface-name] |autodetect interface interface-name remote-as as-number`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

Параметр	***Описание***
ip-address	IP-адрес соседнего узла.
ipv6-address [interface *interface-name*]	IPv6-адрес соседнего узла. Если IPv6-адрес соседнего узла является локальным адресом, то локальный интерфейс также должен быть указан.
autodetect interface *interface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
as-number	Номер AS соседнего узла. Диапазон — от 1 до 429496729. Если номер AS такой же, как и у локального маршрутизатора, узел является внутренним. Если нет, узел является внешним. Соседний узел может унаследовать эту конфигурацию из шаблона узла сети.

no neighbor remote-as

Это команда сбрасывает настройки всех соседних узлов.

Формат: `no neighbor {`*`ip-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`* `remote-as`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

neighbor remove-private-as

Используйте эту команду в режиме конфигурирования маршрутизатора, чтобы удалить частные номера AS при анонсировании IPv4-маршрутов на внешние узлы. Чтобы остановить удаление частных номеров AS, используйте no-форму этой команды.

Команда применима только к внешним узлам. Частные номера AS будут удалены или заменены вне зависимости от того, есть ли в оригинальном AS Path открытые номера AS. При анонсировании AS Path на внешний узел этот атрибут всегда включает хотя бы один экземпляр локального номера AS. Таким образом, удаление частных номеров AS никогда не приводит к анонсированию пустого атрибута AS_PATH. Номера AS от 64512 до 65535 включительно считаются частными. Хотя 65535 является зарезервированным ASN и технически не является частью частного диапазона, при удалении или замене частных ASN этот номер рассматривается как частный.

Значение по умолчанию: частные номера AS не удаляются.

Формат: `neighbor` *`ip-address`* `remove-private-as [all replace-as]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

Параметр	***Описание***
ip-address	IP-адрес соседнего узла.
all replace-as	Чтобы сохранить первоначальную длину AS Path, выполняется замена каждого частного номера AS на локальный номер AS. Это необязательный параметр.

no neighbor remove-private-as

Формат: `no neighbor` *`ip-address`* `remove-private-as`

Режим ввода команд: конфигурирование BGP-маршрутизатора

neighbor rfc5549-support

Используйте эту команду, чтобы выборочно включить анонсирование маршрутов IPv4 через ближайший IPv6-узел в адрес внешнего IPv6-узла. Команда может быть применена только к внешним узлам BGP на расстоянии одного хопа.

Значение по умолчанию: поддержка RFC 5549 включена по умолчанию для всех соседних узлов, если в сборке доступен пакет IPv6.

Формат: `neighbor { ` *`ipv6-address`* ` | autodetect interface` *`interface-name`* ` } rfc5549-support`

Режим ввода команд: конфигурирование BGP-маршрутизатора

Параметр	***Описание***
ipv6-address	IPv6-адрес соседнего узла
autodetect interface *interface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.

no neighbor rfc5549-support

Эта команда выключает анонсирование маршрутов IPv4 через ближайшие IPv6-узлы.

Формат: `no neighbor { ipv6-address | autodetect interface interface-name } rfc5549-support`

Режим ввода команд: конфигурирование BGP-маршрутизатора

neighbor route-map

Используйте данную команду в режиме конфигурирования маршрутизатора, чтобы применить карту маршрута к входящим или исходящим маршрутам указанного соседнего узла. Карту маршрута можно использовать для изменения локального приоритета, MED или AS Path маршрута. Маршруты могут быть выбраны для фильтрации или изменения с использованием списка контроля доступа AS Path или списка префиксов.

Значение по умолчанию: карты маршрутов не применяются.

Формат: `neighbor ip-address route-map map-name {in|out}`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

Параметр	***Описание***
ipv6-address	IP-адрес соседнего узла
map-name	Имя используемой карты маршрута.
in|out	К входящим или исходящим маршрутам применяется указанная карта маршрутов.

no neighbor route-map

Данная команда используется, чтобы удалить карту маршрутов.

Формат: `no neighbor ip-address route-map map-name {in|out}`

Режим ввода команд: конфигурирование BGP-маршрутизатора

neighbor route-reflector-client (конфигурирование BGP-маршрутизатора)

Используйте эту команду в режиме конфигурирования BGP-маршрутизатора для настройки внутреннего узла в качестве IP-клиента Route Reflector.

Как правило, маршрутизатор не выполняет повторное анонсирование BGP-маршрутов, полученных от внутреннего узла, на другие внутренние узлы. Если настроить узел в качестве клиента Route Reflector, то этот маршрутизатор будет повторно анонсировать такие маршруты. Маршрутизатор становится Route Reflector, если на нем установлен один или несколько клиентов Route Reflector. Настройка первого клиента Route Reflector автоматически определяет маршрутизатор как Route Reflector.

Если необходимо настроить в кластере несколько экземпляров Route Reflector, нужно настраивать каждый Route Reflector с одинаковым идентификатором кластера. Используйте команду bgp cluster-id для настройки идентификатора кластера.

Внешний узел не может быть настроен в качестве клиента Route Reflector.

При отражении маршрута BGP игнорирует установленные заявления в исходящей карте маршрута, чтобы принимающее устройство не выполняло вычислений маршрутов, которые не согласуются с другими маршрутизаторами в AS.

Значение по умолчанию: узлы не настроены как клиенты Route Reflector

Формат: `neighbor {ip-address} route-reflector-client`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	*Описание*
ip-address	IP-адрес соседнего узла.

no neighbor route-reflector-client

Формат: `no neighbor {ip-address} route-reflector-client`

Режим ввода команд: конфигурирование BGP-маршрутизатора

neighbor send-community

Данная команда настраивает локальный маршрутизатор для отправки атрибутов BGP-сообщества в сообщениях UPDATE на указанный соседний узел.

Значение по умолчанию: атрибуты сообщества соседнему узлу не отправляются

Формат: `neighbor ip-address send-community`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

Параметр	*Описание*
ip-address	IP-адрес соседнего узла.

no neighbor send-community

Используйте команду *no neighbor send-community*, чтобы вернуться к настройкам по умолчанию.

Формат: `no neighbor ip-address send-community`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование семейства адресов IPv4 VRF
конфигурирование семейства адресов IPv6

neighbor send-community extended

Данная команда, выполненная в режиме конфигурирования семейства адресов VPNv4, настраивает локальный маршрутизатор для отправки атрибутов BGP-сообщества в сообщениях UPDATE на указанный соседний узел.

С помощью этой команды в режиме одноадресного вещания семейства адресов vpnv4 локальному BGP-маршрутизатору разрешается отправка расширенных атрибутов BGP-сообщества в адрес BGP-узла по магистральной сети. В качестве адреса соседнего узла требуется указать тот же IP-адрес, что был использован командой *neighbor remote-as* при создании узла.

Значение по умолчанию: расширенные атрибуты сообщества не отправляются

Формат: `neighbor ip-address send-community [extended | both]`

Режим ввода команд: конфигурирование семейства адресов VPNv4

Параметр	***Описание***
ip-address	IPv4-адрес соседнего узла.
[extended | both]	Действует одно из значений. • Значение extended позволяет маршрутизатору отправлять только расширенные атрибуты сообщества. • Значение both позволяет маршрутизатору отправлять и стандартные, и расширенные атрибуты сообщества.

no neighbor send-community extended

Используйте команду *no neighbor send-community extended*, чтобы выключить обмен VPNv4-префиксами с соседним узлом.

Формат: `no neighbor ip-address send-community`

Режим ввода команд: конфигурирование семейства адресов VPNv4

neighbor shutdown

Используйте эту команду, чтобы выключить смежность с указанным соседним узлом. Если на момент выполнения команды смежность активна, сессия отбрасывается, и вся информация по маршруту, изученная от соседнего узла, удаляется.

Если соседний узел выключен, BGP посылает сообщение NOTIFICATION с кодом ошибки Cease. Когда смежность выключается административно, она остается в неактивном состоянии до тех пор, пока вновь не будет включена в административном порядке (с помощью команды no neighbor shutdown).

Выполнение этой команды в режиме конфигурирования шаблона узла сети (Peer Template) добавляет эту настройку в шаблон.

Значение по умолчанию: соседние узлы не выключаются

Формат: `neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface interface-name } shutdown`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

Параметр	***Описание***
ipv4-address|ipv6-address	IPv4 или IPv6-адрес соседнего узла в соединении между двумя узлами.
autodetect interface interface-name	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.

no neighbor shutdown

Эта команда включает BGP-узел в административном порядке.

Формат: no neighbor {*ipv4-address* | *ipv6-address* [interface *interface-name*]| autodetect interface *interface-name* } shutdown

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

neighbor timers

Используйте эту команду для перезаписи глобальных значений таймера и установки таймеров KeepAlive и Hold для указанного соседнего узла. Новые значения не применяются к смежностям, уже находящимся в состоянии ESTABLISHED. Новые таймеры KeepAlive и Hold применяются при следующем формировании смежности.

Выполнение этой команды в режиме конфигурирования шаблона узла сети (Peer Template) добавляет эту настройку в шаблон.

Значение по умолчанию: KeepAlive – 30 с. Hold – 90 с.

Формат: neighbor {*ipv4-address* | *ipv6-address* [interface *interface-name]*| autodetect interface *interface-name* }timers *keepalive holdtime*

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

Параметр	***Описание***
ipv4-address|ipv6-address	IPv4- или IPv6-адрес соседнего узла. Это IP-адрес соединения между двумя узлами. Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.
autodetect interface *interface-name*	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.
keepalive	Время в секундах между пакетами BGP KEEPALIVE, отправляемыми к соседнему узлу сети. Диапазон — от 0 до 65 535 секунд. К интервалу KeepAlive применяются колебания задержки.
holdtime	Интервал в секундах, в течение которого BGP считает соседний узел активным, не получая от него пакетов BGP KEEPALIVE или UPDATE. Если ни один пакет KEEPALIVE не будет получен от соседнего узла по истечении этого интервала, BGP сбрасывает смежность. Если интервал hold установлен как 0, протокол BGP не применяет этот параметр и не отправляет периодические сообщения KEEPALIVE. Диапазон — от 0 до 65 535 секунд.

no neighbor timers

Эта команда возвращает таймеры KeepAlive и Hold на узле в значение по умолчанию. После выполнения этой команды требуется перезагрузить BGP-узел, и тогда изменения вступят в силу.

Формат: no neighbor {*ipv4-address* | *ipv6-address* [interface *interface-name]*| autodetect interface *interface-name* }timers

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

neighbor update-source

Используйте эту команду для настройки протокола BGP на использование указанного IP-адреса в качестве адреса источника для TCP-соединения с соседним узлом. Значение IP-адреса должно представлять собой IP-адрес, настроенный на узле в качестве адреса соседнего узла для данного маршрутизатора.

IP-адрес, используемый в качестве адреса источника в IP-пакетах отправленных к соседнему узлу, должен совпадать с адресом, использованным для настройки локальной системы в качестве соседнего узла для соседнего маршрутизатора. Другими словами, если источник сообщений UPDATE настроен, он должен иметь IP-адрес, совпадающий с адресом, использованным в команде neighbor remote-as для данного узла.

Обычно IP-адрес используют на loopback-интерфейсе, так как этот интерфейс доступен всегда, при условии что поднят хотя бы один интерфейс маршрутизации. Сессия может продолжаться до тех пор, пока loopback-интерфейс остается доступным. Если IP-адрес используется на интерфейсе маршрутизации, сессия закрывается, если выключается этот интерфейс маршрутизации.

Выполнение этой команды в режиме конфигурирования шаблона узла сети (Peer Template) добавляет эту настройку в шаблон.

Значение по умолчанию: если источник не настроен, TCP-соединения используют основной IPv4-адрес на исходящем интерфейсе соседнего узла

Формат: `neighbor {ipv4-address | autodetect interface interface-name } update-source interface`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

Параметр	***Описание***
ipv4-address|ipv6-address	IPv4- или IPv6-адрес соседнего узла. Это IP-адрес соединения между двумя узлами. Если IPv6-адрес соседнего узла является адресом link-local, локальный интерфейс также требуется указать.
autodetect interface *interface-name*	Локальный IPv6-адрес соседнего узла, который будет автоматически определяться на указанном интерфейсе.
update-source interface	Основной IPv4-адрес на интерфейсе использующийся в качестве IP-адреса источника для TCP-соединения с соседним узлом.

no neighbor update-source

Эта команда настраивает BGP на использование основного IPv4-адреса на исходящем интерфейсе для TCP-соединения.

Формат: `no neighbor {ipv4-address | ipv6-address [interface interface-name]| autodetect interface interface-name } update-source`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование шаблона узла сети

network (конфигурирование BGP-маршрутизатора)

Команда настраивает в BGP анонсирование префикса адреса. Префикс анонсируется только в том случае, если общая таблица маршрутизации содержит маршрут другого протокола (не BGP) с тем же префиксом. Этот маршрут может быть подключенным, статическим или динамическим маршрутом другого протокола маршрутизации.

BGP принимает в семейство адресов до 64 сетей. Команда network может указать маршрут по умолчанию (сеть 0.0.0.0, маска 0.0.0.0).

Если для установки атрибутов анонсируемых маршрутов использована карта маршрута, условия match as-path и match community в карте маршрута игнорируются. Условие match ip-address prefix-list в этом контексте применяется. Если в карте маршрута есть такое условие, сеть анонсируется только в том случае, если список префиксов разрешает префикс этой сети. Если карты маршрута с указанным именем не существует, сеть не анонсируется.

Значение по умолчанию: сеть не анонсируется

Формат: `network` *`prefix`* `mask` *`network-mask`* `[route-map` *`rm-name`*`]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

Параметр	***Описание***
prefix	Префикс IPv4-адреса в представлении с точками.
network-mask	Сетевая маска для префикса в представлении с точками (например, 255.255.0.0).
rm-name	(Необязательный параметр.) Для установки атрибутов пути на маршруте может быть использована карта маршрута.

no network (конфигурирование BGP-маршрутизатора)

Эта команда выключает анонсирование префикса адреса в BGP.

Формат: `no network` *`prefix`* `mask` *`network-mask`* `[route-map` *`rm-name`*`]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

rd

Используйте эту команду, чтобы указать Route Distinguisher (RD) для экземпляра VRF, который использован для создания префикса VPNv4. RD создает таблицы маршрутизации и переадресации и указывает Route Distinguisher по умолчанию для VPN. RD добавляется в начале префиксов IPv4, чтобы сделать их глобально уникальными VPNv4-префиксами.

Значение RD может быть следующим.

- Связанным с ASN: состоит из номера автономной системы и произвольного числа.
- Связанным с IP-адресом: состоит из IP-адреса и произвольного числа.
- Связанным с 4-байтовым ASN: состоит из 4-байтового номера автономной системы и произвольного числа.

Значение по умолчанию: VRF не связан ни с каким RD.

Формат: `rd route-distinguisher`

Режим ввода команд: конфигурирование виртуального маршрутизатора

Параметр	*Описание*
route-distinguisher	8-байтовое значение, которое добавляется к префиксу IPv4, чтобы создать префикс VPNv4. Значение RD может быть указано в любом из следующих форматов. • 16-разрядный номер AS: произвольное 32-битное значение (например, 100 :11); • 32-битный IPv4-адрес: произвольное 16-битное значение (например, 10.1.1.1 :22); • 4-байтовый номер AS: произвольное 32-битное значение (например, 66666 :33).

Эта команда действительна только в том случае, если BGP на маршрутизаторе активен. После настройки RD для VRF не может быть изменен или удален. По этой причине данная команда не имеет no-формы

Чтобы изменить настроенное значение RD, удалите VRF (с помощью команды no ip vrf) и перенастройте его.

redistribute (конфигурирование BGP-маршрутизатора)

Эта команда настраивает BGP анонсировать маршруты, полученные без помощи протокола BGP. BGP может перераспределять локальные (подключенные), статические, OSPF- и RIP-маршруты.

Команда distribute-list out также может быть использована для фильтрации перераспределяемых маршрутов на основании префикса. Для фильтрации можно настроить либо карту перераспределения маршрута, либо список анонсирования, но не одновременно.

Маршрут по умолчанию перераспределяется только в случае выполнения команды default-information originate.

Если настроена карта, условия match as-path и match community игнорируются. Если карты маршрута с указанным именем не существует, префиксы не перераспределяются.

Значение по умолчанию: BGP не перераспределяет маршруты. Если BGP перераспределяет маршруты OSPF, он перераспределяет только внутренние маршруты, пока внешние маршруты не указаны с помощью параметра **match**.

Формат: `redistribute {ospf | rip | connected | static} [metric metric-value]`
`[match {internal | external 1 | external 2 | nssa-external 1 | nssa-external 2}] [route-map map-tag]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

Параметр	*Описание*
ospf, rip, connected, static	Источник перераспределяемого маршрута.
metric metric-value	(Необязательный параметр.) Если указана эта опция, BGP анонсирует префикс с атрибутом пути MED, установленным в заданное значение. Если этот параметр не указан, но для BGP настроена метрика по

	умолчанию, MED принимает значение метрики по умолчанию. Если метрика по умолчанию не настроена, префикс анонсируется без атрибута MED.
match	(Необязательный параметр.) При настройке протокола BGP для перераспределения маршрутов OSPF BGP по умолчанию перераспределяет только внутренние маршруты (OSPF-маршруты внутри зоны и между зонами). Используйте опцию match, чтобы настроить BGP дополнительно перераспределять определенные типы внешних маршрутов или чтобы выключить перераспределение внутренних маршрутов OSPF.
route-map map-tag	(Необязательный параметр.) Карта маршрута может быть использована для фильтрации перераспределяемых маршрутов по префиксу места назначения с использованием списка префиксов. Карта маршрута может быть использована для установки атрибутов перераспределяемых маршрутов.

no redistribute (конфигурирование BGP-маршрутизатора)

Эта команда удаляет в BGP настройки перераспределения маршрутов от указанного протокола источника/маршрутизатора. Команда no redistribute opsf match external 1 отзовет только внешние OSPF-маршруты типа 1, внутренние маршруты OSPF по-прежнему будут перераспределяться.

Формат: `no redistribute {ospf | rip | connected | static} [metric` *`metric-value`*`]`
`[match {internal | external 1 | external 2 | nssa-external 1 | nssa external 2}] [route-map` *`map-tag`*`]`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

конфигурирование семейства адресов IPv6

route-target

Используйте эту команду для создания списка экспорта, импорта или обоих операций в отношении расширенных сообществ route-target (RT) для указанного экземпляра VRF. Введите команду route-target один раз для каждого расширенного сообщества route-target. Маршруты, которые изучены и связаны с указанным расширенным сообществом route-target, импортируются во все VRF, настроенные с помощью этого расширенного сообщества в качестве route-target импорта.

Настроенный экспорт RT выполняется в качестве расширенного сообщества в формате MP-BGP для узла eBGP. Значение RT может быть следующим.

- Связанным с ASN: состоит из номера автономной системы и произвольного числа.
- Связанным с IP-адресом: состоит из IP-адреса и произвольного числа.
- Связанным с 4-байтовым ASN: состоит из 4-байтового номера автономной системы и произвольного числа.

Значение по умолчанию: VRF не связан с RT.

Формат: `route-target {export | import | both}` *`rt-ext-comm`*

Режим ввода команд: конфигурирование виртуального маршрутизатора

Параметр	***Описание***
export	Экспортирует маршрутную информацию в расширенное сообщество

	целевой VPN.
import	Импортирует маршрутную информацию из расширенного сообщества целевой VPN.
both	Экспортирует маршрутную информацию из расширенного сообщества целевой VPN и импортирует ее в это сообщество.
rt-ext-comm	Атрибуты расширенного сообщества route-target, которые будут добавлены в список импорта, экспорта или обоих операций расширенных сообществ. Атрибут route-target указывает расширенное сообщество целевой VPN. Подобно параметру Route Distinguisher, расширенное сообщество route-target может быть определено в любом из следующих форматов. • 16-разрядный номер AS: произвольное 32-битное значение (например, 100 :11); • 32-битный IPv4-адрес: произвольное 16-битное значение (например, 10.1.1.1 :22); • 4-байтовый номер AS: произвольное 32-битное значение (например, 66666 :33).

Эта команда действительна только в том случае, если BGP на маршрутизаторе активен. После настройки RD для VRF не может быть изменен или удален. По этой причине данная команда не имеет no-формы.

Чтобы изменить настроенное значение RD, удалите VRF (с помощью команды no ip vrf) и перенастройте его.

Эта команда действительна только в том случае, если BGP на маршрутизаторе активен.

no route-target

Эта команда удаляет *route-target*, указанный для экземпляра VRF.

Формат: `no route-target {export | import | both} rt-ext-comm`

Режим ввода команд: конфигурирование виртуального маршрутизатора

template peer

Чтобы создать в BGP шаблон узла сети (Peer Template) и войти в режим конфигурирования этого шаблона, используйте команду template peer в режиме конфигурирования маршрутизатора. Шаблон узла сети можно настроить с параметрами, которые применимы ко многим узлам. После этого можно настроить соседние узлы так, чтобы они наследовали параметры указанного шаблона. Шаблон узла сети может включать в себя как параметры сессии, так и политики для узла. Политики узлов настраиваются в режиме конфигурирования семейства адресов и применяются только к указанному семейству адресов. Можно настроить до 32 шаблонов узла. При внесении изменений в шаблон эти изменения немедленно применяются ко всем соседним узлам, которые наследуют параметры от шаблона (при этом изменения политик применяются с трехминутной задержкой).

Команда *remote-as as-number* не поддерживается в режиме конфигурирования шаблона узла сети. Номер AS соседнего устройства требуется указать при создании соседнего узла.

Значение по умолчанию: шаблон узла сети не настроен.

Формат: `template peer name`

Режим ввода команд: конфигурирование BGP-маршрутизатора

Параметр	*Описание*
name	Имя шаблона. Может содержать не более 32 символов.

no template peer

Используйте **no**-форму команды, чтобы удалить шаблон узла сети.

Формат: `no template peer name`

Режим ввода команд: конфигурирование BGP-маршрутизатора

Параметр	*Описание*
name	Имя шаблона. Может содержать не более 32 символов.

address-family

Используйте команду *address-family* в режиме конфигурирования шаблона узла сети, чтобы настроить в шаблоне параметры политики, которая должна применяться к конкретному семейству адресов. Эта команда выполняет вход в режим конфигурирования семейства адресов в рамках шаблона узла сети. Команды политики, настроенные в этом режиме, применяются к семейству адресов. Ниже перечислены команды, которые могут быть добавлены в шаблон узла сети в режиме конфигурирования семейства адресов.

- activate
- advertisement-interval seconds
- default-originate
- filter-list as-path-list-number {in | out}
- maximum-prefix {maximum | unlimited} [threshold]
- next-hop-self
- prefix-list prefix-list-name {in | out}
- remove-private-as [all replace-as]
- route-map map-name {in | out}
- route-reflector-client
- send-community

Формат: `address-family {ipv4 vrf|ipv6} vrf`

Режим ввода команд: привилегированный

Параметр	*Описание*
ipv4	Настраивает параметры политики, которые будут применяться к IPv4-маршрутам.
Ipv6	Настраивает параметры политики, которые будут применяться к IPv6-маршрутам.

no address-family

Для удаления всех команд политики для семейства адресов в шаблоне узла сети используйте no-форму команды.

Формат: `no address-family {ipv4|ipv6}`

Режим ввода команд: привилегированный

Параметр	***Описание***
ipv4	Настраивает параметры политики, которые будут применяться к IPv4-маршрутам.
Ipv6	Настраивает параметры политики, которые будут применяться к IPv6-маршрутам.

activate

Используйте эту команду в режиме конфигурирования шаблона узла сети для активации обмена IPv6-маршрутами.

Формат: `activate`

Режим ввода команд: конфигурирование семейства адресов IPv6

connect-retry-interval

Используйте эту команду в режиме конфигурирования шаблона узла сети, чтобы добавить эту команду в шаблон и настроить интервал повторного подключения. Если соседний узел не реагирует на начальную попытку TCP-подключения, выполняется три повторных попытки. Первая повторная попытка выполняется по истечении интервала повторной попытки, настроенного с помощью команды neighbor connect-retry-interval (конфигурирование BGP-маршрутизатора). Каждая последующая повторная попытка выполняется после удвоенного предыдущего интервала. Таким образом, по умолчанию TCP-подключение повторяется через 2, 4 и 8 секунд. Если ни одна из попыток не будет успешной, смежность сбрасывается в состояние IDLE и запускается таймер продолжительности этого состояния. Протокол BGP пропускает повторные попытки и сразу переходит в состояние IDLE, если TCP при попытке подключения возвращает ошибку «destination unreachable».

Значение по умолчанию: 2 секунды

Формат: `connect-retry-interval` *`retry-time`*

Режим ввода команд: конфигурирование шаблона узла сети

Параметр	***Описание***
retry-time	Интервал ожидания в секундах для выполнения попытки повторного TCP-подключения в указанному соседнему узлу после сбоя прошлой попытки.

no connect-retry-interval

Эта команда сбрасывает к значению по умолчанию интервал для выполнения попытки повторного подключения в шаблоне узла сети.

Формат: `no connect-retry-interval`

Режим ввода команд: конфигурирование шаблона узла сети

description

Данная команда в режиме конфигурирования шаблона узла сети позволяет добавить команду в шаблон и настроить текстовое описание соседнего узла. Описание является информационным и не имеет никакого функционального влияния.

Значение по умолчанию: описание не задано.

Формат: `description` *`text`*

Режим ввода команд: конфигурирование шаблона узла сети

Параметр	***Описание***
text	Текстовое описание соседнего узла. Допустимая длина — до 80 символов.

no description

Используйте эту команду, чтобы удалить текстовое описание соседнего узла из шаблона узла сети.

Формат: `no description`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование шаблона узла сети

password

Применение этой команды в режиме конфигурирования шаблона узла сети добавляет в шаблон настройку TCP-пароля.

Значение по умолчанию: аутентификация MD5 выключена.

Формат: `password` *`string`*

Режим ввода команд: конфигурирование шаблона узла сети

Параметр	***Описание***
string	Пароль, от 1 до 25 символов с учетом регистра.

no password

Эта команда выключает TCP-пароль в шаблоне узла сети.

Формат: `no password`

Режим ввода команд: конфигурирование шаблона узла сети

shutdown

Используйте эту команду в режиме конфигурирования шаблона узла сети для настройки административного статуса в шаблоне.

Значение по умолчанию: соседние узлы не выключаются.

Формат: `shutdown`

Режим ввода команд: конфигурирование шаблона узла сети

no shutdown

Эта команда позволяет административно включить BGP в шаблоне узла сети.

Формат: `no shutdown`

Режим ввода команд: конфигурирование BGP-маршрутизатора
конфигурирование шаблона узла сети

timers

Используйте эту команду в режиме конфигурирования шаблона узла сети, чтобы настроить таймеры KeepAlive и Hold в шаблоне.

Значение по умолчанию: таймеры KeepAlive и Hold настроены глобально в значения по умолчанию с помощью команды address- family.

Формат: `timers keepalive holdtime`

Режим ввода команд: конфигурирование шаблона узла сети

Параметр	*Описание*
keepalive	Время в секундах между пакетами BGP KEEPALIVE, отправляемыми к соседнему узлу сети. Диапазон — от 0 до 65535 секунд. К интервалу KeepAlive применяются колебания задержки.
holdtime	Интервал в секундах, в течение которого BGP считает соседний узел активным, не получая от него пакетов BGP KEEPALIVE или UPDATE. Если ни один пакет KEEPALIVE не будет получен от соседнего узла по истечении этого интервала, BGP отбрасывает смежность. Если интервал hold установлен как 0, протокол BGP не применяет этот параметр и не отправляет периодические сообщения KEEPALIVE. Диапазон — от 0 до 65535 секунд.

no timers

Эта команда возвращает таймеры KeepAlive и Hold в шаблоне узла сети в значение по умолчанию. После выполнения этой команды требуется перезагрузить BGP-узел, и тогда изменения вступят в силу.

Формат: `no timers`

Режим ввода команд: конфигурирование шаблона узла сети

update-source

Используйте эту команду в режиме конфигурирования шаблона узла сети для настройки шаблона на использование указанного IP-адреса в качестве адреса источника для TCP-соединения с соседним узлом. Значение IP-адреса должно представлять собой IP-адрес, настроенный на узле в качестве адреса соседнего узла для данного маршрутизатора.

Значение по умолчанию: если источник не настроен, TCP-соединения используют основной IPv4-адрес на исходящем интерфейсе соседнего узла.

Формат: `update-source {unit/slot/port | vlan id}`

Режим ввода команд: конфигурирование шаблона узла сети

Параметр	*Описание*
update-source interface	Основной IPv4-адрес на интерфейсе используется в качестве IP-адреса

	источника для TCP-соединения с соседним узлом.

no update-source

Эта команда настраивает шаблон узла сети на использование основного IPv4-адреса на исходящем интерфейсе для TCP-соединения.

Формат: `no update-source`

Режим ввода команд: конфигурирование шаблона узла сети

timers bgp

Эта команда настраивает значения KeepAlive и Hold, которые BGP использует для всех соседних узлов.

Если BGP устанавливает смежность, соседние узлы соглашаются использовать минимальное время Hold, настроенное для любого из узлов. BGP посылает сообщения KEEPALIVE с интервалами, равными 1/3 согласованного времени Hold, или с настроенным интервалом KeepAlive, выбирая из этих значений меньшее.

Новые значения не применяются к смежностям, уже находящимся в состоянии ESTABLISHED. Новые таймеры KeepAlive и Hold применяются при следующем формировании смежности.

Значение по умолчанию: Интервал KeepAlive составляет 30 секунд. Интервал Hold составляет 90 секунд.

Формат: `timers bgp keepalive holdtime`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
update-source interface	Время в секундах между пакетами BGP KEEPALIVE, отправляемыми к соседнему узлу сети. Диапазон — от 0 до 65535 секунд. К интервалу KeepAlive применяются колебания задержки.
holdtime	Интервал в секундах, в течение которого BGP считает соседний узел активным, не получая от него пакетов BGP KEEPALIVE или UPDATE. Если ни один пакет KEEPALIVE не будет получен от соседнего узла по истечении этого интервала, BGP отбрасывает смежность. Если интервал hold установлен как 0, протокол BGP не применяет этот параметр и не отправляет периодические сообщения KEEPALIVE. Диапазон — от 0 до 65535 секунд.

no timers bgp

Эта команда возвращает интервалы KeepAlive и Hold, которые BGP использует для всех соседних узлов, в значения по умолчанию.

Формат: `no timers bgp`

Режим ввода команд: конфигурирование BGP-маршрутизатора

timers policy-apply delay

Эта команда настраивает задержку применения для изменений, внесенных в глобальные политики или во входящие/исходящие политики конкретных BGP-узлов.

Каждый раз, когда пользователь вносит изменения в политики (route-maps/prefix-lists/as-path-lists) или атрибуты соседних узлов, такие как send-community, remove private-asn и т. д., политика применяется после установленного интервала задержки. Каждый раз, когда пользователь настраивает интервал задержки, для политик, ожидающих изменения, если таковые имеются, применяется новая задержка, если предыдущий интервал задержки еще не истек. Интервал задержки со значением 0 секунд означает, что изменения применяются немедленно.

При изменениях в исходящих политиках, которые требуется применить к соседним узлам, отправляются пакеты WITHDRAW, а затем, когда задержка истекла и изменения применены, — пакеты UPDATE. В случае внесения изменений в такие атрибуты соседних узлов, как send-community, remove-private-asn и т. д., пакеты WITHDRAW не отправляются, вместо этого по истечении интервала задержки отправляются новые значения в пакетах UPDATE.

Значение по умолчанию: интервал задержки — 180 секунд.

Формат: `timers policy-apply delay` *`delay`*

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

Параметр	***Описание***
delay	Интервал в секундах, по истечении которого применяются глобальные политики или политики для соседних узлов. Диапазон — от 0 до 180 секунд.

no timers policy-apply delay

Данная команда устанавливает задержку применения для изменений, внесенных в глобальные политики или во входящие/исходящие политики конкретных BGP-узлов, в значение по умолчанию.

Формат: `no timers policy-apply delay`

Режим ввода команд: конфигурирование BGP-маршрутизатора

конфигурирование семейства адресов IPv4 VRF

clear ip bgp

Эта команда сбрасывает сессии между узлами, относящимися к указанной подсети, или между всеми узлами. Параметры команды указывают, какие сеансы сбрасываются и какой тип сброса выполняется. Сброс типа soft inbound приводит к тому, что BGP отправляет запрос Route Refresh в адрес каждого сбрасываемого узла. Если соседний узел не поддерживает Route Refresh, обновленная политика применяется к маршрутам, ранее полученным от этого соседнего узла.

При внесении изменений в исходящую политику BGP назначает сброс типа soft outbound для обновления соседних узлов в соответствии с новой политикой. Использование параметра interface указывает, что изменения применяются к указанному порту или VLAN.

Эта команда применяется к маршрутам для всех семейств адресов.

Формат: `clear ip bgp [vrf vrf-name] {* | as-number | ipv4-address | ipv6-address [interface interface-name] | interface inter-face-name | [listen range network/length ]} [soft [in | out]`

Режим ввода команд: привилегированный

Параметр	*Описание*
vrf-name	Имя экземпляра VRF.
*****	Сбрасывает смежность с каждым BGP-узлом.
as-number	Сбрасывает смежность только с BGP-узлами в указанной автономной системе.
ipv4-address	Сбрасывает смежность с одним узлом сети, указанным с помощью IPv4-адреса.
ipv6-address	Сбрасывает смежность с одним узлом сети, указанным с помощью IPv6-адреса. Смежность, которая формируется с функцией AUTODETECT, не может быть сброшена с помощью данной команды.
interface	Сброс смежности только на указанном интерфейсе. Смежность должна быть сформирована с помощью IPv6 link-local или с помощью функции auto detect.
listen range	Сбрасывает все смежности, которые включены в диапазон сети прослушивания.
soft	(Необязательный параметр.) По умолчанию смежности сбрасываются, а затем восстанавливаются. Если указано ключевое слово soft, BGP повторно отправляет к соседним узлам сообщения UPDATE и повторно обрабатывает сообщения UPDATE от них.
in | out	(Необязательный параметр.) Если задано ключевое слово in, повторно обрабатываются сообщения UPDATE от соседнего узла сети. Если задано ключевое слово out, выполняется повторная отправка сообщения UPDATE к соседнему узлу. Если ни одно ключевое слово не задано, сообщения UPDATE повторно обрабатываются в обоих направлениях.

clear ip bgp counters

Эта команда сбрасывает все счетчики BGP до 0. В число счетчиков входят счетчики отправленных и принятых пакетов, а также счетчики префиксов для всех соседних узлов.

Формат: `clear ip bgp [vrf vrf-name] counters`

Режим ввода команд: привилегированный

debug ip bgp

Чтобы включить трассировку отладки событий BGP, используйте команду debug ip bgp в привилегированном режиме. Сообщения отладки отправляются в системный журнал с уровнем критичности DEBUG. Чтобы отобразить их в консоли, включите ведение журналов в консоли для уровня DEBUG (команда logging console debug).

Опции отладки для конкретного соединения являются объединением опций, включенных глобально, и опций, включенных для данного соединения.

Включение одной из опций типа пакета включает пакетную трассировку во входящем и в исходящем направлении.

Значение по умолчанию: трассировка отладки не включена.

Формат: `debug ip bgp [ peer-address | events | keepalives | notification | open | refresh | updates ]`

Режим ввода команд: привилегированный

Параметр	*Описание*
peer-address	IPv4- или IPv6-адрес BGP-узла. Когда эта опция задана, отслеживание отладки включается для определенного узла. Команда может быть выполнена многократно, чтобы включить одновременную трассировку для нескольких узлов (необязательный параметр).
events	Включает отслеживание событий статуса смежности (необязательный параметр).
keepalives	Отслеживание передачи и получения пакетов KEEPALIVE (необязательный параметр).
notification	Отслеживание передачи и получения пакетов NOTIFICATION (необязательный параметр).
open	Отслеживание передачи и получения пакетов OPEN (необязательный параметр).
refresh	Отслеживание передачи и получения пакетов ROUTE REFRESH (необязательный параметр).
updates	Отслеживание передачи и получения пакетов UPDATE (необязательный параметр).

show ip bgp

Используйте команду show ip bgp в привилегированном режиме для просмотра маршрутов в таблице маршрутизации BGP. Вывод команды отображает оптимальные и неоптимальные пути к каждому месту назначения. Если указан экземпляр VRF, отображаются IPv4-маршруты в таблице маршрутизации BGP для этого экземпляра VRF.

Формат: `show ip bgp [vrf vrf-name] [network/pfx-len [ longer-prefixes | shorter-prefixes [length] ] | filter-list as-path-list| prefix-list pfx-list-name]`

Режим ввода команд: привилегированный

Параметр	*Описание*
network/pfx-len	Отображает указанный маршрут, идентифицированный префиксом места назначения (необязательный параметр).
longer-prefixes	Используется с опцией network/pfx-len, чтобы отобразить маршруты, длина префикса которых равна или больше указанного pfx-len. Этот параметр не может использоваться, если задана опция shorter-prefixes (необязательный параметр).
shorter-prefixes [length]	Используется с опцией network/pfx-len, чтобы отобразить маршруты, длина префикса которого меньше указанного pfx-len и, необязательно, больше указанной длины (необязательный параметр). Этот параметр не может использоваться, если задана опция longer-prefixes.
filter-list as-path	Фильтрует вывод команды, отображая маршруты, которые соответствуют указанному списку AS Path (необязательный параметр). Этот параметр не может использоваться, если задана опция network/pfx-len или prefix list.
pfx-list-name	Фильтрует вывод команды, отображая маршруты, которые соответствуют заданному списку префиксов (необязательный параметр). Этот параметр не может использоваться, если задана опция

	network/pfx-len или prefix list.

Вывод команды отображает следующую информацию.

Параметр	*Описание*
BGP table version	Каждый раз, когда фаза 2 процесса принятия решений BGP работает над выбором новых маршрутов BGP, это значение увеличивается.
Status codes	• s — маршрут объединен в агрегированный адрес, настроенный с опцией summary-only; • * — BGP никогда не отображает неверные маршруты; так что этот код отображается всегда; • > — указывает, что BGP выбрал этот путь как оптимальный путь к месту назначения; • i — маршрут изучен от внутреннего узла.
Network	Префикс места назначения.
Next Hop	Ближайший BGP-узел маршрута.
Metric	Атрибут Multi Exit Discriminator.
LocPrf	Локальный приоритет.
Path	AS Path.

Если команда задана с опцией network/pfx-len и без каких-либо других опций, формат вывода перечисляет больше информации об индивидуальном префиксе. Оптимальный маршрут всегда первый в списке, далее следуют неоптимальные маршруты. Ввод команды отображает только атрибуты, включенные в каждый путь.

Параметр	*Описание*
Prefix/Prefix Length	Префикс места назначения и длина префикса.
Generation ID	Версия таблицы BGP-маршрутизации на момент последнего изменения маршрута.
Forwarding	Используется ли этот BGP-маршрут для переадресации.
Advertised To Update Groups	Исходящие группы анонсирования, в адрес которых передается маршрут.
Local Preference	Локальный приоритет, либо полученный от узла, либо установленный в соответствии с локальной политикой.
AS Path	AS Path. Эта форма команды show ip bgp отображает AS Path такой длины, какая разрешена в рамках maxas-limit в BGP.
Origin	Значение атрибута ORIGIN.
Metric	Значение атрибута MED, если он включен.
Type	Получен ли путь от внутреннего или внешнего узла.
IGP Cost	Внутренняя стоимость пограничного шлюза (например, стоимость OSPF) к ближайшему BGP-узлу.
Peer (Peer ID)	IP-адрес узла, который отправил этот маршрут, и его идентификатор маршрутизатора.
BGP Next Hop	Атрибут BGP NEXT HOP.
Atomic Aggregate	Показывает, связан ли с путем атрибут ATOMIC AGGREGATE.
Aggregator	Номер AS и идентификатор маршрутизатора инициатора объединения маршрута.
Communities	BGP-сообщества, связанные с путем.

Originator	Если атрибут ORIGINATOR связан с путем, отображается значение этого атрибута.
Cluster List	Если атрибут CLUSTER_LIST связан с путем, отображается последовательность идентификаторов кластера в списке кластеров.

show ip bgp aggregate-address

Эта команда выводит список настроенных агрегированных адресов и показывает, является ли каждый из них активным. Если указан VRF, отображаются агрегированные адреса, настроенные в этом экземпляре VRF.

Формат: `show ip bgp [vrf vrf-name] aggregate-address`

Режим ввода команд: привилегированный

Параметр	***Описание***
Prefix/Len	Префикс места назначения и длина префикс.
AS Set	Показывает, анонсируется ли с агрегированным адресом пустой AS Path (N) или AS SET анонсируется с набором номеров AS, относящихся ко всем путям в агрегированном адресе (Y).
Summary Only	Показывает, подавляются (Y) или анонсируются (N) отдельные сети.
Active	Показывает, анонсируется ли в настоящее время данный агрегированный адрес.

show ip bgp community

Эта команда показывает маршруты BGP IPv4, которые принадлежат к указанному набору сообществ.

Формат: `show ip bgp [vrf vrf-name] community communities [exact-match]`

Параметр	***Описание***
vrf-name	(Необязательный параметр.) Показывает маршруты, принадлежащие к сообществам, в пределах экземпляра VRF.
communities	Строка из нуля или более значений сообществ, которые могут быть в любом формате и могут содержать хорошо известные ключевые слова сообществ no-advertise и no-export. Вывод команды отображает маршруты, которые принадлежат ко всем сообществам, указанным в команде.
exact-match	(Необязательный параметр.) Отображаются только те маршруты, которые являются членами только тех сообществ, которые были указаны в команде.

show ip bgp community-list

Данная команда отображает IPv4-маршруты, которые соответствуют списку сообществ. Описание формата вывода и полей аналогичны тем, что приведены в команде show ip bgp.

Формат: `show ip bgp [vrf vrf-name] community communities [exact-match]`

Режим ввода команд: привилегированный

Параметр	***Описание***

vrf-name	(Необязательный параметр.) Показывает маршруты, принадлежащие к сообществам, в пределах экземпляра VRF.
name	Имя стандартного списка сообществ.
exact-match	(Необязательный параметр.) Отображаются только те маршруты, которые являются членами только тех сообществ, которые были указаны в списке сообществ.

show ip bgp extcommunity-list

Эта команда отображает все атрибуты разрешений и запретов для указанного расширенного списка сообщества. Если указан параметр list-name, в выводе отображаются атрибуты, которые соответствуют данному list-name; в противном случае отображаются все списки.

Формат: `show ip bgp extcommunity-list [list-name]`

Режим ввода команд: привилегированный

Параметр	***Описание***
list-name	Стандартное имя расширенного списка.

Вывод команды отображает следующую информацию.

Параметр	***Описание***
Standard extended community-list	Стандартное имя расширенного списка сообществ.
permit	Разрешает доступ к условиям совпадения. После того, как значение permit было настроено для заданного набора расширенных сообществ, для всех остальных значений расширенный список сообществ по умолчанию подразумевает отказ.
RT	Атрибут route-target расширенного сообщества.
deny	Запрещает доступ к условиям совпадения.

show ip bgp listen range

Данная команда отображает информацию о диапазоне подсетей прослушивания IPv4 BGP. Если указан параметр *network/length*, сведения отображаются в указанном диапазоне прослушивания.

Формат: `show ip bgp [network/length]`

Режим ввода команд: привилегированный

show ip bgp neighbors

Эта команда отображает подробную информацию о конфигурации соседнего BGP-узла и его статусе. Если соседний узел настроен наследовать параметры конфигурации из шаблона узла сети, вывод команды отображает наследуемые значения.

Формат: `show ip bgp [vrf vrf-name] neighbors [neighbor-address]`

Режим ввода команд: привилегированный

Параметр	***Описание***

vrf-name	(Необязательный параметр.) Показывает соседние узлы, принадлежащие к сообществам в рамках экземпляра VRF.
neighbor-address	(Необязательный параметр.) IP-адрес соседнего узла. Используется для ограничения вывода команды одним узлом.

Вывод команды отображает следующую информацию.

Параметр	***Описание***
Description	Текстовая строка, назначенная с помощью команды neighbor description (конфигурирование BGP-маршрутизатора). Эта строка появляется, только если описание настроено.
Remote Address	IP-адрес соседнего узла.
Remote AS	Номер автономной системы соседнего узла
BFD Enabled to Detect Fast Fallover	Указывает, включен ли BFD для соседних узлов.
Peer ID	Идентификатор маршрутизатора соседнего BGP-узла.
Peer Admin Status	START или STOP.
Peer State	Статус смежности для соседнего узла.
Peer Type	Если соседний узел был создан с использованием функции BGP dynamic neighbors, отображается Dynamic.
Listen Range	Если соседний узел был создан с использованием функции BGP dynamic neighbors, отображается диапазон прослушивания, к которому принадлежит соседний узел.
Local Interface Address	IPv4-адрес, используемый в качестве IP-адреса источника в пакетах, отправляемых к этому соседнему узлу.
Local Port	Номер TCP-порта на локальном конце соединения.
Remote Port	Номер TCP-порта на удаленном конце соединения.
Connection Retry Interval	Интервал ожидания BGP между повторными попытками подключения.
Neighbor Capabilities	Дополнительные возможности, о которых сообщил соседний узел и которые были признаны и приняты этим маршрутизатором. Коды, перечисленные в выводе команды. • MP: многопротокольный узел; • RF: Route Refresh; • AS4: 4-байтовый ASN.
IPv4 Unicast Support	Указывает, можно ли обмениваться одноадресными IPv4-маршрутами с этим узлом. **Both** указывает на то, что IPv4 активен локально, и соседний узел сети указывает на поддержку одноадресного IPv4 в сообщении OPEN. Sent указывает на то, что одноадресный IPv4 активен локально, но соседний узел не включил AFI/SAFI в свое сообщение OPEN. Одноадресный IPv4 всегда доступен на локальном уровне и не может быть выключен. Указывает, можно ли обмениваться одноадресными IPv6-маршрутами с этим узлом.
IPv6 Unicast Support	Значения **Both** и **Sent** имеют тот же смысл, что и для IPv4. **None**

	указывает на то, что ни локальный маршрутизатор, ни соседний узел в этой смежности не имеют включенного IPv6. **Received** указывает на то, что соседний узел сообщает возможность поддержки одноадресного IPv6, но он не включен локально. Одноадресный IPv6 включается локально с помощью команды neighbor activate в режиме конфигурации семейства адресов IPv6.
Update Source	Настроенное значение IP-адреса источника для пакетов, отправляемых на этот узел. Это поле включается в вывод команды, только если источник для сообщений UPDATE настроен.
Configured Hold Time	Интервал в секундах, который этот маршрутизатор предлагает соседнему узлу в качестве времени удержания (hold).
Configured Keep Alive Time	Настроенный интервал KEEPALIVE для этого соседнего узла.
Negotiated Hold Time	Меньшее из значений настроенного времени удержания и времени удержания, полученного в сообщении OPEN от этого соседнего узла. Если локальный маршрутизатор не получает от соседнего узла сообщение KEEPALIVE или UPDATE в пределах этого интервала времени, локальный маршрутизатор отбрасывает смежность. Это поле отображается только в том случае, если смежность имеет статус не ниже OPEN CONFIRM.
Keep Alive Time	Время в секундах между сообщениями KEEPALIVE, отправляемыми к этому соседнему узлу. Это поле отображается только в том случае, если смежность имеет статус не ниже OPEN CONFIRM.
MD5 Password	Пароль TCP MD5, если он настроен, в формате обычного текста.
Last Error (Sent)	Последняя ошибка, которая произошла в процессе соединения с этим соседним узлом.
Last SubError	Подошибка, переданная с последней ошибкой.
Established Transitions	Сколько раз смежность переходила в состояние Established.
Established Time	Время, после того как соединение в последний раз перешло в состояние Established или из него.
Time Since Last Update	Сколько времени прошло с момента получения сообщения UPDATE от соседнего узла.
Message Table	Количество сообщений BGP, отправленных в адрес этого соседнего узла и полученных от него.
Received UPDATE Queue Size	Принятые сообщения UPDATE ставятся в очередь для обработки. Этот раздел показывает текущую длину очереди UPDATE на соседнем узле в байтах, метку верхнего уровня, ограничение и количество сообщений UPDATE, которые были отброшены, поскольку очередь была заполнена.
Следующие поля отображаются как для IPv4, так и IPv6, если IPv6 активен.	
Prefixes Advertised	Динамический счетчик числа префиксов, анонсируемых на этот соседний узел или принятых от него.
Prefixes Withdrawn	Динамический счетчик числа префиксов, включенных в раздел Withdrawn Routes сообщений UPDATE, передаваемых на этот соседний узел и с него.
Prefixes Current	Количество префиксов, в настоящее время анонсируемых на этот соседний узел и принятых от него. Для входящих префиксов это количество включает в себя только префиксы, которые были приняты входной политикой.
Prefixes Accepted	Количество префиксов от этого соседнего узла, которые могут стать активными в локальном RIB. Полученные префиксы не могут быть активированы, если не разрешим ближайший BGP-узел или если AS

	Path содержит петлю. Префикс считается принятым, только если он был пропущен входной политикой.
Prefixes Rejected	Количество префиксов, полученных от этого соседнего узла, которые не были пропущены входной политикой.
Max NLRI per Update	Максимальное количество префиксов, включенных в отдельное сообщение UPDATE от этого соседнего узла или к нему.
Min NLRI per Update	Минимальное количество префиксов, включенных в отдельное сообщение UPDATE от этого соседнего узла или к нему.

Если маршрутизатор получает сообщение UPDATE с недействительным атрибутом пути, маршрутизатор в большинстве случаев отправляет в ответ сообщение NOTIFICATION и сбрасывает смежность. BGP поддерживает счетчики каждого типа ошибок атрибутов пути для каждого соседнего устройства. Эта команда просмотра оперативного состояния устройства отображает каждый ненулевой счетчик сразу после параметра LastSubError. Счетчики, которые могут быть перечислены.

Параметр	***Описание***
Invalid ORIGIN code	Принятое сообщение UPDATE содержит неверный код ORIGIN.
Unexpected first ASN in AS path	Атрибут AS Path от внешнего узла не включает в себя номер AS данного узла в качестве первой AS.
Invalid AS path segment type	AS Path включает в себя сегмент с неправильным типом сегмента.
Invalid BGP NEXT HOP	BGP Next Hop не является допустимым одноадресным адресом.
Bad BGP NEXT HOP	BGP Next Hop совпадает с IP-адресом принимающего устройства, или это IP-адрес за пределами подсети узла.
Invalid AGGREGATOR attribute	Атрибут AGGREGATOR недействителен.
Unrecognized well-known path attribute	Сообщение UPDATE содержит атрибут пути с явным флагом Optional, но маршрутизатор не распознает этот атрибут.
Missing mandatory path attribute	Сообщение UPDATE было получено без обязательного атрибута пути.
Missing LOCAL PREF attribute	Сообщение UPDATE получено от внутреннего узла без атрибута LOCAL PREF.
Invalid prefix in UPDATE NLRI	Сообщение UPDATE, полученное от этого узла, содержит синтаксически неправильный префикс.

show ip bgp neighbors advertised-routes

Эта команда отображает список маршрутов IPv4, анонсируемых на указанный соседний узел. Эти маршруты в смежном RIB для исходящей группы анонсирования соседнего устройства.

Формат: `show ip bgp [vrf vrf-name] neighbors ip-address advertised-routes`

Режим ввода команд: привилегированный

Параметр	***Описание***
vrf-name	(Необязательный параметр.) Показывает сообщества в пределах экземпляра VRF.
ip-address	IP-адрес соседнего узла.

Вывод команды отображает следующую информацию.

Параметр	*Описание*
BGP table version	Каждый раз, когда фаза 2 процесса принятия решений BGP работает над выбором новых маршрутов BGP, это значение увеличивается.
Status codes	p — маршрут был обновлен в Adj-RIB-Out с момента отправки последнего сообщения UPDATE. Передача сообщения UPDATE отложена.
Network	Префикс места назначения
Next Hop	BGP NEXT HOP в том виде, как он анонсируется на узел.
Local Pref	Локальный приоритет. Локальный приоритет никогда не анонсируется на внешние узлы.
Metric	Значение MED, если MED анонсируется на узел.
Path	AS Path. AS Path не включает в себя локальный номер AS, который добавляется к началу AS Path, когда маршрут анонсируется на внешний узел.

Вывод команды указывает, настроен ли BGP на создание маршрута по умолчанию (neighbor default-originate).

Вывод этой команды немного отличается от вывода команды show ip bgp. Подавленные и неоптимальные маршруты не анонсируются, так что соответствующие коды статуса не имеют смысла. Анонсируемые маршруты всегда имеют один ближайший узел, BGP NEXT HOP анонсируется на узел. Локальный приоритет никогда не отправляется на внешние узлы.

show ip bgp neighbors policy

Эта команда отображает входящие и исходящие политики IPv4, настроенные для указанного узла. В выводе обозначены политики, настроенные на самом узле, и политики, которые он наследует из шаблона узла сети.

Формат: `show ip bgp [vrf vrf-name] neighbors [{ip-address]} policy`

Режим ввода команд: привилегированный

Параметр	*Описание*
vrf-name	(Необязательный параметр.) Показывает сообщества в пределах экземпляра VRF.
ip-address	(Необязательный параметр.) Указывает IPv4-адрес соседнего узла, которым ограничивается вывод.

Вывод команды отображает следующую информацию.

Параметр	*Описание*
Neighbor	Адрес соседнего узла сети.
Policy	Политика BGP для указанного узла.
Template	Если политика наследуется из шаблона узла сети, в этом поле отображается имя шаблона.

show ip bgp neighbors {received-routes | routes | rejected-routes}

Эта команда отображает список IPv4-маршрутов, полученных от указанного соседнего узла. Список включает в себя либо все маршруты, полученные от соседнего узла, либо полученные маршруты, которые были пропущены входной политикой, либо маршруты, отклоненные входной политикой. Если указан экземпляр VRF, отображается информация по маршрутам для соседних узлов в указанном экземпляре VRF.

Формат: `show ip bgp [vrf vrf-name] neighbors [ip-address {received-routes | routes | rejected- routes}]`

Режим ввода команд: привилегированный

Параметр	*Описание*
vrf-name	(Необязательный параметр.) Показывает маршруты, принадлежащие к сообществам, в пределах VRF.
ip-address	(Необязательный параметр.) IP-адрес соседнего узла.
received-routes	Показывает все маршруты, полученные от этого соседнего узла, независимо от того, прошли ли маршруты входную политику.
routes	Показывает только маршруты, которые были пропущены входной политикой.
rejected-routes	Показывает только маршруты, которые были отклонены входной политикой.

Вывод команды отображает следующую информацию.

Параметр	*Описание*
Network	Префикс места назначения
Next Hop	BGP NEXT HOP в том виде, как он анонсируется на узел.
Metric	Значение MED, если MED получен от этого узла.
Local Pref	Локальный приоритет, полученный от этого узла.
Path	AS Path, полученные от этого узла
Origin	Значение атрибута Origin, полученное от этого узла

show ip bgp route-reflection

Эта команда отображает всю глобальную конфигурацию, связанную с отражением IPv4-маршрутов, включая идентификатор кластера, настройку отражения маршрутов между клиентами, а также списки всех соседних узлов, которые настроены в качестве клиентов Route Reflector. Если указан VRF, конфигурация сообществ отображается в пределах указанного экземпляра VRF.

Если клиент Route Reflector настроен с использованием карты исходящих маршрутов, вывод команда предупреждает, что установленные заявления в карте маршрута игнорируются при отражении маршрутов к этому клиенту.

Формат: `show ip bgp [vrf vrf-name] route-reflection`

Режим ввода команд: привилегированный

Параметр	*Описание*
Cluster ID	Идентификатор кластера, используемый этим маршрутизатором. Отображается значение, установленное с помощью команды bgp cluster-id. Если идентификатор кластера не настроен, отображается идентификатор локального маршрутизатора с тегом default.
Client-to-client Reflection	Отображает *Enabled*, если маршрутизатор отражает маршруты, полученные от своих клиентов, к другим клиентам; в противном случае отображается *Disabled*.
Clients	Список внутренних узлов этого маршрутизатора, которые были настроены как клиенты Route Reflector.
Non-client Internal Peers	Список внутренних узлов сети маршрутизатора, которые не настроены как клиенты Route Reflector. Маршруты из узлов, не являющихся клиентами, отражаются клиентам, и наоборот.

show ip bgp statistics

Данная команда отображает недавнюю историю процесса принятия решения. Фаза 1 процесса принятия реагирует на сообщение UPDATE, полученное от соседних узлов, определяет, какие новые маршруты должны быть приняты, и удаляет отозванные маршруты из Adj-RIB-In. Фаза 2 определяет наилучший путь для каждого места назначения, обновляет таблицу BGP-маршрутов и общий RIB. Фаза 3 выполняется независимо для каждой исходящей группы обновлений и определяет, какие маршруты должны быть анонсированы на соседние узлы в каждой группе. Каждая запись в таблице показывает статистику для одной фазы процесса принятия решений. В таблице показаны 20 последних повторов процесса принятия решений с наиболее свежей информацией в конце таблицы. Если указан VRF, статистические данные отображаются для сообществ в пределах указанного экземпляра VRF.

Формат: `show ip bgp [vrf vrf-name] statistics`

Режим ввода команд: привилегированный

Команда отображает следующую информацию.

Параметр	*Описание*
Delta T	Показывает, насколько давно был запущен процесс принятия решений. Формат — чч:мм:сс, если прошедшее время меньше суток. В противном случае — дд:чч.
Phase	Какой этап процесса принятия решений был запущен.
Upd Grp	Идентификатор исходящей группы обновлений. Применяется только для фазы 3.
GenId	Идентификатор генерации таблицы маршрутизации BGP на момент запуска процесса принятия решений. Идентификатор генерации увеличивается каждый раз, когда запускается фаза 2 процесса принятия решений и когда происходит изменение в статусе агрегированных адресов.

Reason	Событие, которое инициировало процесс принятия решения.
Peer	Фаза 1 процесса принятия решений может быть вызвана для конкретного узла сети, если произошли изменения входной политики узла или узел был перезагружен. Когда фаза 1 выполняется для одного узла, указывается его IP-адрес.
Duration	Продолжительность процесса принятия решений в миллисекундах.
Adds	Количество добавленных маршрутов. Для фазы 1 это количество префиксов, которое проходит входную политику и добавляется к Accept-RIB-In. Для фазы 2 это количество маршрутов, добавленных в таблицу маршрутизации BGP. Для фазы 3 это количество префиксов, добавленное в группу анонсирования Adj-RIB-Out.
Mods	Количество измененных маршрутов. Всегда 0 для фазы 1.
Dels	Количество удаленных маршрутов. Всегда 0 для фазы 1.

show ip bgp summary

Эта команда отображает сводную информацию о конфигурации и статусе BGP. Если указан экземпляр VRF, отображаются конфигурация и статус для сообществ внутри экземпляра VRF.

Формат: `show ip bgp [vrf vrf-name] summary`

Режим ввода команд: привилегированный

Команда отображает следующую информацию.

Параметр	***Описание***
IPv4 Routing	Включена ли IPv4 маршрутизация глобально. Протокол BGP не поддерживает одноадресный IPv4 AFI/SAFI в отправляемых сообщениях OPEN, если маршрутизация не была включена глобально.
BGP Admin Mode	Включен ли BGP глобально
BGP Router ID	Настроенный идентификатор маршрутизатора
Local AS Number	Номер AS маршрутизатора
Traps	Включены ли BGP-трапы.
Maximum Paths	Максимальное количество ближайших узлов во внешнем маршруте BGP.
Maximum Paths iBGP	Максимальное количество ближайших узлов во внутреннем маршруте протокола BGP.
Default Keep Alive Time	Настроенный интервал KeepAlive, используемый всеми узлами, для которых не был настроен соответствующий индивидуальный интервал.
Default Hold Time	Настроенный интервал Hold, используемый всеми узлами, для которых не был настроен соответствующий индивидуальный интервал.
Number of Network Entries	Количество различных префиксов в местном RIB.
Number of AS Paths	Количество AS Path в местном RIB
Default Metric	Значение MED по умолчанию для перераспределяемых маршрутов.
Default Route Advertise	Настроен ли BGP для анонсирования маршрутов по умолчанию. Соответствует команде default- information originate.
Redistributing Source	Источник маршрутов, который BGP должен перераспределить.
Metric	Метрика, настроенная с помощью команды redistribute.
Match Value	Для маршрутов, перераспределяемых от протокола OSPF, — типы перераспределяемых OSPF-маршрутов.
Distribute List	Имя списка префиксов, используемое для фильтрации

	перераспределяемых маршрутов, если список настроен командой distribute-list prefix out.
Route Map	Имя карты маршрута, используемое для фильтрации перераспределяемых маршрутов.
Dynamic Neighbors	Показывает текущее количество созданных динамических соседних узлов IPv4 BGP, метку верхнего уровня и ограничение для динамических IPv4 соседних узлов, которые могут быть созданы.
Neighbor	IP-адрес соседнего узла. Соседний узел, который создан с помощью функции BGP dynamic neighbors, будет отмечен звездочкой (*).
ASN	ASN соседнего узла
MsgRcvd	Количество сообщений BGP, полученных от данного соседнего узла
MsgSent	Количество сообщений BGP, отправленных данному соседнему узлу
State	Статус смежности. Может обозначаться как IDLE, CONNECT, ACTIVE, OPEN SENT, OPEN CNFRM, EST
Up/Down Time	Время, в течение которого смежность была в состоянии ESTABLISHED, или, если смежность сброшена, — время, в течение которого смежность была неактивна. В формате дд:чч:мм:сс
Pfx Rcvd	Количество префиксов, полученных от соседнего узла

show ip bgp template

Используйте эту команду, чтобы просмотреть информацию обо всех настроенных шаблонах узлов сети или об указанном шаблоне BGP.

Формат: `show ip bgp template` *name*

Режим ввода команд: привилегированный

Параметр	***Описание***
Name	Имя BGP-шаблона узла сети
AF	Семейство адресов, к которому применяется команда конфигурации. Это поле остается пустым для параметров сессии, которые применяются ко всем семействам адресов.
Configuration	Команды конфигурации, которые включены в шаблон.

show ip bgp traffic

Данная команда выводит отчеты глобальных счетчиков переданных и принятых BGP-сообщений наряду с информацией о рабочей очереди BGP. Если указан экземпляр VRF, счетчики отображаются для сообществ в пределах экземпляра VRF.

Формат: `show ip bgp [vrf` *vrf-name*`] traffic`

Режим ввода команд: привилегированный

В первой таблице представлено количество сообщений BGP каждого типа, которые этот маршрутизатор отправил и принял. Следующая таблица содержит информацию о максимальной скорости передачи и приема сообщений UPDATE. Эти скорости измерены за наиболее загруженный интервал продолжительностью в одну секунду.

В таблице статистики очереди представлена информация по рабочим очередям BGP. Для каждой из очередей отображаются следующие значения.

Параметр	*Описание*
Events	Включает большинство событий таймера и изменений конфигурации.
Keepalive Tx	Включает события таймера, которые отправляют сообщения KEEPALIVE на узел.
Dec Proc	Включает события, которые вызывают запуск процесса принятия решений.
Rx Data	Включает входящие сообщения BGP.
RTO Notifications	Включает изменения оптимального маршрута и уведомления об изменении разрешения ближайших узлов из таблицы маршрутизации.
MIB Queries	Включает ожидающие SNMP-запросы для получения статуса BGP

show ip bgp update-group

Данная команда сообщает о статусе исходящих групп анонсирования и их членов. Если указан экземпляр VRF, отображается информация о статусе групп анонсирования для сообществ в пределах экземпляра VRF.

Формат: `show ip bgp [vrf vrf-name] update-group [group-index | peer-address ]`

Режим ввода команд: привилегированный

Параметр	*Описание*
group-index	Если указана, эта опция ограничивает вывод одной группой анонсирования (необязательный параметр).
peer-address	Если указана, эта опция ограничивает вывод группой анонсирования, содержащей узел с данным адресом (необязательный параметр).

Команда отображает следующую информацию.

Параметр	*Описание*
Update Group ID	Уникальный идентификатор для исходящей группы анонсирования.
Peer Type	Внутренние или внешние узлы входят в группу анонсирования.
Minimum Advertisement Interval	Минимальное время в секундах между отправляемыми в группу наборами UPDATE-сообщений.
Send Community	Включаются ли BGP-сообщества анонсы маршрута для членов группы.
Remove Private ASNs	Удаляет ли BGP частные ASN из путей, анонсируемых членам этой группы. • Replace: протокол BGP заменяет частные ASN на локальные ASN; • Remove: частные ASN удаляются; • В остальных случаях: No.
Route Reflector Client	Являются ли узлы в этой группе клиентами Route Reflector.
Neighbor AS Path Access List Out	Список контроля доступа AS Path, который используется для фильтрации сообщений UPDATE, отправленных на узлы группы анонсирования
Neighbor Prefix List Out	Имя списка префиксов, используемое для фильтрации префиксов, анонсируемых на узлы группы анонсирования
Members Added	Число узлов, добавленных к группе с момента ее создания.
Members Removed	Число узлов, удаленных из группы.

Update Version	Сколько раз фаза 3 процесса принятия решений была запущена для этой группы с целью определения маршрутов, которые будут анонсироваться этой группе.
Number of UPDATEs Sent	Число сообщений UPDATE, которые были отправлены в эту группу. Увеличивается на единицу для каждого сообщения UPDATE, независимо от количества членов группы.
Time Since Last UPDATE	Время с момента, когда сообщение UPDATE было отправлено в группу в последний раз. Если сообщения UPDATE не отправлялись в группу, статус указывается как NEVER.
Current Prefixes	Количество префиксов, в настоящее время анонсируемое группе.
Current Paths	Количество путей, в настоящее время анонсируемое группе.
Prefixes Advertised	Общее количество префиксов, анонсированных группе с момента ее создания.
Prefixes Withdrawn	Общее количество префиксов, включенных в поле Withdrawn Routes сообщений UPDATE, отправленных в группу с момента ее создания.
UPDATE Send Failures	Количество сообщений UPDATE, которое не было доставлено всем членам группы.
Current Members	IPv4-адрес всех текущих членов группы.

Таблица истории отправленных сообщений UPDATE показывает статистику по последним десяти процессам отправки сообщений для группы анонсирования. Элементы в таблице истории отображают следующую информацию.

Параметр	***Описание***
Version	Версия сообщения UPDATE.
Delta T	Время, прошедшее с момента начала процесса отправки сообщения, чч::мм::сс.
Duration	Длительность процесса отправки сообщений в миллисекундах.
UPD Built	Количество созданных сообщений UPDATE.
UPD Sent	Количество сообщений UPDATE успешно переданных членам группы. Обычно копия каждого сообщения UPDATE направляется каждому члену группы.
Paths Sent	Количество анонсируемых путей.
Pfxs Adv	Количество анонсируемых префиксов
Pfxs Wd	Количество отозванных префиксов.

show ip bgp vpnv4

Команда отображает информацию об адресах VPNv4 в таблице BGP. Если указано необязательное значение VRF, отображается адресная информация для сообществ внутри инстанса VRF.

Формат: `show ip bgp vpnv4 {all | rd` *`route-distinguisher`* `| vrf` *`vrf-name`*`} [`*`ip-prefix/length`*`]`

Режим ввода команд: привилегированный

Параметр	***Описание***
all	Отображает полную таблицу VPNv4.
rd route-distinguisher	Отображает NLRI-префиксы, которые соответствуют указанному Route Distinguisher.

vrf vrf-name	Отображает NLRI-префиксы, связанные с сообществами в рамках указанного экземпляра VRF.
ip-prefix/length	IP-адрес (в десятичном формате с точками) и длина маски (от 0 до 32). Знак косой черты (/) должен быть включен.

Команда выводит информацию в зависимости от выбранных параметров.

Параметр	***Описание***
BGP table version	Каждый раз, когда фаза 2 процесса принятия решений BGP работает над выбором новых маршрутов BGP, это значение увеличивается.
Status codes	Одно из следующих значений. • s — маршрут объединен в агрегированный адрес, настроенный с опцией summary-only; • * — BGP никогда не отображает неверные маршруты; так что этот код отображается всегда (для поддержания соответствия с промышленным стандартом); • > — указывает, что BGP выбрал этот путь как оптимальный путь к месту назначения; • i — маршрут изучен от внутреннего узла.
Route Distinguisher	RD, связанный с VRF.
Network	Префикс места назначения.
Next Hop	Ближайший BGP-узел в маршруте.
Metric	Метрика BGP.
LocPrf	Локальный приоритет.
Path	AS Path для маршрута.
Prefix/Prefix Length	Префикс места назначения и длина префикса.
Generation ID	Версия таблицы BGP-маршрутизации на момент последнего изменения маршрута.
Forwarding	Используется ли BGP-маршрут для переадресации.
Advertised To Update Groups	Исходящие группы, в которых этот маршрут анонсируется.
Local Preference	Локальный приоритет, либо полученный от узла, либо установленный в соответствии с локальной политикой.
AS Path	AS Path. Эта форма команды отображает AS Path такой длины, какая разрешена параметром bgp maxas-limit.
Origin	Значение атрибута ORIGIN.
Metric	Значение атрибута MED, если он включен.
Type	Получен ли путь от внутреннего или внешнего узла.
IGP Cost	Внутренняя стоимость пограничного шлюза (например, стоимость OSPF) к ближайшему BGP-узлу.
Peer (Peer ID)	IP-адрес узла, который отправил этот маршрут, и его идентификатор маршрутизатора.
BGP Next Hop	Атрибут BGP NEXT HOP.
Atomic Aggregate	Показывает, связан ли с путем атрибут ATOMIC AGGREGATE.
Aggregator	Номер AS и идентификатор маршрутизатора инициатора объединения маршрута.
Communities	BGP-сообщества, связанные с путем.
Originator	Если атрибут ORIGINATOR связан с путем, отображается значение этого атрибута.

Cluster List	Если атрибут CLUSTER_LIST связан с путем, отображается последовательность идентификаторов кластера в списке кластеров.
Extended Community	Атрибут route-target, связанный с указанным маршрутом.

show bgp ipv6

Используйте команду show bgp ipv6 в привилегированном режиме для отображения IPv6-маршрутов в таблице маршрутизации BGP.

Формат: `show bgp ipv6 [`*`ipv6-prefix`*`|`*`prefix-length`*` [longer-prefixes | shorter-prefixes [`*`length`*`]] | filter-list `*`as-path-list`*`]`

Режим ввода команд: привилегированный

Параметр	***Описание***
ipv6-prefix prefix-length	Ограничивает вывод указанным префиксом (необязательный параметр).
longer-prefixes	Отображает указанный префикс и более длинные префиксы в том же диапазоне (необязательный параметр).
shorter-prefixes	Используется совместно с опцией **ipv6-prefix|prefix-length**, чтобы отобразить маршруты, длина префикса которых короче **prefix-length** и, необязательно, больше указанной длины (необязательный параметр). Этот параметр не может использоваться, если задана опция **longer prefixes**.
as-path-list	Фильтрует вывод команды, отображая только маршруты, которые соответствует указанному списку AS Path (необязательный параметр). Этот параметр не может использоваться, если задана опция **ipv6-prefix|prefix-length**.

Вывод команды отображает следующую информацию.

Параметр	***Описание***
BGP table version	Каждый раз, когда фаза 2 процесса принятия решений BGP работает над выбором новых маршрутов BGP, это значение увеличивается.
Status codes	• s — маршрут объединен в агрегированный адрес, настроенный с опцией summary-only; • * — BGP никогда не отображает неверные маршруты; так что этот код отображается всегда; • > — указывает, что BGP выбрал этот путь как оптимальный путь к месту назначения; • i — маршрут изучен от внутреннего узла.
Network	IPv6-префикс места назначения
Next Hop	Ближайший BGP-узел IPv6-маршрута
Metric	Атрибут Multi Exit Discriminator
LocPrf	Локальный приоритет
Path	AS Path
Origin	Значение атрибута Origin

show bgp ipv6 aggregate-address

Эта команда выводит список настроенных агрегированных адресов IPv6 и показывает, является ли каждый из них активным.

Формат: `show bgp ipv6 aggregate-address`

Режим ввода команд: привилегированный

Параметр	*Описание*
Prefix/Len	Префикс места назначения и длина префикса.
AS Set	Показывает, анонсируется ли с агрегированным адресом пустой AS Path (N) или AS SET анонсируется с набором номеров AS, относящихся ко всем путям в агрегированном адресе (Y).
Summary Only	Показывает, подавляются (Y) или анонсируются (N) отдельные сети.
Active	Показывает, анонсируется ли в настоящее время данный агрегированный адрес.

show bgp ipv6 community

Эта команда отображает маршруты IPv6, принадлежащие к данному набору сообществ. Описание формата вывода и полей аналогичны тем, что приведены в команде *show bgp ipv6*.

Формат: `show bgp ipv6 community` *`communities`* `[exact-match]`

Режим ввода команд: привилегированный

Параметр	*Описание*
communities	Строка из нуля или более значений сообществ, которые могут быть в любом формате и могут содержать хорошо известные ключевые слова сообществ no-advertise и no-export. Вывод команды отображает маршруты, которые принадлежат ко всем сообществам, указанным в команде.
exact-match	Отображаются только те маршруты, которые являются членами только тех сообществ, которые были указаны в команде (необязательный параметр).

show bgp ipv6 community-list

Данная команда отображает IPv6-маршруты, которые соответствуют списку сообществ. Описание формата вывода и полей аналогичны тем, что приведены в команде show bgp ipv6.

Формат: `show bgp ipv6 community-list` *`name`* `[exact-match]`

Режим ввода команд: привилегированный

Параметр	*Описание*
name	Имя стандартного списка сообществ.
exact-match	Отображаются только те маршруты, которые являются членами только тех сообществ, которые были указаны в списке сообществ (необязательный параметр).

show bgp ipv6 listen range

Данная команда отображает информацию о диапазонах прослушивания BGP.

Формат: `show bgp ipv6 listen range [`*`network/length`*`]`

Режим ввода команд: привилегированный

Параметр	*Описание*
listen range	Отображает все диапазоны подсетей прослушивания, которые были созданы.
network / length	Отображает информацию об указанных диапазонах прослушивания.

show bgp ipv6 neighbors advertised-routes

Эта команда отображает маршруты IPv6, анонсируемые на указанный соседний узел. Описание формата вывода и полей аналогичны тем, что приведены в IPv4-команде show ip bgp neighbors advertised-routes, за исключением того, что поля Network и Next Hop показывают адреса IPv6 и команда отображает IPv4-маршруты, анонсируемые на указанный соседний узел с RFC 5549.

Формат: `show bgp ipv6 neighbors {`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`]|autodetect interface` *`interface-name`*`} advertised-routes`

Режим ввода команд: привилегированный

show bgp ipv6 neighbors

Эта команда отображает список маршрутов IPv6, полученных от указанного соседнего узла. Список включает в себя либо все маршруты, полученные от соседнего узла, либо полученные маршруты, которые были пропущены входной политикой, либо маршруты, отклоненные входной политикой. Описание формата вывода и полей аналогичны тем, что приведены в IPv4-команде show ip bgp neighbors, за исключением следующих моментов.

- Перечисляются IPv6-маршруты
- Если адрес узла (Remote Address) является адресом link local, следующая строка вывода указывает область действия адреса.
- Параметр IPv4 Outbound Group Update не выводится.
- Не отображается статистика префикса IPv4.
- Поддержка RFC 5549 отображается только в том случае, если путь к соседнему BGP-узлу проходит через сеть IPv6.
- Если узел настроен как autodetect, Remote Address показывает обнаруженный IPv6-адрес или значение Unresolved в случае, если узел не обнаружен функцией autodetect.
- Статус Autodetect отображается только в том случае, когда узел был настроен как autodetect. В поле отображается один из следующих статусов: Peer is detected, Peer is not detected или Multiple peers are detected.

Формат: `show bgp ipv6 neighbors [`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`* `{received-routes | routes | rejected-routes}`

Режим ввода команд: привилегированный

show bgp ipv6 neighbors policy

Используйте эту команду, чтобы отобразить входящие и исходящие политики IPv6, настроенные для указанного узла. В выводе обозначены политики, настроенные на самом узле, и политики, которые он наследует из шаблона узла сети. Указание IPv4- или IPv6-адреса ограничивает

вывод одним соседним узлом. Если адрес соседнего узла является адресом link-local, интерфейс также требуется указать.

Формат: `show bgp ipv6 neighbors [`*`ipv4-address`* `|` *`ipv6-address`* `[interface` *`interface-name`*`] | autodetect interface` *`interface-name`* `policy`

Режим ввода команд: привилегированный

show bgp ipv6 route-reflection

Эта команда отображает конфигурацию локального маршрутизатора в качестве Route Reflector.

Формат: `show bgp ipv6 route-reflection`

Режим ввода команд: привилегированный

Параметр	***Описание***
Cluster ID	Идентификатор кластера, используемый этим маршрутизатором. Отображается значение, установленное с помощью команды bgp cluster-id. Если идентификатор кластера не настроен, отображается идентификатор локального маршрутизатора с тегом default.
Client-to-client Reflection	Отображает Enabled, если маршрутизатор отражает маршруты, полученные от своих клиентов, к другим клиентам; в противном случае отображается Disabled.
Clients	Список внутренних узлов этого маршрутизатора, которые были настроены как клиенты Route Reflector.
Non-client Internal Peers	Список внутренних узлов сети маршрутизатора, которые не настроены как клиенты Route Reflector. Маршруты из узлов, не являющихся клиентами, отражаются клиентам, и наоборот.

show bgp ipv6 statistics

Эта команда отображает статистику для процесса принятия решений IPv6. Описание вывода и полей аналогичны тем, что приведены в команде show ip bgp statistics.

Формат: `show bgp ipv6 statistics`

Режим ввода команд: привилегированный

show bgp ipv6 summary

Эта команда отображает сводную информацию об IPv6-конфигурации и статусе BGP. Описания вывода и поля аналогичны тем, что приведены в команде show ip bgp summary, за исключением, что в Number of Network Entries, Number of AS Paths и Pfx Rcvd учитывается маршрутная информация IPv6, а не IPv4. Команда выводит список всех смежностей, которые были настроены для выполнения IPv6-маршрутов.

Формат: `show bgp ipv6 summary`

Режим ввода команд: привилегированный

show bgp ipv6 update-group

Данная команда сообщает статус исходящих групп анонсирования и их номера. Описание вывода и полей аналогичны тем, что приведены в команде show ip bgp template.

Формат: show bgp ipv6 update-group [*group-index* | *ipv4-address* | *ipv6-address* [interface *interface-name*] autodetect interface *interface-name*

Режим ввода команд: привилегированный

Параметр	*Описание*
group-index	Если указана, эта опция ограничивает вывод одной группой анонсирования (необязательный параметр).
ipv4-address	IPv4-адрес узла, включенный для обмена IPv6-префиксами. Если указана, эта опция ограничивает вывод группой анонсирования, содержащей узел с данным адресом.
ipv6-address	IPv6-адрес соседнего узла. Если адрес узла является адресом link local, то интерфейс, который определяет область адреса, также должен быть указан. Если указан адрес узла, эта опция ограничивает вывод группой анонсирования, содержащей узел с данным адресом.
autodetect interface	Интерфейс маршрутизации, на котором IPv6-адрес link-local соседнего узла определяется автоматически.

13.1 Команды настройки политики маршрутизации

Внешние протоколы маршрутизации, такие как BGP, используют стандартную отраслевую политику маршрутизации для фильтрации и изменения маршрутной информации, которой они обмениваются с соседними узлами. Протокол BGP использует следующие элементы политик маршрутизации:

- списки контроля доступа AS Path;
- списки BGP-сообществ.

Используйте команды настройки политики маршрутизации, чтобы настроить следующие варианты политик:

- совпадение по AS Path;
- изменение AS Path;
- установка локального приоритета;
- установка метрики маршрута;
- установка ближайшего IPv6-узла;
- установка или совпадение BGP-сообщества.

ip as-path access-list

Чтобы создать список контроля доступа (ACL) AS Path, используйте команду ip as-path access-list в режиме глобальной конфигурации. ACL AS Path фильтрует маршруты BGP на основании их атрибута AS Path. Атрибут AS Path представляет собой список номеров автономных систем, затронутых по пути к месту назначения. ACL AS Path — это упорядоченная последовательность заявлений. Каждое заявление содержит регулярное выражение и связанное с ним действие permit

или deny. Если регулярное действие соответствует атрибуту AS Path маршрута, выраженному как строка символов ASCII, путь признается соответствующим и к нему применяется указанное действие. В конце списка AS Path подразумевается заявление deny. Если путь не соответствует ни одному из заявлений в ACL AS Path, к нему применяется действие deny, т. е. путь отклоняется.

После создания ACL AS Path из него нельзя удалить отдельное заявление. Если требуется удалить отдельное заявление, необходимо удалить ACL AS Path и создать его заново без указанного заявления.

Заявления применяются в том порядке, в котором созданы. Новые заявления добавляются в конец списка. К маршруту применяется заявление с первым совпадающим регулярным выражением.

Маршрутизатор позволяет настроить до 128 списков контроля доступа AS Path; в каждом списке может содержаться до 64 заявлений.

Чтобы ввести в регулярное выражение знак вопроса, требуется сначала ввести CTRL-V, чтобы CLI не интерпретировал знак вопроса как запрос помощи.

Таблица 13.1 показывает синтаксис регулярных выражений ACL AS Path.

Значение по умолчанию: ACL AS Path не настроен. Для параметров этой команды нет значений по умолчанию.

Формат: `ip as-path access-list` *`as-path-list-number`* `{permit|deny}` *`re-gexp`*

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
as-path-list-number	Число от 1 до 500, уникальный идентификатор списка. ACL AS Path с совпадающими значениями as-path-list-number считаются частями одного списка.
permit	(Необязательный параметр.) Разрешает маршруты, в которых атрибуты AS Path соответствуют регулярному выражению.
deny	(Необязательный параметр.) Запрещает маршруты, в которых атрибуты AS Path соответствуют регулярному выражению.
regexp	Регулярное выражение, которое используется для сопоставления с атрибутом AS Path, причем AS Path рассматривается как строка ASCII-символов.

Таблица 13.1 - Синтаксис регулярных выражений ACL AS Path

Специальный символ	***Символ***	***Действие***
звездочка	*	Соответствует нулю или нескольким последовательным символам.
кв. скобки	[]	Обозначают диапазон односимвольных шаблонов.
знак вставки	^	Отмечает начало строки ввода.
знак доллара	$	Отмечает конец строки ввода.
дефис	–	Разделяет конечные точки диапазона.
точка	.	Соответствует любому одному символу, включая пробелы.
плюс	+	Соответствует одному или нескольким последовательным символам.

вопросительный знак	?	Соответствует нулевому или однократному вхождению шаблона.
нижнее подчеркивание	_	Соответствует запятой (,), левой фигурной скобке ({), правой фигурной скобке (}), левой или правой скобке, началу строки ввода, концу строки ввода или пробелу.

no ip as-path access-list

Для удаления ACL AS Path используйте no-форму команды.

Формат: `no ip as-path access-list` *`as-path-list-number`*

Режим ввода команд: глобальная конфигурация

ip bgp-community new-format

Для отображения стандартных сообществ BGP в формате AA:NN используйте данную команду в режиме глобальной конфигурации. RFC 1997 указывает, что первые два байта номера сообщества считаются номером автономной системы. Новый формат отображает номер сообщества как ASN с последующим 16-битным специальным номером для AS.

Значение по умолчанию: стандартные сообщества отображаются в формате AA:NN.

Формат: `ip bgp-community new-format`

Режим ввода команд: глобальная конфигурация

no ip bgp-community new-format

Для отображения стандартных сообществ протокола BGP в виде 32-битных целых чисел используйте **no**-форму команды.

Формат: `no ip bgp-community new-format`

Режим ввода команд: глобальная конфигурация

ip community-list

Чтобы создать или настроить список сообществ BGP, используйте команду ip community-list в режиме глобальной конфигурации. Заявление списка сообществ без указанных значений сообществ считается совпадением для всех маршрутов, независимо от их членства в сообществе. К примеру, заявление ip community-list bullseye permit считается заявлением permit all.

Номер сообщества может быть введен в любом формате, в виде 32-битного целого числа или пары 16-битных целых чисел, разделенных двоеточием, независимо от того, является ли команда ip bgp-community new-format активной. В одной команде можно указать до 16 сообществ, в том числе хорошо известных. С заданным именем списка сообщества можно настроить до 32 заявлений. Всего можно настроить до 128 уникальных имен сообществ.

Значение по умолчанию: списки сообществ не настроены.

Формат: `ip community-list standard` *`list-name`* `{permit | deny} [`*`commu-nity-number`*`] [no- advertise] [no-export]`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***

standard list-name	Определяет имя стандартного списка сообществ. Имя может содержать до 32 символов.
permit	Указывает, что совпадающие маршруты разрешены.
deny	Указывает, что совпадающие маршруты запрещены.
community-number	До 16 номеров сообщества в формате 32-битных целых чисел или в формате AA:NN, где AA — это 16-битный номер автономной системы, а NN представляет собой 16-битное целое число. Диапазон составляет от 1 до 4 294 967 295 (любое 32-битное целое число, отличное от 0). Сообщества разделяются пробелами.
no-advertise	Хорошо известное стандартное сообщество, NO_ADVERTISE (0xFFFFFF02).
no-export	Хорошо известное стандартное сообщество, NO_EXPORT, (0xFFFFFF01).

no ip community-list

Чтобы удалить список сообществ, используйте **no**-форму команды.

Формат: `no ip community-list standard` *`list-name`*

Режим ввода команд: глобальная конфигурация

show ip as-path-access-list

Данная команда отображает содержимое списков контроля доступа AS Path.

Формат: `show ip as-path-access-list [`*`as-path-list-number`*`]`

Режим ввода команд: привилегированный

Параметр	***Описание***
as-path-list-number	Если данный параметр указан, вывод ограничивается единственным указанным списком AS Path (необязательный параметр). Значение number — целое число от 1 до 500.

show ip community-list

Эта команда отображает списки сообществ. Формат вывода значений сообщества диктуется командой *ip bgp community new-format*.

Формат: `show ip community-list [`*`community-list-name`*`]`

Режим ввода команд: привилегированный

Параметр	***Описание***
community-list-name	Стандартное имя списка сообщества (необязательный параметр). Эта опция ограничивает вывод одним списком.

clear ip community-list

Эта команда очищает списки сообществ.

Формат: `clear ip community-list [`*`community-list-name`*`]`

Режим ввода команд: привилегированный

Параметр	***Описание***
community-list-name	(Необязательный параметр.) Имя списка сообщества.

14 КОМАНДЫ УПРАВЛЕНИЯ ПРОТОКОЛОМ IPV6

В этом разделе описываются команды управления протоколом IPv6, доступные в CLI.

Команды в этом разделе делятся на три функциональные группы:

- **Команды просмотра оперативного состояния устройства, которые отображают настройки коммутатора, статистику и другую информацию.**
- **Команды настройки, которые задают характеристики и настройки коммутатора. Для каждой команды настройки существует команда просмотра оперативного состояния устройства, отображающая текущие параметры конфигурации.**
- **Команды очистки, которые возвращают отдельные параметры или все настройки к заводским.**

14.1 Команды настройки управления через протокол IPv6

Коммутатор обеспечивает перечисленные ниже возможности IPv6.

- Статическую привязку IPv6-адресов и пограничных шлюзов к сервисным/сетевым портам.
- Возможность проверки IPv6-адреса link-local через сервисный/сетевой порт с использованием команды ping.
- Возможность отправлять SNMP-трапы и запросы через сервисный/сетевой порт с использованием команд управления протоколом IPv6.
- Пользователь может управлять устройством через сетевой порт (в дополнение к управлению через интерфейс маршрутизации или сервисный порт).

serviceport ipv6 enable

Используйте эту команду, чтобы включить использование протокола IPv6 на сервисном порте. По умолчанию использование IPv6 на сервисном порте включено.

Значение по умолчанию: включено

Формат: `serviceport ipv6 enable`

Режим ввода команд: привилегированный

no serviceport ipv6 enable

Эта команда выключает использование IPv6-протокола на сервисном порте.

Формат: `no serviceport ipv6 enable`

Режим ввода команд: привилегированный

network ipv6 enable

Используйте эту команду, чтобы включить использование протокола IPv6 на сетевом порте. По умолчанию использование IPv6 на сетевом порте включено.

Значение по умолчанию: включено

Формат: `network ipv6 enable`

Режим ввода команд: привилегированный

no network ipv6 enable

Эта команда выключает использование IPv6-протокола на сетевом порте.

Формат: `no network ipv6 enable`

Режим ввода команд: привилегированный

serviceport ipv6 address

Используйте опции данной команды, чтобы вручную настроить глобальный IPv6-адрес, включить/выключить автоматическую настройку глобального адреса без сохранения состояния и включить/выключить информацию DHCPv6-клиента на сервисном порте.

На сервисном порте можно настроить несколько IPv6-префиксов.

Формат: `serviceport ipv6 address {address/prefix-length [eui64]|auto-config|dhcp}`

Режим ввода команд: привилегированный

Параметр	***Описание***
address	IPv6-префикс в формате глобального IPv6-адреса.
prefix-length	Значение длины IPv6-префикса.
eui64	Формулировка IPv6-адреса в формате eui64.
autoconfig	Конфигурация автоматической настройки глобальных адресов без сохранения состояния.
dhcp	Настройка протокола DHCPv6-клиента.

no serviceport ipv6 address

Команда *no serviceport ipv6 address* удаляет все настроенные IPv6-префиксы на интерфейсе сервисного порта.

Используйте команду с опцией *address*, чтобы удалить настроенный вручную глобальный IPv6-адрес на интерфейсе сервисного порта.

Используйте команду с опцией *autoconfig* для выключения на сервисном порте автоматической настройки глобальных адресов без сохранения состояния.

Используйте команду с опцией *dhcp*, чтобы выключить на сервисном порте протокол DHCPv6-клиента.

Формат: `no serviceport ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}`

Режим ввода команд: привилегированный

serviceport ipv6 gateway

Команда настраивает информацию IPv6-шлюза (т. е. значение маршрутизатора по умолчанию) для сервисного порта.

Для сервисного порта можно настроить только один IPv6-адрес шлюза. Можно использовать сочетание явным образом настроенных IPv6-префиксов и шлюзов с теми, что устанавливаются путем автоматической настройки на подключенном IPv6-маршрутизаторе, на соответствующем интерфейсе сервисного порта.

Формат: `serviceport ipv6 gateway` *`gateway-address`*

Режим ввода команд: привилегированный

Параметр	*Описание*
gateway-address	Адрес шлюза в формате глобального IPv6-адреса или адреса link-local.

no serviceport ipv6 gateway

Используйте эту команду для удаления IPv6-шлюзов на интерфейсе сервисного порта.

Формат: `no serviceport ipv6 gateway`

Режим ввода команд: привилегированный

serviceport ipv6 neighbor

Данная команда позволяет вручную добавить соседние узлы IPv6 в таблицу IPv6-соседей сервисного порта. Если соседний узел IPv6 уже присутствует в таблице, соответствующая запись автоматически преобразуется в статическую. Статические записи не меняются в процессе обнаружения соседних узлов. Тем не менее они наравне с остальными записями используются для IPv6-переадресации. Статические записи о соседних IPv6-узлах применяются на уровне стека ядра и аппаратного обеспечения, если соответствующий интерфейс оперативно активен.

Формат: `serviceport ipv6 neighbor` *`ipv6-address macaddr`*

Режим ввода команд: привилегированный

Параметр	*Описание*
ipv6-address	IPv6-адрес соседнего узла или интерфейса.
macaddr	MAC-адрес соседнего узла или интерфейса.

no serviceport ipv6 neighbor

Используйте эту команду, чтобы удалить соседние узлы IPv6 из таблицы IPv6-соседей сервисного порта.

Формат: `no serviceport ipv6 neighbor` *`ipv6-address macaddr`*

Режим ввода команд: привилегированный

network ipv6 address

Используйте опции данной команды, чтобы вручную настроить глобальный IPv6-адрес, включить/выключить автоматическую настройку глобального адреса без сохранения состояния и включить/выключить информацию DHCPv6-клиента на сетевом порте. На сетевом порте можно настроить несколько IPv6-адресов.

Формат: `network ipv6 address {address/prefix-length [eui64] | auto-config | dhcp}`

Режим ввода команд: привилегированный

Параметр	***Описание***
address	IPv6-префикс в формате глобального IPv6-адреса.
prefix-length	Значение длины IPv6-префикса.
eui64	Формулировка IPv6-адреса в формате eui64.
autoconfig	Конфигурация автоматической настройки глобальных адресов без сохранения состояния.
dhcp	Настройка протокола DHCPv6-клиента.

no network ipv6 address

Команда *no network ipv6 address* удаляет все настроенные IPv6-префиксы.

Используйте команду с опцией *address*, чтобы удалить настроенный вручную глобальный IPv6-адрес на интерфейсе сетевого порта.

Используйте команду с опцией autoconfig для выключения на сетевом порте автоматической настройки глобальных адресов без сохранения состояния.

Используйте эту команду с опцией *dhcp*, чтобы выключить на сетевом порте протокол DHCPv6-клиента.

Формат: `no network ipv6 address {address/prefix-length [eui64] | autoconfig | dhcp}`

Режим ввода команд: привилегированный

network ipv6 gateway

Данная команда настраивает информацию IPv6-шлюза (т. е. значение маршрутизатора по умолчанию) для сетевого порта.

Формат: `network ipv6 gateway gateway-address`

Режим ввода команд: привилегированный

Параметр	***Описание***
gateway-address	Адрес шлюза в формате глобального IPv6-адреса или адреса link-local.

no network ipv6 gateway

Используйте эту команду для удаления IPv6-шлюзов на интерфейсе сетевого порта.

Формат: `no network ipv6 gateway`

Режим ввода команд: привилегированный

network ipv6 neighbor

Данная команда позволяет вручную добавить соседние узлы IPv6 в таблицу IPv6-соседей сетевого порта. Если соседний узел IPv6 уже присутствует в таблице, соответствующая запись автоматически преобразуется в статическую. Статические записи не меняются в процессе обнаружения соседних узлов. Тем не менее они наравне с остальными записями используются для IPv6-переадресации. Статические записи о соседних IPv6-узлах применяются на уровне стека ядра и аппаратного обеспечения, если соответствующий интерфейс оперативно активен.

Формат: `network ipv6 neighbor` *`ipv6-address macaddr`*

Режим ввода команд: привилегированный

Параметр	*Описание*
ipv6-address	IPv6-адрес соседнего узла или интерфейса.
macaddr	MAC-адрес соседнего узла или интерфейса.

no network ipv6 neighbor

Используйте эту команду, чтобы удалить соседние узлы IPv6 из таблицы IPv6-соседей.

Формат: `no network ipv6 neighbor` *`ipv6-address macaddr`*

Режим ввода команд: привилегированный

show network ipv6 neighbors

Эта команда отображает состояние записей о соседних IPv6-узлах, которые сохранены в соответствующей таблице на сетевом порте. Состояние обновляется, чтобы отобразить тип записи.

Значение по умолчанию: отсутствует

Формат: `show network ipv6 neighbors`

Режим ввода команд: привилегированный

Параметр	*Описание*
IPv6 Address	IPv6-адрес соседнего узла.
MAC Address	MAC-адрес соседнего узла.
isRtr	Показывает, является ли соседний узел маршрутизатором. При значении TRUE соседний узел является маршрутизатором; при значении FALSE — не является.
Neighbor State	Состояние записи о соседнем узле в таблице. Возможные значения: Incomplete, Reachable, Stale, Delay, Probe и Unknown.
Age	Время в секундах, прошедшее с момента добавления записи в таблицу.
Type	Тип записи о соседнем узле. Имеет значение Static, если запись настроена вручную, и Dynamic, если запись добавлена динамически.

show serviceport ipv6 neighbors

Данная команда отображает состояние записей о соседних IPv6-узлах, которые сохранены в соответствующей таблице на сервисном порте. Состояние обновляется, чтобы отобразить тип записи.

Значение по умолчанию: отсутствует

Формат: `show serviceport ipv6 neighbors`

Режим ввода команд: привилегированный

Параметр	*Описание*
IPv6 Address	IPv6-адрес соседнего узла.
MAC Address	MAC-адрес соседнего узла.
isRtr	Показывает, является ли соседний узел маршрутизатором. При значении TRUE соседний узел является маршрутизатором; при значении FALSE — не является.
Neighbor State	Состояние записи о соседнем узле в таблице. Возможные значения: Incomplete, Reachable, Stale, Delay, Probe и Unknown.
Age	Время в секундах, прошедшее с момента добавления записи в таблицу.
Type	Тип записи о соседнем узле. Имеет значение Static, если запись настроена вручную, и Dynamic, если запись добавлена динамически.

ping ipv6

Используйте эту команду, чтобы определить, есть ли другой компьютер в сети. Команда ping при вызове в CLI обеспечивает синхронный ответ. Чтобы использовать команду, требуется настроить на коммутаторе стандартное (in-band) сетевое подключение. Коммутатор можно вызывать командой *ping* с любого IP-адреса рабочей станции, подключенной к коммутатору посредством виртуальной сети по умолчанию (VLAN 1), если между коммутатором и рабочей станцией есть физически доступный маршрут. Интерфейс терминала отправляет к целевой станции три сигнала ping. Используйте параметр *ipv6-address|hostname*, чтобы вызывать интерфейс с использованием его глобального IPv6-адреса. Используйте необязательное ключевое слово *size*, чтобы указать размер пакета ping. Используйте опцию outgoing-interface, чтобы указать исходящий интерфейс для многоадресного IP/IPv6-вызова ping.

При использовании глобального IPv6-адреса *ipv6-global-address|hostname* можно применять команды ping или traceroute для сетевых/служебных портов. Любая привязка глобальных IPv6-адресов или шлюзов для этих интерфейсов приводит к установке в рамках IP-стека IPv6-маршрутов таким образом, что запросы *ping* или *traceroute* переадресуются с сервисного/сетевого порта должным образом. При обращении к IPv6-адресу *link-local* необходимо также указать интерфейс сервисного или сетевого порта с помощью параметра *serviceport* или *network*.

Значение по умолчанию: счетчик по умолчанию: 1;

интервал по умолчанию: 3 секунды;

размер по умолчанию: 0 байт.

Формат: `ping ipv6 {ipv6-global-address|hostname | {interface {unit/slot/port | vlan vlan-id| serviceport | loopback | tunnel | network} link-local-address} [size datagram-size][outgoing-interface {unit/slot/port | vlan 1-4093 | serviceport | network}]}`

Режим ввода команд: привилегированный

пользовательский

ping ipv6 interface

Используйте эту команду, чтобы определить, есть ли другой компьютер в сети. Чтобы использовать команду, требуется настроить на коммутаторе стандартное (in-band) сетевое подключение. Коммутатор можно вызывать командой ping с любого IP-адреса рабочей станции, подключенной к коммутатору посредством виртуальной сети по умолчанию (VLAN 1), если между коммутатором и рабочей станцией есть физически доступный маршрут. Интерфейс терминала отправляет к целевой станции три сигнала *ping*. Используйте ключевое слово *interface*, чтобы вызывать интерфейс с использованием адреса *link-local* или глобального IPv6-адреса интерфейса. В качестве интерфейса источника можно использовать loopback-интерфейс, сетевой или сервисный порт, туннель или физический интерфейс. Используйте необязательное ключевое слово *size*, чтобы указать размер пакета ping. Параметр *ipv6-address* представляет собой IPv6-адрес локального подключения запрашиваемого устройства. Используйте опцию outgoing-interface, чтобы указать исходящий интерфейс для многоадресного IP/IPv6-вызова ping.

Формат: `ping ipv6 interface {`*`unit/slot/port`* `| loopback` *`loopback-id`* `|network |serviceport|tunnel` *`tunnel-id`*`} {link-local-address` *`link-local-address`* `|` *`ipv6-address`*`} [size` *`datagram-size`*`] [out-going-interface {`*`unit/slot/port`* `| vlan 1-4093 | serviceport | network}]`

Режимы ввода команд: привилегированный

пользовательский

Ключевое слово	***Описание***
interface	Используйте ключевое слово interface, чтобы вызывать интерфейс с использованием адреса link-local или глобального IPv6-адреса интерфейса.
size	Используйте необязательное ключевое слово size, чтобы указать размер пакета ping.
ipv6-address	IPv6-адрес локального подключения запрашиваемого устройства.

14.2 Команды настройки туннельного интерфейса

Команды, приведенные в этой части, помогают создавать и удалять туннельные интерфейсы, а также управлять ими. Несколько различных типов туннелей обеспечивают функциональные возможности для ускорения перехода от IPv4-сетей к IPv6-сетям. Типы туннелей разделены на два класса: настроенные и автоматические. Различие состоит в том, что настроенные туннели имеют явную конфигурацию с указанием пункта назначения или конечной точки туннеля. А автоматические туннели определяют конечную точку на основании адреса назначения пакетов, которые маршрутизируются в этот туннель. Чтобы назначить IP-адрес туннельному интерфейсу, см. команду ip address. Чтобы назначить IPv6-адрес туннельному интерфейсу, см. команду ipv6 address.

interface tunnel

Используйте эту команду для входа в режим конфигурирования интерфейса для туннельного интерфейса. Диапазон значений для *tunnel-id* — от 0 до 7.

Формат: `interface tunnel` *`tunnel-id`*

Режим ввода команд: глобальная конфигурация

no interface tunnel

Эта команда удаляет туннельный интерфейс и соответствующие параметры конфигурации указанного туннельного интерфейса.

Формат: `no interface tunnel tunnel-id`

Режим ввода команд: глобальная конфигурация

tunnel source

Данная команда указывает исходный транспортный адрес туннеля — явным образом либо путем ссылки на интерфейс.

Формат: `tunnel source {ipv4-address | ethernet unit/slot/port}`

Режим ввода команд: конфигурирование интерфейса

tunnel destination

Эта команда указывает целевой транспортный адрес туннеля.

Формат: `tunnel destination {ipv4-address}`

Режим ввода команд: конфигурирование интерфейса

tunnel mode ipv6ip

Данная команда устанавливает режим туннеля. При указании необязательного аргумента 6to4 режим туннеля устанавливается как 6to4 automatic. Без дополнительного аргумента 6to4 режим туннеля устанавливается как configured.

Формат: `tunnel mode ipv6ip [6to4]`

Режим ввода команд: конфигурирование интерфейса

show interface tunnel

Эта команда отображает параметры, относящиеся к туннелю, например режим туннеля, исходный адрес туннеля и адрес назначения туннеля.

Формат: `show interface tunnel [tunnel-id]`

Режим ввода команд: привилегированный

Если идентификатор туннеля не указан, команда отображает для каждого настроенного туннеля следующую информацию.

Термин	*Значение*
Tunnel ID	Идентификационный номер туннеля.
Interface	Имя туннельного интерфейса.
Tunnel Mode	Режим туннеля.
Source Address	Исходный транспортный адрес туннеля.
Destination Address	Целевой транспортный адрес туннеля.

Если идентификатор туннеля указан, команда отображает для туннеля следующую информацию.

Термин	*Значение*
Interface Link Status	Показывает, создано или разорвано соединение.
MTU Size	Значение MTU для пакетов на данном интерфейсе.
IPv6 Address/ Length	Если на интерфейсе включен IPv6 и назначен адрес, команда отображает IPv6-адрес и префикс.

14.3 Команды настройки loopback-интерфейса

В этой части представлены команды, с помощью которых можно создавать и удалять *loopback*-интерфейсы, а также управлять ими. Ожидается, что *loopback*-интерфейс всегда находится в поднятом состоянии. Такой интерфейс может предоставлять адрес источника для отправляемых пакетов и принимать как локальные, так и удаленные пакеты. Loopback-интерфейсы обычно используются протоколами маршрутизации.

Чтобы назначить *loopback*-интерфейсу IP-адрес, см. команду *ip address*. Чтобы назначить IPv6-адрес *loopback*-интерфейсу, см. команду *ipv6 address*.

interface loopback

Используйте эту команду для входа в режим конфигурирования интерфейса для loopback-интерфейса. Диапазон идентификатора: от 0 до 7.

Формат: `interface loopback` *`Loopback-id`*

Режим ввода команд: глобальная конфигурация

no interface loopback

Эта команда удаляет *loopback*-интерфейс и соответствующие параметры конфигурации указанного loopback-интерфейса.

Формат: `no interface loopback` *`Loopback-id`*

Режим ввода команд: глобальная конфигурация

show interface loopback

Данная команда отображает информацию о настроенном *loopback*-интерфейсе.

Формат: `show interface loopback [`*`Loopback-id`*`]`

Режим ввода команд: привилегированный

Если идентификатор *loopback*-интерфейса не указан, для каждого loopback-интерфейса в системе отображается следующая информация.

Термин	*Значение*
Loopback ID	Идентификатор loopback-интерфейса, состояние которого отображается в данной строке.
Interface	Имя интерфейса.

IP Address	IPv4-адрес интерфейса.

При указании идентификатора loopback-интерфейса отображается следующая информация.

Термин	***Значение***
Interface Link Status	Показывает, создано или разорвано соединение.
IP Address	IPv4-адрес интерфейса.
MTU size	Значение MTU для пакетов на данном интерфейсе в байтах.

14.4 Команды IPv6-маршрутизации

В этой части приведены команды, используемые для настройки протокола IPv6 на уровне системы и конкретных интерфейсов. Здесь также описаны команды управления настройками IPv6 и команды просмотра оперативного состояния устройства.

ipv6 hop-limit

Эта команда устанавливает количество хопов для одноадресных ipv6-пакетов, которые создаются на данном узле. Данное значение также включается в анонсы маршрутизатора. Действительные значения параметра hops находятся в диапазоне 1–255 включительно. Значение по умолчанию «не настроено» означает, что в анонсах маршрутизатора указывается значение, равное нулю, а в пакетах, создаваемых на данном узле, передается значение 64. Примечание: настройка значения 64 приводит к другим результатам.

Значение по умолчанию: не настроено

Формат: `ipv6 hop-limit` *hops*

Режим ввода команд: глобальная конфигурация

no ipv6 hop-limit

Эта команда возвращает количество хопов в значение по умолчанию.

Формат: `no ipv6 hop-limit`

Режим ввода команд: глобальная конфигурация

ipv6 unicast-routing

Используйте эту команду, чтобы включить переадресацию одноадресных IPv6-дейтаграмм.

Значение по умолчанию: выключено

Формат: `ipv6 unicast-routing`

Режим ввода команд: глобальная конфигурация

no ipv6 unicast-routing

Данная команда выключает переадресацию одноадресных IPv6-дейтаграмм.

Формат: `no ipv6 unicast-routing`

Режим ввода команд: глобальная конфигурация

ipv6 enable

Используйте эту команду для включения IPv6-маршрутизации на интерфейсе или диапазоне интерфейсов, включая туннельные и loopback-интерфейсы, для которых не был явным образом настроен IPv6-адрес. При использовании этой команды интерфейс автоматически настраивается с адресом link-local. Не используйте эту команду, если на интерфейсе настроен глобальный IPv6-адрес.

Значение по умолчанию: выключено

Формат: `ipv6 enable`

Режим ввода команд: конфигурирование интерфейса

no ipv6 enable

Команда для выключения IPv6-маршрутизации на интерфейсе.

Формат: `no ipv6 enable`

Режим ввода команд: конфигурирование интерфейса

ipv6 address

Используйте эту команду, чтобы настроить IPv6-адрес на интерфейсе или наборе интерфейсов, включая туннельный и loopback-интерфейс, а также включить обработку IPv6 на этом интерфейсе. С помощью этой команды для интерфейса можно назначить несколько глобально доступных адресов. Назначать с помощью этой команды адрес link-local не требуется, поскольку он создается автоматически. Поле prefix состоит из битов настраиваемого адреса. Значение prefix_length устанавливает, сколько смежных битов высокого порядка данного адреса составляют префикс.

IPv6-адреса можно выразить в восьми блоках. Отметим также, что блоки разделяются между собой двоеточиями, а не точками. Для упрощения начальные нули каждого 16-разрядного блока могут быть опущены. Одна последовательность 16-битовых блоков, содержащих только нули, может быть заменена двойным двоеточием "::", но не более одного раза подряд (в противном случае адрес не будет являться уникальным).

- С пропусками нулей: `3ffe:ffff:100:f101:0:0:0:1` becomes `3ffe:ffff:100:f101::1`
- Локальный сервер: `0000:0000:0000:0000:0000:0000:0000:0001` becomes `::1`
- Любой сервер: `0000:0000:0000:0000:0000:0000:0000:0000` becomes `::`

Буквы, используемые в шестнадцатеричных IPv6-адресах, не чувствительны к регистру. Примером выражения префикса и длины префикса IPv6 является `3ffe:1::1234/64`.

Необязательное поле [eui-64] обозначает, что обработка IPv6 на интерфейсах была включена с использованием идентификатора интерфейса EUI-64 в 64 битах низкого порядка в адресе. При использовании этой опции значение prefix_length должно составлять 64 бита.

Формат: `ipv6 address` *`prefix/prefix_length`* `[eui64]`

Режим ввода команд: конфигурирование интерфейса

no ipv6 address

Используйте эту команду, чтобы удалить все IPv6-адреса на интерфейсе или конкретный IPv6-адрес. Параметр prefix состоит из битов настраиваемого адреса. Значение prefix_length устанавливает, сколько смежных битов высокого порядка данного адреса составляют префикс. Необязательное поле [eui-64] обозначает, что обработка IPv6 на интерфейсах была включена с использованием идентификатора интерфейса EUI-64 в 64 битах низкого порядка в адресе.

Если никакие параметры не указаны, команда удаляет все IPv6-адреса на интерфейсе.

Формат: `no ipv6 address [prefix/prefix_length] [eui64]`

Режим ввода команд: конфигурирование интерфейса

ipv6 address autoconfig

Данная команда позволяет стандартному (in-band) интерфейсу получить IPv6-адрес посредством IPv6 Neighbor Discovery Protocol (NDP) и использования сообщений анонсов маршрутизатора.

Значение по умолчанию: выключено

Формат: `ipv6 address autoconfig`

Режим ввода команд: конфигурирование интерфейса

no ipv6 address autoconfig

Данная команда устанавливает состояние автоматической настройки IPv6 на интерфейсе в значение по умолчанию.

Формат: `no ipv6 address autoconfig`

Режим ввода команд: конфигурирование интерфейса

ipv6 address dhcp

Эта команда включает DHCPv6-клиент на стандартном интерфейсе, позволяя ему получать информацию о сети, например IPv6-адрес, от сетевого DHCP-сервера.

Значение по умолчанию: выключено

Формат: `ipv6 address dhcp`

Режим ввода команд: конфигурирование интерфейса

no ipv6 address dhcp

Данная команда освобождает арендованный адрес и выключает DHCPv6 на интерфейсе.

Формат: `no ipv6 address dhcp`

Режим ввода команд: конфигурирование интерфейса

ipv6 route

Используйте эту команду, чтобы настроить статический IPv6-маршрут. Параметр ipv6-prefix — это целевая IPv6-сеть для данного статического маршрута. Prefix_length это десятичное значение

(обычно 0–64), которое показывает, сколько смежных битов высокого порядка данного адреса составляют префикс. Значению prefix_length должна предшествовать косая черта. Next-hop-address — это IPv6-адрес ближайшего узла, который может быть использован для доступа в указанную сеть. При указании Null0 в качестве значения ближайшего маршрутизатора происходит добавление статического маршрута отказа. Параметр preference используется маршрутизатором при сравнении данного маршрута с маршрутами из других источников, которые имеют тот же пункт назначения. Диапазон значений preference — 1–255, значение по умолчанию равно 1. Аргумент unit/slot/port относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово vlan используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата unit/slot/port). Чтобы идентифицировать прямые статические маршруты из двухточечных соединений и широковещательных интерфейсов, можно указывать параметры unit/slot/port, vlan id или tunnel tunnel_id. При использовании адреса link-local в качестве соседнего узла необходимо указать интерфейс. Маршрут со значением preference 255 нельзя использовать для передачи трафика.

Значение по умолчанию: выключено

Формат: `ipv6 route` *`ipv6-prefix/prefix_length`* {*`next-hop-address`* | `Null0` | `interface` {*`unit/ slot/port`*|`vlan` *`1-4093`*|`tunnel` *`tunnel_id`*} *`next-hop-address`*} [*`preference`*]

Режим ввода команд: глобальная конфигурация

no ipv6 route

Команда используется для удаления статического IPv6-маршрута. Используйте эту команду без указания необязательных параметров, чтобы удалить все статические маршруты к указанному месту назначения. Используйте параметр *preference*, чтобы установить приоритет маршрута в значение по умолчанию.

Формат: `no ipv6 route` *`ipv6-prefix/prefix_length`* [{*`next-hop-address`* | `Null0` | `interface` {*`unit/ slot/port`*|`vlan` *`1-4093`*|`tunnel` *`tunnel_id`*} *`next-hop-address`* | *`preference`*}]

Режим ввода команд: глобальная конфигурация

ipv6 route distance

Эта команда устанавливает дистанцию (приоритет) по умолчанию для статичных IPv6-маршрутов. При определении оптимального маршрута предпочтение отдается более низким значениям дистанции маршрута. Команда ipv6 route позволяет дополнительно установить дистанцию (приоритет) для конкретных статических маршрутов. Если дистанция не указана с помощью этой команды, используется дистанция по умолчанию.

Изменение дистанции по умолчанию не обновляет дистанцию существующих статических маршрутов, даже если изначально они были назначены дистанциями по умолчанию. Новая дистанция по умолчанию будет применяться только к статическим маршрутам, созданным после выполнения команды ipv6 route distance.

Значение по умолчанию: 1

Формат: `ipv6 route distance` *`1-255`*

Режим ввода команд: глобальная конфигурация

no ipv6 route distance

Эта команда сбрасывает приоритет статического маршрута на маршрутизаторе до первоначального значения по умолчанию. При определении оптимального маршрута предпочтение отдается более низким значениям приоритета маршрута.

Формат: `no ipv6 route distance`

Режим ввода команд: глобальная конфигурация

ipv6 route net-prototype

Эта команда добавляет сетевые прототипы маршрутов IPv6.

Формат: `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
prefix/prefix-length	Целевая сеть и маска маршрута.
nexthopip	Ближайший IP-адрес, который должен принадлежать активному интерфейсу маршрутизации, но не обязательно быть разрешенным.
num-routes	Количество маршрутов, которые необходимо добавить, начиная с указанного аргумента префикса и в пределах длины указанного префикса.

no ipv6 route net-prototype

Команда удаляет все добавленные сетевые прототипы маршрутов IPv6.

Формат: `ip route net-prototype` *`prefix/prefix-length nexthopip num-routes`*

Режим ввода команд: глобальная конфигурация

ipv6 mtu

Данная команда устанавливает значение Maximum Transmission Unit (MTU) в байтах для IPv6-пакетов на интерфейсе маршрутизации или диапазоне интерфейсов. Команда заменяет значение по умолчанию или MTU соединения новым значением MTU.

Значение MTU по умолчанию для туннельного интерфейса равно 1280. Это значение изменить нельзя

Значение по умолчанию: 1500

Формат: `ipv6 mtu 1280-12270`

Режим ввода команд: конфигурирование интерфейса

no ipv6 mtu

Эта команда устанавливает MTU в значение по умолчанию.

Формат: `no ipv6 mtu`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd dad attempts

Эта команда устанавливает количество запросов по обнаружению дубликатов адресов, передаваемых на интерфейсе или диапазоне интерфейсов. Запросы по обнаружению дубликатов адресов проверяют, является ли IPv6-адрес на интерфейсе уникальным.

Значение по умолчанию: 1

Формат: `ipv6 nd dad attempts` *`0 - 600`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd dad attempts

Эта команда сбрасывает количество запросов по обнаружению дубликатов адресов к значению по умолчанию.

Формат: `no ipv6 nd dad attempts`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd managed-config-flag

Данная команда устанавливает значение флага «managed address configuration» в анонсах маршрутизатора на интерфейсе или диапазоне интерфейсов. Когда указано значение true, конечные узлы используют DHCPv6. Когда указано значение false, конечные узлы настраивают адреса автоматически.

Значение по умолчанию: false

Формат: `ipv6 nd managed-config-flag`

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd managed-config-flag

Эта команда возвращает флаг «managed address configuration» в анонсах маршрутизатора в значение по умолчанию.

Формат: `no ipv6 nd managed-config-flag`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd ns-interval

Эта команда настраивает интервал (в миллисекундах) между анонсами маршрутизатора для передачи сообщений Neighbor Solicitation. Анонсируемое значение 0 означает, что интервал не задан. Команда выполняет настройку отдельного интерфейса или диапазона интерфейсов.

Значение по умолчанию: 0

Формат: `ipv6 nd ns-interval {`*`1000-4294967295 | 0`*`}`

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd ns-interval

Эта команда возвращает интервал повторной передачи сообщений Neighbor Solicitation на указанном интерфейсе в значение по умолчанию.

Формат: `no ipv6 nd ns-interval`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd other-config-flag

Данная команда устанавливает значение флага «other stateful configuration» в анонсах маршрутизатора, отправляемых с интерфейса.

Значение по умолчанию: false

Формат: `ipv6 nd other-config-flag`

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd other-config-flag

Команда возвращает флаг «other stateful configuration» в анонсах маршрутизатора, отправляемых с интерфейса, в значение по умолчанию.

Формат: `no ipv6 nd other-config-flag`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd ra-interval

Данная команда устанавливает интервал передачи между анонсами маршрутизатора на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: 600

Формат: `ipv6 nd ra-interval-max` *`4- 1800`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd ra-interval

Команда возвращает интервал между анонсами маршрутизатора в значение по умолчанию.

Формат: `no ipv6 nd ra-interval-max`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd ra-lifetime

Эта команда устанавливает значение в секундах для поля *Router Lifetime* в анонсах маршрутизатора, отправленных с интерфейса или диапазона интерфейсов. Значение *lifetime* указывается как ноль или должно быть целым числом в пределах между значением интервала передачи анонсов маршрутизатора и 9000. Нулевое значение означает, что этот маршрутизатор не предполагается использовать в качестве маршрутизатора по умолчанию.

Значение по умолчанию: 1800

Формат: `ipv6 nd ra-lifetime` *`lifetime`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd ra-lifetime

Команда возвращает поле Router Lifetime в значение по умолчанию.

Формат: `no ipv6 nd ra-lifetime`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd ra hop-limit unspecified

Данная команда настраивает маршрутизатор на интерфейсе на отправку сообщений Router Advertisement с неустановленным (0) текущим значением Hop Limit. Для серверов на данном соединении такое значение является указанием игнорировать Hop Limit с этого маршрутизатора.

Значение по умолчанию: выключено

Формат: `ipv6 nd ra hop-limit unspecified`

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd ra hop-limit unspecified

Команда настраивает маршрутизатор на интерфейсе на отправку сообщений Router Advertisement с глобально настроенным значением Hop Limit.

Формат: `no ipv6 nd ra hop-limit unspecified`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd reachable-time

Эта команда устанавливает время для анонсов маршрутизатора, в течение которого (с момента получения подтверждения обнаружения) соседний узел будет считаться доступным. Период доступности указывается в миллисекундах. Нулевое значение означает, что период для маршрутизатора не определен. Команда выполняет настройку отдельного интерфейса или диапазона интерфейсов.

Значение по умолчанию: 0

Формат: `ipv6 nd reachable-time` *`0–4294967295`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd reachable-time

Эта команда означает, что период для маршрутизатора не определен.

Формат: `no ipv6 nd reachable-time`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd router-preference

Используйте эту команду для настройки приоритета маршрутизатора по умолчанию, который интерфейс будет передавать в сообщениях анонсов маршрутизатора.

Значение по умолчанию: medium

Формат: `ipv6 nd router-preference { low | medium | high}`

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd router-preference

Эта команда сбрасывает настройку приоритета маршрутизатора по умолчанию, передаваемую интерфейсом, в значение по умолчанию.

Формат: `no ipv6 nd router-preference`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd suppress-ra

Эта команда подавляет передачу анонсов маршрутизатора на интерфейсе или диапазоне интерфейсов.

Значение по умолчанию: выключено

Формат: `ipv6 nd suppress-ra`

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd suppress-ra

Эта команда позволяет осуществлять передачу анонсов маршрутизатора на интерфейсе.

Формат: `no ipv6 nd suppress-ra`

Режим ввода команд: конфигурирование интерфейса

ipv6 nd prefix

Команда *ipv6 nd pr*efix используется для настройки параметров, связанных с префиксами, которые маршрутизатор передает в своих анонсах. Первый необязательный параметр — lifetime данного маршрутизатора, в секундах. Можно указать конкретное время или установить для lifetime бесконечное значение (infinite). Второй необязательный параметр — *preferred* lifetime маршрутизатора.

Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Маршрутизатор анонсирует глобальные префиксы IPv6 в сообщениях Router Advertisement (RA). RA включает в себя только префиксы IPv6-адресов, настроенные на передающем интерфейсе. Адреса настраиваются с помощью команды *ipv6 address* в режиме конфигурирования интерфейса. Каждый анонс префикса включает в себя информацию о префиксе, например значение параметра lifetime и указание, должны ли серверы использовать для определения соединения этот префикс или автоматическую настройку адреса. Используйте команду ipv6 nd prefix для настройки всех этих значений.

Команда *ipv6 nd prefix* позволяет настроить значения префикса RA перед настройкой связанного адреса интерфейса. Чтобы префикс был включен в сообщения RA, необходимо настроить адрес, соответствующий префиксу, с помощью команды *ipv6 address*. Префиксы, заданные с помощью *ipv6 nd prefix* без соответствующего адреса интерфейса, не будут включены в RA и использованы в конфигурации устройства.

Значение по умолчанию: valid-lifetime — 2 592 000;

preferred-lifetime — 604 800;

autoconfig — enabled;

on-link — enabled.

Формат: `ipv6 nd prefix` *`prefix/prefix_length [{0-4294967295 | infinite} {0-4294967295 | infinite}] [no-autoconfig off-link]`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 nd prefix

Эта команда устанавливает конфигурацию префикса в значение по умолчанию.

Формат: `no ipv6 nd prefix` *`prefix/prefix_length`*

Режим ввода команд: конфигурирование интерфейса

ipv6 neighbor

Команда настраивает статический соседний IPv6-узел сети с указанными IPv6- и MAC-адресами на интерфейсе маршрутизации или узловом интерфейсе.

Формат: `ipv6 neighbor` *`ipv6address {unit/slot/port`*`|vlan` *`1-4093}`* *`mac-addr`*

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
ipv6address	IPv6-адрес соседнего узла.
unit/slot/port	Значение *unit/slot/port* указанного интерфейса.
vlan	VLAN для интерфейса.
macaddr	MAC-адрес соседнего узла.

no ipv6 neighbor

Эта команда удаляет статический соседний IPv6-узел с указанным IPv6-адресом на интерфейсе маршрутизации или интерфейсе сервера.

Формат: `no ipv6 neighbor` *`ipv6address {unit/slot/port`*`|vlan` *`1-4093}`*

Режим ввода команд: глобальная конфигурация

ipv6 neighbors dynamicrenew

Используйте эту команду, чтобы автоматически обновлять записи соседних IPv6-узлов. Выполнение данной команды включает/выключает отправку периодических запросов NUD (Neighbor Unreachability Detection) для существующих записей о соседних IPv6-узлах на основании активности этих записей в аппаратном обеспечении. Если отправка выключена, запросы NUD по истечении заданного интервала STALE (1200 секунд) отправляются только для тех записей, которые активно

используются на данном аппаратном обеспечении. Если отправка включена, каждые 40 секунд выполняются запросы NUD для всех 300 записей, независимо от их использования.

Значение по умолчанию: выключено

Формат: `ipv6 neighbors dynamicrenew`

Режим ввода команд: глобальная конфигурация

no ipv6 neighbors dynamicrenew

Команда выключает автоматическое обновление записей соседних IPv6-узлов.

Формат: `no ipv6 neighbors dynamicrenew`

Режим ввода команд: глобальная конфигурация

ipv6 nud

Используйте эту команду для настройки запросов NUD. Запросы NUD выполняют проверку связи с соседними узлами сети.

Формат: `ipv6 nud {backoff-multiple | max-multicast-solicits | max-unicast-solicits}`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
backoff-multiple	Устанавливает экспоненциальный множитель для вычисления отсрочки передачи сообщений Neighbor Solicitation (NS) во время запросов NUD. Значение может быть от 1 до 5. Значение по умолчанию — 1. Если значение с расчетом экспоненциальной отсрочки получается более 60 секунд, интервал ограничивается максимальным значением 60 секунд.
max-multicast-solicits	Устанавливает максимальное количество многоадресных сообщений NS, отправленных в процессе NUD. Значение может быть от 3 до 255. Значение по умолчанию — 3.
max-unicast-solicits	Устанавливает максимальное количество одноадресных сообщений NS, отправленных в процессе NUD. Значение может быть от 3 до 10. Значение по умолчанию — 3.

ipv6 prefix-list

Чтобы создать список префиксов или добавить запись в такой список, используйте команду *ipv6 prefix-list* в режиме глобальной конфигурации. Списки префиксов позволяют сопоставлять префиксы маршрутов с префиксами, указанными в списке. Каждый список префиксов включает в себя последовательность записей префиксов, упорядоченных в соответствии с порядковыми номерами. Маршрутизатор последовательно проверяет каждый элемент списка префиксов, чтобы определить, совпадает ли префикс маршрута с префиксом записи. Если список префиксов пуст или не существует, разрешены все префиксы. Отказ подразумевается для тех случаев, когда префикс не соответствует ни одной записи из списка. Найдя совпадение или получив отказ, маршрутизатор не проверяет остальную часть списка. Список префиксов можно использовать в карте маршрутов для сопоставления префикса маршрута при использовании команды *match ip address*.

Настроить можно до 128 списков префиксов. Максимальное количество записей в списке префиксов — 64.

Значение по умолчанию: По умолчанию списки префиксов отсутствуют. Если опции **ge** и **le** не настроены, префикс места назначения должен точно совпадать с сетью/длиной. Если настроена опция **ge** без опции **le**, любой префикс с маской сети, равной или превышающей значение **ge,** считается совпадением. Аналогично, если настроена опция **le** без опции **ge**, префикс с маской сети, равной или меньше значения **le,** считается совпадением.

Формат: `ipv6 prefix-list` *`list-name`* {[`seq` *`number`*] {`permit` | `deny`} *`ipv6-prefix/prefix-length`* [`ge` *`length`*] [`le` *`length`*] | `renumber` *`re-number-interval first-statement-number`*}

Режим ввода команд: глобальная конфигурация

Термин	***Значение***
list-name	Текстовое имя списка префиксов. Длина — до 32 символов.
seq number	Порядковый номер данного заявления в списке префиксов (необязательный параметр). Заявления в списке префиксов упорядочены от наименьшего порядкового номера к большему и применяются в указанном порядке. Если вы не указываете порядковый номер, система автоматически присваивает заявлению порядковый номер на пять единиц больше последнего номера в списке. Нельзя настроить два заявления с одним и тем же порядковым номером. Значение может быть от 1 до 4294967294.
permit	Разрешить маршруты, префикс места назначения в которых совпадает с записью.
deny	Отклонить маршруты, префикс места назначения в которых совпадает с записью.
ipv6-prefix/prefix-length	Указывает критерий совпадения для маршрутов, сопоставляемых с записями списка префиксов. Значение ipv6-prefix может обозначать любой действительный IP-префикс. Значение length может обозначать любой префикс IPv6 длиной от 0 до 32.
ge length	(Необязательный параметр.) Если эта опция настроена, префикс считается совпадением, если длина маски сети больше либо равна указанному значению. Значение должно быть больше длины сети и меньше либо равно 32.
le length	(Необязательный параметр.) Если эта опция настроена, префикс считается совпадением, если длина маски сети меньше либо равна указанному значению. Значение должно быть больше длины ge и меньше либо равно 32.
renumber	(Необязательный параметр.) Предоставляет возможность изменить порядковую нумерацию записей в списке IP-префиксов с заданным интервалом, начиная с указанного порядкового номера. Диапазон значений для renumber-interval — 1–100, диапазон значений для first-statement-number — 1–1000.

no ipv6 prefix-list

Чтобы удалить список префиксов или запись в списке префиксов, используйте **no**-форму данной команды. Команда **no ipv6 prefix-list list-name** удаляет весь список префиксов. Чтобы удалить отдельную запись в списке префиксов, необходимо точно указать эту запись со всеми опциями.

Формат: `no ipv6 prefix-list` *`list-name`* [`seq` *`number`*] {`permit` | `deny`} *`network/length`* [`ge` *`length`*] [`le` *`length`*]

Режим ввода команд: глобальная конфигурация

ipv6 unreachables

Команда позволяет включить генерацию сообщений ICMPv6 Destination Unreachable на интерфейсе или диапазоне интерфейсов. По умолчанию генерация сообщений ICMPv6 Destination Unreachable включена.

Значение по умолчанию: включено

Формат: `ipv6 unreachables`

Режим ввода команд: конфигурирование интерфейса

no ipv6 unreachables

Используйте эту команду, чтобы запретить генерацию сообщений ICMPv6 Destination Unreachable.

Формат: `no ipv6 unreachables`

Режим ввода команд: конфигурирование интерфейса

ipv6 unresolved-traffic

Данная команда позволяет контролировать скорость, с которой IPv6-пакеты данных поступают в процессор. По умолчанию ограничение скорости выключено. Если ограничение включено, скорость может составлять от 50 до 1024 пакетов в секунду.

Значение по умолчанию: 1024

Формат: `ipv6 unresolved-traffic rate-limit <50-1024>`

Режим ввода команд: глобальная конфигурация

no ipv6 unresolved-traffic

Используйте эту команду, чтобы вернуть ограничение скорости входящего трафика в значение по умолчанию.

Формат: `no ipv6 unresolved-traffic rate-limit`

Режим ввода команд: глобальная конфигурация

ipv6 icmp error-interval

Используйте данную команду, чтобы ограничить скорость, с которой отсылаются сообщения об ошибке ICMPv6. Ограничение скорости настраивается как группа с двумя настраиваемыми параметрами: *burst-size* и *burst-interval*.

Параметр *burst-interval* определяет, как часто группа инициализируется с параметрами burst-size. Значение *burst-interval* — от 0 до 2 147 483 647 миллисекунд (мс).

Параметр *burst-size* — это количество ICMPv6-сообщений об ошибке, которые могут быть посланы за время *burst-interv*al. Диапазон: от 1 до 200 сообщений.

Чтобы выключить ограничение скорости ICMP, необходимо установить параметр *burst-interval* на ноль (0).

Значение по умолчанию: *burst-interval* – 1000 мс

burst-size – 100 сообщений

Формат: ipv6 icmp error-interval *burst-interval* [*burst-size*]

Режим ввода команд: глобальная конфигурация

no ipv6 icmp error-interval

Используйте **no**-форму команды, чтобы вернуть *burst-interval* и *burst-size* в значения по умолчанию.

Формат: `no ipv6 icmp error-interval`

Режим ввода команд: глобальная конфигурация

show ipv6 brief

Данная команда отображает состояния режима IPv6-переадресации и режима одноадресной IPv6-маршрутизации.

Формат: `show ipv6 brief`

Режим ввода команд: привилегированный

Термин	*Значение*
IPv6 Forwarding Mode	Показывает, включен ли режим IPv6-переадресации.
IPv6 Unicast Routing Mode	Показывает, включен ли режим одноадресной IPv6-маршрутизации.
IPv6 Hop Limit	Показывает количество хопов для одноадресных IPv6-пакетов, которые создаются на данном узле. Подробнее см. в описании команды ipv6 hop-limit.
ICMPv6 Rate Limit Error Interval	Показывает, как часто группа инициализируется с параметрами burst-size. Подробнее см. в описании команды ipv6 icmp error-interval.
ICMPv6 Rate Limit Burst Size	Показывает количество сообщений об ошибках ICMPv6, которые могут быть присланы за один период burst-interval. Подробнее см. в описании команды ipv6 icmp error-interval.
Maximum Routes	Показывает максимальный размер таблицы IPv6-маршрутизации.
IPv6 Unresolved Data Rate Limit	Показывает скорость (в пакетах в секунду) для IPv6-пакетов данных, отправленных на CPU, после того как эти пакеты не удалось перенаправить из-за неразрешенного сбоя переадресации.
IPv6 Neighbors Dynamic Renew	Показывает режим отправки периодических запросов NUD (Neighbor Unreachability Detection) для существующих записей о соседних IPv6-узлах на основании активности этих записей в аппаратном обеспечении.
IPv6 NUD Maximum Unicast Solicits	Показывает максимальное число одноадресных сообщений Neighbor Solicitations (NS), отправленных в процессе NUD перед коммутацией на отправку многоадресных NS-сообщений.
IPv6 NUD Maximum Multicast Solicits	Показывает максимальное число многоадресных NS-сообщений, отправленных в процессе NUD в адрес соседних устройств в состоянии UNREACHABLE.
IPv6 NUD Exponential Backoff Multiple	Показывает экспоненциальный множитель для вычисления интервала передачи NS-сообщений в процессе NUD в соответствии с алгоритмом экспоненциальной отсрочки.

show ipv6 interface

Используйте эту команду, чтобы отобразить состояние использования интерфейсов IPv6 и возможность отправки сообщений ICMPv6 Destination Unreachable. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Ключевое слово **loopback** непосредственно определяет loopback-интерфейс. Ключевое слово tunnel определяет туннельный IPv6-интерфейс.

Формат: `show ipv6 interface {brief | unit/slot/port|vlan 1-4093|loopback 0-7|tunnel 0-7}`

Режим ввода команд: привилегированный

Если использован параметр *brief*, для всех настроенных IPv6-интерфейсов отображается следующая информация.

Термин	***Значение***
Interface	Интерфейс в формате unit/slot/port.
IPv6 Operational Mode	Показывает, включен ли данный режим.
IPv6 Address/Length	Показывает IPv6-адрес и длину префикса для интерфейсов, где IPv6 включен.
Method	Указывает, как был назначен каждый IP-адрес. Поле содержит одно из следующих значений: • DHCP — адрес предоставлен DHCP-сервером; • Manual — адрес настроен вручную. Глобальные адреса без аннотации считаются настроенными вручную.

Если указан конкретный интерфейс, дополнительно отображается следующая информация.

Термин	***Значение***
Routing Mode	Показывает, включена ли IPv6-маршрутизация.
IPv6 Enable Mode	Показывает, включен ли IPv6 на интерфейсе.
Administrative Mode	Показывает, включен ли административный режим интерфейса.
Bandwidth	Пропускная способность интерфейса.
Interface Maximum Transmission Unit	Размер MTU в байтах.
Router Duplicate Address Detection Transmits	Количество последовательных запросов по обнаружению дубликатов адресов, которое будет передано.
Address Autoconfigure Mode	Показывает, включен ли режим автоматической настройки.
Address DHCP Mode	Показывает, включен ли на интерфейсе DHCPv6-клиент.
IPv6 Hop Limit Unspecified	Указывает, настроен ли маршрутизатор на этом интерфейсе на отправку сообщений Router Advertisements с неустановленным (0) текущим значением Hop Limit.
Router Advertisement NS Interval	Интервал в миллисекундах между отправкой анонсов маршрутизатора при выполнении NS-запросов.
Router Advertisement Lifetime	Показывает значение lifetime для маршрутизатора на данном интерфейсе, передаваемое в анонсах маршрутизатора.
Router Advertisement Reachable Time	Время в миллисекундах, в течение которого (с момента получения подтверждения обнаружения) соседний узел будет считаться доступным.

Router Advertisement Interval	Частота отправки анонсов маршрутизатора в секундах.
Router Advertisement Managed Config Flag	Показывает, установлен (включен) ли флаг «managed address configuration» в анонсах маршрутизатора на интерфейсе.
Router Advertisement Other Config Flag	Показывает, установлен (включен) ли флаг «other configuration» в анонсах маршрутизатора на интерфейсе.
Router Advertisement Router Preference	Показывает приоритет маршрутизатора.
Router Advertisement Suppress Flag	Показывает, работает ли в отношении анонсов маршрутизатора подавление (значение enabled), или они отправляются (значение disabled).
IPv6 Destination Unreachables	Показывает, разрешена отправка сообщений ICMPv6 Destination Unreachable (значение enabled) или запрещена (значение disabled).
ICMPv6 Redirect	Указывает, может ли маршрутизатор отправиться ICMPv6-сообщения о перенаправлении обратно отправителю, если на интерфейсе включен сценарий переадресации.

Если на интерфейсе настроен IPv6-префикс, дополнительно отображается следующая информация.

Термин	***Значение***
IPv6 Prefix is	IPv6-префикс для указанного интерфейса.
Preferred Lifetime	В течение какого времени анонсированный префикс является приоритетным префиксом.
Valid Lifetime	В течение какого времени анонсированный префикс является действительным.
Onlink Flag	Показывает, установлен (включен) ли флаг «onlink» в префиксе.
Autonomous Flag	Показывает, установлен (включен) ли флаг «autonomous address-configuration» (автоматическая настройка) в префиксе.

show ipv6 interface vlan

Используйте команду *show ipv6 interface vlan* в привилегированном режиме, чтобы показать состояние использования IPv6-интерфейсов VLAN.

Формат: `show ipv6 interface vlan` *`vlan-id`* `[prefix]`

Режим ввода команд: привилегированный

пользовательский

Параметр	***Описание***
vlan-id	Действительный идентификатор VLAN.
prefix	Отображает информацию IPv6-префикса на интерфейсе.

show ipv6 dhcp interface

Эта команда отображает список IPv6-адресов, которые в настоящее время выделены DHCP-сервером для указанного стандартного (in-band) интерфейса. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ipv6 dhcp [interface {unit/slot/port|vlan 1-4093}]`

Режимы ввода команд: привилегированный

Термин	*Значение*
Mode	Показывает, находится ли указанный интерфейс в режиме клиента.
State	Состояние DHCPv6-клиента на указанном интерфейсе. Возможны следующие значения: INACTIVE, SOLICIT, REQUEST, ACTIVE, RENEW, REBIND и RELEASE.
Server DUID	Уникальный идентификатор DHCPv6-сервера на данном интерфейсе.
T1 Time	Время T1, заданное DHCPv6-сервером. По истечении этого времени клиент должен предпринять попытку обновить аренду адреса, которым он пользовался.
T2 Time	Время T2, заданное DHCPv6-сервером. Если по истечении этого времени продлить аренду не удается, клиент отправляет на сервер сообщение Rebind.
Interface IAID	Идентификатор Identity Association, выбранной данным клиентом.
Leased Address	IPv6-адрес, выделенный DHCPv6-сервером для этого интерфейса.
Preferred Lifetime	Приоритетное время жизни IPv6-адреса согласно определению стандарта RFC 2462.
Valid Lifetime	Действительное время жизни IPv6-адреса согласно определению стандарта RFC 2462.
Renew Time	Остаток времени до следующей попытки клиента продлить аренду.
Expiry Time	Остаток времени до истечения срока действия адреса.

show ipv6 nd raguard policy

Эта команда отображает состояние функции IPv6 RA GUARD на коммутаторе. При выводе перечисляются порты/интерфейсы, на которых эта функция включена, и соответствующие роли устройства.

Формат: `show ipv6 nd raguard policy`

Режим ввода команд: привилегированный

Параметр	*Описание*
Interface	Порт/интерфейс, на котором включена функция.
Role	Роль связанного устройства для интерфейса.

show ipv6 neighbors

Используйте эту команду, чтобы отобразить информацию о соседних IPv6-узлах.

Формат: `show ipv6 neighbor [interface {unit/slot/port | vlan 1-4093 | tunnel 0-7} | ipv6- address]`

Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Интерфейс в формате unit/slot/port. IPv6 Address IPV6-адрес соседнего узла или интерфейса.
MAC Address	MAC-адрес соседнего узла.

IsRtr	Показывает, является ли соседний узел маршрутизатором. При значении TRUE соседний узел известен как маршрутизатор; при значении FALSE — нет. Значение FALSE может означать, что маршрутизаторы не всегда известны как маршрутизаторы.
Neighbor State	Состояние записи о соседнем узле в таблице. Возможные значения: Incomplete, Reachable, Stale, Delay, Probe и Unknown.
Age	Время в секундах, прошедшее с момента добавления записи в таблицу.
Type	Тип записи о соседнем узле. Имеет значение Static, если запись настроена вручную, и Dynamic, если запись разрешается динамически.

clear ipv6 neighbors

Используйте эту команду, чтобы удалить все записи из таблицы соседних IPv6-узлов или запись, связанную с определенным интерфейсом. Используйте параметр *unit/slot/port* для указания интерфейса, параметр *ipv6address* для указания IPv6-адреса или параметр vlan для указания сети VLAN.

Формат: `clear ipv6 neighbors [{`*`unit/slot/port`* | *`ipv6address`* | `vlan` *`id`*`}]`

Режим ввода команд: привилегированный

show ipv6 protocols

Эта команда отображает сводную информацию о конфигурации и состоянии активных протоколов IPv6-маршрутизации. Команда выводит список протоколов маршрутизации, которые настроены и включены. Если в командной строке выбран определенный протокол, вывод команды будет ограничен только этим протоколом.

Формат: `show ipv6 protocols [bgp|ospf]`

Режим ввода команд: привилегированный

Термин	***Значение***
Раздел BGP	
Routing Protocol	BGP.
Router ID	Идентификатор маршрутизатора, настроенный для BGP.
Local AS Number	Номер AS, к которой относится локальный маршрутизатор.
BGP Admin Mode	Глобальная настройка BGP: enabled или disabled.
Maximum Paths	Максимальное количество ближайших узлов на внутреннем или внешнем маршруте BGP.
Always Compare MED	Настроен ли BGP на сравнение MED для маршрутов, полученных от подключенных устройств в других AS.
Maximum AS Path Length	Ограничение длины AS-путей, которые BGP принимает от соседних устройств.
Fast Internal Failover	Будет ли BGP немедленно выключать смежности iBGP, если менеджер таблицы маршрутизации сообщит, что адрес партнерского устройства больше не доступен.
Fast External Failover	Будет ли BGP немедленно выключать смежности eBGP, если соединение с соседним устройством прервется.
Distance	Административная дистанция (или «приоритет маршрута») по умолчанию для внешних, внутренних и локальных маршрутов BGP. В отображаемой следом таблице перечисляются диапазоны соседних

	адресов, которые были настроены, чтобы переопределить дистанцию по умолчанию на дистанцию указанного соседа. Если адрес соседа подпадает в один из этих диапазонов, маршрутам от этого соседа назначаются настроенные дистанции. Если список префиксов сконфигурирован, дистанция назначается только префиксам от соседних устройств, которые разрешены списком префиксов.
Redistribution	Таблица с информацией для каждого протокола-источника маршрутов(connected, static, rip и ospf). Для каждого из этих источников показывается список анонсирования и карта маршрутов, а также настроенная метрика. Не настроенные поля остаются пустыми. Для OSPF дополнительная строка показывает настроенные параметры соответствия OSPF.
Prefix List In	Глобальный список префиксов, используемых для фильтрации входящих маршрутов от всех соседних устройств.
Prefix List Out	Глобальный список префиксов, используемых для фильтрации исходящих маршрутов для всех соседних устройств.
Networks Originated	Набор сетей, созданных с помощью команды network. Сети, анонсированные соседним устройствам, отмечены как active.
Neighbors	Список настроенных соседних устройств и настроенные для каждого из них входящие и исходящие политики.
Раздел OSPFv3	
Routing Protocol	OSPFv3.
Router ID	Идентификатор маршрутизатора, настроенный для OSPFv3.
OSPF Admin Mode	Включен ли OSPF глобально.
Maximum Paths	Максимальное количество ближайших узлов на маршруте OSPF.
Default Route Advertise	Настроен ли OSPF на создание маршрута по умолчанию.
Always	Зависит ли анонсирование маршрута по умолчанию от наличия маршрута по умолчанию в общей таблице маршрутизации.
Metric	Метрика, настроенная для анонсирования с маршрутом по умолчанию.
Metric Type	Тип метрики для маршрута по умолчанию.

show ipv6 route

Эта команда отображает таблицу IPv6-маршрутизации. Параметр *ipv6-address* указывает конкретный IPv6-адрес, для которого будет отображаться самый оптимальный маршрут. Параметры *ipv6-prefix/ipv6-prefix-length* определяют конкретную IPv6-сеть, для которой будет отображаться оптимальный маршрут. Параметр *interface* указывает, что будут показаны маршруты с ближайшими узлами на данном интерфейсе. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Параметр *protocol* указывает протокол, которым установлены маршруты. Для *protocol* возможны следующие значения: *connected, ospf, static.* Параметр *all* указывает на то, что отображаются все маршруты, включая оптимальные и не оптимальные. При его отсутствии отображаются только оптимальные маршруты.

Если использовать для *protocol* ключевое слово *connected*, опция *all* будет недоступна, потому что наиболее и наименее подходящих подключенных маршрутов не существует.

Формат: show ipv6 route [{*ipv6-address* [*protocol*] | {*ipv6-prefix/ipv6-prefix-length* | *unit/ slot/port*|vlan *1-4093*} [*protocol*] | *protocol* | summary} [all] | all}]

Режимы ввода команд: привилегированный

пользовательский

Столбцы таблицы маршрутизации отображают следующую информацию.

Термин	***Значение***
Code	Коды для протоколов маршрутизации, создавших маршруты.
Default Gateway	IPv6-адрес шлюза по умолчанию. Когда в системе нет более точного маршрута до места назначения пакета, пакет отправляется на шлюз по умолчанию.
IPv6-Prefix/IPv6- Prefix-Length	IPv6-префикс и длина префикса целевой IPv6-сети, соответствующая данному маршруту.
Preference/Metric	Административная дистанция (приоритет) и стоимость (метрика), связанные с этим маршрутом. Пример вывода: [1/0], где 1 является приоритетом, а 0 является метрикой.
Tag	Десятичное значение тега, связанного с перераспределением маршрута, если параметр не равен 0.
Next-Hop	IPv6-адрес следующего маршрутизатора(если таковой существует), через который доступна целевая IPv6-сеть.
Route-Timestamp	Время последнего обновления для динамических маршрутов. Формат для временной метки маршрута будет в виде: • дд:чч:мм, если прошло дней > = 1; • чч:мм:сс если прошло дней < 1.
Interface	Интерфейс маршрутизатора, используемый для направления трафика к следующему целевому узлу. Для отклоненных маршрутов ближайшим будет интерфейс Null0.
T	Флаг, добавляемый к IPv6-маршруту, чтобы указать, что это ECMP-маршрут, но только один из его ближайших узлов был установлен в таблице маршрутизации. Таблица маршрутизации может ограничивать количество ECMP-маршрутов или ECMP-групп. Если ECMP-маршрут не удается установить, потому что достигнуто установленное ограничение, маршрут устанавливается с помощью одного ближайшего узла. Такие сокращенные маршруты обозначаются флагом T после имени интерфейса.

Чтобы административно контролировать трафик, назначенный на определенную сеть, и предотвратить его передачу через маршрутизатор, можно настроить на маршрутизаторе статический маршрут отказа. Такой трафик будет отброшен, и ICMP-сообщение о недоступности места назначения будет послано обратно к источнику. Обычно такой способ используют для предотвращения маршрутных петель. Маршрут отказа, добавленный в RTO, относится к типу OSPF Inter-Area. Маршруты отказа (маршруты типа REJECT, установленные любым протоколом) не распространяются протоколами OSPF/RIP. Маршруты отказа поддерживаются и в OSPFv2, и в OSPFv3.

show ipv6 route ecmp-groups

Эта команда выдает отчет обо всех ECMP-группах в таблице маршрутизации IPv6. ECMP-группы — это набор из двух или более соседних узлов, используемых в одном или нескольких маршрутах. Группы нумеруются произвольно от 1 до n. Вывод команды показывает количество соседних узлов в группе и количество маршрутов, использующих набор этих соседних узлов. При

выводе также указывается IPv6-адрес и исходящий интерфейс для каждого перехода в каждой группе.

Формат: `show ipv6 route ecmp-groups`

Режим ввода команд: привилегированный

show ipv6 route hw-failure

Используйте эту команду для отображения маршрутов, которые не удалось добавить из-за ошибок хэша или переполнения таблицы маршрутизации.

Формат: `show ipv6 route hw-failure`

Режим ввода команд: привилегированный

show ipv6 route net-prototype

Данная команда отображает маршруты прототипа сети. Маршруты прототипов сетей отображаются с меткой P.

Формат: `show ipv6 route net-prototype`

Режимы ввода команд: привилегированный

show ipv6 route preferences

Используйте эту команду, чтобы отобразить значение приоритета, связанного с типом маршрута. Меньшие значения имеют больший приоритет. Маршрут со значением preference 255 нельзя использовать для передачи трафика.

Формат: `show ipv6 route preferences`

Режим ввода команд: привилегированный

Термин	***Значение***
Local	Приоритет непосредственно подключенных маршрутов.
Static	Приоритет статических маршрутов.
OSPF Intra	Приоритет маршрутов в пределах OSPF-зоны.
OSPF Inter	Приоритет маршрутов относительно других OSPF-маршрутов, которые находятся за пределами зоны.
OSPF External	Приоритет внешних OSPF-маршрутов.
BGP External	Приоритет внешних BGP-маршрутов.
BGP Internal	Приоритет маршрутов относительно других BGP-маршрутов, которые находятся за пределами зоны.
BGP Local	Приоритет маршрутов в пределах BGP-зоны.

show ipv6 route summary

Эта команда показывает сводную информацию о состоянии таблицы маршрутизации. Если введено дополнительное ключевое слово *all*, некоторая статистика, например количество маршрутов от каждого источника, включает альтернативные маршруты. Альтернативный маршрут — это маршрут, который не является наиболее приоритетным для места назначения и поэтому не попадает в таблицу маршрутизации. Чтобы включить только количество оптимальных маршрутов, не используйте необязательное ключевое слово.

Формат: `show ipv6 route summary [all]`

Режимы ввода команд: привилегированный
пользовательский

Термин	*Значение*
Connected Routes	Общее количество подключенных маршрутов в таблице маршрутизации.
Static Routes	Общее количество статических маршрутов в таблице маршрутизации.
BGP Routes	Общее количество маршрутов, установленных протоколом BGP.
External	Количество внешних BGP-маршрутов.
Internal	Количество внутренних BGP-маршрутов.
Local	Количество локальных BGP-маршрутов.
OSPF Routes	Общее количество маршрутов, установленных протоколом OSPFv3.
Reject Routes	Общее количество маршрутов отказа, установленных всеми протоколами.
Net Prototype Routes	Общее количество маршрутов прототипов сети.
Number of Prefixes	Суммарное количество маршрутов с префиксами различной длины.
Total Routes	Общее количество маршрутов в таблице маршрутизации.
Best Routes	Количество оптимальных маршрутов в таблице маршрутизации на данный момент. Это количество учитывает только наиболее подходящие маршруты к каждому месту назначения.
Alternate Routes	Количество альтернативных маршрутов в таблице маршрутизации на данный момент. Альтернативный маршрут — это маршрут, который не был определен как оптимальный маршрут к месту назначения.
Route Adds	Количество маршрутов, добавленных в таблицу маршрутизации.
Route Modifies	Количество маршрутов, измененных после того, как они были первоначально добавлены в таблицу маршрутизации.
Route Deletes	Количество маршрутов, которые были удалены из таблицы маршрутизации.
Unresolved Route Adds	Количество добавлений маршрутов, не удавшихся по причине того, что ни один из ближайших узлов не находился в локальной подсети. Обратите внимание: статические маршруты в начале работу могут не добавиться в таблицу маршрутизации, потому что интерфейсы маршрутизации еще не запущены. В этом случае счетчик работает поэтапно. Статические маршруты добавляются в таблицу маршрутизации по мере включения интерфейсов маршрутизации.
Invalid Route Adds	Количество добавлений маршрутов, не удавшихся по причине того, что маршрут был недействительным. Для каждого из таких сбоев выполняется запись в журнале.
Failed Route Adds	Количество добавлений маршрутов, не удавшихся по причине ограничения ресурсов в таблице маршрутизации.
Hardware Failed Route Adds	Количество маршрутов, не добавленных в таблицу маршрутизации по причине ошибки хэша или переполнения таблицы.
Reserved Locals	Количество записей в таблице маршрутизации, зарезервированных для локальной подсети на интерфейсе маршрутизации, который выключен. Место для локальных маршрутов всегда резервируется, чтобы они могли быть установлены в случае отказа интерфейса маршрутизации.
Unique Next Hops	Количество отдельных соседних узлов, используемых всеми текущими маршрутами в таблице маршрутизации. Сюда относятся локальные

	интерфейсы для локальных маршрутов и соседи для непрямых маршрутов.
Unique Next Hops High Water	Наибольшее значение количества отдельных соседних узлов с момента последнего обнуления счетчиков.
Next Hop Groups	Текущее количество групп ближайших узлов, используемых одним или несколькими маршрутами. Каждая группа ближайших узлов включает в себя один или несколько соседних узлов.
Next Hop Groups High Water	Наибольшее значение количества групп ближайших узлов с момента последнего обнуления счетчиков.
ECMP Groups	Количество групп соседних узлов с несколькими узлами.
ECMP Routes	Количество маршрутов с несколькими соседними узлами, находящееся в таблице на данный момент.
Truncated ECMP Routes	Количество ECMP-маршрутов с единственным ближайшим узлом, установленных в таблице маршрутизации на данный момент. Таблица маршрутизации может ограничивать количество ECMP-маршрутов или ECMP-групп. Если ECMP-маршрут не удается установить, потому что достигнуто установленное ограничение, маршрут устанавливается с помощью одного ближайшего узла.
ECMP Retries	Количество ECMP-маршрутов, которые были установлены в таблицу маршрутизации после того, как изначально были установлены с единственным ближайшим узлом.
Routes with n Next Hops	Текущее количество маршрутов для каждого количества соседних узлов.

show ipv6 snooping counters

Эта команда отображает счетчики, связанные с функцией IPv6 RA GUARD. При выводе команды отображается количество анонсов маршрутизатора и переадресованных маршрутизатором пакетов, отброшенных коммутатором глобально из-за включенной функции RA GUARD.

Формат: `show ipv6 snooping counters`

Режимы ввода команд: привилегированный

глобальная конфигурация

show ipv6 vlan

Эта команда отображает адреса виртуальных интерфейсов IPv6-маршрутизации.

Формат: `show ipv6 vlan`

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
MAC Address used by Routing VLANs	Отображает MAC-адрес.

Остальная часть вывода этой команды отображается в виде таблицы со следующими заголовками столбцов:

Заголовок	***Значение***
VLAN ID	Идентификатор настроенной VLAN.

Logical Interface	Интерфейс, связанный с идентификатором VLAN, в формате unit/slot/port.
IPv6 Address/Prefix Length	IPv6-префикс и длина префикса, связанные с идентификатором VLAN.

show ipv6 traffic

Используйте эту команду, чтобы отобразить статистику для IPv6- и ICMPv6-трафика. Укажите логический, туннельный или loopback-интерфейс для просмотра информации о трафике на определенном интерфейсе. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Если интерфейс не указан, команда отображает информацию о трафике на всех интерфейсах.

Формат: `show ipv6 traffic [{`*`unit/slot/port`*`|vlan `*`1-4093`*`| loopback `*`loop-back-id`*` | tunnel `*`tunnel- id`*`}]`

Режим ввода команд: привилегированный

Термин	***Значение***
Total Datagrams Received	Общее число входных дейтаграмм, полученных интерфейсом, в том числе полученных по ошибке.
Received Datagrams Locally Delivered	Общее количество дейтаграмм, успешно доставленных пользовательским протоколам IPv6 (включая ICMP). Количество учитывается на интерфейсе, к которому были адресованы эти дейтаграммы, причем для некоторых дейтаграмм это не обязательно будет входной интерфейс.
Received Datagrams Discarded Due To Header Errors	Количество входных дейтаграмм, отброшенных из-за ошибок в IPv6-заголовках, в том числе из-за несовпадения номера версии, других ошибок формата, превышения количества хопов, ошибок при обработке IPv6-опций и т. д.
Received Datagrams Discarded Due To MTU	Количество входящих дейтаграмм, которые не могут быть переадресованы из-за превышения размера MTU, настроенного для соединения исходящего интерфейса.
Received Datagrams Discarded Due To No Route	Количество отброшенных входящих дейтаграмм по причине невозможности найти маршрут для их передачи по назначению.
Received Datagrams With Unknown Protocol	Количество дейтаграмм, адресованных локально, которые были получены, но отброшены из-за неизвестного или не поддерживаемого протокола. Количество учитывается на интерфейсе, к которому были адресованы эти дейтаграммы, причем для некоторых дейтаграмм это не обязательно будет входной интерфейс.
Received Datagrams Discarded Due To Invalid Address	Количество входящих дейтаграмм, которые были отброшены, потому что IPv6-адрес в поле назначения заголовка не являлся действительным адресом для получения на этом объекте. Это количество включает недействительные адреса (например, ::0) и не поддерживаемые адреса (например, адреса с нераспределенными префиксами). Для объектов, которые не являются IPv6-маршрутизаторами и, следовательно, не пересылают дейтаграммы, в это количество включаются дейтаграммы, отброшенные из-за того, что адрес назначения не являлся локальным адресом.
Received Datagrams Discarded Due To Truncated Data	Количество входящих дейтаграмм, отброшенных из-за того, что кадр дейтаграммы содержал недостаточно данных.
Received Datagrams Discarded Other	Количество входящих IPv6-дейтаграмм, для которых не возникало проблем, мешающих последовательной обработке, но которые были отброшены (например, из-за отсутствия памяти в буфере). Обратите

	внимание, что этот счетчик не включает дейтаграммы, отброшенные в ожидании повторной сборки.
Received Datagrams Reassembly Required	Количество полученных IPv6-фрагментов, которые требуют повторной сборки на этом интерфейсе. Заметим, что это количество учитывается на интерфейсе, к которому были адресованы эти фрагменты, причем для некоторых фрагментов это не обязательно будет входной интерфейс.
Datagrams Successfully Reassembled	Количество IPv6-дейтаграмм, для которых успешно выполнена повторная сборка. Заметим, что это количество учитывается на интерфейсе, к которому были адресованы эти дейтаграммы, причем для некоторых дейтаграмм это не обязательно будет входной интерфейс.
Datagrams Failed To Reassemble	Число сбоев, обнаруженных алгоритмом повторной сборки IPv6 (по любой причине: истекло время ожидания, возникли ошибки и т. д.). Обратите внимание, что это количество не обязательно означает отброшенные IPv6-фрагменты, так как некоторые способны комбинировать фрагменты по мере поступления. Количество учитывается на интерфейсе, к которому были адресованы эти фрагменты, причем для некоторых фрагментов это не обязательно будет входной интерфейс.
Datagrams Forwarded	Количество исходящих дейтаграмм, которые данный объект получил и переадресовал в конечные пункты назначения. В объектах, которые не выступают в роли IPv6-маршрутизаторов, это количество будет включать в себя только те пакеты, которые успешно прошли обработку Source-Route на данном объекте. Обратите внимание, что при успешной переадресации дейтаграммы увеличивается параметр количества на исходящем интерфейсе.
Datagrams Locally Transmitted	Общее количество IPv6-дейтаграмм, которые были переданы локальными пользовательскими IPv6-протоколами (включая ICMP) в запросах на переадресацию. Обратите внимание, что этот счетчик не включает дейтаграммы, подсчитанные как ipv6IfStatsOutForwDatagrams.
Datagrams Transmit Failed	Количество исходящих дейтаграмм, для которых не было обнаружено ни одной проблемы, способной предотвратить их передачу к месту назначения, но которые были отброшены (например, из-за отсутствия буферного пространства). Обратите внимание, что этот счетчик будет включать в себя дейтаграммы, подсчитанные как ipv6IfStatsOutForwDatagrams, если среди них встречаются подходящие
Fragments Created	Количество фрагментов исходящей дейтаграммы, которые были созданы в результате фрагментации на этом выходном интерфейсе.
Datagrams Successfully Fragmented	Количество IPv6-дейтаграмм, которые были успешно фрагментированы на данном выходном интерфейсе.
Datagrams Failed To Fragment	Количество IPv6-дейтаграмм, которые были отброшены, поскольку требовалась их фрагментация на данном выходном интерфейсе, которая не была выполнена.
Fragments Created	Количество фрагментов, которые были созданы.
Multicast Datagrams Received	Количество многоадресных пакетов, принятых интерфейсом.
Multicast Datagrams Transmitted	Количество многоадресных пакетов, переданных интерфейсом.
Total ICMPv6 messages received	Общее количество ICMP-сообщений, принятых интерфейсом, в том числе подсчитанные как ipv6IfIcmpInErrors. Обратите внимание, что речь идет об интерфейсе, к которому были адресованы ICMP-сообщения; это не обязательно будет входной интерфейс для данных сообщений.
ICMPv6 Messages with errors	Количество ICMP-сообщений, которые были приняты на интерфейсе,

	но определены как имеющие специфичные ICMP-ошибки (bad ICMP checksums, bad length и т. д.).
ICMPv6 Destination Unreachable Messages Received	Количество сообщений ICMP Destination Unreachable, принятых интерфейсом.
ICMPv6 Messages Prohibited Administratively Received	Количество сообщений ICMP Destination Unreachable/Communication Administratively Prohibited, принятых интерфейсом.
ICMPv6 Time Exceeded Messages Received	Количество сообщений ICMP Time Exceeded, принятых интерфейсом.
ICMPv6 Parameter Problem Messages Received	Количество сообщений ICMP Parameter Problem, принятых интерфейсом.
ICMPv6 Packet Too Big Messages Received	Количество сообщений ICMP Packet Too Big, принятых интерфейсом.
ICMPv6 Echo Request Messages Received	Количество запросов ICMP Echo, принятых интерфейсом.
ICMPv6 Router Solicit Messages Received	Количество сообщений ICMP Router Solicit, принятых интерфейсом.
ICMPv6 Neighbor Advertisement Messages Received	Количество сообщений ICMP Neighbor Advertisement, принятых интерфейсом.
ICMPv6 Redirect Messages Received	Количество сообщений ICMP Redirect, принятых интерфейсом.
ICMPv6 Group Membership Query Messages Received	Количество сообщений ICMPv6 Group Membership Query, принятых интерфейсом.
ICMPv6 Group Membership Response Messages Received	Количество сообщений ICMPv6 Group Membership Response, принятых интерфейсом.
ICMPv6 Group Membership Reduction Messages Received	Количество сообщений ICMPv6 Group Membership Reduction, принятых интерфейсом.
Total ICMPv6 Messages Transmitted	Общее количество ICMP-сообщений, которые пытался отправить этот интерфейс. Обратите внимание, что в это количество включены сообщения icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	Количество ICMP-сообщений, которые этот интерфейс не отправил из-за ICMP-проблем, например недостаточного объема буфера. Это значение не должно включать ошибки, обнаруженные вне уровня ICMP, например невозможность IPv6-маршрутизации итоговой дейтаграммы. В некоторых вариантах установки не существует типов ошибок, которые учитывались бы в данном значении.
ICMPv6 Destination Unreachable Messages Transmitted	Количество сообщений ICMP Destination Unreachable, отправленных интерфейсом.
ICMPv6 Messages Prohibited Administratively Transmitted	Количество сообщений ICMP Destination Unreachable/Communication Administratively Prohibited, отправленных интерфейсом.
ICMPv6 Time Exceeded Messages Transmitted	Количество сообщений ICMP Time Exceeded, отправленных интерфейсом.
ICMPv6 Parameter Problem Messages Transmitted	Количество сообщений ICMP Parameter Problem, отправленных интерфейсом.
ICMPv6 Packet Too Big Messages Transmitted	Количество сообщений ICMP Packet Too Big, отправленных интерфейсом.
ICMPv6 Echo Request Messages Transmitted	Количество запросов ICMP Echo, отправленных интерфейсом.
ICMPv6 Echo Reply Messages Transmitted	Количество сообщений ICMP Echo Reply, отправленных интерфейсом.
ICMPv6 Router Solicit Messages Transmitted	Количество сообщений ICMP Router Solicitation, отправленных интерфейсом.

ICMPv6 Router Advertisement Messages Transmitted	Количество сообщений ICMP Router Advertisement, отправленных интерфейсом.
ICMPv6 Neighbor Solicit Messages Transmitted	Количество сообщений ICMP Neighbor Solicitation, отправленных интерфейсом.
ICMPv6 Neighbor Advertisement Messages Transmitted	Количество сообщений ICMP Neighbor Advertisement, отправленных интерфейсом.
ICMPv6 Redirect Messages Received	Количество сообщений Redirect, отправленных интерфейсом.
ICMPv6 Group Membership Query Messages Transmitted	Количество сообщений ICMP Group Membership Query, отправленных интерфейсом.
ICMPv6 Group Membership Response Messages Transmitted	Количество сообщений ICMP Group Membership Response, отправленных интерфейсом.
ICMPv6 Group Membership Reduction Messages Transmitted	Количество сообщений ICMP Group Membership Reduction, отправленных интерфейсом.
ICMPv6 Duplicate Address Detects	Количество дублирующих адресов, обнаруженных интерфейсом.

clear ipv6 route counters

Команда сбрасывает счетчики таблицы маршрутизации протокола IPv6, указанные в отчете команды *show ipv6 route summary*. Команда сбрасывает только счетчики событий. Счетчики, показывающие текущее состояние таблицы маршрутизации, такие как количество маршрутов каждого типа, не сбрасываются.

Формат: `clear ipv6 route counters`

Режим ввода команд: привилегированный

clear ipv6 snooping counters

Данная команда сбрасывает счетчики связанные с функцией IPv6 RA GUARD.

Формат: `clear ipv6 snooping counters`

Режим ввода команд: привилегированный

глобальная конфигурация

clear ipv6 statistics

Используйте эту команду, чтобы очистить статистику IPv6 для всех интерфейсов или для конкретного интерфейса, в том числе туннельного, loopback-интерфейса или интерфейса VLAN. Статистика IPv6 отображается в выводе команды *show ipv6 traffic*. Если интерфейс не указан, значения всей статистики трафика IPv6 сбрасываются до нуля.

Формат: `clear ipv6 statistics [{`*`unit/slot/port`*` | loopback `*`loopback-id`*` | tunnel `*`tunnel-id`*` | vlan `*`id`*`}]`

Режим ввода команд: привилегированный

Термин	***Значение***
Local	Приоритет непосредственно подключенных маршрутов.
Static	Приоритет статических маршрутов.
OSPF Intra	Приоритет маршрутов в пределах OSPF-зоны.
OSPF Inter	Приоритет маршрутов относительно других OSPF-маршрутов, которые находятся за пределами зоны.

OSPF External	Приоритет внешних OSPF-маршрутов.
BGP External	Приоритет внешних BGP-маршрутов.
BGP Internal	Приоритет маршрутов относительно других BGP-маршрутов, которые находятся за пределами зоны.
BGP Local	Приоритет маршрутов в пределах BGP-зоны.

14.5 Команды настройки OSPFv3

В этом разделе описаны команды, используемые для просмотра и настройки OSPF — протокола маршрутизации, который используется для маршрутизации трафика в сети.

Команды глобальной настройки OSPFv3

ipv6 router ospf

Используйте эту команду, чтобы войти в режим конфигурирования OSPFv3-маршрутизатора.

Формат: `router ospf`

Режим ввода команд: глобальная конфигурация

area default-cost

Эта команда настраивает значение стоимости по умолчанию для stub-зоны. Оператор должен указать идентификатор зоны и целое значение в диапазоне 1–16 777 215.

Формат: `area areaid default-cost 1-16777215`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area nssa

Эта команда настраивает зону с указанным идентификатором в качестве NSSA.

Формат: `area areaid nssa`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area nssa

Эта команда выключает NSSA для указанного идентификатора зоны.

Формат: `no area areaid nssa`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area nssa default-info-originate

Эта команда настраивает значение метрики и тип маршрута по умолчанию, анонсируемый в NSSA. Необязательный параметр metric определяет метрику маршрута по умолчанию и должен быть в диапазоне от 1 до 16 777 214. Если метрика не указана, значение по умолчанию — 10. Тип метрики может быть сопоставимым (nssa-external 1) или несопоставимым (nssa-external 2).

Формат: `area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area nssa default-info-originate

Команда выключает маршрут по умолчанию, анонсируемый в NSSA.

Формат: `no area areaid nssa default-info-originate [metric] [{comparable | non-comparable}]`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area nssa no-redistribute

Эта команда настраивает NSSA ABR так, чтобы изученные внешние маршруты не были перераспределены в NSSA.

Формат: `area areaid nssa no-redistribute`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area nssa no-redistribute

Эта команда выключает NSSA ABR так, чтобы изученные внешние маршруты перераспределялись в NSSA.

Формат: `no area areaid nssa no-redistribute`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area nssa no-summary

Эта команда настраивает NSSA так, что суммарные LSA не анонсируются в NSSA.

Формат: `area areaid nssa no-summary`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area nssa no-summary

Эта команда выключает запрет анонсирования суммарных LSA в NSSA.

Формат: `no area areaid nssa no-summary`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area nssa translator-role

Данная команда настраивает NSSA в роли транслятора. Значение *always* заставляет маршрутизатор принять роль транслятора, как только он станет пограничным маршрутизатором, а значение *candidate* вынуждает маршрутизатор участвовать в процессе выборов, когда он достигает статуса пограничного маршрутизатора.

Формат: `area areaid nssa translator-role {always | candidate}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area nssa translator-role

Данная команда выключает роль транслятора NSSA из указанного идентификатора зоны.

Формат: `no area areaid nssa translator-role {always | candidate}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area nssa translator-stab-intv

Эта команда настраивает *stabilityinterval* для транслятора NSSA. *stabilityinterval* — это период времени, в течение которого выбранный транслятор продолжает выполнять свои обязанности после определения факта, что его статус транслятора был замещен другим маршрутизатором.

Формат: `area areaid nssa translator-stab-intv stabilityinterval`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area nssa translator-stab-intv

Эта команда возвращает *stabilityinterval* транслятора NSSA в значение по умолчанию

Формат: `no area areaid nssa translator-stab-intv stabilityinterval`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area range

Используйте эту команду, чтобы настроить суммарный префикс, который пограничный маршрутизатор зоны будет анонсировать в определенной зоне.

Значение по умолчанию: диапазоны зон не настроены; затраты не настроены

Формат: `area area-id range prefix netmask {summarylink | nssaexternallink} [advertise | not-advertise] [cost cost]`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

Термин	*Значение*
area-id	Идентификатор зоны для зоны, сети которой будут суммироваться.
prefix netmask	Суммарный префикс, анонсируемый, когда ABR вычисляет маршрут к одной или нескольким сетям в пределах этого префикса в данной зоне.
summarylink	Если указано это ключевое слово, суммируются префиксы анонсируемые в LSA типа 3.
nssaexternallink	Если указано это ключевое слово, суммируются префиксы при трансляции LSA типа 7 в тип 5.
advertise	(Необязательный параметр.) Если указано это ключевое слово, суммарный префикс анонсируется, если активны вложенные префиксы для указанного диапазона префиксов. Это значение используется по умолчанию.
not-advertise	(Необязательный параметр.) Если указано это ключевое слово, ни суммарные, ни вложенные префиксы не анонсируются, если активны вложенные префиксы для указанного диапазона префиксов. Если указана опция not-advertise, любые статические значения стоимости, настроенные ранее, удаляются из конфигурации системы.
cost	(Необязательный параметр.) Если указана стоимость, OSPF устанавливает поле метрики в суммированной LSA в настроенное значение вместо установки метрики на наибольшую стоимость среди сетей в диапазоне префиксов зоны.

no area range

Используйте **no**-форму данной команды, чтобы удалить суммарный префикс или удалить статическую стоимость.

Формат: `no area` *`areaid`* `range` *`prefix netmask`* `{summarylink | nssaexternallink} cost`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area stub

Эта команда создает stub-зону для указанного идентификатора зоны. Stub-зона характеризуется тем, что внешние AS LSA в ней не распространяются. Удаление внешних AS LSA и суммарных LSA может существенно ухудшить состояние связи для базы данных маршрутизаторов в stub-зоне.

Формат: `area` *`areaid`* `stub`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area stub

Эта команда удаляет stub-зону для указанного идентификатора зоны.

Формат: `no area` *`areaid`* `stub`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area stub no-summary

Эта команда выключает импорт суммарных LSA для stub-зоны, заданной параметром *areaid*.

Значение по умолчанию: включено

Формат: `area` *`areaid`* `stub no-summary`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area stub no-summary

Эта команда устанавливает в значение по умолчанию режим импорта сумарных LSA для stub-зоны, заданной параметром *areaid.*

Формат: `no area` *`areaid`* `stub summarylsa`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area virtual-link

Данная команда создает виртуальный интерфейс OSPF для указанного *areaid* или *neighbor*. Параметр *neighbor*— это идентификатор маршрутизатора соседнего устройства.

Формат: `area` *`areaid`* `virtual-link` *`neighbor`*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area virtual-link

Эта команда удаляет виртуальный интерфейс OSPF для указанного интерфейса *areaid* или *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `no area areaid virtual-link neighbor`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area virtual-link dead-interval

Эта команда настраивает Dead-интервал для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Диапазон значений для *seconds* — от 1 до 65 535.

Значение по умолчанию: 40

Формат: `area areaid virtual-link neighbor dead-interval seconds`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area virtual-link dead-interval

Команда устанавливает Dead-интервал в значение по умолчанию для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `no area areaid virtual-link neighbor dead-interval`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area virtual-link hello-interval

Эта команда настраивает Hello-интервал для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Диапазон значений для *seconds* — от 1 до 65 535.

Значение по умолчанию: 10

Формат: `area areaid virtual-link neighbor hello-interval seconds`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area virtual-link hello-interval

Команда устанавливает в значение по умолчанию Hello-интервал для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `no area areaid virtual-link neighbor hello-interval`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area virtual-link retransmit-interval

Данная команда настраивает интервал повторной передачи для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Диапазон значений для *seconds* — от 0 до 3600.

Значение по умолчанию: 5

Формат: `area areaid virtual-link neighbor retransmit-interval seconds`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area virtual-link retransmit-interval

Эта команда устанавливает в значение по умолчанию интервал повторной передачи для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `no area areaid virtual-link neighbor retransmit-interval`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

area virtual-link transmit-delay

Данная команда настраивает задержку передачи для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства. Диапазон секунд составляет от 0 до 3600 (1 час).

Значение по умолчанию: 1

Формат: `area areaid virtual-link neighbor transmit-delay seconds`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no area virtual-link transmit-delay

Данная команда настраивает задержку передачи по умолчанию для виртуального интерфейса OSPF, определяемом *areaid* и *neighbor*. Параметр *neighbor* — это идентификатор маршрутизатора соседнего устройства.

Формат: `no area areaid virtual-link neighbor transmit-delay`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

auto-cost

По умолчанию OSPF рассчитывает стоимость соединения для каждого интерфейса на основании пропускной способности интерфейса. Быстрые соединения имеют более низкие метрики, что повышает их приоритет при выборе маршрута. Параметры настройки в командах *auto-cost reference bandwidth* и *bandwidth* предоставляют возможность управлять стоимостью соединения по умолчанию. Можно настроить для OSPF пропускную способность интерфейса независимо от фактической скорости соединения. Второй параметр настройки позволяет контролировать соотношение пропускной способности интерфейса к стоимости соединения. Стоимость соединения рассчитывается как соотношение эталонной пропускной способности к пропускной способности интерфейса (*ref_bw / interface bandwidth*), при этом пропускная способность интерфейса устанавливается командой bandwidth. Поскольку по умолчанию эталонная пропускная способность составляет 100 Мбит/с, OSPF использует одинаковую стоимость соединения по умолчанию для всех интерфейсов, пропускная способность которых равна или более 100 Мбит/с. Команда auto-cost позволяет изменить эталонную пропускную способность, указав ее значение в Мбит/с. Значение эталонной пропускной способности может быть от 1 до 4294967 Мбит/с.

Значение по умолчанию: 100 Мбит/с

Формат: `auto-cost reference-bandwidth 1-4294967`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no auto-cost reference-bandwidth

Используйте эту команду, чтобы установить эталонную пропускную способность в значение по умолчанию.

Формат: `no auto-cost reference-bandwidth`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

clear ipv6 ospf

Команда позволяет выключить и повторно включить протокол OSPF.

Формат: `clear ipv6 ospf`

Режим ввода команд: привилегированный

clear ipv6 ospf configuration

Используйте эту команду, чтобы сбросить конфигурацию OSPF к заводским настройкам.

Формат: `clear ipv6 ospf configuration`

Режим ввода команд: привилегированный

clear ipv6 ospf counters

Данная команда сбрасывает статистику на глобальном уровне и уровне интерфейса.

Формат: `clear ipv6 ospf counters`

Режим ввода команд: привилегированный

clear ipv6 ospf neighbor

Используйте эту команду, чтобы сбросить соседство со всеми OSPF-соседями. На каждый соседний интерфейс отправляется одностороннее сообщение «Hello». После этого соседсто переустанавливается. Чтобы сбросить соседство с определенным маршрутизатором, необходимо указать идентификатор соседнего маршрутизатора, используя необязательный параметр [neighbor-id].

Формат: `clear ipv6 ospf neighbor` *`[neighbor-id]`*

Режим ввода команд: привилегированный

clear ipv6 ospf neighbor interface

Чтобы сбросить соседство со всеми соседями для указанного интерфейса, используйте необязательный параметр [unit/slot/port]. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Чтобы сбросить соседство с определенным идентификатором маршрутизатора на указанном интерфейсе, используйте необязательный параметр *[neighbor-id]*.

Формат: `clear ipv6 ospf neighbor interface [`*`unit/slot/port`*`|vlan` *`1-4093] [neighbor-id]`*

Режим ввода команд: привилегированный

clear ipv6 ospf redistribution

Команда позволяет очистить все сгенерированные внешние LSA. По мере необходимости можно повторно применить настройки перераспределения и создать префиксы.

Формат: `clear ipv6 ospf redistribution`

Режим ввода команд: привилегированный

default-information originate

Эта команда используется, чтобы управлять анонсами маршрутов по умолчанию.

Значение по умолчанию: метрика — не определена;

тип — 2

Формат: `default-information originate [always] [metric` *`0-16777214`*`] [metric-type {1 | 2}]`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no default-information originate

Эта команда используется, чтобы управлять анонсами маршрутов по умолчанию.

Формат: `no default-information originate` *`[metric] [metric-type]`*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

default-metric

Данная команда используется, чтобы установить значения по умолчанию для метрик распределенных маршрутов.

Формат: `default-metric` *`1-16777214`*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no default-metric

Данная команда используется, чтобы установить значения по умолчанию для метрик распределенных маршрутов.

Формат: `no default-metric`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

distance ospf

Эта команда устанавливает значение приоритета для типов OSPF-маршрутов на маршрутизаторе. При определении оптимального маршрута предпочтение отдается более низким значениям приоритета маршрута. Тип OSPF-маршрута может обозначаться как intra, inter или external. Всем маршрутам типа external присваивается одинаковое значение приоритета. Диапазон значений для *preference* — от 1 до 255.

Значение по умолчанию: 110

Формат: `distance ospf {intra-area` *`1-255`* `| inter-area` *`1-255`* `| external` *`1-255`*`}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no distance ospf

Эта команда устанавливает приоритет OSPF-маршрута на маршрутизаторе в значение по умолчанию. Тип OSPF-маршрута может обозначаться как intra, inter или external. Всем маршрутам типа external присваивается одинаковое значение приоритета.

Формат: `no distance ospf {intra-area | inter-area | external}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

enable

Эта команда устанавливает административный режим OSPF-маршрутизатора в значение по умолчанию (активен).

Значение по умолчанию: включено

Формат: `enable`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no enable

Эта команда устанавливает административный режим OSPF-маршрутизатора как неактивный.

Формат: `no enable`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

exit-overflow-interval

Данная команда настраивает интервал выхода из режима переполнения для OSPF. Он обозначает время в секундах после входа в состояние переполнения, в течение которого маршрутизатор выжидает и не пытается выходить из этого состояния. Это позволяет маршрутизатору снова создать AS-external-LSA не по умолчанию. Если интервал установлен как 0, маршрутизатор не пытается самостоятельно выходить из состояния переполнения и требует перезапуска. Диапазон значений для *seconds* — от 0 до 2147483647 секунд.

Значение по умолчанию: 0

Формат: `exit-overflow-interval` *`seconds`*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no exit-overflow-interval

Эта команда устанавливает интервал выхода из режима переполнения для OSPF в значение по умолчанию.

Формат: `no exit-overflow-interval`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

external-lsdb-limit

Эта команда настраивает ограничение внешних LSDB для OSPF. Если значение установлено как -1, ограничений не существует. Если количество AS-external-LSA не по умолчанию в базе данных состояния соединения маршрутизатора достигает ограничения LSDB, маршрутизатор входит в состояние переполнения. Маршрутизатор никогда не хранит в базе данных AS-external-LSA, превышающие по количеству установленное LSDB-ограничение. Ограничение для внешних LSDB должно быть установлено на одном уровне на всех маршрутизаторах, подключенных к OSPF-магистрали и/или любой обычной OSPF-зоне. Диапазон значений для limit — от -1 до 2 147 483 647.

Значение по умолчанию: -1

Формат: `external-lsdb-limit` *`limit`*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no external-lsdb-limit

Эта команда устанавливает ограничение внешних LSDB для OSPF в значение по умолчанию.

Формат: `no external-lsdb-limit`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

maximum-paths

Эта команда устанавливает количество путей для заданного места назначения, о которых OSPF может сообщать.

Значение по умолчанию: 4

Формат: `maximum-paths` *`maxpaths`*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no maximum-paths

Данная команда устанавливает количество путей для заданного места назначения, о которых OSPF может сообщать, в значение по умолчанию.

Формат: `no maximum-paths`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

passive-interface default

Используйте эту команду, чтобы включить глобальный пассивный режим по умолчанию для всех интерфейсов. Команда перезаписывает любой уровень пассивного режима интерфейса. OSPF не будет формировать соседство через пассивные интерфейсы.

Значение по умолчанию: выключено

Формат: `passive-interface default`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no passive-interface default

Эта команда выключает глобальный пассивный режим по умолчанию для всех интерфейсов. Любой интерфейс, ранее настроенный на пассивный режим, по исполнению команды выходит из него.

Формат: `no passive-interface default`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

passive-interface

Используйте эту команду, чтобы настроить стандартный или туннельный интерфейс как пассивный. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Команда перезаписывает глобальный пассивный режим, который уже действует на стандартном или туннельном интерфейсе.

Значение по умолчанию: выключено

Формат: `passive-interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`|tunnel `*`tunnel-id`*`}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no passive-interface

Используйте эту команду, чтобы установить интерфейс или туннель как непассивный. Команда перезаписывает глобальный пассивный режим, который уже действует на стандартном или туннельном интерфейсе.

Формат: `no passive-interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`|tunnel `*`tunnel-id`*`}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

redistribute

Эта команда настраивает OSPFv3-протокол на разрешение перераспределения маршрутов от указанных передающих протоколов/маршрутизаторов. При использовании ключевого слова bgp для перераспределения BGP-маршрутов в OSPFv3 перераспределены будут только внешние маршруты.

Значение по умолчанию: метрика — не определена;

тип — 2;

тег — 0.

Формат: `redistribute {static | connected | bgp} [metric `*`0-16777214`*`] [metric-type {1 | 2}] [tag `*`0-4294967295`*`]`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no redistribute

Эта команда настраивает OSPF-протокол на запрет перераспределения маршрутов от указанных передающих протоколов/маршрутизаторов.

Формат: `no redistribute {static | connected} `*`[metric] [metric-type] [tag]`*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

router-id

Эта команда устанавливает уникальный идентификатор OSPF-маршрутизатора.

Формат: `router-id` *ipaddress*

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

timers pacing lsa-group

Используйте эту команду для настройки групп LSA в OSPFv3 для периодического обновления. OSPFv3 обновляет сгенерированные LSA приблизительно каждые 30 минут. Когда OSPFv3 обновляет LSA, он учитывает все сгенерированные LSA, период существования которых составляет от 1800 до 1800 плюс размер интервала группы. Группировка LSA для обновления позволяет OSPFv3 объединять обновляемые LSA в минимальное количество пакетов LS Update. Сокращение количества пакетов LS Update делает распространение LSA более эффективным.

Если OSPFv3 генерирует новый или измененный LSA, он выбирает для него случайную задержку обновления. По истечении задержки обновления OSPFv3 обновляет LSA. Выбирая случайную задержку обновления, OSPFv3 избегает обновления большого количества LSA за один раз, даже если таковые возникли в одно время.

Параметр seconds — это продолжительность окна, за которое обновляются LSA. Диапазон — от 10 до 1800 секунд.

Значение по умолчанию: 60 секунд

Формат: `timers pacing lsa-group` *seconds*

Режим ввода команд: привилегированный

no timers pacing lsa-group

Данная команда возвращает параметр LSA Group Pacing к заводским настройкам (60 секунд).

Формат: `no timers pacing lsa-group`

Режим ввода команд: привилегированный

timers throttle spf

Изначально интервал ожидания установлен на величину задержки, определенную значением spf-hold. Если в ходе текущего интервала ожидания расчет SPF не планируется, следующий расчет SPF будет запланирован через период задержки *spf-start*. Если в ходе текущего интервала ожидания расчет SPF был запланирован, значение интервала ожидания будет каждый раз устанавливаться в два раза больше текущего значения, пока интервал ожидания не достигнет максимального времени в миллисекундах, заданного параметром *spf- maximum*. В дальнейшем интервал ожидания будет сохранять максимальное значение, пока это значение не будет сброшено или не будет получен LSA между расчетами SPF.

Значение по умолчанию: *spf-start* = 2000 мс;
spf-hold = 5000 мс;
spf-maximum = 5000 мс.

Формат: `timers throttle spf` *spf-start spf-hold spf-maximum*

Режим ввода команд: привилегированный

Параметр	*Описание*
spf-start	Указывает задержку расписания SPF в миллисекундах, если расчет SPF не был запланирован в ходе текущего интервала ожидания. Диапазон значений составляет от 1 до 600 000 миллисекунд.
spf-hold	Указывает начальный период ожидания для SPF в миллисекундах. Диапазон значений составляет от 1 до 600 000 миллисекунд.
spf-maximum	Указывает максимальный период ожидания для SPF в миллисекундах. Диапазон значений составляет от 1 до 600 000 миллисекунд.

no timers throttle spf

Данная команда возвращает параметры SPF-ограничений к заводским настройкам.

Формат: `no timers throttle spf`

Режим ввода команд: привилегированный

trapflags

Используйте данную команду, чтобы включить индивидуальные OSPF-трапы, одновременно включить группу флагов для трапов или одновременно включить все флаги для трапов. Различные группы флагов для трапов и отдельные флаги для трапов (OSPFv3) каждой группы перечислены в таблице ниже.

Группа	*Флаги*
errors	• authentication-failure • bad-packet • config-error • virt-authentication-failure • virt-bad-packet • virt-config-error
lsa	• lsa-maxage • lsa-originate
overflow	• lsdb-overflow • lsdb-approaching-overflow
retransmit	• packets • virt-packets
state-change	• if-state-change • neighbor-state-change • virtif-state-change • virtneighbor-state-change

- Чтобы включить отдельный флаг, введите group name и затем выбранный флаг.
- Чтобы включить все флаги группы, введите имя группы и ключевое слово all.

- Чтобы включить все флаги, введите команду trapflags all.

Значение по умолчанию: выключено

Формат: `trapflags { all |errors {all | authentication-failure | bad-packet | config-error | virt- authentication-failure | virt-bad-packet | virt-config-error} |lsa {all | lsa-maxage | lsa-originate} |overflow {all | lsdb-overflow | lsdb-approaching-overflow} | retransmit {all | packets | virt-packets} |state-change {all | if-state-change | neighbor-state-change | vir-tif-state-change | virtneighbor-state-change}}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

no trapflags

Команда устанавливает настройки OSPF-трапов и соответствующих флагов в значение по умолчанию.

- Чтобы выключить отдельный флаг, введите group name и затем выбранный флаг.
- Чтобы выключить все флаги группы, введите имя группы и ключевое слово all.
- Чтобы выключить все флаги, введите команду с указанием trapflags all.

Формат: `no trapflags { all |errors {all | authentication-failure | bad-packet | config-error | virt- authentication-failure | virt-bad-packet | virt-config-error} |lsa {all | lsa-maxage | lsa-originate} |overflow {all | lsdb-overflow | lsdb-approach-ing-overflow} | retransmit {all | packets | virt-packets} |state-change {all | if-state-change | neighbor-state-change | virtif-state- change | virtneighbor-state-change}}`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

Команды OSPFv3-интерфейса

ipv6 ospf area

Эта команда устанавливает зону OSPF, к которой принадлежит указанный интерфейс маршрутизатора или диапазон интерфейсов. Она также включает OSPF на указанном интерфейсе маршрутизатора или диапазоне интерфейсов. Параметр *area* — это 32-битное значение, представленное IPv4-адресом или десятичным значением в диапазоне от 0 до 4 294 967 295. Параметр *area* уникальным образом идентифицирует зону, к которой подключен интерфейс. Присвоение идентификатора несуществующей зоне приводит к созданию этой зоны с настройками по умолчанию.

Формат: `ipv6 ospf area` *`0-4294967295`*

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf cost

Данная команда настраивает стоимость на OSPF-интерфейсе или диапазоне интерфейсов. Параметр *cost* имеет диапазон от 1 до 65 535.

Значение по умолчанию: 10

Формат: `ipv6 ospf cost` *`1-65535`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf cost

Эта команда устанавливает стоимость на OSPF-интерфейсе в значение по умолчанию.

Формат: `no ipv6 ospf cost`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf dead-interval

Эта команда настраивает Dead-интервал OSPF для указанного интерфейса или диапазона интерфейсов. Параметр *seconds* — это действительное положительное целое число, время в секундах, в течение которого пакеты Hello не отправляются с маршрутизатора до того момента, пока соседние маршрутизаторы не объявляют, что маршрутизатор выключен. Значение Dead-интервала должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Это значение должно быть кратно Hello-интервалу (т. е. 4). Диапазон допустимых значений для *seconds* — от 1 до 2 147 483 647.

Значение по умолчанию: 40

Формат: `ipv6 ospf dead-interval` *`1-2147483647`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf dead-interval

Эта команда устанавливает Dead-интервал OSPF для указанного интерфейса или диапазона интерфейсов в значение по умолчанию.

Формат: `no ipv6 ospf dead-interval`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf hello-interval

Данная команда устанавливает Hello-интервал OSPF для указанного интерфейса. Значение для *seconds* — это действительное положительное целое число, время в секундах. Значение Hello-интервала должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Диапазон допустимых значений для *seconds* — от 1 до 65 535.

Значение по умолчанию: 10

Формат: `ipv6 ospf hello-interval` *`seconds`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf hello-interval

Эта команда устанавливает Hello-интервал OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ipv6 ospf hello-interval`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf link-lsa-suppression

Используйте эту команду, чтобы включить на интерфейсе функцию Link LSA Suppression. Когда Link LSA Suppression включена на интерфейсе двухточечного соединения, пакеты протокола Link LSA на интерфейсе не создаются и не транслируются. Эта конфигурация относится только к интерфейсам двухточечного соединения.

Значение по умолчанию: False

Формат: `ipv6 ospf link-lsa-suppression`

Режим ввода команд: привилегированный

no ipv6 ospf link-lsa-suppression

Данная команда выключает функцию Link LSA Suppression на интерфейсе. Когда Link LSA Suppression выключена, пакеты протокола Link LSA на интерфейсе двухточечного соединения создаются и транслируются.

Формат: `no ipv6 ospf link-lsa-suppression`

Режим ввода команд: привилегированный

ipv6 ospf mtu-ignore

Эта команда выключает OSPF-обнаружение несоответствия MTU на интерфейсе или диапазоне интерфейсов. Пакеты OSPF Database Description задают размер наибольшего IP-пакета, который может быть отправлен на интерфейсе без фрагментации. Если маршрутизатор получает пакет Database Description, он проверяет значение MTU, анонсируемое соседом. По умолчанию, если MTU больше, чем маршрутизатор может принять, пакет Database Description отбрасывается и OSPF-соседство не устанавливается.

Значение по умолчанию: включено

Формат: `ipv6 ospf mtu-ignore`

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf mtu-ignore

Эта команда включает OSPF-обнаружение несоответствия MTU.

Формат: `no ipv6 ospf mtu-ignore`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf network

Эта команда изменяет тип OSPF-сети по умолчанию для интерфейса или диапазона интерфейсов. Как правило, тип сети определяется на основании физического типа IP-сети. По умолчанию все сети Ethernet в OSPF определяются как тип broadcast. Аналогичным образом, туннельные интерфейсы по умолчанию относятся к типу point-to-point. Когда порт Ethernet используется как одна большая полоса пропускания IP-сети между двумя маршрутизаторами, тип сети может быть определен как point-to-point, поскольку используются только два маршрутизатора. Используя тип сети point-to-point, можно избежать проблем с выбором назначенного OSPF-

маршрутизатора. Значение типа broadcast для туннельных интерфейсов, как правило, не используется.

Значение по умолчанию: broadcast

Формат: `ipv6 ospf network {broadcast | point-to-point}`

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf network

Данная команда устанавливает тип интерфейса в значение по умолчанию.

Формат: `no ipv6 ospf network {broadcast | point-to-point}`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf prefix-suppression

Эта команда подавляет анонсирование всех IPv6-префиксов, связанных с интерфейсом, кроме префиксов, связанных с вторичными IPv6-адресами. Данная команда перекрывает глобальную конфигурацию. Если данная конфигурация не определена, применяется конфигурация глобального подавления префиксов.

Подавление префиксов может быть выключено на уровне интерфейса с использованием опции disable. Опция disable полезна тем, что выделяет отдельные интерфейсы из выполнения подавления префиксов, если функция включена глобально. Следует отметить, что функция disable не эквивалентна отсутствию настроек подавления префиксов на отдельных интерфейсах.

Значение по умолчанию: подавление префиксов не настроено.

Формат: `ipv6 ospf prefix-suppression [disable]`

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf prefix-suppression

Данная команда удаляет настройки подавления префиксов на уровне интерфейса. Когда используется команда no ipv6 ospf prefix-suppression, на интерфейсе применяется глобальное подавление префиксов. Отсутствие настройки команды не эквивалентно выключению подавления префиксов на уровне интерфейса.

Формат: `no ipv6 ospf prefix-suppression`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf priority

Эта команда устанавливает OSPF-приоритет для указанного интерфейса маршрутизатора или диапазона интерфейсов. Приоритет интерфейса — это целое число от 0 до 255. Нулевое значение обозначает, что маршрутизатор не подходит на роль назначенного маршрутизатора в данной сети.

Значение по умолчанию: 1, наивысший приоритет маршрутизатора

Формат: `ipv6 ospf priority` *`0-255`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf priority

Эта команда устанавливает OSPF-приоритет для указанного интерфейса маршрутизатора в значение по умолчанию.

Формат: `no ipv6 ospf priority`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf retransmit-interval

Эта команда настраивает интервал повторной передачи OSPF для указанного интерфейса или диапазона интерфейсов. Интервал повторной передачи указывается в секундах. Значение seconds — это число секунд между повторной отправкой LSA для смежностей, принадлежащих интерфейсу данного маршрутизатора. Это значение также используется при повторной передаче описания базы данных и пакетов с запросами состояния канала. Диапазон — от 0 до 3600 секунд (1 час).

Значение по умолчанию: 5

Формат: `ipv6 ospf retransmit-interval` *`seconds`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf retransmit-interval

Команда устанавливает интервал повторной передачи OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ipv6 ospf retransmit-interval`

Режим ввода команд: конфигурирование интерфейса

ipv6 ospf transmit-delay

Данная команда устанавливает задержку передачи OSPF для указанного интерфейса или диапазона интерфейсов. Задержка передачи указывается в секундах. Кроме того, она устанавливает ожидаемое количество секунд, которое требуется для передачи пакета с обновлением состояния соединения через этот интерфейс. Интервал действительных значений для *`seconds`* — от 1 до 3600 (1 час).

Значение по умолчанию: 1

Формат: `ipv6 ospf transmit-delay` *`seconds`*

Режим ввода команд: конфигурирование интерфейса

no ipv6 ospf transmit-delay

Команда устанавливает задержку передачи OSPF для указанного интерфейса в значение по умолчанию.

Формат: `no ipv6 ospf transmit-delay`

Режим ввода команд: конфигурирование интерфейса

Команды настройки Graceful Restart в OSPFv3

Использование функционала Graceful Restart позволяет производить «щадящую перезагрузку» маршрутизаторов, при которой смежные маршрутизаторы продолжают пересылать IPv4 пакеты с использование OSPFv3-маршрутов анонсированных перезагружаемым коммутатором.

Смежный маршрутизатор входит в режим помощника, если он получает от перезагружающегося маршрутизатора LSA-graceful, обозначающий его намерение выполнить щадящую перезагрузку. В режиме помощника коммутатор продолжает отправлять анонсы остальной сети, что они имеют полную смежность с перезагружающимся маршрутизатором, тем самым избегая перестроения OSPFv3-топологии и потенциального переполнения LSA и SPF (которые определяют маршруты OSPFv3). Соседи-помощники продолжают направлять пакеты через перезагружающийся маршрутизатор. Перезагружающийся маршрутизатор заново узнает топологию сети от своих соседей-помощников.

Функция Graceful Restart может быть включена для плановых, внеплановых или для обоих типов перезагрузки. Плановая перезагрузка выполняется оператором через управляющую команду initiate failover.

nsf

Используйте эту команду, чтобы включить функцию OSPF Graceful Restart на интерфейсе.

Значение по умолчанию: выключено

Формат: `nsf [ietf] [planned-only]`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

Параметр	***Описание***
ietf	Это ключевое слово принимается, но не является обязательным.
planned-only	Это необязательное ключевое слово обозначает, что OSPF должен выполнить щадящую перезагрузку, только если перезагрузка плановая (например, если перезагрузка — результат команды initiate failover).

no nsf

Используйте эту команду, чтобы выключить Graceful Restart для любых перезагрузок.

Формат: `no nsf [ietf]`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

nsf restart-interval

Команда настраивает интервал в секундах, в течение которого перезагружающийся маршрутизатор будет просить своих соседей ожидать, прежде чем входить в режим помощника. Этот интервал называют «щадящим периодом». Перезагружающийся маршрутизатор включает щадящий период в свои анонсы LSA. Для плановых перезагрузок (используя команду initiate failover) щадящие LSA отсылаются до перезагрузки блока управления, а в случае внеплановых — отсылаются после начала перезагрузки.

Щадящий период должен быть достаточно долгим, чтобы позволить перезагружающемуся маршрутизатору восстановить все свои смежности и выполнить полный обмен базы данных с каждым из соседей.

Значение по умолчанию: 120 секунд

Формат: `nsf [ietf] restart-interval` *`1-1800`*

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

Параметр	***Описание***
ietf	Это ключевое слово принимается, но не является обязательным.
seconds	Количество секунд, которое перезагружающийся маршрутизатор запрашивает на ожидание у своих соседей перед тем, как они войдут в режим помощника. Диапазон — от 1 до 1800 секунд.

no nsfrestart-interval

Используйте эту команду, чтобы вернуть значение щадящего периода в значение по умолчанию.

Формат: `no [ietf] nsf restart-interval`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

nsf helper

Команда включает функцию соседей-помощников для протокола OSPF. Данную функцию можно включить для плановых, внеплановых или обоих типов перезагрузок.

Значение по умолчанию: OSPF может выступать как сосед-помощник для плановых и внеплановых перезагрузок.

Формат: `nsf helper [planned-only]`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

Параметр	***Описание***
planned-only	Это необязательное ключевое слово указывает, что OSPF следует назначать помощников только маршрутизатору, выполняющему плановую перезагрузку.

no nsf helper

Используйте эту команду, чтобы выключить функцию соседей-помощников для протокола OSPF.

Формат: `no nsf helper`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

nsf ietf helper disable

Используйте эту команду, чтобы выключить функцию соседей-помощников для протокола OSPF.

Команды no nsf helper и nsf ietf helper disable функционально равнозначны. Команда nsf ietf helper disable поддерживается исключительно для совместимости с CLI других вариантов программного обеспечения сети.

Формат: `nsf ietf helper disable`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

nsf helper strict-lsa-checking

Перезагружающийся маршрутизатор не может реагировать на изменения топологии. В частности, перезагружающийся маршрутизатор не будет мгновенно обновлять свою таблицу маршрутизации, а значит, изменение топологии может привести к петлям при пересылке или «черным дырам», которые сохраняются до тех пор, пока не завершится щадящая перезагрузка. При выходе из «щадящей перезагрузки» на изменение в топологии, маршрутизатор пытается устранить петли или «черные дыры» так быстро, как это возможно, за счет маршрутизации в обход перезапускающегося маршрутизатора. Сосед-помощник считает не поднятое соединение с перезагружающимся маршрутизатором изменением топологии, независимо от строгой конфигурации проверки LSA.

Используйте данную команду, чтобы потребовать от соседа-помощника OSPF выходить из режима помощника, как только происходит изменение топологии.

Значение по умолчанию: включено.

Формат: `nsf [ietf] helper strict-lsa-checking`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

Параметр	*Описание*
ietf	Это ключевое слово принимается, но не является обязательным.

no nsf [ietf] helper strict-lsa-checking

Данная команда позволяет OSPF продолжать использовать соседа-помощника, несмотря на изменение топологии.

Значение по умолчанию: включено.

Формат: `nsf [ietf] helper strict-lsa-checking`

Режимы ввода команд: конфигурирование OSPFv3-маршрутизатора

Параметр	*Описание*
external-lsa	Отправляет максимальные значения метрик для внешних LSA (необязательный параметр). Атрибут max-metric-value является максимально допустимым значением метрики для использования в LSA. Диапазон значений — от 1 до 16 777 215 (0xFFFFFF). Значение по умолчанию равно 16 711 680 (0xFF0000).
inter-area-lsas	Отправляет максимальные значения метрик для LSA Inter-Area-Router (необязательный параметр).
on-startup	Запускает OSPF в режиме Stub Router (необязательный параметр). Параметр seconds означает время в секундах, которое OSPF будет находится в режиме Stub Router после перезагрузки. Диапазон — от 5 до 86 400 секунд. Значение по умолчанию отсутствует.

summary-lsa	Отправляет максимальные значения метрик для суммарных LSA (необязательный параметр).

no max-metric router-lsa

Используйте данную команду в режиме конфигурирования OSPFv3-маршрутизатора, чтобы выключить режим Stub Router. Команда очищает любой тип режима (always или on-startup) и сбрасывает все опции LSA. Если OSPF настроен входить в режим при запуске, и вы собираетесь в обычном оперативном режиме немедленно поместить OSPF в режим Stub Router, введите команду **no max-metric router-lsa on-startup**. Команда **no max-metric** с указанными опциями external-lsa, inter-area-lsas или опцией summary-lsa, указанной как **router-lsa summary-lsa** приводит к тому, что OSPF отправляет суммарные LSA с метриками, вычисленными с использованием стандартных процедур.

Формат: `no max-metric router-lsa [external-lsa] [inter-area-lsas] [on-startup] [summary-lsa]`

Режим ввода команд: конфигурирование OSPFv3-маршрутизатора

clear ipv6 ospf stub-router

Используйте эту команду, чтобы принудительно вывести OSPF из режима Stub Router, когда он автоматически перешел в этот режим из-за ограниченности ресурсов. OSPF выходит из режима Stub Router только по причине ограничения ресурсов или если маршрутизатор находится в нем с момента запуска. Эта команда не имеет действия, если OSPF настроен находиться в режиме Stub Router постоянно.

Формат: `clear ipv6 ospf stub-router`

Режим ввода команд: привилегированный

Команды просмотра оперативного состояния OSPFv3

show ipv6 ospf

Данная команда отображает информацию, относящуюся к OSPF-маршрутизатору.

Формат: `show ipv6 ospf`

Режим ввода команд: привилегированный

пользовательский

Некоторая информация из представленной ниже отображается, только если включен протокол OSPF и настроены определенные функции.

Термин	*Значение*
Router ID	Уникальный идентификатор маршрутизатора в сети.
OSPF Admin Mode	Показывает, включен или выключен административный режим OSPF на маршрутизаторе. Это значение можно настраивать.
External LSDB Limit	Максимальное количество записей AS-external-LSA не по умолчанию, которые могут быть помещены в базу данных статуса соединения.
Exit Overflow Interval	Время в секундах после входа в состояние переполнения, по истечении которого маршрутизатор будет пытаться выйти из этого состояния.
SPF Start Time	Время отсрочки вычисления SPF в миллисекундах, когда расчет SPF не был запланирован на текущий интервал ожидания.
SPF Hold Time	Начальный интервал ожидания в миллисекундах.
SPF Maximum Hold Time	Максимальное значение интервала ожидания в миллисекундах.
LSA Refresh Group Pacing Time	Размер окна для обновления группы LSA в секундах.
AutoCost Ref BW	Показывает значение эталонной пропускной способности для автоматического расчёта стоимости интерфейса.
Default Passive Setting	Показывает, являются ли интерфейсы пассивными по умолчанию.
Maximum Paths	Максимальное количество маршрутов, которые OSPF может предложить для данного места назначения.
Default Metric	Значение метрики по умолчанию для распространяемых маршрутов.
Default Route Advertise	Указывает, анонсируются ли маршруты по умолчанию, полученные от других протоколов-источников.
Always	Показывает, всегда ли анонсируются маршруты по умолчанию.
Metric	Метрика для анонсируемых маршрутов по умолчанию. Если метрики не настроены, это поле остается пустым.
Metric Type	Показывает тип маршрутов: External Type 1 или External Type 2.
Number of Active Areas	Количество активных зон OSPF. Активная зона OSPF — это зона с хотя бы одним работающим интерфейсом.
ABR Status	Показывает, является ли маршрутизатор пограничным маршрутизатором зоны OSPF (ABR).
ASBR Status	Показывает, является ли маршрутизатор пограничным маршрутизатором автономной системы OSPF (ASBR).
Stub Router Status	Состояние Stub Router: Active или Inactive.
Stub Router Reason	Эта опция отображается только в том случае, если режим Stub Router активен. Показывает причину входа в режим Stub Router: Configured, Startup или Resource Limitation.
Stub Router Startup Time Remaining	Эта опция отображается только в том случае, если режим Stub Router установлен при включении. Время в секундах до того, как OSPF выйдет из режима Stub Router.
Stub Router Duration	Эта строка отображается только если Stub Router активен и маршрутизатор вошел в режим Stub Router по причине ограничения ресурсов. Время, прошедшее с момента последнего входа маршрутизатора в режим Stub Router. Продолжительность отображается в формате дд:чч:мм:сс.
External LSDB Overflow	Если количество внешних LSA не по умолчанию превышает настроенный лимит, External LSDB Limit, OSPF входит в состояние переполнения. В этом состоянии OSPF отзывает все свои сгенерированные внешние LSA не по умолчанию. По истечении установленного времени Exit Overflow Interval OSPF выходит из состояния переполнения, если количество внешних LSA было уменьшено.

External LSA Count	Количество внешних анонсов состояния соединения (LS типа 5) в базе данных состояния соединения.
External LSA Checksum	Сумма контрольных сумм LS внешних LSA, содержащихся в базе данных состояния соединения.
New LSAs Originated	Количество новых возникших анонсов состояния соединения.
LSAs Received	Количество полученных анонсов состояния соединения, определенных как новые.
LSA Count	Общее количество LSA, находящихся в данный момент в базе данных состояния соединения.
Maximum Number of LSAs	Максимальное количество LSA, которые OSPF может хранить.
LSA High Water Mark	Максимальный размер базы данных состояния соединения с момента запуска системы.
Retransmit List Entries	Общее количество LSA, ждущих подтверждения всеми соседями. Любые LSA могут ожидать подтверждения более чем одним соседним устройством.
Maximum Number of Retransmit Entries	Максимальное количество LSA, которые могут ожидать подтверждения в любое время.
Retransmit Entries High Water Mark	Максимальное количество LSA, которые когда-либо ожидали подтверждения.
Redistributing	Поле является заголовком и появляется только тогда, когда система настроена принимать маршруты, изученные от источника, отличного от OSPF, и анонсировать их партнерским устройствам.
Source	Показывает исходящие протоколы/ маршруты, которые подлежат перераспределению. Возможные значения: static, connected, BGP или RIP.
Metric	Метрика перераспределяемых маршрутов.
Metric Type	Показывает тип маршрутов: External Type 1 или External Type 2.
Tag	Десятичное значение, назначаемое для каждого внешнего маршрута.
Subnets	При перераспределении маршрутов в OSPF этот параметр показывает объем перераспределения для указанного протокола.
Distribute-List	Список контроля доступа, который используется для фильтрации перераспределяемых маршрутов.
Prefix-suppression	Показывает, включено ли подавление префиксов на данном интерфейсе.
NSF Support	Указывает, включена ли безостановочная обработка трафика (NSF) для протокола OSPF при плановых или внеплановых перезагрузках или для обоих типов (Always).
NSF Restart Interval	Настраиваемый пользователем щадящий интервал, во время которого соседний маршрутизатор будет находится в режиме помощника после получения уведомления о том, что блок управления выполняет щадящую перезагрузку.
NSF Restart Status	Действующий статус щадящей перезагрузки маршрутизатора.
NSF Restart Age	Количество секунд до того, как закончится интервал щадящей перезагрузки.
NSF Restart Exit Reason	Показывает, по какой причине маршрутизатор последний раз выходил из последней перезагрузки: • **None** — щадящая перезагрузка не проводилась. • **In Progress** — перезагрузка в процессе. • **Completed** — предыдущая щадящая перезагрузка выполнена успешно.

	• **Timed Out** — время предыдущей щадящей перезагрузки истекло. • **Topology Changed** — предыдущая щадящая перезагрузка досрочно прекращена из-за изменения топологии.
NSF Help Support	Показывает, включена ли функция соседа-помощника для OSPF для плановых или внеплановых перезагрузок либо обоих типов (Always).
NSF help Strict LSA checking	Показывает, включена ли строгая проверка LSA. Если включена, то сосед-помощник OSPF выйдет из режима помощника, как только произойдет изменение топологии. Если выключена, сосед-помощник OSPF продолжит работать в этом режиме, несмотря на изменение топологии.

show ipv6 ospf abr

Эта команда отображает внутренние маршруты OSPFv3 для достижения маршрутизатора ABR. Команда не принимает дополнительных опций.

Формат: `show ipv6 ospf abr`

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
Type	Тип маршрута к месту назначения. Может быть: • intra — маршрут внутри зоны; • inter — маршрут вне зоны.
Router ID	Идентификатор маршрутизатора места назначения.
Cost	Стоимость использования этого маршрута.
Area ID	Идентификатор зоны, от которой изучен данный маршрут.
Next Hop	Ближайший узел по направлению к месту назначения.
Next Hop Intf	Интерфейс исходящего маршрутизатора, используемый для направления трафика к ближайшему узлу.

show ipv6 ospf area

Данная команда отображает информацию о зоне. Параметр *areaid* указывает OSPF-зону, которая будет отображаться.

Формат: `show ipv6 ospf area` *areaid*

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
AreaID	Идентификатор запрошенной OSPF-зоны.
External Routing	Число, представляющее возможности внешней маршрутизации для этой зоны.
Spf Runs	Количество случаев, когда таблица маршрутизации внутри зоны была рассчитана с использованием базы данных состояний соединений этой зоны.
Area Border Router Count	Общее количество пограничных маршрутизаторов в диапазоне данной зоны.
Area LSA Count	Общее количество LSA в базе данных состояния соединения этой зоны, исключая внешние AS LSA.

Area LSA Checksum	Число, представляющее контрольную сумму LSA зоны для указанного AreaID, исключая внешние LSA (LS типа 5).
Stub Mode	Представляет, является ли указанная зона stub-зоной. Возможные значения: enabled и disabled.
Import Summary LSAs	Показывает, импортируются ли суммарные LSA (при значении Stub Mode enabled).
OSPF Stub Metric Value	Значение метрики stub-зоны. Это поле отображается только если зона сконфигурирована как stub-зона.

Следующая информация OSPF NSSA отображается только в том случае, если зона настроена как NSSA.

Термин	***Значение***
Import Summary LSAs	Показывает, импортируются ли суммарные LSA в NSSA.
Redistribute into NSSA	Показывает, распространяется ли информация в NSSA.
Default Information Originate	Показывает, анонсируется ли NSSA маршрут по умолчанию
Default Metric	Значение метрики для маршрута по умолчанию, анонсируемого NSSA.
Default Metric Type	Тип метрики для маршрута по умолчанию, анонсируемого NSSA.
Translator Role	Роль транслятора NSSA для ABR: always или candidate.
Translator Stability Interval	Период времени, в течение которого выбранный транслятор продолжает выполнять свои обязанности после определения факта, что его статус транслятора был замещен другим маршрутизатором.
Translator State	Показывает статус маршрутизатора ABR: disabled, always или elected.

show ipv6 ospf asbr

Эта команда отображает внутренние маршруты OSPFv3 для достижения маршрутизатора ASBR. Команда не принимает дополнительных опций.

Формат: `show ipv6 ospf asbr`

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
Type	Тип маршрута к месту назначения. Может быть: • intra — маршрут внутри зоны; • inter — маршрут вне зоны.
Router ID	Идентификатор маршрутизатора места назначения.
Cost	Стоимость использования этого маршрута.
Area ID	Идентификатор зоны, от которой изучен данный маршрут.
Next Hop	Ближайший узел по направлению к месту назначения.
Next Hop Intf	Интерфейс исходящего маршрутизатора, используемый для направления трафика к ближайшему узлу.

show ipv6 ospf database

Данная команда отображает информацию о базе данных состояния соединения, когда OSPFv3 включен. Если не указывать дополнительных параметров, команда отобразит заголовки LSA для всех зон. Используйте необязательный параметр *areaid*, чтобы отобразить информацию базы данных для

определенной зоны. Используйте другие необязательные параметры, чтобы указать тип отображаемых анонсов состояния соединения. Используйте *external* для отображения внешних LSA. Используйте *inter-area* для отображения внутризональных LSA. Используйте *link* для отображения LSA соединения. Используйте *network*, чтобы отобразить сетевые LSA. Используйте nssa-external для отображения внешних LSA NSSA. Используйте *prefix* для отображения внутризонального префикса LSA. Используйте *router* для отображения LSA маршрутизатора. Используйте *unknown area, unknown as* или *unknown link*, чтобы отобразить LSA для неизвестной зоны или автономной системы или для соединения соответственно. Используйте *lsid* для указания идентификатора состояния связи (LSID). Используйте *adv-router*, чтобы показать LSA, которые ограничены анонсирующим маршрутизатором. Используйте *self-originate*, чтобы отобразить собственные LSA. Приведенная ниже информация отображается только в том случае, если OSPF включен.

Формат: `show ipv6 ospf [areaid] database [{external | inter-area {prefix | router} | link | network | nssa-external | prefix | router | unknown {area | as | link}}] [lsid] [{adv- router [rtrid] | self-originate}]`

Режимы ввода команд: привилегированный

пользовательский

Для каждого типа соединения и зоны отображается следующая информация:

Термин	***Значение***
Link Id	Число, обозначающее LSA, создаваемый маршрутизатором из всех остальных сгенерированных LSA того же типа LS.
Adv Router	Анонсирующий маршрутизатор. IP-адрес, обозначающий LSDB-интерфейс.
Age	Число, представляющее время существования LSA в секундах.
Sequence	Число, представляющее текущую версию LSA.
Checksum	Итоговая контрольная сумма LSA.
Prefix	IPv6-префикс.
Interface	Интерфейс для соединения.
Rtr Count	Количество маршрутизаторов, подключенных к сети.

show ipv6 ospf database database-summary

Используйте эту команду, чтобы отобразить количество LSA каждого типа и общего количества LSA в базе данных.

Формат: `show ipv6 ospf database database-summary`

Режимы ввода команд: привилегированный
пользовательский

Термин	***Значение***
Router	Общее количество LSA маршрутизатора в базе данных состояния соединения OSPFv3.
Network	Общее количество сетевых LSA в базе данных состояния соединения OSPFv3.
Inter-area Prefix	Общее количество LSA с межзональным префиксом в базе данных состояния соединения OSPFv3.
Inter-area Router	Общее количество LSA межзональных маршрутизаторов в базе данных

	состояния соединения OSPFv3.
Type-7 Ext	Общее количество внешних LSA NSSA в базе данных состояния соединения OSPFv3.
Link	Общее количество LSA соединения в базе данных состояния соединения OSPFv3.
Intra-area Prefix	Общее количество LSA с внутризональными префиксами в базе данных состояния соединения OSPFv3.
Link Unknown	Общее количество LSA с неизвестным источником в базе данных состояния соединения OSPFv3.
Area Unknown	Общее число LSA неизвестных зон в базе данных состояния соединения OSPFv3.
AS Unknown	Общее число LSA неизвестных AS в базе данных состояния соединения OSPFv3.
Type-5 Ext	Общее число LSA внешних AS в базе данных состояния соединения OSPFv3.
Self-Originated	Общее количество собственных сгенерированных внешних LSA AS в базе данных состояния соединения OSPFv3.
Total	Общее количество LSA маршрутизатора в базе данных состояния соединения OSPFv3.

show ipv6 ospf interface

Эта команда отображает информацию для объекта IFO или таблицы виртуального интерфейса. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*).

Формат: `show ipv6 ospf interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`|loopback `*`loopback-id`*` | tunnel `*`tunnel-id`*`}`

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
IP Address	IPv6-адрес интерфейса.
ifIndex	Индекс интерфейса, связанный с данным интерфейсом.
OSPF Admin Mode	Показывает, включен или выключен административный режим.
OSPF Area ID	Идентификатор зоны, связанной с этим интерфейсом.
Router Priority	Приоритет маршрутизатора. Приоритет маршрутизатора определяет, какой маршрутизатор является назначенным маршрутизатором.
Retransmit Interval	Частота в секундах, с которой интерфейс отправляет LSA.
Hello Interval	Частота в секундах, с которой интерфейс отправляет пакеты Hello.
Dead Interval	Промежуток времени в секундах, в течение которого интерфейс ожидает, прежде чем определить, что соседний узел не функционирует.
LSA Ack Interval	Промежуток времени в секундах, в течение которого интерфейс задерживает отправку подтверждения LSA после получения LSA.
Interface Transmit Delay	Количество секунд, которые интерфейс добавляется к возрасту LSA-пакетов перед передачей.
Authentication Type	Тип аутентификации интерфейса, выполняемой в отношении принимаемых LSA.

Metric Cost	Приоритет пути. Низкая стоимость имеет более высокий приоритет по сравнению с высокой.
Prefix-suppression	Отображает статус подавления префиксов на данном интерфейсе: enabled, disabled или unconfigured.
Passive Status	Показывает, является ли интерфейс пассивным.
OSPF MTU-ignore	Показывает, игнорируются ли несовпадения MTU в пакетах-дескрипторах базы данных, присланных соседними маршрутизаторами.
Link LSA Suppression	Настроенное состояние подавления LSA соединения для интерфейса.

Следующая информация отображается только в том случае, если на интерфейсе инициализирован OSPF.

Термин	***Значение***
OSPF Interface Type	Тип OSPF-интерфейса broadcast или ptp.
State	Состояния OSPF-интерфейса могут обозначаться как own, loopback, waiting, point-to-point, designated router и backup designated router.
Designated Router	Идентификатор маршрутизатора, представляющий назначенный маршрутизатор.
Backup Designated Router	Идентификатор маршрутизатора, представляющий резервный назначенный маршрутизатор.
Number of Link Events	Количество событий соединения.
Metric Cost	Стоимость OSPF-интерфейса.

show ipv6 ospf interface brief

Эта команда выводит на экран краткую информацию для объекта IFO или таблиц виртуального интерфейса.

Формат: `show ipv6 ospf interface brief`

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
Interface	Интерфейс в формате *unit/slot/port*.
OSPF Admin Mode	Указывает, включен ли OSPF на интерфейсе маршрутизатора.
OSPF Area ID	Идентификатор OSPF-зоны для указанного интерфейса.
Router Priority	Приоритет маршрутизатора. Приоритет маршрутизатора определяет, какой маршрутизатор является назначенным маршрутизатором.
Metric Cost	Приоритет пути. Низкая стоимость имеет более высокий приоритет по сравнению с высокой.
Hello Interval	Частота в секундах, с которой интерфейс отправляет пакеты Hello.
Dead Interval	Промежуток времени в секундах, в течение которого интерфейс ожидает, прежде чем определить, что соседний узел не функционирует.
Retransmit Interval	Частота в секундах, с которой интерфейс отправляет LSA. Частота в секундах, с которой интерфейс отправляет LSA.
Retransmit Delay Interval	Количество секунд, которые интерфейс добавляется к возрасту LSA-пакетов перед передачей.
LSA Ack Interval	Промежуток времени в секундах, в течение которого интерфейс

	задерживает отправку подтверждения LSA после получения LSA.

show ipv6 ospf interface stats

Команда отображает статистику для указанного интерфейса. Информация отображается только в том случае, если OSPF включен.

Формат: `show ipv6 ospf interface stats {`*`unit/slot/port`* `| vlan` *`id`*`}`

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
OSPFv3 Area ID	Идентификатор OSPF-зоны для указанного интерфейса.
IP Address	IP-адрес, связанный с данным OSPF-интерфейсом.
OSPFv3 Interface Events	Количество случаев, когда указанный OSPF-интерфейс менял свой статус или когда происходили ошибки.
Virtual Events	Количество изменений статуса или ошибок, зафиксированных на данном виртуальном соединении.
Neighbor Events	Количество случаев, когда соседнее устройство меняло свой статус или происходила ошибка.
Packets Received	Количество OSPFv3-пакетов, принятых на интерфейсе.
Packets Transmitted	Количество OSPFv3-пакетов, отправленных на интерфейсе.
LSAs Sent	Общее количество LSA, отправленных на интерфейс.
LSA Acks Received	Общее количество LSA, подтвержденных этим интерфейсом.
LSA Acks Sent	Общее количество LSA, подтвержденных для этого интерфейса.
Sent Packets	Количество OSPF-пакетов, переданных на интерфейсе.
Received Packets	Количество действительных OSPF-пакетов, принятых интерфейсом.
Discards	Количество принятых OSPF-пакетов, отброшенных по причине ошибки в пакете или при его обработке
Bad Version	Количество принятых OSPF-пакетов, чье поле версии в заголовке OSPF не совпадало с версией OSPF-процесса, который обрабатывал пакет.
Virtual Link Not Found	Количество принятых пакетов, отброшенных из-за того, что входной интерфейс находится не в магистральной зоне, а заголовок OSPF идентифицировал пакет как принадлежащий к магистрали, но у OSPF не было виртуального канала для отправителя пакета.
Area Mismatch	Количество OSPF-пакетов, отброшенных из-за того, что идентификатор зоны в OSPF-заголовке не совпадает с идентификатором, настроенным на входном интерфейсе.
Invalid Destination Address	Количество OSPF-пакетов, отброшенных из-за того, что их IP-адрес назначения не является адресом входного интерфейса и адресом многоадресной рассылки AllDrRouters или AllSpfRouters.
No Neighbor at Source Address	Количество пакетов, OSPF-отброшенных из-за того, что отправитель — несуществующий сосед или IP-адрес отправителя не совпадает с предыдущим записанным IP-адресом для этого соседа. ПРИМЕЧАНИЕ. Не относится к Hello-пакетам.
Invalid OSPF Packet Type	Количество OSPF-пакетов, отброшенных из-за того, что поле packet type в OSPF-заголовке является неизвестным типом.
Hellos Ignored	Количество принятых Hello-пакетов, которые игнорируются данным маршрутизатором от новых соседей после того, как было достигнуто

	предельное количество соседей на данном интерфейсе или в системе в целом.

show ipv6 ospf lsa-group

Эта команда отображает количество сгенерированных LSA внутри каждой группы LSA.

Формат: `show ipv6 ospf lsa-group`

Режимы ввода команд: привилегированный

пользовательский

show ipv6 ospf max-metric

Данная команда отображает настроенные максимальные метрики для режима Stub-Router.

Формат: `show ipv6 ospf max-metric`

Режимы ввода команд: привилегированный

пользовательский

show ipv6 ospf neighbor

Данная команда отображает информацию о соседних OSPF-узлах. Если не указать IP-адрес соседа, команда отобразит общую информацию в таблице. Если указан стандартный или туннельный интерфейс, команда отображает информацию для этого интерфейса или туннеля. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Параметр *ip-address* — IP-адрес соседа, и если его указать, отобразится подробная информация об этом соседе. Информация ниже отображается только в том случае, если включен OSPF и у интерфейса есть соседи.

Формат: `show ipv6 ospf neighbor [interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`|tunnel `*`tunnel_id`*`}][`*`ip- address`*`]`

Режимы ввода команд: привилегированный

пользовательский

Если не указать IP-адрес, таблица с данными столбцами отобразится для всех соседей или для соседа, связанного с интерфейсом, который вы укажете:

Термин	***Значение***
Router ID	Идентификатор соседнего маршрутизатора.
Priority	OSPF-приоритет указанного интерфейса. Приоритет интерфейса — это целое число от 0 до 255. Нулевое значение обозначает, что маршрутизатор не подходит на роль назначенного маршрутизатора в данной сети.
Intf ID	Идентификатор интерфейса соседнего узла.
Interface	Интерфейс локального маршрутизатора в формате *unit/slot/port*.
State	Состояние соседних маршрутизаторов. Возможные значения перечислены ниже. • **Down** — исходное состояние соседа; от соседа не было получено свежей информации. • **Attempt** — от соседа не было получено свежей информации, но более согласованные усилия должны быть приложены, чтобы

	связаться с соседом. • **Init** — от соседа недавно был замечен Hello-пакет, но двунаправленное соединение пока еще не установлено. • **way** — между двумя маршрутизаторами установлено двунаправленное соединение. • **Exchange start** — первый шаг в создании смежности между двумя соседними маршрутизаторами: цель состоит в том, чтобы решить, какой маршрутизатор является главным, и принять решение относительно начального номера последовательности DD. • **Exchange** — маршрутизатор описывает всю свою базу данных состояния соединения путем отправки пакетов Database Description соседу. • **Full** — соседние маршрутизаторы полностью смежны, и теперь они будут появляться в LSA маршрутизаторов и LSA сети.
Dead Time	Время в секундах, которое маршрутизатор ожидает перед тем, как посчитать соседа недоступным.
Restart Helper Status	Указывает статус данного маршрутизатора как помощника во время щадящей перезагрузки маршрутизатора, указанного в командной строке. • Helping — данный маршрутизатор является соседом-помощником для указанного маршрутизатора. • Not Helping — данный маршрутизатор не является соседом-помощником в данный момент.
Restart Reason	Если маршрутизатор находится в режиме соседа-помощника, это отображает причину перезапуска, данную перезапускающимся маршрутизатором.
Remaining Grace Time	Количество секунд, оставшихся от интервала текущей щадящей перезагрузки. Отображается, только когда данный маршрутизатор в настоящее время находится в режиме соседа-помощника для указанного в команде маршрутизатора.
Restart Helper Exit Reason	Указывает причину, по которой указанный маршрутизатор вышел из щадящей перезагрузки в последний раз. • **None** — щадящая перезагрузка не проводилась. • **In Progress** — перезагрузка в процессе. • **Completed** — предыдущая щадящая перезагрузка выполнена успешно. • **Timed Out** — время предыдущей щадящей перезагрузки истекло. • **Topology Changed** — предыдущая щадящая перезагрузка досрочно прекращена из-за изменения топологии.

Если указать IP-адрес соседнего маршрутизатора, отобразится следующая информация:

Термин	***Значение***
Interface	Интерфейс локального маршрутизатора в формате *unit/slot/port*.
Area ID	Идентификатор зоны, связанной с интерфейсом.
Options	Целое число, обозначающее необязательные OSPF-возможности, поддерживаемые соседним устройством. Они перечислены в пакетах Hello. Это позволяет Hello-пакетам быть отклоненными (например, если с соседом еще не было установлено соединение), если происходит несоответствие в некоторых ключевых OSPF-возможностях.
Router Priority	Приоритет маршрутизатора для указанного интерфейса.
Dead Timer Due	Время в секундах, которое маршрутизатор ожидает перед тем, как посчитать соседа недоступным.

State	Состояние соседних маршрутизаторов.
Events	Количество случаев, когда соседнее устройство меняло свой статус или происходила ошибка.
Retransmission Queue Length	Целое число, обозначающее текущую длину очереди повторной передачи для указанного идентификатора соседнего маршрутизатора на указанном интерфейсе.

show ipv6 ospf range

Эта команда отображает набор диапазонов префиксов зоны OSPFv3, настроенных для суммирования.

Формат: `show ipv6 ospf range` *`areaid`*

Режимы ввода команд: привилегированный

Термин	***Значение***
Area ID	Зона, префиксы которой суммируются.
IPv6 Prefix/Prefix Length	Суммарный префикс и длина префикса.
Type	**S** (суммарное соединение) или **E** (внешнее соединение)
Action	**Enabled** или **Disabled**
Cost	Метрики, которые анонсируются, если диапазон активен.

show ipv6 ospf statistics

Эта команда отображает информацию о 15 последних результатах расчетов Shortest Path First (SPF). SPF — это расчеты таблицы маршрутизации OSPF.

Формат: `show ipv6 ospf statistics`

Режимы ввода команд: привилегированный

пользовательский

Команда выводит следующую информацию, отображая самые последние статистические данные в конце таблицы.

Термин	***Значение***
Delta T	Время с момента расчета таблицы маршрутизации. Указывается в формате часов, минут и секунд (чч:мм:сс).
Intra	Время, ушедшее на подсчет маршрутов внутри зоны, в миллисекундах.
Summ	Время, ушедшее на подсчет маршрутов между зонами, в миллисекундах.
Ext	Время, ушедшее на подсчет внешних маршрутов, в миллисекундах.
SPF Total	Общее время, ушедшее на вычисление маршрутов, в миллисекундах. Может превышать сумму соответствующих полей для внешних, внутренних и межзональных маршрутов.
RIB Update	Время, прошедшее с последнего выполненного подсчета таблицы маршрутизации, до момента, пока все изменения не были выполнены в общей таблице маршрутизации (RIB), в миллисекундах.
Reason	События, запустившие SPF. Коды причин перечислены ниже. • R: LSA нового маршрутизатора • N: LSA новой сети • SN: суммарный LSA новой сети (межзональный префикс)

	• SA: LSA нового ASBR- (межзонального) маршрутизатора • X: новый внешний LSA • IP: LSA нового внутризонального префикса • L: LSA нового соединения

show ipv6 ospf stub table

Эта команда отображает stub-таблицу OSPF. Информация ниже отображается только в том случае, если на коммутаторе инициализирован OSPF.

Формат: `show ipv6 ospf stub table`

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
Area ID	32-битный идентификатор созданной stub-зоны.
Type of Service	Тип сервиса, связанного со stub-метриками. Для данной версии поддерживается только тип Normal TOS.
Metric Val	Значения метрик, применяемые на основе TOS. По умолчанию устанавливаются наименьшие значения вида обслуживания среди интерфейсов других зон. OSPF-стоимость маршрута является функцией от значения этой метрики.
Import Summary LSA	Управляет импортом суммарных LSA в stub-зоны.

show ipv6 ospf virtual-link

Эта команда отображает информацию виртуального интерфейса OSPF для указанной зоны и соседнего узла. Параметр areaid определяет зону, а параметр neighbor — идентификатор соседнего маршрутизатора.

Формат: `show ipv6 ospf virtual-link` *`areaid neighbor`*

Режимы ввода команд: привилегированный

пользовательский

Термин	***Значение***
Area ID	Идентификатор запрошенной OSPF-зоны.
Neighbor Router ID	Входной идентификатор соседнего маршрутизатора.
Hello Interval	Настроенный интервал Hello для виртуального интерфейса OSPF.
Dead Interval	Настроенный Dead-интервал для виртуального интерфейса OSPF.
Interface Transmit Delay	Настроенная задержка передачи для виртуального интерфейса OSPF.
Retransmit Interval	Настроенный интервал ретрансляции для указанного OSPF-интерфейса.
Authentication Type	Тип аутентификации интерфейса, выполняемой в отношении принимаемых LSA.
State	Состояния OSPF-интерфейса могут обозначаться как own, loopback, waiting, point-to-point, designated router и backup designated router. Этот параметр показывает статус OSPF-интерфейса.
Neighbor State	Состояние соседнего узла.

show ipv6 ospf virtual-link brief

Эта команда отображает краткую информацию виртуального интерфейса OSPFv3 для всех зон в системе.

Формат: `show ipv6 ospf virtual-link brief`

Режимы ввода команд: привилегированный
пользовательский

Термин	*Значение*
Area ID	Идентификатор запрошенной OSPFv3-зоны.
Neighbor	Соседний интерфейс виртуального OSPFv3-интерфейса.
Hello Interval	Настроенный интервал Hello для виртуального OSPFv3-интерфейса.
Dead Interval	Настроенный Dead-интервал для виртуального OSPFv3-интерфейса.
Retransmit Interval	Настроенный интервал повторной передачи для виртуального OSPFv3-интерфейса.
Transmit Delay	Настроенная задержка передачи для виртуального OSPFv3-интерфейса.

14.6 Команды настройки DHCPv6

В этом разделе описаны команды, которые можно использовать для настройки DHCPv6-сервера в системе и просмотра информации, связанной с DHCPv6.

service dhcpv6

Эта команда включает DHCPv6-конфигурацию на маршрутизаторе.

Значение по умолчанию: включено

Формат: `service dhcpv6`

Режим ввода команд: глобальная конфигурация

no service dhcpv6

Команда выключает DHCPv6-конфигурацию на маршрутизаторе.

Формат: `no service dhcpv6`
Режим ввода команд: глобальная конфигурация

ipv6 dhcp client pd

Команда позволяет включить протокол DHCP для клиентского процесса IPv6 (если процесс не запущен) и разрешить запросы Prefix Delegation через указанный интерфейс. Когда запросы Prefix Delegation включены и префикс успешно получен, он сохраняется в общем пуле IPv6-префиксов с внутренним именем, заданным с помощью автоматического аргумента.

Клиент Prefix Delegation поддерживается только на одном IP-интерфейсе.

Параметр rapid-commit позволяет использовать метод обмена двумя сообщениями для делегирования префикса и другие конфигурации. Если этот параметр включен, клиент может выполнять быстрый обмен запросами.

Функции DHCP для IPv6-клиента, сервера и ретранслятора на интерфейсе являются взаимоисключающими. Если одна из этих функций уже включена и пользователь пытается настроить другую функцию на том же интерфейсе, появится соответствующее сообщение.

Значение по умолчанию: Выключено

Формат: `ipv6 dhcp client pd [rapid-commit]`

Режим ввода команд: конфигурирование интерфейса

no ipv6 dhcp client pd

Эта команда выключает запросы Prefix Delegation.

Формат: `no ipv6 dhcp client pd`

Режим ввода команд: конфигурирование интерфейса

ipv6 dhcp server

Используйте эту команду для настройки функционала DHCPv6-сервера на интерфейсе или диапазоне интерфейсов. Параметр pool-name определяет DHCPv6-пул, содержащий параметры stateless и/или prefix delegation. Параметр automatic позволяет серверу автоматически определять, какой пул использовать при выделении адресов для клиента. rapid-commit — это опция, которая позволяет сокращенный обмен сообщениями между клиентом и сервером. Значение pref-value используется клиентами для определения предпочтений между несколькими DHCPv6-серверами. Для конкретного интерфейса функции DHCPv6-сервера и DHCPv6-ретранслятора являются взаимоисключающими.

Формат: `ipv6 dhcp server {`*`pool-name`*` | automatic}[rapid-commit] [preference `*`pref-value`*`]`

Режим ввода команд: конфигурирование интерфейса

ipv6 dhcp relay destination

Используйте эту команду, чтобы настроить интерфейс для работы в качестве DHCPv6-ретранслятора на интерфейсе или диапазоне интерфейсов. Используйте ключевое слово destination для настройки IPv6-адреса сервера ретрансляции. Параметр relay-address — это IPv6-адрес сервера DHCPv6-ретранслятора. Используйте ключевое слово interface, чтобы установить интерфейс сервера ретрансляции. Параметр relay- interface обозначает интерфейс (unit/slot/port) для доступа к серверу ретрансляции. Необязательный параметр remote-id позволяет агенту ретрансляции добавлять информационную опцию «remote ID» к ретранслируемым сообщениям. Для этого параметра можно использовать специальное ключевое слово duid-ifid, и в этом случае «remote ID» будет определяться на основании DUID DHCPv6-сервера и номера интерфейса ретранслятора. В противном случае значение этой опции может быть определено в виде строки, заданной пользователем.

Если *relay-address* является глобальным IPv6-адресом, параметр *relay-interface* не является обязательным. Если *relay-address* является групповым адресом или адресом link-local, параметр *relay-interface* является обязательным. И наконец, если значение для *relay-address* не указано, значение *relay-interface* должно быть указано в обязательном порядке, а для ретрансляции DHCPv6-сообщений к серверу ретрансляции будет использоваться групповой адрес DHCPV6-ALL-AGENTS (т. е. FF02::1:2).

Формат: `ipv6 dhcp relay {destination [`*`relay-address`*`] interface [`*`relay-interface`*`]| interface [`*`relay-interface`*`]} [remote-id (`*`duid-ifid`*` | user-defined-string)]`

Режим ввода команд: конфигурирование интерфейса

ipv6 dhcp pool

Используйте эту команду в режиме глобальной конфигурации для входа в режим конфигурирования пула DHCPv6. Параметр pool-name должен включать до 30 буквенно-цифровых символов. Пулы DHCPv6 используются для указания DHCPv6-серверу информации для распространения по DHCPv6-клиентам. Эти пулы являются общими для нескольких интерфейсов, через которые настраиваются возможности DHCPv6-сервера.

После того, как информационный пул DHCP для IPv6 был создан, используйте команду ipv6 dhcp server, чтобы связать пул с сервером на интерфейсе. Если информационный пул не настроен, используйте команду настройки ipv6 dhcp server interface, чтобы включить функцию DHCPv6-сервера на интерфейсе.

Когда вы связываете пул DHCPv6 с интерфейсом, на соответствующем интерфейсе обслуживаются только сервисные запросы данного пула. Пул также обслуживает другие интерфейсы. Если вы не связываете пул DHCPv6 с интерфейсом, он может обслуживать запросы на любом интерфейсе. Если префикс IPv6-адреса не используется, пул возвращает только настроенные опции.

Формат: `ipv6 dhcp pool` *`pool-name`*

Режим ввода команд: глобальная конфигурация

no ipv6 dhcp pool

Данная команда удаляет указанный пул DHCPv6.

Формат: `no ipv6 dhcp pool` *`pool-name`*

Режим ввода команд: глобальная конфигурация

address prefix (IPv6)

Используйте эту команду для установки IPv6-префикса. Адрес должен быть в шестнадцатеричном формате с использованием 16-битных значений разделённых двоеточиями.

Если значения lifetime не настроены, значения valid-lifetime и preferred-lifetime по умолчанию считаются бесконечными.

Формат: `address prefix` *`ipv6-prefix`* `[lifetime {`*`valid-lifetime preferred-lifetime`*` | infinite}]`

Режим ввода команд: конфигурирование пула DHCPv6

Термин	***Значение***
lifetime	(Необязательный параметр.) Указывает, в течение какого периода сервер должен помнить анонсы маршрутизатора. При настройке этого параметра обязательно требуется также указать значения для *valid-lifetime* и *preferred-lifetime*.
valid-lifetime	Период времени в секундах, в течение которого префикс остается действительным для запрашивающего маршрутизатора. Диапазон — от 60 до 4 294 967 294. Значение *preferred-lifetime* не может быть больше значения *valid-lifetime*.
preferred-lifetime	Период времени в секундах, в течение которого префикс остается приоритетным для запрашивающего маршрутизатора. Диапазон — от 60 до 4 294 967 294. Значение *preferred-lifetime* не может быть больше значения *valid-lifetime*.

infinite	Неограниченное время жизни.

domain-name (IPv6)

Эта команда устанавливает имя домена DNS, который предоставляется DHCPv6-клиенту DHCPv6-сервером. Доменное имя включает не более 31 буквенно-цифровых символов. Пул DHCPv6 может иметь несколько доменных имен, максимум 8.

Формат: `domain-name` *`dns-domain-name`*

Режим ввода команд: конфигурирование пула DHCPv6

no domain-name

Данная команда удаляет доменное имя DHCPv6 из пула DHCPv6.

Формат: `no domain-name` *`dns-domain-name`*

Режим ввода команд: конфигурирование пула DHCPv6

dns-server (IPv6)

Эта команда устанавливает IPv6-адрес DNS-сервера, который предоставляется DHCPv6-клиенту DHCPv6-сервером. Пул DHCPv6 может иметь несколько доменных имен, максимум 8.

Формат: `dns-server` *`dns-server-address`*

Режим ввода команд: конфигурирование пула DHCPv6

no dns-server

Данная команда удаляет адрес DNS-сервера с DHCPv6-сервера.

Формат: `no dns-server` *`dns-server-address`*

Режим ввода команд: конфигурирование пула DHCPv6

prefix-delegation (IPv6)

Для распределения определенным клиентам делегирования DHCPv6-префикса в пуле можно определить несколько префиксов IPv6. Prefix — это делегированный префикс IPv6. DUID — это уникальное значение DUID клиента (пример: 00:01:00:09:f8:79:4e:00:04:76:73:43:76). Name — это текстовое имя клиента длиной 31 символ, которое используется только для журналов или отслеживаний. Valid lifetime — это действительное время жизни для делегированного префикса в секундах; preferred lifetime является предпочтительным временем жизни для делегированного префикса в секундах.

Значение по умолчанию: valid-lifetime — 2 592 000;

preferred-lifetime — 604 800.

Формат: `prefix-delegation` *`prefix/prefixlength DUID`* `[name` *`host-name`*`][valid-lifetime` *`04294967295`*`][preferred-lifetime` *`0-4294967295`*`]`

Режим ввода команд: конфигурирование пула DHCPv6

no prefix-delegation

Эта команда удаляет конкретного клиента делегирования префиксов.

Формат: `no prefix-delegation` *`prefix/prefix-delegation DUID`*

Режим ввода команд: конфигурирование пула DHCPv6

show ipv6 dhcp

Эта команда отображает имя и состояние DHCPv6-сервера.

Формат: `show ipv6 dhcp`

Режим ввода команд: привилегированный

Термин	*Значение*
DHCPv6 is Enabled (Disabled)	Состояние DHCPv6-сервера.
Server DUID	Уникальный идентификатор DHCPv6, если настроен.

show ipv6 dhcp statistics

Эта команда отображает статистику IPv6 DHCP для всех интерфейсов.

Формат: `show ipv6 dhcp statistics`

Режим ввода команд: привилегированный

Термин	*Значение*
DHCPv6 Solicit Packets Received	Статистика по количеству полученных пакетов Solicit.
DHCPv6 Request Packets Received	Статистика по количеству полученных пакетов Request.
DHCPv6 Confirm Packets Received	Статистика по количеству полученных пакетов Confirm.
DHCPv6 Renew Packets Received	Статистика по количеству полученных пакетов Renew.
DHCPv6 Rebind Packets Received	Статистика по количеству полученных пакетов Rebind.
DHCPv6 Release Packets Received	Статистика по количеству полученных пакетов Release.
DHCPv6 Decline Packets Received	Статистика по количеству полученных пакетов Decline.
DHCPv6 Inform Packets Received	Статистика по количеству полученных пакетов Inform
DHCPv6 Relay-forward Packets Received	Статистика по количеству полученных пакетов Relay-forward.
DHCPv6 Relay-reply Packets Received	Статистика по количеству полученных пакетов Relay-reply
DHCPv6 Malformed Packets Received	Статистика по количеству полученных повреждённых пакетов.
Received DHCPv6 Packets Discarded	Статистика по количеству отброшенных DHCPv6-пакетов.
Total DHCPv6 Packets Received	Статистика по общему количеству принятых DHCPv6-пакетов.
DHCPv6 Advertisement Packets Transmitted	Статистика по количеству отправленных анонсов.
DHCPv6 Reply Packets Transmitted	Статистика по количеству отправленных пакетов Reply.
DHCPv6 Reconfig Packets Transmitted	Статистика по количеству отправленных пакетов Reconfig.
DHCPv6 Relay-reply Packets Transmitted	Статистика по количеству отправленных пакетов Relay-reply.
DHCPv6 Relay-forward Packets Transmitted	Статистика по количеству отправленных пакетов Relay-forward.

Total DHCPv6 Packets Transmitted	Статистика по общему количеству отправленных DHCPv6-пакетов.

show ipv6 dhcp interface

Эта команда отображает информацию DHCPv6 для всех связанных интерфейсов или указанного интерфейса. Аргумент *unit/slot/port* относится к физическому или виртуальному интерфейсу маршрутизации. Ключевое слово **vlan** используется для прямого указания идентификатора VLAN на маршрутизирующем VLAN-интерфейсе (вместо формата *unit/slot/port*). Если указан интерфейс, можно использовать необязательный параметр statistics для просмотра статистики указанного интерфейса.

Формат: `show ipv6 dhcp interface {`*`unit/slot/port`*`|vlan `*`1-4093`*`} [statistics]`

Режим ввода команд: привилегированный

Термин	***Значение***
IPv6 Interface	Имя интерфейса в формате *unit/slot/port*.
Mode	Показывает, является интерфейс IPv6 DHCP ретранслятором или сервером.

Если режим интерфейса — сервер, отображается следующая информация.

Термин	***Значение***
Pool Name	Имя пула, определяющего информацию для распространения DHCPv6-сервером в адрес DHCPv6-клиентов.
Server Preference	Приоритет сервера.
Option Flags	Показывает, включена ли функция rapid commit.

Если режим интерфейса — ретранслятор, отображается следующая информация.

Термин	***Значение***
Relay Address	IPv6-адрес сервера ретрансляции.
Relay Interface Number	Интерфейс сервера ретрансляции в формате *unit/slot/port*.
Relay Remote ID	Отображает имя удаленного ретранслятора, если таковой настроен.
Option Flags	Показывает, настроена ли функция rapid commit.

Если используется параметр statistics, команда отображает статистику IPv6 DHCP для указанного интерфейса. Подробнее о выводе см. в описании команды show ipv6 dhcp statistics.

show ipv6 dhcp binding

Эта команда отображает настроенный пул DHCP.

Формат: `show ipv6 dhcp binding `*`[ipv6-address]`*

Режим ввода команд: привилегированный

Термин	***Значение***
DHCP Client Address	Адрес DHCP-клиента.
DUID	Строка, которая представляет DUID клиента.
IAID	Идентификатор Identity Association.
Prefix/Prefix Length	IPv6-адрес и маска длины для делегированного префикса.

Prefix Type	Тип IPV6-префикса (IPAD, IANA или IATA).
Client Address	Адрес DHCP-клиента.
Client Interface	IPv6-адрес DHCP-клиента.
Expiration	Адрес DNS-сервера.
Valid Lifetime	Действительное время жизни для делегированного префикса в секундах.
Preferred Lifetime	Предпочтительное время жизни для делегированного префикса в секундах.

show ipv6 dhcp pool

Эта команда отображает настроенный пул DHCP.

Формат: `show ipv6 dhcp pool` *`pool-name`*

Режим ввода команд: привилегированный

Термин	***Значение***
DHCP Pool Name	Уникальная конфигурация имени пула.
Client DUID	Уникальный DHCP-идентификатор клиента. DUID создается с использованием комбинации предустановленного MAC-адреса локальной системы и значения временной метки.
Host	Имя клиента.
Prefix/Prefix Length	IPv6-адрес и маска длины для делегированного префикса.
Preferred Lifetime	Предпочтительное время жизни для делегированного префикса в секундах.
Valid Lifetime	Действительное время жизни для делегированного префикса в секундах.
DNS Server Address	Адрес DNS-сервера.
Domain Name	Доменное имя DNS.

show network ipv6 dhcp statistics

Эта команда отображает статистику DHCPv6-клиента, работающего на сетевом интерфейсе управления.

Формат: `show network ipv6 dhcp statistics`

Режим ввода команд: привилегированный

пользовательский

Поле	***Описание***
DHCPv6 Advertisement Packets Received	Количество пакетов DHCPv6 Advertisement, принятых на сетевом интерфейсе.
DHCPv6 Reply Packets Received	Количество пакетов DHCPv6 Reply, принятых на сетевом интерфейсе.
Received DHCPv6 Advertisement Packets Discarded	Количество пакетов DHCPv6 Advertisement, отброшенных на сетевом интерфейсе.
Received DHCPv6 Reply Packets Discarded	Количество пакетов DHCPv6 Reply, отброшенных на сетевом интерфейсе.
DHCPv6 Malformed Packets Received	Количество DHCPv6-пакетов с искажениями, принятых на сетевом интерфейсе.

Total DHCPv6 Packets Received	Общее количество DHCPv6-пакетов, принятых на сетевом интерфейсе.
DHCPv6 Solicit Packets Transmitted	Количество пакетов DHCPv6 Solicit, отправленных на сетевом интерфейсе.
DHCPv6 Request Packets Transmitted	Количество пакетов DHCPv6 Request, отправленных на сетевом интерфейсе.
DHCPv6 Renew Packets Transmitted	Количество пакетов DHCPv6 Renew, отправленных на сетевом интерфейсе.
DHCPv6 Rebind Packets Transmitted	Количество пакетов DHCPv6 Rebind, отправленных на сетевом интерфейсе.
DHCPv6 Release Packets Transmitted	Количество пакетов DHCPv6 Release, отправленных на сетевом интерфейсе.
Total DHCPv6 Packets Transmitted	Общее количество DHCPv6-пакетов, отправленных на сетевом интерфейсе.

show serviceport ipv6 dhcp statistics

Данная команда отображает статистику DHCPv6-клиента, работающего на интерфейсе управления

Формат: `show serviceport ipv6 dhcp statistics`

Режим ввода команд: привилегированный

пользовательский

Поле	***Описание***
DHCPv6 Advertisement Packets Received	Количество пакетов DHCPv6 Advertisement, принятых на сетевом интерфейсе.
DHCPv6 Reply Packets Received	Количество пакетов DHCPv6 Reply, принятых на сетевом интерфейсе.
Received DHCPv6 Advertisement Packets Discarded	Количество пакетов DHCPv6 Advertisement, отброшенных на сетевом интерфейсе.
Received DHCPv6 Reply Packets Discarded	Количество пакетов DHCPv6 Reply, отброшенных на сетевом интерфейсе.
DHCPv6 Malformed Packets Received	Количество DHCPv6-пакетов с искажениями, принятых на сетевом интерфейсе.
Total DHCPv6 Packets Received	Общее количество DHCPv6-пакетов, принятых на сетевом интерфейсе.
DHCPv6 Solicit Packets Transmitted	Количество пакетов DHCPv6 Solicit, отправленных на сетевом интерфейсе.
DHCPv6 Request Packets Transmitted	Количество пакетов DHCPv6 Request, отправленных на сетевом интерфейсе.
DHCPv6 Renew Packets Transmitted	Количество пакетов DHCPv6 Renew, отправленных на сетевом интерфейсе.
DHCPv6 Rebind Packets Transmitted	Количество пакетов DHCPv6 Rebind, отправленных на сетевом интерфейсе.
DHCPv6 Release Packets Transmitted	Количество пакетов DHCPv6 Release, отправленных на сетевом интерфейсе.
Total DHCPv6 Packets Transmitted	Общее количество DHCPv6-пакетов, отправленных на сетевом интерфейсе.

clear ipv6 dhcp

Команда позволяет очистить статистику DHCPv6 для всех интерфейсов или для конкретного интерфейса. Используйте параметр unit/slot/port, чтобы указать интерфейс, и параметр vlan, чтобы указать VLAN.

Формат: `clear ipv6 dhcp {statistics | interface {`*`unit/slot/port`*` | vlan `*`id`*`}}`

Режим ввода команд: привилегированный

clear ipv6 dhcp binding

Эта команда удаляет автоматическую привязку адресов из базы данных DHCPv6-сервера. Параметр address является действительным IPv6-адресом.

Для записи привязки в таблице DHCPv6-сервера автоматически выполняются следующие операции:

- создание, когда префикс делегируется клиенту из настроенного пула;
- обновление, когда клиент обновляет, повторно связывает или подтверждает делегирование префикса;
- удаление, когда клиент освобождает все связанные префиксы добровольно, истек период valid lifetimes для всех префиксов или администратор запускает команду **clear ipv6 dhcp binding**.

Если команда clear ipv6 dhcp binding используется с необязательным аргументом ipv6-address, удаляется только привязку для указанного клиента. Если команда clear ipv6 dhcp binding используется без аргумента ipv6-address, из таблицы привязки DHCPv6-сервера удаляются все автоматически выполненные привязки клиентов.

Формат: `clear ipv6 dhcp binding [`*`ipv6-address`*`]`

Режим ввода команд: привилегированный

clear network ipv6 dhcp statistics

Используйте эту команду, чтобы сбросить статистику DHCPv6 на сетевом интерфейсе управления.

Формат: `clear network ipv6 dhcp statistics`

Режим ввода команд: привилегированный

clear serviceport ipv6 dhcp statistics

Используйте эту команду, чтобы очистить статистику DHCPv6-клиента на интерфейсе сервисного порта.

Формат: `clear serviceport ipv6 dhcp statistics`

Режим ввода команд: привилегированный

14.7 Команды настройки DHCPv6 Snooping

В этом разделе описаны команды, используемые для настройки функции IPv6 DHCP Snooping.

ipv6 dhcp snooping

Используйте эту команду, чтобы глобально включить IPv6 DHCP Snooping.

Значение по умолчанию: выключено

Формат: `ipv6 dhcp snooping`

Режим ввода команд: глобальная конфигурация

no ipv6 dhcp snooping

Команда используется, чтобы глобально выключить IPv6 DHCP Snooping.

Формат: `no ipv6 dhcp snooping`

Режим ввода команд: глобальная конфигурация

ipv6 dhcp snooping vlan

Используйте эту команду, чтобы включить DHCP Snooping на списке диапазонов VLAN, перечисленных через запятую.

Значение по умолчанию: выключено

Формат: `ipv6 dhcp snooping vlan` *`vlan-list`*

Режим ввода команд: глобальная конфигурация

no ipv6 dhcp snooping vlan

Используйте эту команду, чтобы выключить DHCP Snooping на указанных VLAN.

Формат: `no ipv6 dhcp snooping vlan` *`vlan-list`*

Режим ввода команд: глобальная конфигурация

ipv6 dhcp snooping verify mac-address

Команда включает проверку MAC-адреса источника сообщения и MAC-адреса клиента в полученном DHCP-сообщении.

Значение по умолчанию: включено

Формат: `ipv6 dhcp snooping verify mac-address`

Режим ввода команд: глобальная конфигурация

no ipv6 dhcp snooping verify mac-address

Используйте эту команду, чтобы выключить проверку MAC-адреса источника.

Формат: `no ipv6 dhcp snooping verify mac-address`

Режим ввода команд: глобальная конфигурация

ipv6 dhcp snooping database

Используйте эту команду, чтобы настроить постоянное расположение для базы данных DHCP Snooping. Расположение может быть локальным или в виде удаленного файла на устройстве с указанным IP-адресом.

Значение по умолчанию: local

Формат: `ipv6 dhcp snooping database {local|tftp://hostIP/filename}`

Режим ввода команд: глобальная конфигурация

ip dhcp snooping database write-delay

Используйте эту команду, чтобы настроить интервал в секундах, в течение которого база данных DHCP Snooping должна быть сохранена. Значение интервала находится в диапазоне от 15 до 86 400 секунд.

Значение по умолчанию: 300 секунд

Формат: `ip dhcp snooping database write-delay` *`in seconds`*

Режим ввода команд: глобальная конфигурация

no ip dhcp snooping database write-delay

Команда устанавливает write-delay в значение по умолчанию.

Формат: `no ip dhcp snooping database write-delay`

Режим ввода команд: глобальная конфигурация

ipv6 dhcp snooping binding

Команда для настройки статичной привязки DHCP Snooping.

Формат: `ipv6 dhcp snooping binding` *`mac-address`* `vlan` *`vlan id ip address`* `interface` *`interface id`*

Режим ввода команд: глобальная конфигурация

no ipv6 dhcp snooping binding

Команда удаляет статичную запись DHCP из базы данных DHCP Snooping.

Формат: `no ipv6 dhcp snooping binding` *`mac-address`*

Режим ввода команд: глобальная конфигурация

ipv6 dhcp snooping trust

Используйте эту команду, чтобы настроить интерфейс или диапазон интерфейсов как доверенные.

Значение по умолчанию: выключено

Формат: `ipv6 dhcp snooping trust`

Режим ввода команд: конфигурирование интерфейса

no ipv6 dhcp snooping trust

Команда настраивает порт как не доверенный.

Формат: `no ipv6 dhcp snooping trust`

Режим ввода команд: конфигурирование интерфейса

ipv6 dhcp snooping log-invalid

Используйте данную команду, чтобы управлять фильтрацией DHCP-сообщений для ведения журнала приложением DHCP Snooping. Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Значение по умолчанию: выключено

Формат: `ipv6 dhcp snooping log-invalid`

Режим ввода команд: конфигурирование интерфейса

no ipv6 dhcp snooping log-invalid

Используйте данную команду, чтобы выключить фильтрацию DHCP-сообщений для ведения журнала приложением DHCP Snooping.

Формат: `no ipv6 dhcp snooping log-invalid`

Режим ввода команд: конфигурирование интерфейса

ipv6 dhcp snooping limit

Команда помогает управлять скоростью, с которой сообщения DHCP Snooping приходят на интерфейс или диапазон интерфейсов. По умолчанию ограничение скорости выключено. Если ограничение включено, скорость может составлять от 0 до 300 пакетов в секунду. Диапазон уровней всплесков — от 1 до 15 секунд. Ограничение скорости настраивается на физическом порте и может быть применено к надежным и ненадежным портам.

Значение по умолчанию: выключено (ограничений нет).

Формат: `ipv6 dhcp snooping limit {rate pps [burst interval seconds]}`

Режим ввода команд: конфигурирование интерфейса

no ipv6 dhcp snooping limit

Команда устанавливает значение скорости, с которой приходят сообщения DHCP Snooping, и уровень всплесков в значения по умолчанию.

Формат: `no ipv6 dhcp snooping limit`

Режим ввода команд: конфигурирование интерфейса

ipv6 verify source

Используйте эту команду, чтобы настроить функционал IPv6 Source Guard. Идентификатор источника — это сочетание IP-адреса и MAC-адреса. Обычная команда включает фильтрацию трафика на основе IP-адреса. С опцией port-security трафик данных будет фильтроваться на основе IP-адресов и MAC-адресов.

Данная команда может использоваться для настройки одного интерфейса или диапазона интерфейсов.

Значение по умолчанию: выключено

Формат: `ipv6 verify source {port-security}`

Режим ввода команд: конфигурирование интерфейса

no ipv6 verify source

Используйте эту команду, чтобы выключить функционал IPv6 Source Guard в системе. Невозможно выключить отдельно port-security, если этот параметр настроен.

Формат: `no ipv6 verify source`

Режим ввода команд: конфигурирование интерфейса

ipv6 verify binding

Используйте данную команду, чтобы настроить статичные записи IPv6 Source Guard (IPv6SG).

Формат: `ipv6 verify binding` *`mac-address`* `vlan` *`vlan id ipv6 address`* `interface` *`interface id`*

Режим ввода команд: глобальная конфигурация

no ipv6 verify binding

Используйте данную команду, чтобы удалить статичную запись IPv6SG из базы данных IPv6SG.

Формат: `no ipv6 verify binding` *`mac-address`* `vlan` *`vlan id ipv6 address`* `interface` *`interface id`*

Режим ввода команд: глобальная конфигурация

show ipv6 dhcp snooping

Используйте эту команду, чтобы отобразить глобальные настройки DHCP Snooping и настройки для каждого порта.

Формат: `show ipv6 dhcp snooping`

Режим ввода команд: привилегированный

пользовательский

Термин	***Значение***
Interface	Интерфейс, для которого отображается информация.
Trusted	При значении enabled DHCP Snooping считает этот порт надежным.
Log Invalid Pkts	При значении enabled DHCP Snooping вносит в журнал на данном интерфейсе сбойные пакеты.

show ipv6 dhcp snooping binding

Используйте эту команду, чтобы отобразить записи привязки DHCP Snooping. Чтобы упорядочить вывод информации, используйте следующие опции:

- Dynamic: ограничить вывод по DHCP Snooping.
- Interface: ограничить вывод по определенному интерфейсу.
- Static: ограничить вывод по статичным записям.
- VLAN: ограничить вывод по VLAN.

Формат: `show ipv6 dhcp snooping binding [{static/dynamic}] [interface` *`unit/slot/port`*`] [vlan id]`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
MAC Address	Отображает MAC-адрес для добавленной привязки. MAC-адрес — это ключ к базе данных привязки.
IPv6 Address	Отображает действительный IPv6-адрес для правил привязки.
VLAN	VLAN для правил привязки.
Interface	Интерфейс, к которому добавляется привязка интерфейса DHCP Snooping.
Type	Тип привязки: статично настраивается в CLI или изучается динамически.
Lease (sec)	Оставшийся срок аренды для записи.

show ipv6 dhcp snooping database

Используйте эту команду, чтобы отобразить настройки DHCP Snooping, относящиеся к сохранению базы данных.

Формат: `show ipv6 dhcp snooping database`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
Agent URL	URL агента базы данных.
Write Delay	Максимальное время записи базы данных (локальной или удаленной).

Формат: `show ipv6 dhcp snooping interfaces [interface` *`unit/slot/port`*`]`

Режим ввода команд: привилегированный

show ipv6 dhcp snooping statistics

Используйте эту команду, чтобы перечислить статистику нарушений безопасности DHCPv6 Snooping на ненадежных портах.

Формат: `show ipv6 dhcp snooping statistics`

Режим ввода команд: привилегированный

пользовательский

Термин	*Значение*
Interface	IPv6-адрес интерфейса в формате *unit/slot/port*.
MAC Verify Failures	Отображает количество DHCP-сообщений, отфильтрованных на ненадежных интерфейсах из-за несовпадения MAC-адреса источника и аппаратного адреса клиента.
Client Ifc Mismatch	Отображает количество DHCP-сообщений Release и Deny, которые были получены на разных портах, изученных ранее.
DHCP Server Msgs Rec'd	Отображает количество сообщений DHCP-сервера, полученных от ненадежных портов.

clear ipv6 dhcp snooping binding

Используйте данную команду, чтобы удалить все привязки DHCPv6 Snooping на всех интерфейсах или указанном интерфейсе.

Формат: `clear ipv6 dhcp snooping binding [interface` *`unit/slot/port`*`]`

Режим ввода команд: привилегированный

пользовательский

clear ipv6 dhcp snooping statistics

Команда удаляет всю статистику DHCPv6 Snooping.

Формат: `clear ipv6 dhcp snooping statistics`

Режим ввода команд: привилегированный

пользовательский

show ipv6 verify

Используйте эту команду для отображения IPv6-конфигурации Source Guard для заданного интерфейса unit/slot/port.

Формат: `show ipv6 verify` *`interface`*

Режим ввода команд: привилегированный

пользовательский

Термин	***Значение***
Interface	IP-адрес интерфейса в формате unit/slot/port.
Filter Type	Может принимать одно из значений. • ip-v6mac: пользователь настроил фильтрацию по MAC-адресу на данном интерфейсе; • ipv6: на этом интерфейсе для фильтрации используется только IPv6-адрес.

show ipv6 verify source

Используйте данную команду, чтобы отобразить настройки IPv6SG на всех портах. Если указана опция interface, вывод ограничивается настройками указанного unit/slot/port.

Формат: `show ipv6 verify source {`*`interface`*`}`

Режим ввода команд: привилегированный

пользовательский

Термин	***Значение***
Interface	IP-адрес интерфейса в формате *unit/slot/port*.
Filter Type	Может принимать одно из значений. • ip-v6mac: пользователь настроил фильтрацию по MAC-адресу на данном интерфейсе. • ipv6: на этом интерфейсе для фильтрации используется только IPv6-адрес.
IPv6 Address	IPv6-адрес интерфейса.
MAC Address	Если на интерфейсе не настроена фильтрация по MAC-адресу, это поле остается пустым. Если на интерфейсе выключена защита портов, поле MAC Address отображает «permit-all».
VLAN	VLAN для правил привязки.

show ipv6 source binding

Используйте эту команду, чтобы отобразить привязки IPv6SG.

Формат: `show ipv6 source binding [{dhcp-snooping|static}] [interface` *`unit/slot/port`*`] [vlan id]`

Режим ввода команд: привилегированный

пользовательский

Термин	***Значение***
MAC Address	MAC-адрес добавляемой записи.
IP Address	IP-адрес добавляемой записи.
Type	Тип записи: статично настроенный в CLI или динамически изученный с помощью DHCP Snooping
VLAN	VLAN записи.
Interface	IP-адрес интерфейса в формате *unit/slot/port*.

15 КОМАНДЫ НАСТРОЙКИ QUALITY OF SERVICE

В этом разделе описываются команды управления технологией Quality of Service, доступные в CLI.

Команды в этом разделе делятся на две функциональные группы.

- **Команды просмотра оперативного состояния устройства, которые отображают настройки коммутатора, статистику и другую информацию.**
- **Команды настройки, которые задают характеристики и настройки коммутатора. Для каждой команды конфигурации существует команда просмотра оперативного состояния устройства, отображающая текущие параметры конфигурации.**

15.1 Команды управления Class of Service

В этой части приведены команды, которые используются для просмотра и настройки параметров Class of Service (CoS) на коммутаторе. Эти команды позволяют управлять приоритетами и скоростью передачи трафика.

- **Команды, вводимые в режиме конфигурирования интерфейса, выполняются для одного интерфейса.**
- **Команды, вводимые в режиме глобальной конфигурации выполняются для всех интерфейсов.**

classofservice dot1p-mapping

Эта команда связывает приоритеты 802.1p с внутренними классами трафика. Значения userpriority указываются в диапазоне от 0 до 7. Значения trafficclass могут быть в диапазоне от 0 до 6.

Формат: `classofservice dot1p-mapping userpriority trafficclass`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no classofservice dot1p-mapping

Эта команда связывает приоритеты 802.1p с внутренними классами трафика по умолчанию.

Формат: `no classofservice dot1p-mapping`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

classofservice ip-dscp-mapping

Данная команда связывает значения IP DSCP с внутренними классами трафика. Значение ipdscp можно задать как целыми числами от 0 до 63, так и описательно, с использованием следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Значения trafficclass могут быть в диапазоне от 0 до 6.

Формат: `classofservice ip-dscp-mapping ipdscp trafficclass`

Режим ввода команд: глобальная конфигурация

no classofservice ip-dscp-mapping

Команда связывает каждое значение IP DSCP с соответствующим внутренним классом трафика по умолчанию.

Формат: `no classofservice ip-dscp-mapping`

Режим ввода команд: глобальная конфигурация

classofservice trust

Эта команда устанавливает режим CoS-надежности для интерфейса или диапазона интерфейсов. Режим можно настроить на принятие в качестве надежных пакетов с одним из следующих маркеров: dot1p (802.1p) или IP DSCP. Кроме того, режим интерфейса можно установить как ненадежный. Если настроить интерфейс на принятие dot1p, режим не будет отображаться в выводе команды show running-config, поскольку dot1p является значением по умолчанию.

Значение по умолчанию: dot1p

Формат: `classofservice trust {dot1p | ip-dscp | untrusted}`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no classofservice trust

Эта команда устанавливает режим интерфейса в значение по умолчанию.

Формат: `no classofservice trust`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

cos-queue max-bandwidth

Эта команда определяет гарантированную максимальную пропускную способность передачи для каждой очереди на интерфейсе, диапазоне интерфейсов или на всех интерфейсах. Для каждой поддерживаемой очереди требуется указать значение в диапазоне 0–100 (процент от скорости соединения), причем 0 указывает на отсутствие максимальной пропускной способности. Сумма всех введенных значений не должна превышать 100.

Формат: `cos-queue max-bandwidth bw-0 bw-1 … bw-n`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no cos-queue max-bandwidth

Эта команда восстанавливает значения по умолчанию для максимальной пропускной способности каждой очереди.

Формат: `no cos-queue max-bandwidth`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

cos-queue min-bandwidth

Эта команда определяет гарантированную минимальную пропускную способность передачи для каждой очереди на интерфейсе, диапазоне интерфейсов или на всех интерфейсах. Для каждой поддерживаемой очереди требуется указать значение в диапазоне 0–100 (процент от скорости соединения), причем 0 указывает на отсутствие гарантированной минимальной пропускной способности. Сумма всех введенных значений не должна превышать 100.

Формат: `cos-queue min-bandwidth bw-0 bw-1 … bw-n`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no cos-queue min-bandwidth

Эта команда восстанавливает значения по умолчанию для минимальной пропускной способности каждой очереди.

Формат: `no cos-queue min-bandwidth`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

cos-queue random-detect

Данная команда активирует функцию Weighted Random Early Discard (WRED) для каждой указанной очереди на интерфейсе. Параметры WRED настраиваются с помощью команд random-detect queue-parms и random-detect exponential-weighting-constant.

При выполнении в режиме конфигурирования интерфейса команда действует только на один интерфейс, а в режиме глобальной конфигурации применяется для всех интерфейсов.

В этой команде требуется указать по крайней мере одно, но не более n значений идентификаторов очередей. Повторяющиеся значения идентификаторов очереди игнорируются. Значение идентификатора очереди может быть в диапазоне от 0 до (n - 1), где n означает общее количество очередей, поддерживаемых на интерфейсе. Значение n = 7 и соответствует количеству поддерживаемых очередей (классов трафика).

Формат: `cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no cos-queue random-detect

Используйте эту команду, чтобы выключить WRED и восстановить таким образом операцию отброса последнего элемента для указанных очередей на интерфейсе.

Формат: `no cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

cos-queue strict

Эта команда активирует режим планировщика со строгим приоритетом для каждой указанной очереди на интерфейсе, диапазоне интерфейсов или всех интерфейсах.

Формат: `cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no cos-queue strict

Эта команда восстанавливает режим взвешенного планировщика по умолчанию для каждой указанной очереди.

Формат: `no cos-queue strict queue-id-1 [queue-id-2 … queue-id-n]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

random-detect

Данная команда может включить функцию WRED для всего интерфейса и доступна только тогда, когда активация WRED для конкретных очередей не поддерживается устройством. Параметры WRED настраиваются с помощью команд random-detect queue-parms и random-detect exponential-weighting-constant.

При выполнении в режиме конфигурирования интерфейса команда действует только на один интерфейс, а в режиме глобальной конфигурации применяется для всех интерфейсов.

Формат: `random-detect`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no random-detect

Используйте эту команду, чтобы выключить WRED и восстановить таким образом операцию отброса последнего элемента для всех очередей на интерфейсе.

Формат: `no random-detect`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

random-detect exponential weighting-constant

Эта команда используется для настройки степени затухания WRED для интерфейса CoS-очереди.

Формат: `random-detect exponential-weighting-constant 0-15`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no random-detect exponential-weighting-constant

Используйте эту команду, чтобы установить степень затухания WRED в значение по умолчанию.

Формат: `no random-detect exponential-weighting-constant`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

random-detect queue-parms

Данная команда используется для настройки параметров WRED для каждого уровня приоритета отбрасывания, поддерживаемого очередью. Команда используется только тогда, когда включена настройка параметров для каждой COS-очереди (с помощью команды cos-queue random-detect).

Формат: `random-detect queue-parms queue-id-1 [queue-id-2 … queue-id-n] min-thresh thresh- prec-1 … thresh-prec-n max-thresh thresh-prec-1 … thresh-prec-n drop-probability prob-prec-1 … prob-prec-n`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

Каждый параметр указывается для каждого возможного значения приоритета отбрасывания (цвета TCP-трафика). Последнее значение приоритета применяется ко всему трафику, не относящемуся к TCP. Например, при трехцветной системе указывается четыре значения для каждого параметра: для зеленого TCP-трафика, желтого TCP-трафика, красного TCP-трафика и трафика, не относящегося к TCP.

Термин	***Значение***
min-thresh	Минимальный порог глубины очереди (в процентах), при котором WRED начинает маркировку и отброс трафика.
max-thresh	Максимальный порог глубины очереди (в процентах), при превышении которого WRED маркирует/отбрасывает весь трафик.
drop-probability	Вероятность (в процентах) того, что WRED маркирует/отбросит пакет, если глубина очереди приближается к максимальному порогу. (Вероятность отброса возрастает линейно от 0 при уровне, близком к минимальному порогу, до указанного значения при максимальном пороге глубины очереди, а затем доходит до 100% при его превышении).

no random-detect queue-parms

Используйте эту команду, чтобы установить конфигурацию WRED в значение по умолчанию.

Формат: `no random-detect queue-parms queue-id-1 [queue-id-2 … queue-id-n]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

traffic-shape

Эта команда определяет максимальную пропускную способность передачи для интерфейса в целом. Значение пропускной способности может быть от 0 до 100 с шагом 1. Это значение можно указать для диапазона интерфейсов или для всех интерфейсов. Эту операцию также называют ограничением скорости исходящего трафика, она помогает распределить временные всплески трафика по времени, ограничивая объем передаваемого трафика.

Формат: `traffic-shape bw`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no traffic-shape

Данная команда возвращает уровень ограничения скорости в значение по умолчанию.

Формат: `no traffic-shape`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

show classofservice dot1p-mapping

Используйте эту команду для отображения текущей привязки приоритетов dot1p (802.1p) к внутренним классам трафика на указанном интерфейсе. Если указан параметр unit/slot/port, отображается таблица привязки 802.1p данного интерфейса. Если этот параметр опущен, отображаются последние настройки глобальной конфигурации.

Формат: `show classofservice dot1p-mapping [unit/slot/port]`

Режим ввода команд: привилегированный

Термин	*Значение*
User Priority	Значение 802.1p-приоритета пользователя.
Traffic Class	Идентификатор очереди внутреннего класса трафика, к которой привязано значение приоритета пользователя.

show classofservice ip-dscp-mapping

Эта команда отображает текущую привязку IP DSCP к внутренним классам трафика для глобальной конфигурации.

Формат: `show classofservice ip-dscp-mapping`

Режим ввода команд: привилегированный

Следующая информация повторяется для каждого приоритета пользователя.

Термин	*Значение*
IP DSCP	Значение IP DSCP.
Traffic Class	Идентификатор очереди внутреннего класса трафика, к которой привязано значение IP DSCP.

show classofservice trust

Эта команда отображает текущую настройку режима надежности для указанного интерфейса. Если указан интерфейс unit/slot/port, команда отображает режим надежности для этого интерфейса. Если интерфейс не указан, команда отображает последние настройки глобальной конфигурации.

Формат: `show classofservice trust [unit/slot/port]`

Режим ввода команд: привилегированный

Термин	*Значение*

Class of Service Trust Mode	Режим надежности, возможные значения: dot1p, IP DSCP или Untrusted.
Non-IP Traffic Class	Только в режиме IP DSCP. Класс для трафика, не относящегося к TCP.
Untrusted Traffic Class	Только в режиме Untrusted. Класс для всего ненадежного трафика.

show interfaces cos-queue

Данная команда отображает конфигурацию CoS-очереди для указанного интерфейса. Если указан параметр unit/slot/port, отображается конфигурация CoS-очереди для указанного интерфейса. Если этот параметр опущен, отображаются последние настройки глобальной конфигурации.

Формат: `show interfaces cos-queue [unit/slot/port]`

Режим ввода команд: привилегированный

Термин	*Значение*
Interface Shaping Rate	Глобальный уровень ограничения скорости на интерфейсе.
WRED Decay Exponent	Глобальное значение степени затухания WRED.
Queue Id	Интерфейс поддерживает 7 очередей, пронумерованных от 0 до 6
Minimum Bandwidth	Гарантированная минимальная пропускная способность для очереди, выраженная в процентах. Значение 0 означает, что пропускная способность не гарантируется и очередь работает по принципу максимально возможных значений.
Maximum Bandwidth	Гарантированная максимальная пропускная способность для очереди, выраженная в процентах. Значение 0 означает, что пропускная способность не гарантируется и очередь работает по принципу максимально возможных значений.
Scheduler Type	Указывает, запланирована эта очередь для передачи со строгим приоритетом или с использованием взвешенной схемы.
Queue Management Type	Используемая техника управления глубиной очереди (отброс последнего элемента).

Если указан интерфейс, команда дополнительно отображает следующую информацию.

Термин	*Значение*
Interface	unit/slot/port указанного интерфейса. При выводе в режиме глобальной конфигурации эта строка заменяется информированием глобальной конфигурации.
Interface Shaping Rate	Максимальная пропускная способность передачи для интерфейса в целом. Этот параметр не зависит от максимальных значений пропускной способности отдельных очередей на интерфейсе.
WRED Decay Exponent	Настроенная степень затухания WRED для интерфейса CoS-очереди.

show interfaces random-detect

Эта команда отображает глобальные настройки WRED для каждой CoS-очереди. При указании unit/slot/port команда отображает настройки WRED для каждой CoS-очереди на указанном интерфейсе.

Формат: `show interfaces random-detect [unit/slot/port]`

Режим ввода команд: привилегированный

Термин	*Значение*

Queue ID	Интерфейс поддерживает 7 очередей, пронумерованных от 0 до 6
WRED Minimum Threshold	Настроенный минимальный порог глубины очереди (в процентах), при котором WRED начинает маркировку и отброс трафика.
WRED Maximum Threshold	Настроенный максимальный порог глубины очереди (в процентах), при превышении которого WRED выполняет маркировку и отброс всего трафика.
WRED Drop Probability	Настроенная вероятность (в процентах) того, что WRED маркирует/отбросит пакет, если глубина очереди приближается к максимальному порогу. (Вероятность отброса возрастает линейно от 0 при уровне, близком к минимальному порогу, до указанного значения при максимальном пороге глубины очереди, а затем доходит до 100% при его превышении).

show interfaces tail-drop-threshold

Эта команда отображает информацию о пороге отброса последнего элемента. При указании unit/slot/port команда отображает информацию о пороге отброса последнего элемента на указанном интерфейсе.

Формат: `show interfaces tail-drop-threshold [unit/slot/port]`

Режим ввода команд: привилегированный

15.2 Команды настройки Differentiated Services

В этой части описываются команды, которые вы используете для настройки QOS Differentiated Services (DiffServ). Настройка DiffServ осуществляется в несколько этапов путем указания трех компонентов DiffServ.

1 Класс

a. Создание и удаление классов.

b. Определение критериев соответствия для класса.

2 Политика

a. Создание и удаление политик.

b. Соотнесение классов с политикой.

c. Формирование записей политик для сочетаний классов и политик.

3 Сервис

a. Добавление политики к входящему интерфейсу или ее удаление.

Класс DiffServ определяет критерии фильтрации пакетов. Атрибуты политики DiffServ определяют способ отработки пакетов на коммутаторе. Атрибуты политики можно задать для каждого экземпляра класса. Коммутатор применяет эти атрибуты, когда происходит совпадение.

Обработка пакетов начинается в тот момент, когда коммутатор проверяет критерии соответствия для пакета. Коммутатор применяет к пакету политику, когда он находит совпадение класса в рамках этой политики.

При создании класса DiffServ применяются следующие правила.

- Каждый класс может содержать не более одного ссылочного (вложенного) класса.
- Определения классов не поддерживают иерархические политики сервисов.

Определение класса может содержать не более одной ссылки на другой класс. Можно комбинировать ссылки с другими критериями соответствия. При ссылке указывается действительный ссылочный класс, а не его копия, поскольку дополнения к ссылочному классу будут влиять на все классы, которые ссылаются на него. Изменения в любом определении класса, на который в данный момент ссылается некий другой класс, должны приводить к действительному определению для всех производных классов, в противном случае коммутатор отклонит изменения. Ссылку на класс можно удалить из определения класса.

Существует лишь один способ удалить индивидуальный критерий соответствия из существующего определения класса: удалить этот класс и создать его заново.

Возможности маркировки для применения политик включают CoS, IP DSCP и IP Precedence. В то время как две последние имеют смысл только для типов IP-пакетов, маркировка с использованием CoS применима как для IP-пакетов, так и для прочих, поскольку в этом случае происходит обновление поля 802.1p-приоритета пользователя в теге VLAN, используемом в заголовке пакетов layer 2.

diffserv

Эта команда устанавливает оперативный режим DiffServ в активное состояние. Если режим DiffServ выключен, его конфигурация сохраняется и доступна для редактирования, но не активирована. Если режим включен, сервисы DiffServ активируются.

Формат: `diffserv`

Режим ввода команд: глобальная конфигурация

no diffserv

Данная команда устанавливает оперативный режим DiffServ в неактивное состояние. Если режим DiffServ выключен, его конфигурация сохраняется и доступна для редактирования, но не активирована. Если режим включен, сервисы DiffServ активируются.

Формат: `no diffserv`

Режим ввода команд: глобальная конфигурация

15.3 Команды настройки класса DiffServ

Используйте команды настройки класса DiffServ, чтобы задать настройки классификации трафика. Для классификации трафика необходимо указать параметр Behavior Aggregate (BA) на основе классов трафика DSCP и Multi-Field (MF) (указывается имя и критерии соответствия).

Данная группа команд состоит из команд создания/удаления класса и команд сопоставления классов, определяющих общие критерии соответствия для Layer 3 и Layer 2, а также общие критерии соответствия. Критерии соответствия класса также известны как правила класса, где определение класса состоит из одного или нескольких правил, идентифицирующих принадлежащий к данному классу трафик.

После создания критерия соответствия для класса изменить или удалить этот критерий нельзя. Чтобы изменить или удалить критерий соответствия класса, необходимо удалить и заново создать весь класс.

Корень этой группы команд в CLI — `class-map`.

class-map

Эта команда определяет класс DiffServ для общего соответствия. При использовании команды без каких-либо условий соответствия команда выполняет вход в режим class-map. class-map-name представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует существующий класс DiffServ.

Значение default для class-map-name является зарезервированным и не должно использоваться.

Тип класса match-all указывает, что для пакетов, причисляемых к классу, должны выполняться все индивидуальные условия соответствия. Эта команда может использоваться без указания типа класса для входа в режим конфигурирования Class-Map для существующего класса DiffServ.

Необязательные ключевые слова [{ipv4 | IPv6}] определяют протокол Layer 3 для данного класса. Значение по умолчанию (если иное не указано) — IPv4.

Если эта команда успешно выполняется, в зависимости от указанного ключевого слова [{IPv4 | IPv6}] CLI переходит в режим конфигурирования Class-Map или IPV6-Class-Map.

Формат: `class-map match-all class-map-name [{ipv4 | IPv6}]{}`

Режим ввода команд: глобальная конфигурация

no class-map

Эта команда удаляет существующий класс DiffServ. class-map-name является именем существующего класса DiffServ. (Имя класса default зарезервировано и здесь не применимо.) Эта команда может быть выполнена в любое время; но если на данный класс ссылается хотя бы одна политика или другой класс, удаление заканчивается ошибкой.

Формат: `no class-map class-map-name`

Режим ввода команд: глобальная конфигурация

class-map rename

Данная команда изменяет имя класса DiffServ. class-map-name является именем существующего класса DiffServ. Параметр new-class-map-name представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует класс.

Значение по умолчанию: отсутствует

Формат: `class-map rename class-map-name new-class-map-name`

Режим ввода команд: глобальная конфигурация

match ethertype

Эта команда добавляет к определению указанного класса условие соответствия, основанное на значении Ethertype. Значение ethertype определяется как одно из следующих ключевых слов: appletalk, arp, ibmsna, ipv4, IPv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp или как пользовательское значение Ethertype в диапазоне 0x0600–0xFFFF. Используйте опцию [not] для указания отрицательного условия соответствия.

Формат: `match [not] ethertype {keyword | custom 0x0600-0xFFFF}`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match access-group

Эта команда настраивает для указанного класса условие соответствия на основе настроенного номера списка доступа IPv4. Значение `acl-number` – допустимый стандартный или расширенный ACL в диапазоне от 1 до 199.

Формат: `match access-group` *`acl-number`*

Режим ввода команд: Конфигурирование Class-Map

match access-group name

Эта команда настраивает для указанного класса условие соответствия на основе имени настроенного списка доступа. acl-name может принимать значения в диапазоне от 1 до 199.

При использовании этой команды важно учитывать:

- Class-map содержащие список доступа в качестве критерия соответствия, могут применяться только к входным политикам.
- Предложения действия (mirror, redirect, time-range и т.д.) в списках доступа, на которые ссылается политика, игнорируются в целях применения политики. Списки доступа используются только для сопоставления трафика.
- Данная команда не имеет no-формы.
- С помощью этой команды можно настроить списки ACL IPv4, IPv6 и MAC в качестве критериев соответствия.

Формат: `match access-group name` *`acl-name`*

Режим ввода команд: Конфигурирование Class-Map

match any

Эта команда добавляет к определению указанного класса условие соответствия, согласно которому принадлежащими к классу считаются все пакеты. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] any`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match class-map

Эта команда добавляет к определению указанного класса набор условий соответствия, определенных для другого класса. Параметр refclassname — это имя существующего класса DiffServ, условия которого должны быть добавлены к определению указанного класса.

Значение по умолчанию: отсутствует

Формат: `match class-map refclassname`

Режим ввода команд: конфигурирование Class-Map

конфигурирование IPv6-Class-Map

- **Параметры refclassname и class-map-name не могут быть одинаковыми.**
- **Класс может ссылаться только на один другой класс.**
- **Любые попытки удалить класс refclassname, пока на него ссылается класс class-map-name, будут заканчиваться ошибками.**
- **Объединенные критерии соответствия для class-map-name и refclassname должны представлять собой разрешенную комбинацию на основе типа класса.**
- **Любые последующие изменения в критерии соответствия класса refclassname должны оставаться в рамках этой разрешенной комбинации, иначе попытка изменения будет отклонена.**
- **Общее количество правил класса, образованных полной цепочкой ссылочного класса, не должно превышать максимальное значение для конкретной платформы. В некоторых случаях, каждое правило, удаленное из ссылочного класса, уменьшает максимальное число доступных правил для определения класса на единицу.**

no match class-map

Эта команда удаляет из определения указанного класса набор условий соответствия другого класса. Параметр refclassname — это имя существующего класса DiffServ, условия которого должны быть добавлены к определению указанного класса.

Формат: `no match class-map refclassname`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match cos

Эта команда добавляет к определению указанного класса условие соответствия для значения Class of Service (это единственный тег в пакете или первый/внешний 802.1Q-тег в пакете Double VLAN). Значение может быть от 0 до 7. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] cos 0-7`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match secondary-cos

Эта команда добавляет к определению указанного класса условие соответствия для вторичного значения Class of Service (это внутренний 802.1Q-тег в пакете Double VLAN). Значение может быть от 0 до 7. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not]secondary-cos 0-7`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match destination-address mac

Эта команда добавляет к определению указанного класса условие соответствия, основанное на значении целевого MAC-адреса пакета. Параметр macaddr является любым MAC-адресом layer 2 в формате шести двузначных шестнадцатеричных чисел, разделенных двоеточиями (например, 00:11:22:dd:ee:ff). Параметр macmask представляет собой маску несмежных битов MAC-адреса layer 2, в формате шести двузначных шестнадцатеричных чисел, разделенных двоеточиями

(например, ff:07:23:ff:fe:dc). Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] destination-address mac macaddr macmask`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match dstip

Эта команда добавляет к определению указанного класса условие соответствия, основанное на значении целевого IP-адреса пакета. Параметр ipaddr определяет IP-адрес. Параметр ipmask определяет маску битов IP-адреса и должен состоять из набора смежных ведущих единичных битов. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] dstip ipaddr ipmask`

Режим ввода команд: конфигурирование Class-Map

match dstip6

Эта команда добавляет к определению указанного класса условие соответствия, основанное на значении целевого IPv6-адреса пакета. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] dstip6 destination-IPv6-prefix/prefix-length`

Режим ввода команд: конфигурирование IPv6-Class-Map

match dstl4port

Эта команда добавляет к определению указанного класса условие соответствия, которое основано на порте назначения layer 4; при этом используется одно ключевое слово или числовое обозначение. Чтобы задать условие соответствия как одно ключевое слово, значение portkey должно быть одним из поддерживаемых ключевых слов для имени порта. В настоящее время поддерживаются следующие значения portkey: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Каждое из них переводится в эквивалентный номер порта. Чтобы задать условие соответствия с использованием числового обозначения, требуется один номер порта layer 4. Номер порта представляет собой целое число от 0 до 65535. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] dstl4port {portkey | 0-65535}`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match ip dscp

Данная команда добавляет к определению указанного класса условие соответствия на основе значения поля IP DiffServ Code Point (DSCP) в пакете. Это значение определяется как высокоуровневые шесть битов октета Service Type в IP-заголовке (два низкоуровневых бита не проверяются).

Значение dscpval определяется как целое число от 0 до 63 или символически как одно из следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0,

cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef. Используйте опцию [not] для указания отрицательного условия соответствия.

Условия соответствия IP DSCP, IP Precedence и ip tos являются альтернативными способами указания критерия соответствия для того же поля Service Type в IP-заголовке, но с несколько иным обозначением пользователя.

Значение по умолчанию: отсутствует

Формат: `match [not] ip dscp dscpval`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match ip precedence

Данная команда добавляет к определению указанного класса условие соответствия на основе значения поля IP Precedence в пакете. Это значение определяется как высокоуровневые три бита октета Service Type в IP-заголовке (пять низкоуровневых битов не проверяются). Значение precedence представляет собой целое число от 0 до 7. Используйте опцию [not] для указания отрицательного условия соответствия.

Условия соответствия IP DSCP, IP Precedence и IP ToS являются альтернативными способами указания критерия соответствия для того же поля Service Type в IP-заголовке, но с несколько иным обозначением пользователя.

Значение по умолчанию: отсутствует

Формат: `match [not] ip precedence 0-7`

Режим ввода команд: конфигурирование Class-Map

match ip tos

Эта команда добавляет к определению указанного класса условие соответствия на основе значения поля IP TOS в пакете. Это значение определяется как все восемь битов октета Service Type в IP-заголовке. Значение tosbits является двузначным шестнадцатеричным числом от 00 до ff. Значение tosmask является двузначным шестнадцатеричным числом от 00 до ff. tosmask обозначает позиции битов в tosbits, которые используются для сравнения с полем IP TOS в пакете. Например, для проверки IP-TOS значения, имеющего настроенные биты 7 и 5 и пустой бит 1, где бит 7 является наиболее важным, используйте значение tosbits a0 (шестн.) и tosmask a2 (шестн.). Используйте опцию [not] для указания отрицательного условия соответствия.

Условия соответствия IP DSCP, IP Precedence и IP ToS являются альтернативными способами указания критерия соответствия для того же поля Service Type в IP-заголовке, но с несколько иным обозначением пользователя.

Эта версия «свободной формы» для условий соответствия IP DSCP/Precedence/TOS дает пользователю полный контроль над тем, какие биты поля Service Type будут проверяться.

Значение по умолчанию: отсутствует

Формат: `match [not] ip tos tosbits tosmask`

Режим ввода команд: конфигурирование Class-Map

match ip6flowlbl

Используйте эту команду, чтобы ввести значение IPv6 Flow Label. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] ip6flowlbl label 0-1048575`

Режим ввода команд: конфигурирование IPv6-Class-Map

match protocol

Данная команда добавляет к определению указанного класса условие соответствия, которое основано на значении поля IP Protocol в пакете; при этом используется одно ключевое слово или числовое обозначение.

Чтобы задать условие соответствия как определение из одного ключевого слова, значение protocol-name должно быть одним из поддерживаемых ключевых слов для имени протокола. В настоящее время поддерживаются следующие значения: icmp, igmp, ip, tcp, udp. Значение ip подходит для любого значения номера протокола.

Чтобы задать условие соответствия с помощью числового обозначения, номер протокола рассматривается как стандартное значение, присвоенное IANA, и интерпретируется как целое число от 0 до 255. Используйте опцию [not] для указания отрицательного условия соответствия.

Эта команда не проверяет значение номера протокола по текущему списку IANA.

Значение по умолчанию: отсутствует

Формат: `match [not] protocol {protocol-name | 0-255}`

Режим ввода команд: конфигурирование Class-Map

конфигурирование IPv6-Class-Map

match source-address mac

Эта команда добавляет к определению указанного класса условие соответствия на основе MAC-адреса источника пакета. Параметр address является любым MAC-адресом layer 2 в формате шести двузначных шестнадцатеричных чисел, разделенных двоеточиями (например, 00:11:22:dd:ee:ff). Параметр macmask представляет собой маску несмежных битов MAC-адреса layer 2, в формате шести двузначных шестнадцатеричных чисел, разделенных двоеточиями (например, ff:07:23:ff:fe:dc). Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] source-address mac address macmask`

Режим ввода команд: конфигурирование Class-Map

конфигурирование IPv6-Class-Map

match srcip

Эта команда добавляет к определению указанного класса условие соответствия на основе IP-адреса источника пакета. Параметр ipaddr определяет IP-адрес. Параметр ipmask определяет маску битов IP-адреса и должен состоять из набора смежных ведущих единичных битов. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] srcip ipaddr ipmask`

Режим ввода команд: конфигурирование Class-Map

match srcip6

Эта команда добавляет к определению указанного класса условие соответствия на основе IPv6-адреса источника пакета. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] srcip6 source-IPv6-prefix/prefix-length`

Режим ввода команд: конфигурирование IPv6-Class-Map

match srcl4port

Эта команда добавляет к определению указанного класса условие соответствия, которое основано на порте источника layer 4; при этом используется одно ключевое слово или числовое обозначение. Чтобы задать условие соответствия как одно ключевое слово, значение portkey должно быть одним из поддерживаемых ключевых слов для имени порта (см. ниже). В настоящее время поддерживаются следующие значения portkey: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Каждое из них переводится в эквивалентный номер порта, который используется в качестве начала и конца диапазона портов.

Чтобы задать условие соответствия как числовое обозначение, требуется один номер порта layer 4. Номер порта представляет собой целое число от 0 до 65535. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] srcl4port {portkey | 0-65535}`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match vlan

Эта команда добавляет к определению указанного класса условие соответствия на основании значения поля идентификатора VLAN layer 2 (это единственный тег в пакете с одним тегом или первый/внешний тег в пакете Double VLAN). Идентификатор VLAN представляет собой целое число от 0 до 4093. Используйте опцию [not] для указания отрицательного условия соответствия.

Значение по умолчанию: отсутствует

Формат: `match [not] vlan 0-4093`

Режим ввода команд: конфигурирование Class-Map
конфигурирование IPv6-Class-Map

match secondary-vlan

Эта команда добавляет к определению указанного класса условие соответствия на основании значения поля идентификатора вторичной VLAN layer 2 (внутренний тег 802.1Q в пакете VLAN с двойным тегом). Идентификатор вторичной VLAN — это целое число от 0 до 4093. Используйте опцию [not] для указания отрицательного условия соответствия.

Эта команда недоступна на платформе 5630x.

Значение по умолчанию: отсутствует

Формат: `match [not] secondary-vlan 0-4093`

Режим ввода команд: конфигурирование Class-Map

конфигурирование IPv6-Class-Map

15.4 Команды настройки политики DiffServ

Используйте команды настройки политик DiffServ, чтобы определить действия по обработке трафика, такие как применение политик и маркировка для распределения по классам трафика

Команды настройки политик помогают связать класс трафика, который можно определить с помощью набора команд настройки класса с одним или несколькими атрибутами QoS-политики. Для интерфейса назначается связь класса и политики с целью формирования сервиса. При создании политики необходимо указать имя.

Каждый класс трафика определяет особый режим обработки для пакетов, которые соответствуют определению класса. С одной политикой можно связать несколько классов трафика. Когда пакет удовлетворяет условиям более чем одного класса, выбор основывается на том порядке, в котором классы добавлены к политике. Класс, добавленный первым, имеет наивысший приоритет.

Данная группа команд состоит из команд для создания/удаления политики, добавления/удаления класса, а также отдельных атрибутов политики.

Единственный способ удалить отдельный атрибут политики из экземпляра класса в рамках политики заключается в удалении экземпляра класса и повторном его добавлении к политике. Значения, связанные с атрибутом существующей политики, могут быть изменены без удаления экземпляра класса.

Корень этой группы команд в CLI — `policy-map`.

assign-queue

Эта команда настраивает идентификатор очереди, в которую назначается соответствующий поток трафика. Параметр queueid представляет собой целое число от 0 до 6.

Формат: `assign-queue queueid`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop

drop

Данная команда указывает, что все пакеты для соответствующего потока трафика должны быть отброшены на входе.

Формат: `drop`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Assign Queue, Mark (все формы), Mirror, Police, Redirect

mirror

Эта команда указывает, что все входящие пакеты для соответствующего потока трафика копируются на указанный выходной интерфейс (физический или LAG-интерфейс).

Формат: `mirror unit/slot/port`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Redirect

redirect

Эта команда указывает, что все входящие пакеты для соответствующего потока трафика направляются на указанный выходной интерфейс (физический или LAG-интерфейс).

Формат: `redirect unit/slot/port`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Mirror

conform-color

Используйте эту команду, чтобы включить политики трафика на основании цвета и указать привязку классов для соответствующих цветов. Используется в сочетании с командой политики, где указаны поля для соответствующего уровня. Параметр class-map-name является именем существующего класса привязки DiffServ.

Эту команду можно использовать только после указания команды политики для данного экземпляра класса политики.

Формат: `conform-color class-map-name`

Режим ввода команд: конфигурирование политик Class-Map

class

Эта команда создает экземпляр определения класса в рамках указанной политики с целью определения обработки класса трафика через последующие атрибуты политики. Параметр *classname* — это имя существующего класса DiffServ.

Эта команда приводит к тому, что указанная политика создает ссылку на определение класса.

Формат: `class classname`

Режим ввода команд: конфигурирование Policy-Map

no class

Данная команда удаляет экземпляр определенного класса и его заданную обработку из указанной политики.

Параметр *classname* — это имя существующего класса DiffServ.

Эта команда удаляет ссылку на определение класса для указанной политики.

Формат: `no class classname`

Режим ввода команд: конфигурирование Policy-Map

mark cos

Эта команда маркирует все пакеты для соответствующего потока трафика с указанным значением CoS в поле приоритета заголовка 802.1p (это единственный тег в пакете или первый/внешний 802.1Q-тег в пакете Double VLAN). Если пакет еще не содержит такой заголовок, он добавляется. Значение CoS представляет собой целое число от 0 до 7.

Значение по умолчанию: 1

Формат: `mark-cos 0-7`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Mark IP DSCP, IP Precedence, Police

mark secondary-cos

Данная команда маркирует внешние теги VLAN в пакетах для соответствующего потока трафика как вторичные значения CoS.

Значение по умолчанию: 1

Формат: `mark secondary-cos 0-7`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Mark IP DSCP, IP Precedence, Police

mark cos-as-sec-cos

Эта команда маркирует биты приоритета внешнего тега VLAN всех пакетов в качестве внутреннего приоритета VLAN-тегов. По сути это означает, что внутренние CoS-теги VLAN копируются во внешние CoS-теги VLAN.

Формат: `mark-cos-as-sec-cos`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Mark IP DSCP, IP Precedence, Police

mark ip-dscp

Эта команда маркирует все пакеты для связанного потока трафика с указанным значением IP DSCP.

Значение *dscpval* определяется как целое число от 0 до 63 или символически как одно из следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Формат: `mark ip-dscp dscpval`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

Эта команда маркирует все пакеты для связанного потока трафика с указанным значением IP Precedence. Значение IP Precedence представляет собой целое число от 0 до 7.

Эта команда не применима для классов IPv6. В IPv6 отсутствует поле приоритета.

Формат: `mark ip-precedence 0-7`

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Mark IP DSCP, IP Precedence, Police

Тип политики: In

police-simple

Данная команда используется для определения стиля политики трафика для указанного класса. Простая форма команды **police** настраивает только скорость передачи данных и размер пакета, в результате чего получается только два результата: трафик пропускается или отбрасывается при превышении установленных ограничений. Скорость передачи данных указана в килобитах в секунду (кбит/с) и представляет собой целое число от 1 до 4 294 967 295. Размер пакета указывается в килобайтах (КБ) и представляет собой целое число от 1 до 128.

Для каждого результата список возможных действий включает drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos- transmit, set-dscp-transmit, set-pref-transmit или transmit. В этой простой форме команды police действие по умолчанию при соответствии — transmit, а действие по умолчанию при нарушении — drop. Когда стиль настроен, эти действия можно настроить с помощью этой же команды.

Для действия set-dscp-transmit требуется значение *dscpval* (определяется как целое число от 0 до 63 или символически через одно из следующих ключевых слов: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef).

Для действия set-prec-transmit требуется значение IP Precedence (определяется как целое число от 0 до 7). Для действия set-cos-transmit требуется значение 802.1p priority (определяется как целое число от 0 до 7).

Формат:

```
police-simple {1-4294967295 1-128 conform-action {drop | set-
cos-as-sec-cos | set- cos-transmit 0-7 | set-sec-cos-transmit
0-7 | set-prec-transmit 0-7 | set-dscp- transmit 0-63 | trans-
mit} [violate-action {drop | set-cos-as-sec-cos | set-cos-
```

```
transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit
0-7 | set-dscp- transmit 0-63 | transmit}]}
```

Режим ввода команд: конфигурирование политик Class-Map

Несовместимые команды: Drop, Mark (все формы)

police-single-rate

Эта команда является подвидом команды **police** с указанием одной скорости и используется для установления стиля политики трафика для указанного класса. Для каждого результата список возможных действий включает drop, set-cos-as-sec-cost, set-cos- transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit и transmit. В данной форме команды police действие по умолчанию при соответствии — send, а действие по умолчанию при нарушении — drop. Когда стиль настроен, эти действия можно настроить с помощью этой же команды.

Формат:

```
police-single-rate {1-4294967295 1-128 1-128 conform-action
{drop | set-cos-as- sec-cos | set-cos-transmit 0-7 | set-sec-
cos-transmit 0-7 | set-prec-transmit 0- 7 | set-dscp-transmit
0-63 | transmit} exceed-action {drop | set-cos-as-sec-cos |
set-cos-transmit 0-7 | set-sec-cos-transmit 0-7 | set-prec-
transmit 0-7 | set- dscp-transmit 0-63 | transmit} [violate-
action {drop | set-cos-as-sec-cos-transmit| set-cos-transmit
0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-
dscp-transmit 0-63 | transmit}]}
```

Режим ввода команд: конфигурирование политик Class-Map

police-two-rate

Эта команда является подвидом команды **police** с указанием двух скоростей и используется для установления стиля политики трафика для указанного класса. Для каждого результата список возможных действий включает drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit и transmit. В данной форме команды police действие по умолчанию при соответствии — send, действие по умолчанию при превышении — drop, действие по умолчанию при нарушении — drop. Когда стиль настроен, эти действия можно настроить с помощью этой же команды.

Формат:

```
police-two-rate {1-4294967295 1-4294967295 1-128 1-128 con-
form-action {drop | set- cos-as-sec-cos | set-cos-transmit 0-
7 | set-sec-cos-transmit 0-7 | set-prec- transmit 0-7 | set-
dscp-transmit 0-63 | transmit} exceed-action {drop | set-cos-
as-sec-cos | set-cos-transmit 0-7 | set-sec-cos-transmit 0-7
| set-prec-transmit 0-7 | set-dscp-transmit 0-63 | transmit}
[violate-action {drop | set-cos-as-sec- cos | set-cos-transmit
0-7 | set-sec-cos-transmit 0-7 | set-prec-transmit 0-7 | set-
dscp-transmit 0-63 | transmit}]}
```

Режим ввода команд: конфигурирование политик Class-Map

policy-map

Эта команда создает новую политику DiffServ. Параметр *policyname* представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует политику. Тип политики связан с входящим направлением трафика, если указан параметр in, или с исходящим направлением трафика, если указан параметр *out*.

При успешном выполнении команды режим CLI изменяется на конфигурирование Policy-Map.

Формат: `policy-map` *`policyname`* `{in|out}`

Режим ввода команд: глобальная конфигурация

no policy-map

Эта команда удаляет существующую политику DiffServ. Параметр *policyname* — это имя существующей политики DiffServ. Данная команда может быть выполнена в любое время. Если на политику ссылаются один или несколько интерфейсов, попытка удаления завершается ошибкой.

Формат: `no policy-map` *`policyname`*

Режим ввода команд: глобальная конфигурация

policy-map rename

Эта команда изменяет имя политики DiffServ. Параметр *policyname* — это имя существующей политики DiffServ. Параметр *newpolicyname* представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует политику.

Формат: `policy-map rename` *`policyname newpolicyname`*

Режим ввода команд: глобальная конфигурация

15.5 Команды настройки сервисов DiffServ

Используйте команды настройки сервисов DiffServ, чтобы назначить политику обработки трафика при поступлении на интерфейс. Команды сервисов закрепляют определенные политики за направлениями интерфейса. За один раз можно назначить только одну политику для интерфейса.

Эта группа команд состоит из команд добавления/удаления сервисов. Корень этой группы команд в CLI — service-policy.

service-policy

Эта команда назначает политику для интерфейса во входящем направлении, если указан параметр *in*, или в исходящем направлении, если указан параметр *out*. Параметр *policyname* — это имя существующей политики DiffServ. Данная команда приводит к тому, что сервис создает ссылку на политику.

Эта команда дополнительно включает DiffServ на интерфейсе во входящем направлении. Для DiffServ не существует отдельной команды перехода в административный режим.

Данная команда не будет выполнена, если какие-либо атрибуты в определении политики превышают возможности интерфейса. После того как политика успешно назначена интерфейсу, любая попытка изменить определение политики, способная привести к превышению возможностей интерфейса, заканчивается ошибкой.

Формат: `service-policy {in|out}` *`policymapname`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no service-policy

Эта команда открепляет политику для интерфейса во входящем направлении, если указан параметр *in*, или в исходящем направлении, если указан параметр *out*. Параметр *policyname* — это имя существующей политики DiffServ.

Данная команда приводит к тому, что сервис удаляет ссылку на политику. Эта команда выключает DiffServ на интерфейсе во входящем или в исходящем направлении.

Для DiffServ не существует отдельной команды перехода в административный режим.

Формат: `no service-policy {in|out} policymapname`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

15.6 Команды просмотра оперативного состояния DiffServ

Используйте команды просмотра оперативного состояния DiffServ для отображения информации о конфигурации и состоянии классов, политик и сервисов. Вы можете отобразить состояние DiffServ в сводном или подробном формате. Информация о состоянии отображается только тогда, когда административный режим DiffServ включен.

show class-map

Данная команда отображает всю информацию о конфигурации для указанного класса. Параметр *class-name* — это имя существующего класса DiffServ.

Формат: `show class-map class-name`

Режим ввода команд: привилегированный
пользовательский

Если указано class-name, отображаются следующие поля:

Термин	*Значение*
Class Name	Название этого класса.
Class Type	Тип класса all означает, что все критерии соответствия, определенные для класса, оцениваются одновременно и должны соблюдаться.
Class Layer3 Protocol	Протокол Layer 3 для этого класса. Возможные значения: IPv4 и IPv6.
Match Criteria	Поля Match Criteria отображаются только в том случае, если они настроены. Они отображаются в том порядке, как вводились пользователем. Поля определяются в соответствии с типом класса. Возможные поля Match Criteria: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address и Source Layer 4 Port.
Values	Значения для Match Criteria.

Если параметр Class Name не указан, команда выводит список всех определенных классов DiffServ. Отображаются следующие поля:

Термин	*Значение*
Class Name	Название этого класса (Обратите внимание, что порядок, в котором отображаются классы, не обязательно отражает порядок, в котором они были созданы.)
Class Type	Тип класса all означает, что все критерии соответствия, определенные для класса, оцениваются одновременно и должны соблюдаться
Ref class name	Имя существующего класса DiffServ, на условия которого в настоящее время ссылается указанный класс

show diffserv

Эта команда отображает состояние DiffServ General Status Group, которое включает в себя текущую настройку административного режима, а также текущее и максимальное количество строк в каждой из основных таблиц частной базы управляющей информации DiffServ. Команда не принимает дополнительных опций.

Формат: `show diffserv`

Режим ввода команд: привилегированный

Термин	*Значение*
DiffServ Admin mode	Текущее значение административного режима DiffServ.
Class Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице Class Table.
Class Rule Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице Class Rule Table.
Policy Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице Policy Table.
Policy Instance Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице Policy Instance Table.
Policy Attribute Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице Policy Attribute Table.
Service Table Size Current/Max	Текущее и максимальное количество записей (строк) в таблице Service Table.

show policy-map

Данная команда отображает всю информацию о конфигурации для указанной политики. Параметр *policyname* — это имя существующей политики DiffServ.

Формат: `show policy-map` *`[policyname]`*

Режим ввода команд: привилегированный

Если указано Policy Name, отображаются следующие поля.

Термин	*Значение*
Policy Name	Название этой политики
Policy Type	Тип политики
Class Members	Класс, который является частью политики

Следующая информация повторяется для каждого класса, связанного с этой политикой (отображаются только те атрибуты алгоритма, которые на самом деле настроены).

Термин	*Значение*
Assign Queue	Направляет поток трафика к указанной очереди QoS. Это позволяет классификатору трафика указать, какая из поддерживаемых аппаратных очередей используется для обработки пакетов, принадлежащих к классу.
Class Name	Название этого класса.
Committed Burst Size (KB)	Размер пакета, используемый в простой политике.
Committed Rate (Kbps)	Скорость, используемая в простой политике.
Conform Action	Текущие настройки действия в отношении пакета, который признан соответствующим параметрам политики. Не отображается, если в рамках этой политики действия не выполняются.
Conform Color Mode	Текущая настройка цветового режима. Политики могут использовать режимы color blind или color aware. Режим color blind игнорирует цвет (маркировку) входящего пакета. Режим color aware учитывает текущую маркировку пакета при определении результатов применения политики.
Conform COS	Значение CoS-метки, если выполняется действие set-cos-transmit.
Conform DSCP Value	Значение DSCP-метки, если выполняется действие set-dscp-transmit.
Conform IP Precedence Value	Значение метки IP Precedence, если выполняется действие set-prec-transmit.
Drop	Отбрасывает пакет при получении. Это полезно для имитации списков контроля доступа с помощью DiffServ, особенно когда DiffServ и ACL не могут сосуществовать на одном интерфейсе.
Exceed Action	Действие в отношении трафика, который превышает параметры, заданные администратором сети.
Exceed Color Mode	Текущая настройка цвета избыточного трафика, которую пользователь может указать (необязательно).
Mark CoS	Значение CoS, заданное в 802.1p-заголовке входящих пакетов. Не отображается, если маркер cos не был указан.
Mark CoS as Secondary CoS	Значение вторичного приоритета 802.1p (второй/внутренний тег VLAN). Аналогично маркировке CoS (802.1p), но значение dot1p используется для повторного определения из значений dot1p во вторичном (т. е. внутреннем) теге пакета с двойными тегами.
Mark IP DSCP	Значение mark/re-mark, которое используется в качестве DSCP для трафика, соответствующего этому классу. Не отображается, если описание ip mark не задано.
Mark IP Precedence	Значение mark/re-mark, которое используется в качестве IP Precedence для трафика, соответствующего этому классу. Не отображается, если маркировка IP precedence не задана.
Mirror	Копирует определенный поток трафика на указанный выходной порт (физический или LAG-интерфейс). Может использоваться в дополнение к какой-либо маркировке или действиям политики. Может быть указано вместе с назначением очереди QoS. Это поле не отображается на платформах 5630x.
Non-Conform Action	Текущее значение действий в отношении пакета, который считается не соответствующим параметрам политики. Не отображается, если в рамках этой политики действия не выполняются.
Non-Conform COS	Значение CoS-метки, если при несоответствии выполняется действие set-cos-transmit.

Non-Conform DSCP Value	Значение DSCP-метки, если при несоответствии выполняется действие set-dscp-transmit.
Non-Conform IP Precedence Value	Значение метки IP Precedence, если при несоответствии выполняется действие set-prec-transmit.

Термин	*Значение*
Peak Rate	Гарантированная скорость передачи, также передает избыточный трафик до заданной пользователем пиковой скорости, понимая, что нисходящий сетевой элемент (например, политика ближайших узлов) может отбросить этот избыточный трафик. Трафик удерживается в очереди до тех пор, пока не будет передан или отброшен (в соответствии с настройками глубины очереди). Значение пиковой скорости может быть настроено для потока исходящей передачи для класса трафика AF (Assured Forwarding). Может использоваться и значение средней скорости.
Peak Burst Size (PBS)	Администратор сети может установить PBS в качестве средства, чтобы ограничить ущерб от ускоренной переадресации трафика. Весь избыточный трафик при этом отбрасывается.
Policing Style	Используемый стиль политики, если таковой имеется (простой).
Redirect	Принудительно направляет классифицированный поток трафика на указанный выходной порт (физический или LAG-интерфейс). Может использоваться в дополнение к какой-либо маркировке или действиям политики. Может быть указано вместе с назначением очереди QoS.

Если имя политики не указано, эта команда выводит список всех определенных политик DiffServ. Отображаются следующие поля:

Термин	*Значение*
Policy Name	Название этой политики (порядок, в котором отображаются политики, не обязательно отражает порядок, в котором они были созданы).
Policy Type	Тип политики (только входящие политики поддерживаются для этой платформы).
Class Members	Список всех имен классов, связанных с этой политикой.

show diffserv service

Данная команда отображает состояние политики сервиса для указанного интерфейса и направления. Параметр *unit/slot/ port* определяет допустимый интерфейс системы.

Формат: `show diffserv service` *`unit/slot/port`* `[in | out]`

Режим ввода команд: привилегированный

Термин	*Значение*
DiffServ Admin Mode	Текущая настройка административного режима DiffServ. Связанная политика действует на интерфейсе только тогда, когда DiffServ находится во включенном режиме.
Interface	Интерфейс в формате *unit/slot/port.*
Direction	Направление трафика на интерфейсе сервиса.
Operational Status	Текущий оперативный статус данного интерфейса сервиса DiffServ.
Policy Name	Название политики, прикрепленной к интерфейсу в указанном направлении.

Policy Details	Прикрепленные подробности политики, содержание которых идентично выводу команды show policy-map *policymapname* (содержание не повторяется здесь для краткости).

show diffserv service brief

Эта команда отображает все интерфейсы в системе, к которым была прикреплена политика DiffServ. Параметр входящего направления не является обязательным.

Формат: `show diffserv service brief [in | out]`

Режим ввода команд: привилегированный

Термин	*Значение*
DiffServ Mode	Текущая настройка административного режима DiffServ. Связанная политика активна на интерфейсе только тогда, когда DiffServ находится в включенном режиме.

Следующая информация повторяется для интерфейсов и направлений (отображаются только те интерфейсы, которые были настроены с прикрепленным алгоритмом).

Термин	*Значение*
Interface	Интерфейс в формате *unit/slot/port.*
Direction	Направление трафика на интерфейсе сервиса.
OperStatus	Текущий оперативный статус данного интерфейса сервиса DiffServ.
Policy Name	Название политики, прикрепленной к интерфейсу в указанном направлении.

show policy-map interface

Данная команда отображает статистику, связанную с политиками, для указанного интерфейса и направления. Параметр *unit/ slot/port* определяет допустимый интерфейс для системы. Вместо параметра *unit/slot/port* можно использовать *lag lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр *lag lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG.

Формат: `show policy-map interface` *unit/slot/port* `[in | out]`

Режим ввода команд: привилегированный

Термин	*Значение*
Interface	Интерфейс в формате *unit/slot/port.*
Direction	Направление трафика на интерфейсе сервиса.
OperStatus	Текущий оперативный статус данного интерфейса сервиса DiffServ.
Policy Name	Название политики, прикрепленной к интерфейсу в указанном направлении.

Следующая информация повторяется для каждого экземпляра класса в рамках этой политики.

Термин	*Значение*
Class Name	Имя этого экземпляра класса.
In Discarded Packets	Счетчик пакетов, по какой-либо причине отброшенных для данного экземпляра класса при DiffServ-обработке.

show service-policy

Эта команда отображает сводную статистику по политикам для всех интерфейсов в указанном направлении.

Формат: `show service-policy in`

Режим ввода команд: привилегированный

Следующая информация повторяется для каждого интерфейса и направления (отображаются только те интерфейсы, которые были настроены с прикрепленной политикой).

Термин	*Значение*
Interface	Интерфейс в формате *unit/slot/port.*
Operational Status	Текущий оперативный статус данного интерфейса сервиса DiffServ.
Policy Name	Название политики, прикрепленной к интерфейсу.

15.7 Команды настройки MAC ACL

Ниже описаны команды для настройки параметров списка контроля доступа (ACL) MAC. MAC ACL гарантируют, что только авторизованные пользователи получат доступ к определенным ресурсам, и блокируют любые попытки необоснованного доступа к сетевым ресурсам.

К MAC ACL применяются следующие правила.

- Максимальное количество ACL, которые можно создать, зависит от платформы. Ограничение применяется ко всем ACL, независимо от типа.
- Максимальное количество правил для всех MAC ACL зависит от платформы.
- Система поддерживает только кадры типа Ethernet II.

mac access-list extended

Эта команда создает MAC ACL с идентификацией по параметру *name*, состоящему из полей классификации, определенных для заголовка Layer 2 в кадрах Ethernet. Параметр *name* представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует MAC ACL. Если MAC ACL с указанным именем уже существует, эта команда входит в режим конфигурирования MAC Access-List, обновляя существующий MAC ACL.

При успешном выполнении команды режим CLI сменяется на конфигурирование MAC Access-List.

Формат: `mac access-list extended` *name*

Режим ввода команд: глобальная конфигурация

no mac access-list extended

Эта команда удаляет MAC ACL, идентифицированный по значению *name* в системе.

Формат: `no mac access-list extended` *name*

Режим ввода команд: глобальная конфигурация

mac access-list extended rename

Эта команда изменяет имя списка MAC ACL. Параметр *name* является именем существующего MAC ACL. Параметр *newname* представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует MAC ACL. Команда не будет выполнена, если MAC ACL с именем *newname* уже существует.

Формат: `mac access-list extended rename` *name newname*

Режим ввода команд: глобальная конфигурация

mac access-list resequence

Используйте эту команду, чтобы изменить порядковые номера записей для указанного MAC ACL с заданным значением шага, начиная с указанного порядкового номера. Команда используется для редактирования последовательности правил ACL и изменяет порядок, в котором применяются записи. Эта команда не сохраняется в конфигурации запуска и не отображается в текущей конфигурации.

Если созданный командой порядковый номер превышает максимальный порядковый номер, создание правила ACL не удаются, выводится информационное сообщение.

Значение по умолчанию: 10

Формат: `mac access-list resequence {name| id } starting-sequence-number increment`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
starting-sequence- number	Начальный порядковый номер. Диапазон — 1–2147483647. Значение по умолчанию: 10.
increment	Шаг увеличения. Диапазон — 1–2147483647. Значение по умолчанию: 10.

{deny | permit} (MAC ACL)

Данная команда создает новое правило для текущего MAC ACL. Правило может либо запретить, либо разрешить трафик в соответствии с указанными полями классификации. Как минимум требуется указать значение MAC-адреса отправителя и получателя, каждый из которых может быть замещен с помощью ключевого слова any для указания любого значения в этой области. Остальные параметры команды являются необязательными, но наиболее часто используемые параметры отображаются в том же относительном порядке, как показано в формате команды.

Формат: `[sequence-number] {deny|permit} {srcmac | any} {dstmac | any} [ethertypekey | 0x0600- 0xFFFF] [vlan {eq 0-4095}] [cos 0-7] [[log] [time-range time-range-name] [assign-queue queue-id]] [{mirror | redirect} unit/slot/port][rate-limit rate burst-size]`

Режим ввода команд: конфигурирование MAC Access-List

Явно выраженное MAC-правило deny all всегда останавливает действие ACL.

sequence-number определяет порядковый номер для правила ACL. Порядковый номер указывается пользователем или генерируется устройством.

Если порядковый номер для правила не указан, используется порядковый номер на 10 больше, чем последний порядковый номер в ACL, и правило помещается в конец списка. Если это первое правило в данном ACL, ему присваивается порядковый номер 10. Если расчетный порядковый номер превышает максимальное значение номера последовательности, создание правила ACL заканчивается ошибкой. Правило не может быть создано, если оно дублирует уже существующее.

Правило не может быть настроено с порядковым номером, который уже используется для другого правила.

Например, если пользователь добавляет новое правило ACL без указания порядкового номера, оно помещается в конец списка. Изменив порядковый номер, пользователь может перемещать правило ACL в другое местоположение.

Ethertype может быть определен как ключевое слово или четырехзначное шестнадцатеричное значение в диапазоне 0x0600–0xFFFF. В настоящее время поддерживаются следующие значения *ethertypekey*: appletalk, arp, ibmsna, ipv4, IPv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Каждое из них переводится в эквивалентное значение Ethertype.

Ключевое слово Ethertype	***Соответствующее значение***
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
IPv4	0x0800
IPv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

Параметры vlan и cos относятся к идентификатору VLAN и значению пользовательского приоритета 802.1p соответственно. Для пакетов, содержащих двойной тег VLAN, это первый (или внешний) тег.

Параметр time-range позволяет наложить ограничение времени на правило MAC ACL, как это определено параметром *time-range-name*. Если временной диапазон с указанным именем не существует и MAC ACL, содержащий это правило ACL, применяется к интерфейсу или к VLAN, правило ACL применяется немедленно. Если временной диапазон с указанным именем существует и MAC ACL, содержащий это правило ACL, применяется к интерфейсу или к VLAN, правило ACL применяется, если временной диапазон с указанным именем становится активным. Правило ACL не применяется, если временной диапазон с указанным именем становится неактивным.

Параметр assign-queue позволяет указать конкретную очередь для обработки трафика, который соответствует этому правилу. Допустимое значение *queue-id* — от 0 до 6. Параметр *assign-queue* действителен только для правил permit.

Параметр *mirror* позволяет трафику быть скопированным в *unit/slot/port*, а параметр redirect позволяет трафику быть переадресованным на указанный *unit/slot/port*. Параметры *assign-queue* и *redirect* действительны только для правил permit.

Необязательный атрибут *rate limit* команды *permit* позволяет разрешить только допустимую скорость передачи, настроенную в Кбит/с, и пиковый размер в килобайтах.

no sequence-number

Используйте эту команду для удаления правила ACL с указанным порядковым номером из ACL.

Формат: no *sequence-number*

Режим ввода команд: конфигурирование MAC Access-List

mac access-group

Эта команда либо закрепляет определенный MAC ACL, идентифицируемый по параметру *name,* к интерфейсу или набору интерфейсов, или связывает его с VLAN ID в заданном направлении. Параметр *name* должен быть именем существующего MAC ACL.

Необязательный порядковый номер может быть указан, чтобы указать порядок этого MAC ACL по отношению к другим MAC ACL, уже назначенным этому интерфейсу и направлению. Меньшее число указывает на более высокий приоритет. Если порядковый номер уже используется для этого интерфейса и направления, указанный MAC ACL заменяет используемый в настоящее время MAC ACL с этим номером. Если порядковый номер для этой команды не определен, будет использоваться порядковый номер, который на единицу больше, чем самый высокий порядковый номер для этого интерфейса и направления.

Эта команда, выполненная в режиме конфигурирования интерфейса, действует только на один интерфейс, в то время как в режиме глобальной конфигурации применяется для всех интерфейсов. Ключевое слово VLAN применяется только в режиме глобальной конфигурации.

Опция *control-plane* задается, чтобы применить MAC ACL на порту CPU. Пакеты управления, такие как BPDU, также отбрасываются из-за подразумеваемого присутствия правила deny all в конце списка. Для того, чтобы это изменить, требуется добавить разрешающие правила, которые позволят передавать пакеты управления.

Ключевое слово *control-plane* доступно только в режиме глобальной конфигурации.

Формат: `mac access-group` *`name`* `{{control-plane|in|out} vlan` *`vlan-id`* `{in|out}} [sequence` *`1– 4294967295`*`]`

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

Параметр	***Описание***
name	Имя списка управления доступом.
sequence	Необязательный порядковый номер, который указывает порядок этого MAC ACL по отношению к другим спискам MAC ACL, уже присвоенных этому интерфейсу и направлению. Диапазон составляет от 1 до 4294967295.
vlan-id	Идентификатор VLAN, связанный с определенным MAC ACL в заданном направлении.

no mac access-group

Эта команда удаляет MAC ACL, идентифицируемый по параметру *name*, из интерфейса в заданном направлении.

Формат: `no mac access-group` *`name`* `{{control-plane|in|out} vlan` *`vlan-id`* `{in|out}}`

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

remark

Эта команда добавляет новый комментарий к правилу ACL.

Используйте ключевое слово remark, чтобы добавить комментарий (примечание) к записям правил ACL, относящимся к IPv4, IPv6, MAC или ARP ACL. Общая длина замечания не может превышать 100 символов. Замечание может содержать символы в диапазоне A–Z, a–z, 0–9, а также специальные символы, такие как пробел, дефис, подчеркивание. Если правило ACL удаляется, удаляются и соответствующие примечания. Примечания отображаются только в команде *show running-config* и не отображаются в *show ip access-lists*.

Примечания могут быть добавлены только до создания правила. Если пользователь создает до 10 примечаний, каждое из них будет связано со следующим созданным правилом.

Значение по умолчанию: отсутствует

Формат: `remark` *`comment`*

Режим ввода команд: конфигурирование IPv4 Access-list
конфигурирование IPv6 Access-list
конфигурирование MAC Access-list
конфигурирование ARP Access-list

no remark

Используйте эту команду, чтобы удалить замечание из ACL.

Если первое вхождение замечания в ACL найдено, замечание удаляется. Повторное выполнение этой команды с тем же замечанием, удаляет замечание из следующего правила ACL, которое имеет замечание, связанное с ним (если нет правил, настроенных с тем же замечанием). Если правил с этим замечанием больше нет, выводится сообщение об ошибке

Если такого замечания, связанного с любым правилом, не существует, при этом есть несвязанное замечание, оно удаляется.

Значение по умолчанию: отсутствует

Формат: `no remark` *`comment`*

Режим ввода команд: конфигурирование IPv4 Access-list
конфигурирование IPv6 Access-list
конфигурирование MAC Access-list
конфигурирование ARP Access-list

show mac access-lists

Эта команда отображает сводную информацию для всех Mac ACL и счетчик совпадения для правил ACL, соответствующих настроенному правилу ACL внутри ACL. При достижении максимального значения счетчик начинает дальнейший отсчет с нуля. Существует специальный счетчик для каждого правила ACL. Счетчики ACL не взаимодействуют с PBR-счетчиками.

Для счетчиков ACL, если правило настроено без указания RATE-LIMIT, значение счетчика является количеством переадресованных/отброшенных пакетов попадающих под данное правило. Например, для всплеска в 100 пакетов значение счетчика равно 100.

Если правило ACL настроено с RATE LIMIT, значение счетчика указывает число пакетов попадающих под данное правило независимо от отграничения скорости для данной записи.

Счетчики ACL не взаимодействуют с политиками DiffServ.

Используйте имя списка доступа для отображения подробной информации об указанном MAC ACL.

Вывод команды может меняться в зависимости от критериев соответствия, настроенных в рамках правил в ACL.

Формат: `show mac access-lists [`*`name`*`]`
Режим ввода команд: привилегированный

Термин	*Значение*
Rule Number	Идентификатор (номер) правила, определенное в MAC ACL.
Action	Действие, связанное с каждым правилом. Возможные значения: Permit или Deny.
Source MAC Address	MAC-адрес источника для этого правила.
Source MAC Mask	Маска MAC-адреса источника для этого правила.
Committed Rate	Гарантированная скорость, определяется атрибутом ограничения скорости.
Committed Burst Size	Указанный размер пакета в соответствии с пиковым значением параметра.
Destination MAC Address	MAC-адрес назначения для этого правила.
EtherType	Ключевое слово EtherType или пользовательские значения для этого правила.
VLAN ID	Значение идентификатора VLAN или диапазон VLAN для этого правила.
COS	Значение COS (802.1p) для этого правила.
Log	Показывает, включено ли ведение журнала для правила.
Assign Queue	Идентификатор очереди, с которой связаны пакеты, соответствующие этому правилу.
Mirror Interface	Параметр unit/slot/port, на который копируются пакеты, соответствующие этому правилу.
Redirect Interface	Параметр unit/slot/port, на который пересылаются пакеты, соответствующие этому правилу.
Time Range Name	Отображает имя временного диапазона, если правило MAC ACL ссылается на таковой.
Rule Status	Статус правила MAC ACL (Active/Inactive).
ACL Hit Count	Счетчик выполнения правила ACL для пакетов, соответствующих настроенному правилу.

15.8 Команды настройки IP ACL

Ниже описаны команды для настройки параметров списка контроля доступа (ACL) IP. IP ACL гарантируют, что только авторизованные пользователи получат доступ к определенным ресурсам, и блокируют любые попытки необоснованного доступа к сетевым ресурсам.

К IP ACL применяются следующие правила:

- Коммутатор не поддерживает конфигурацию IP ACL для фрагментов IP-пакетов.
- Максимальное количество ACL, которые можно создать, зависит от платформы. Ограничение применяется ко всем ACL, независимо от типа.
- Максимальное количество правил в IP ACL зависит от платформы.

access-list

Эта команда создает список IP ACL, который идентифицируется номером списка доступа: 1–99 для стандартных списков контроля доступа или 100–199 для расширенных списков ACL.

Стандартный IP ACL.

Формат: access-list *1-99* {remark *comment*} | {[*sequence-number*]}] {deny | permit} {every | *srcip srcmask* | host *srcip*} [time-range *time-range-name*] [log] [assign-queue *queue- id*] [{mirror | redirect} *unit/slot/port*] [rate-limit *rate burst-size*]

Режим ввода команд: глобальная конфигурация

Расширенный IP ACL.

Формат: access-list *100-199* {remark *comment*} | {[*sequence-number*]} [rule *1-1023*] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp |*0-255*} {*srcip* srcmask|any|host *srcip*}[range {*portkey*|*startport*} {*portkey*|*endport*} {eq|neq|lt|gt} {portkey|0-65535}{dstip dstmask|any|host dstip}[{range {portkey|startport} {portkey|endport} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp- message] [igmp-type igmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst-size]

Режим ввода команд: глобальная конфигурация

Расширенный IPv4 ACL доступа имеет следующие ограничения для исходящих списков контроля доступа:

- **Совпадение по диапазону портов не поддерживается;**
- **команда ограничения скорости не поддерживается.**

Параметр	*Описание*
remark *comment*	Используйте ключевое слово remark, чтобы добавить комментарий (замечание) к стандартным или расширенным IP ACL. Примечания упрощают просмотр и понимание ACL. Длина замечания не может превышать 100 символов. Замечание может содержать символы в

	диапазоне A-Z, A-Z, 0-9, а также специальные символы: пробел, дефис, подчеркивание. Для стандартных и расширенных ACL можно добавлять по одному замечанию на правило. Удалять разрешается только замечания, не связанные с правилами. Связанные с правилами замечания удаляются только вместе с правилами.
sequence-number	Определяет порядковый номер правила ACL. Порядковый номер получает каждое правило. Порядковый номер задается пользователем или генерируется устройством. Если порядковый номер для правила не указан, используется порядковый номер на 10 больше, чем последний порядковый номер в ACL, и правило помещается в конец списка. Если это первое правило в данном ACL, ему присваивается порядковый номер 10. Если расчетный порядковый номер превышает максимальное значение номера последовательности, создание правила ACL заканчивается ошибкой. Не разрешается создавать правило, если оно дублирует уже существующее. Правило не может быть настроено с порядковым номером, который уже используется для другого правила. Например, если пользователь добавляет новое правило ACL без указания порядкового номера, оно помещается в нижнюю часть списка. Изменив порядковый номер, пользователь может перемещать правило ACL в другое положение.
1–99 или 100–199	В диапазоне 1–99 задаются номера для стандартных IP ACL. В диапазоне 100–199 задаются номера для расширенных IP ACL.
[rule *1-1023*]	Указывает правило IP ACL.
{deny | permit}	Указывает, выполняется или запрещается действие в результате применения правила IP ACL. ***Примечание***. В правилах запрета можно настроить параметры assign-queue, redirect и mirror attributes, но они не будут иметь действия.
every	Совпадает каждый пакет.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0-255*}	Указывает протокол, который должен соответствовать правилу расширенного IP ACL.
srcip srcmask*|any|host *scrip	Указывает IP-адрес источника и маску подсети для соответствия состояния правила IP ACL. Указание any подразумевает указания *srcip* как 0.0.0.0 и *srcmask* как 255.255.255.255. Указание host *A.B.C.D* подразумевает *srcip* как "A.B.C.D" и *srcmask* как "0.0.0.0".
{{range{portkey|startport}{portkey |endport}|{eq|neq|lt|gt} {*portkey* | *0-65535*}]	***Примечание.*** Эта опция доступна только с протоколами TCP или UDP. Определяет условия соответствия для порта источника layer 4 в правиле IP ACL. Вы можете использовать номер порта, который находится в пределах от 0–65535, или указать параметр *portkey*, который может быть одним из следующих ключевых слов. • Для TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3*. • Для UDP: *domain, echo, ntp, rip, snmp, tftp*, *time* и *who*. Для протоколов TCP и UDP каждое из этих ключевых слов транслируется в эквивалент номера порта, который используется в качестве начала и конца диапазона портов. Если указан *range,* правило IP ACL соответствует, только если номер порта layer 4 находится в пределах указанного диапазона. Параметры *startport* и *endport* определяют первый и последний порты, которые являются частью диапазона портов. Они имеют значение от 0 до 65535. Конечный порт должен иметь значение равное или больше, чем исходный порт. Исходный порт и все порты между ними будут частью диапазона портов layer 4. Когда *eq* задан, правило IP ACL соответствует, только если номер порта layer 4 равен указанному номеру или ключу порта.

	Когда *lt* задан, правило IP ACL соответствует, если номер порта layer 4 меньше указанного номера или ключа порта. Это эквивалентно заданию диапазона от 0 до <указанный номер порта - 1>. При указании *gt* правило IP ACL соответствует, если номер порта layer 4 больше, чем указанный номер или ключ порта. Это эквивалентно заданию диапазона <указанный номер порта + 1> до 65535. При указании *neq* правило IP ACL соответствует, только если номер порта layer 4 не равно номеру или ключу порта. Два правила добавляются с диапазоном от 0 до <указанного номера порта - 1> и одно с диапазоном << указанный номер порта _ + 1 до 65535>>. ***Примечание.*** Номер порта совпадения применяется только к нефрагментированным пакетам или первым фрагментам.
dstip dstmask*|any|host *dstip	Указывает IP-адрес назначения и маску подсети для соответствия состояния правила IP ACL. Указание any подразумевает указания *dstip* как 0.0.0.0 и *dstmask* как 255.255.255.255. Указание хоста A.B.C.D подразумевает *dstip* как A.B.C.D и *dstmask* как 0.0.0.0.
[precedence *precedence* | tos *tos* [*tosmask*] | dscp *dscp*]	Определяет TOS для правила IP ACL в зависимости от соотношения приоритета или DSCP-значений с использованием параметров *dscp, precedence*, *tos/tosmask*. ***Примечание.*** Параметр *tosmask* является необязательным.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	***Примечание.*** Эта опция доступна только в случае, если используется протокол TCP. Указывает, что правило IP ACL использует соответствие по TCP-флагам. Когда + <tcpflagname> указан, совпадение имеет место, если указанный флаг <tcpflagname> устанавливается в TCP-заголовке. Когда - <tcpflagname> указывается, совпадение имеет место, если указанный флаг <tcpflagname> не установлен в TCP-заголовке. Если указано ключевое слово established , совпадение происходит, если указанные RST- или ACK-биты установлены в TCP-заголовке. В системе устанавливаются два правила, если указан этот параметр.
[icmp-type *icmp-type* [icmp-code *icmp-code*] | icmp-message *icmp-message*]	***Примечание.*** Эта опция доступна только в случае, если используется протокол ICMP. Указывает условие соответствия для пакетов ICMP. При указании *icmp-type* правило IP ACL совпадает с указанным типом ICMP-сообщения, значением от 0 до 255. При указании *icmp-code* правило IP ACL совпадает с указанным кодом ICMP-сообщения, значением от 0 до 255. Указание *icmp-message* означает, что указаны параметры *icmp-type* и *icmp-code.* Поддерживаются следующие ICMP-сообщения: *echo*, *echo-reply*, *host-redirect*, *mobile-redirect*, *net-redirect*, *net- unreachable*, *redirect*, *packet-too-big*, *port-unreachable*, *source- quench*, *router-solicitation*, *router-advertisement*, *time-exceeded*, *ttl- exceeded* и *unreachable*.
igmp-type *igmp-type*	***Примечание.*** Эта опция доступна только в случае, если используется протокол IGMP. При указании *igmp-type* правило IP ACL проверяет совпадение с указанным типом ICMP-сообщения, значением от 0 до 255.
fragments	Указывает, что правило IP ACL совпадает с фрагментированными IP-пакетами.
[log]	Указывает, что это правило должно быть записано в журнал.
[time-range *time-range-name*]	Позволяет применять ограничение времени на правило ACL, как это определено параметром time-range-name. Если временного диапазона с указанным именем не существует и ACL, содержащий это правило, применяется к интерфейсу или к VLAN, правило ACL применяется немедленно. Если временной диапазон с указанным именем существует и ACL, содержащий это

	правило, применяется к интерфейсу или к VLAN, правило ACL применяется, если временной диапазон с указанным именем становится активным. Правило ACL становится неактивным, если временной диапазон с указанным именем становится неактивным.
[assign-queue *queue-id*]	Определяет связанную очередь, т. е. идентификатор очереди, к которой пакеты, соответствующие этому правилу, назначаются.
[{mirror | redirect} *unit/slot/ port*]	Указывается mirror- или redirect-интерфейс *unit/slot/port* к которому пакеты, соответствующие этому правилу, копируются или пересылаются соответственно.
[rate-limit *rate burst-size*]	Определяет допустимую скорость передачи в соответствии с заданной скоростью в Кбит/с и с пиковым размером буфера в килобайтах.

no access-list

Эта команда удаляет IP ACL, который определен с помощью параметра *accesslistnumber*. Диапазон *accesslistnumber*: 1–99 для стандартных списков доступа и 100–199 для расширенных списков доступа.

Формат: `no access-list` *`accesslistnumber`* `[rule` *`1-1023`*`]`

Режим ввода команд: глобальная конфигурация

ip access-list

Эта команда создает расширенный IP ACL, идентифицируемый параметром name и состоящий из полей классификации, определенных для IP-заголовка IPv4. Параметр name представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует IP ACL.

Если IP ACL с таким именем уже существует, эта команда входит в режим конфигурирования IPv4 Access-List, чтобы обновить существующий IP ACL.

При успешном выполнении команды режим CLI сменяется на конфигурирование IPv4 Access-List.

Формат: `ip access-list` *`name`*

Режим ввода команд: глобальная конфигурация

no ip access-list

Эта команда удаляет IP ACL, идентифицируемый по имени системы.

Формат: `no ip access-list` *`name`*

Режим ввода команд: глобальная конфигурация

ip access-list rename

Эта команда изменяет имя списка IP ACL. Параметр *name* является именем существующего IP ACL. Параметр new*name* представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует IP ACL.

Команда не будет выполнена, если IP ACL с именем *newname* уже существует.

Формат: `ip access-list rename name newname`

Режим ввода команд: глобальная конфигурация

ip access-list resequence

Используйте эту команду, чтобы изменить порядковые номера записей для указанного IP ACL с заданным значением шага, начиная с указанного порядкового номера. Команда используется для редактирования последовательности правил ACL и изменяет порядок, в котором применяются записи. Эта команда не сохраняется в конфигурации запуска и не отображается в текущей конфигурации.

Если созданный командой порядковый номер превышает максимальный порядковый номер, создание правила ACL не удается, выводится информационное сообщение.

Значение по умолчанию: 10

Формат: `ip access-list resequence {name| id } starting-sequence-number increment`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
starting-sequence- number	Начальный порядковый номер. Диапазон — 1–2147483647. Значение по умолчанию: 10.
increment	Шаг увеличения. Диапазон — 1–2147483647. Значение по умолчанию: 10.

{deny | permit} (IP ACL)

Данная команда создает новое правило для текущего IP ACL. Правило может либо запретить, либо разрешить трафик в соответствии с указанными полями классификации. Как минимум, ключевое слово every или протокол, адрес источника и значение адреса назначения должны быть указаны. Поля источника и назначения IP-адреса могут быть определены с помощью ключевого слова any, указанного для любого значения в этой области. Остальные параметры команды являются необязательными, но наиболее часто используемые параметры отображаются в том же относительном порядке, как показано в формате команды.

Формат: `[sequence-number] {deny | permit} {every | {{eigrp | gre | icmp | igmp | ip | ipinip| ospf | pim | tcp | udp | 0 -255} {srcip srcmask | any | host srcip} [{range {portkey| startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] {dstip dstmask | any | host dstip} [{range {portkey | startport} {portkey | endport} | {eq| neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | - rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp-message] [igmp-type igmp-type] [fragments] [precedence precedence | tos tos [tosmask] | dscp dscp]| [ttl eq 0-255]}} [time-range time-range-name] [log] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst-size]`

Режим ввода команд: конфигурирование IPv4 Access-list

Явно выраженное IP-правило deny all всегда останавливает действие ACL.

Параметр *mirror* позволяет трафику быть скопированным в *unit/slot/port*, а параметр redirect позволяет трафику быть переадресованным на указанный *unit/slot/port*. Параметры *assign-queue* и *redirect* действительны только для правил permit.

Для IPv4 действуют следующие ограничения исходящих списков контроля доступа:

- **Совпадение по диапазону портов не поддерживается.**
- **Команда rate-limit.**

Параметр	*Описание*
sequence-number	*Sequence-number* определяет порядковый номер для правила ACL. Порядковый номер указывается пользователем или генерируется устройством. Если порядковый номер для правила не указан, используется порядковый номер на 10 больше, чем последний порядковый номер в ACL, и правило помещается в конец списка. Если это первое правило в данном ACL, ему присваивается порядковый номер 10. Если расчетный порядковый номер превышает максимальное значение номера последовательности, создание правила ACL заканчивается ошибкой. Правило не может быть создано, если оно дублирует уже существующее. Правило не может быть настроено с порядковым номером, который уже используется для другого правила. Например, если пользователь добавляет новое правило ACL без указания порядкового номера, оно помещается в конец списка. Изменив порядковый номер, пользователь может перемещать правило ACL в другое положение.
{deny | permit}	Указывает, выполняется или запрещается действие в результате применения правила IP ACL к трафику.
every	Совпадает каждый пакет.
{eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp | *0 -255*}	Указывает протокол, который должен соответствовать правилу IP ACL.
srcip srcmask | any | host *srcip*	Указывает IP-адрес источника и маску подсети для соответствия состояния правилу ACL. Указание any подразумевает значение для *srcip* 0.0.0.0 и для srcmask — 255.255.255.255. Указание host A.B.C.D подразумевает *srcip* как A.B.C.D и srcmask как 0.0.0.0.
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	***Примечание.*** Эта опция доступна только с протоколами TCP или UDP. Определяет условия соответствия для порта layer 4 в правиле IP ACL. Можно использовать номер порта, который находится в пределах от 0–65535, или указать параметр portkey, который может быть одним из следующих ключевых слов. • Для TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3. • Для UDP: domain, echo, ntp, rip, snmp, tftp, time и who. Каждое из ключевых слов переводится в эквивалентный номер порта. Если указан range, правило IP ACL может определить соответствие, только если номер порта layer 4 находится в пределах указанного диапазона. Параметры startport и endport определяют первый и последний порты, которые являются частью диапазона портов. Они

	имеют значение от 0 до 65535. Конечный порт должен иметь значение равное или превышающее исходный порт. Исходный порт и все порты между ними будут частью диапазона портов layer 4. Когда eq задан, правило IP ACL соответствует, только если номер порта layer 4 равен указанному номеру или ключу порта. Когда lt задан, IP ACL правило соответствует, если номер порта layer 4 меньше указанного номера или ключа порта. Это эквивалентно заданию диапазона от 0 до <указанный номер порта - 1>. При указании gt правило IP ACL соответствует, если номер порта layer 4 больше, чем указанный номер или ключ порта. Это эквивалентно заданию диапазона <указанный номер порта + 1> до 65535. При указании neq правило IP ACL соответствует, только если номер порта layer 4 не равно указанному номеру или ключу порта. Два правила добавляются с диапазоном от 0 до <указанный номер порта - 1> и одно с диапазоном << указанный номер порта _ + 1 до 65535>>. ***Примечание.*** Номер порта совпадения применяется только к нефрагментированным пакетам или первым фрагментам.
dstip dstmask **| any | host** ***dstip***	Указывает IP-адрес назначения и маску подсети для соответствия состояния правила IP ACL. Указание any подразумевает указания dstip как 0.0.0.0 и dstmask как 255.255.255.255. Указание хоста A.B.C.D подразумевает dstip, как A.B.C.D и dstmask как 0.0.0.0.
[precedence ***precedence*** **| tos** ***tos*** **[*tosmask*] | dscp dscp]**	Определяет TOS для правила IP ACL в зависимости от соотношения приоритета или DSCP значений с использованием параметров *dscp*, *precedence*, *tos/tosmask.* Параметр tosmask является необязательным.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Указывает, что правило IP ACL использует соответствие по TCP-флагам. Когда +<tcpflagname> указан, совпадение имеет место, если указанный флаг <tcpflagname> установлен в TCP-заголовке. Когда -<tcpflagname> указан, совпадение имеет место, если указанный флаг <tcpflagname> НЕ установлен в TCP-заголовке. Если указано ключевое слово established, совпадение происходит, если указанные RST- или ACK-биты устанавливаются в TCP-заголовке. В системе устанавливаются два правила, если указан этот параметр. Эта опция доступна только в случае, если используется протокол TCP.
[icmp-type ***icmp-type*** **[icmp-code** ***icmp-code*****] | icmp-message** ***icmp-message***]	***Примечание.*** Эта опция доступна только в случае, если используется протокол ICMP. Указывает условие соответствия для пакетов ICMP. При указании *icmp-type* правило IP ACL совпадает с указанным типом ICMP-сообщения, числом от 0 до 255. При указании *icmp-code* правило IP ACL совпадает с указанным кодом ICMP-сообщения, числом от 0 до 255. Указание *icmp-message* означает, что указаны параметры *icmp-type* и *icmp-code.* Следующие ICMP-сообщения поддерживаются: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port- unreachable, source- quench, router-solicitation, router- advertisement, time-exceeded, ttl-exceeded и unreachable. Сообщение ICMP декодируется в соответствующий тип ICMP и ICMP-кода в пределах этого типа ICMP.
igmp-type ***igmp-type***	***Примечание.*** Эта опция доступна только в случае, если используется протокол IGMP. При указании *igmp-type* правило IP ACL проверяет совпадение с указанным типом ICMP-сообщения, числом от 0 до 255.
fragments	Указывает, что правило IP ACL совпадает с фрагментированными пакетами IP.

ttl eq	Указывает, что правило IP ACL совпадает с пакетами с указанным значением Time To Live (TTL).
log	Указывает, что это правило должно быть записано в журнал.
time-range *time-range-name*	Позволяет применять ограничение времени к правилу ACL, как это определено параметром time-range-name. Если временной диапазон с указанным именем не существует и ACL, содержащий это правило ACL, применяется к интерфейсу или привязан к VLAN, правило ACL применяется немедленно. Если временной диапазон с указанным именем существует и ACL, содержащий это правило ACL, применяется к интерфейсу или привязан к VLAN, правило ACL применяется, если временной диапазон с указанным именем становится активным. Правило ACL удаляется, если временной диапазон с указанным именем становится неактивным.
assign-queue *queue-id*	Определяет связанную очередь, т. е. идентификатор очереди, к которой пакеты, соответствующие этому правилу, назначаются.
{mirror | redirect} *unit/slot/ port*	Определяет mirror или redirect интерфейс unit/slot/port, к которому пакеты, соответствующие этому правилу, копируются или пересылаются соответственно.
rate-limit *rate burst-size*	Определяет допустимую скорость передави данных в соответствии с заданной скоростью в Кбит/с и с пиковым размером буфера в килобайтах.

no sequence-number

Используйте эту команду для удаления правила ACL с указанным порядковым номером из ACL.

Формат: no *sequence-number*

Режим ввода команд: конфигурирование IPv4 Access-list

ip access-group

Эта команда либо закрепляет определенный IP ACL, идентифицируемый по параметру accesslistnumber или name, к интерфейсу (включая интерфейсы маршрутизации VLAN), диапазону интерфейсов или всем интерфейсам — или связывает его с VLAN ID в заданном направлении. Параметр name — это имя Access Control List.

Необязательный порядковый номер может быть указан, чтобы указать порядок этого IP ACL по отношению к другим IP ACL, уже назначенным этому интерфейсу и направлению. Меньшее значение указывает на более высокий приоритет. Если порядковый номер уже используется для этого интерфейса и направления, указанный IP ACL заменяет используемый в настоящее время IP ACL. Если порядковый номер для этой команды не определен, будет использоваться порядковый номер, который на единицу больше, чем самый высокий порядковый номер для этого интерфейса и направления.

Дополнительный параметр *control-plane* задается, чтобы применить ACL на порту CPU. Пакеты управления IPv4, такие как RADIUS и TACACS+, также отбрасываются из-за подразумеваемого присутствия правила **deny all** в конце списка. Для того, чтобы это изменить, требуется добавить разрешающие правила, которые позволят передавать IPv4-пакеты управления.

Ключевое слово *control-plane* доступно только в режиме глобальной конфигурации.

Значение по умолчанию: отсутствует

Формат: `ip access-group {`*`accesslistnumber`*`|`*`name`*`} {{`*`control-plane`*`|`*`in`*`|`*`out`*`}|vlan `*`vlan-id`*` {in|out}} [sequence `*`1-4294967295`*`]`

Режим ввода команд: конфигурирование интерфейса

глобальная конфигурация

Параметр	*Описание*
accesslistnumber	Определяет конкретный IP ACL. Диапазон составляет от 1 до 199.
sequence	Необязательный порядковый номер, который указывает порядок этого списка доступа IP по отношению к другим спискам IP-доступа, уже присвоенных этому интерфейсу и направлению. Диапазон составляет от 1 до 4294967295.
vlan-id	Идентификатор VLAN, связанный с определенным IP ACL в заданном направлении (доступно только в режиме глобальной конфигурации).
name	Имя списка контроля доступа.

no ip access-group

Эта команда удаляет заданный IP ACL из интерфейса.

Значение по умолчанию: отсутствует

Формат: `no ip access-group {`*`accesslistnumber`*`|`*`name`*`} {{`*`control-plane`*`|`*`in`*`|`*`out`*`}|vlan `*`vlan-id`*`{in|out}}`

Режим ввода команд: конфигурирование интерфейса

глобальная конфигурация

acl-trapflags

Данная команда включает отправку ACL-трапов.

Значение по умолчанию: выключено

Формат: `acl-trapflags`

Режим ввода команд: глобальная конфигурация

no acl-trapflags

Эта команда выключает режим ACL-трапа.

Формат: `no acl-trapflags`

Режим ввода команд: глобальная конфигурация

show ip access-lists

Используйте эту команду, чтобы просмотреть сводную информацию обо всех IP ACL, настроенных на коммутаторе. Для просмотра подробной информации о конкретном списке доступа, укажите номер ACL или имя, которое используется для идентификации IP ACL. Отображается информация committed rate, committed burst size и ACL rule hit count, соответствующая настроенному правилу внутри ACL. При достижении максимального значения счетчик начинает дальнейший отсчет с нуля. Существует специальный счетчик для каждого правила ACL. Счетчики ACL не взаимодействуют с PBR-счетчиками.

Для ACL с несколькими правилами, когда совпадение происходит в каком-либо одном конкретном правиле, увеличиваются только счетчики, связанные с этим правилом.

Для счетчиков ACL, если не настроено правило RATE-LIMIT, значение счетчика является количеством переадресованных/отброшенных пакетов. (К примеру, если на интерфейс получено 100 пакетов, значение счетчика увеличится на 100).

Если правило ACL настроено с RATE LIMIT, значение счетчика будет отражать количество пакетов попадающих под правило, независимо от ограничения скорости. Если входящая скорость

передачи трафика превышает установленный предел, счетчики все равно будут расти(несмотря на то, что они отбрасываются при превышении установленных ограничений, поскольку критерий соответствия выполняется). Счетчики ACL не взаимодействуют с политиками DiffServ.

Формат: `show ip access-lists [accesslistnumber | name]`

Режим ввода команд: привилегированный

Термин	*Значение*
ACL ID/Name	Определяет указанный номер или имя ACL.
Rules	Определяет количество правил, настроенных для ACL.
Direction	Показывает, применяется ли ACL к входящему или исходящему трафику на интерфейсе.
Interface(s)	Определяет интерфейс(ы), к которым применяется список управления доступом (привязки ACL к интерфейсам).
VLAN(s)	Определяет сети VLAN, к которым применяются ACL (привязки ACL к VLAN).

Если вы указываете номер IP ACL или имя, отображается следующая информация.

Вывод команды может меняться в зависимости от критериев соответствия, настроенных в рамках правил в ACL.

Термин	*Значение*
Rule Number	Идентификатор номера для каждого правила, которое определяется для IP ACL.
Action	Действие, связанное с каждым правилом. Возможные значения: Permit или Deny.
Match All	Указывает, применяется ли этот список доступа к каждому пакету. Возможные значения: True или False.
Protocol	Протокол фильтрации.
ICMP Type	***Примечание.*** Это отображается только в том случае, если используется протокол ICMP. Тип ICMP-сообщения для этого правила.
Starting Source L4 port	Начальный порт источника Layer 4.
Ending Source L4 port	Конечный порт источника Layer 4.
Starting Destination L4 port	Исходный порт назначения Layer 4.
Ending Destination L4 port	Конечный порт назначения Layer 4.
ICMP Code	***Примечание.*** Это отображается только в том случае, если используется протокол ICMP. Код ICMP-сообщения для этого правила.
Committed Rate	Гарантированная скорость, определяется атрибутом rate-limit.
Committed Burst Size	Пиковый размер буфера, определяется атрибутом rate-limit.
Source IP Address	IP-адрес источника для этого правила.
Source IP Mask	IP-маска назначения для этого правила.
Source L4 Port Keyword	Порт источника для этого правила.
Destination IP Address	IP-адрес назначения для этого правила.
Destination IP Mask	IP-маска назначения для этого правила.
Destination L4 Port Keyword	Порт назначения для этого правила.
IP DSCP	Значение, указанное для IP DSCP.
IP Precedence	Значение, указанное IP Precedence.
IP TOS	Значение, указанное для IP TOS.
Fragments	Указывает, включено ли правило IP ACL для совпадения с фрагментированными IP-пакетами.
TTL Field Value	Значение, указанное для TTL.

Log	Показывает, включено ли ведение журнала для правила.
Assign Queue	Идентификатор очереди, с которой связаны пакеты, соответствующие этому правилу.
Mirror Interface	Unit/slot/port, к которому копируются пакеты, соответствующие этому правилу.
Redirect Interface	Unit/slot/port, к которому пересылаются пакеты, соответствующие этому правилу.
Time Range Name	Отображает имя временного диапазона, если правило IP ACL ссылается на диапазон времени.
Rule Status	Статус правила IP ACL (Active/Inactive).
ACL Hit Count	Счетчик выполнения правила ACL для пакетов, соответствующих настроенному правилу ACL внутри ACL.

show access-lists

Эта команда отображает информацию списков IP ACL, IPv6 ACL и MAC ACL для назначенного интерфейса и направления. Вместо параметра *unit/slot/port* можно использовать lag *lag-intf-num* как альтернативный вариант определения LAG-интерфейса. Параметр lag *lag-intf-num* можно использовать для определения конкретного LAG-интерфейса, при этом значение *lag-intf-num* должно указывать номер порта LAG. Используйте ключевое слово **control-plane**, чтобы отобразить списки ACL, применяемые на порте CPU.

Формат: `show access-lists interface {`*`unit/slot/port`* `in|out | control-plane}`

Режим ввода команд: привилегированный

Термин	***Значение***
ACL Type	Тип списка доступа (IP, IPv6, или MAC).
ACL ID	Имя списка доступа для списка доступа MAC или IPv6 или числовой идентификатор для IP ACL.
Sequence Number	Порядковый номер ACL по отношению к другим ACL, уже назначенным этому интерфейсу и направлению. Меньшее значение указывает на более высокий приоритет.
in|out	• in — отображает информацию ACL для конкретного интерфейса во входящем направлении; • out — отображает информацию ACL для конкретного интерфейса в исходящем направлении.

show access-lists vlan

Эта команда отображает информацию ACL для конкретной VLAN ID. Параметр *vlan-id* является идентификатором VLAN. Параметр {in | out} определяет направление для просмотра информации VLAN ACL.

Формат: `show access-lists vlan` *`vlan-id`* `in|out`

Режим ввода команд: привилегированный

Термин	***Значение***
ACL Type	Тип списка доступа (IP, IPv6, или MAC).
ACL ID	Имя списка доступа MAC, IP или IPv6 или числовой идентификатор для IP ACL.
Sequence Number	Порядковый номер ACL по отношению к другим ACL, уже назначенным этому интерфейсу и направлению. Меньшее значение указывает на более высокий приоритет.

15.9 Команды настройки IPv6 ACL

В этой части описаны команды, используемые для настройки параметров IPv6 ACL. IPv6 ACL гарантируют, что только авторизованные пользователи получат доступ к определенным ресурсам, и блокируют любые попытки необоснованного доступа к сетевым ресурсам.

К IPv6 ACL применяются следующие правила.

- Максимальное количество создаваемых списков контроля доступа — 100, независимо от типа.
- Система поддерживает только кадры типа Ethernet II.
- Максимальное количество правил на IPv6 ACL зависит от платформы.

IPv6 access-list

Эта команда создает IPv6 ACL, идентифицируемый параметром *name* и состоящий из полей классификации, определенных для IP-заголовка IPv6-кадра. Параметр *name* представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует IPv6 ACL. Если IPv6 ACL с таким именем уже существует, эта команда входит в режим конфигурирования IPv6 Access-List, чтобы обновить существующий IPv6 ACL.

При успешном выполнении команды режим CLI сменяется на конфигурирование IPv6 Access-List.

Формат: `IPv6 access-list` *name*

Режим ввода команд: глобальная конфигурация

no IPv6 access-list

Эта команда удаляет IPv6 ACL, идентифицируемый параметром *name*, из системы.

Формат: `no IPv6 access-list` *name*

Режим ввода команд: глобальная конфигурация

IPv6 access-list rename

Эта команда изменяет имя на IPv6 ACL. Параметр *name* является именем существующего IPv6 ACL. Параметр newname является чувствительным к регистру буквенно-цифровой строки от 1 до 31 символа, однозначно идентифицирующим список доступа IPv6.

Команда не будет выполнена, если IPv6 ACL с именем *newname* уже существует.

Формат: `IPv6 access-list rename` *name newname*

Режим ввода команд: глобальная конфигурация

IPv6 access-list resequence

Используйте эту команду, чтобы изменить нумерацию порядкового номера правил для указанного списка доступа IPv6 с заданным значением приращения, начиная с определенного порядкового номера. Команда используется для редактирования последовательности правил ACL и

изменяет порядок, в котором применяются записи. Эта команда не сохраняется в конфигурации запуска и не отображается в текущей конфигурации.

Если созданный командой порядковый номер превышает максимальный порядковый номер, создание правила ACL не удается, выводится информационное сообщение.

Значение по умолчанию: 10

Формат: `IPv6 access-list resequence {name| id } starting-sequence-number increment`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
starting-sequence- number	Начальный порядковый номер. Диапазон — 1–2147483647. Значение по умолчанию: 10.
increment	Шаг увеличения. Диапазон — 1–2147483647. Значение по умолчанию: 10.

{deny | permit} (IPv6)

Эта команда создает новое правило для текущего IPv6 ACL. Правило может либо запретить, либо разрешить трафик в соответствии с указанными полями классификации. Как минимум, ключевое слово *every* или протокол, адрес источника и адреса назначения должны быть указаны. Поля IPv6-адреса источника и назначения могут быть определены с помощью ключевого слова *any*, указанного для любого значения в этой области. Остальные параметры команды являются необязательными, но наиболее часто используемые параметры отображаются в том же относительном порядке, как показано в формате команды.

Формат: `{deny | permit} {every | {{icmpv6 | IPv6 | tcp | udp | 0-255} {source-IPv6-prefix/ prefix-length | any | host source-IPv6-address} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] {destination-IPv6-prefix/ prefix-length | any | host destination-IPv6-address} [{range {portkey | startport} {portkey | endport} | {eq | neq | lt | gt} {portkey | 0-65535}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [flow-label value] [icmp-type icmp-type [icmp-code icmp-code] | icmp-message icmp- message] [routing] [fragments] [sequence sequence-number] [dscp dscp]}} [log] [assign-queue queue-id] [{mirror | redirect} unit/slot/port] [rate-limit rate burst- size]`

Режим ввода команд: конфигурирование IPv6 Access-list

Явно выраженное IPv6-правило deny all всегда останавливает действие ACL.

Параметр	*Описание*
{deny | permit}	Указывает, выполняется или запрещается правило IP ACL для соответствующего трафика.
every	Соотносит каждый пакет.

{*protocolkey* | *number*}	Задает протокол, который должен соответствовать правилу IP ACL. icmpv6, IPv6, tcp, and udp.
source-IPv6-prefix/prefix-length* | any | *host source-IPv6-address	Задает IP-адрес источника и маску сети источника, который должен соответствовать правилу IP ACL. Указание any подразумевает указания «::/0 »
[{range {*portkey* | *startport*} {*portkey* | *endport*} | {eq | neq | lt | gt} {*portkey* | *0-65535*}]	***Примечание.*** Эта опция доступна только с протоколами TCP или UDP. Определяет условия соответствия порта источника 4-го уровня для правила IP ACL. Вы можете использовать номер порта, который находится в пределах от 0–65535, или указать портключ, который может быть одним из следующих ключевых слов: • Для TCP: *bgp*, *domain*, *echo*, *ftp*, *ftp-data*, *http*, *smtp*, *telnet*, *www*, *pop2*, *pop3;* • Для UDP: *domain*, *echo*, *ntp*, *rip*, *snmp*, *tftp*, *time*, *who*. Каждое из ключевых слов переводится в эквивалентный номер порта. Если указан диапазон, правило IP ACL соответствует, только если номер порта уровня 4 находится в пределах указанного диапазона портов. Параметры *startport* и *endport* определяют первый и последний порты, которые являются частью диапазона портов. Они имеют значение от 0 до 65535. Конечный порт должен иметь значение равное или больше, чем начальный порт. Когда eq задан, то правило IPv6 ACL соответствует только если номер порта уровня 4 равен указанному номеру порта или портключа. Когда lt указан, IPv6 ACL-правило соответствует, если номер порта уровня 4 меньше указанного номера порта или портключа. Это эквивалентно заданию диапазона от 0 до <указанный номер порта - 1>. При указании gt, правило IPv6 ACL соответствует, если номер порта уровня 4 больше, чем указанный номер порта или портключа. Это эквивалентно заданию диапазона <указанный номер порта + 1> до 65535. При указании neq, IPv6 правило ACL соответствует только если номер порта уровня 4 не равен указанному номеру порта или портключу. Два правила добавляются с диапазоном от 0 до <указанный номера порта - 1> и один с диапазоном << указанный номер порта + 1 до 65535>>.
destination-IPv6-prefix/prefix-length* | any | *host destination-IPv6-address	Указывает IP-адрес назначения и маску подсети для соответствия состояния правила IP ACL. Указание any подразумевает значение «::/0». Указание *host destination-IPv6-address* подразумевает совпадение с указанным IPv6-адресом. Аргумент *destination-IPv6-address* должен указываться в формате RFC 2373, т. е. в шестнадцатеричном формате с использованием 16-битных значений между двоеточиями.
sequence *sequence-number*	Определяет порядковый номер правила ACL. Порядковый номер получает каждое правило. Порядковый номер указывается пользователем или генерируется устройством. Если порядковый номер для правила не указан, используется порядковый номер на 10 больше, чем последний порядковый номер в ACL, и правило помещается в конец списка. Если это первое правило в данном ACL, ему присваивается порядковый номер 10. Если расчетный порядковый номер превышает максимальное значение номера последовательности, создание правила ACL заканчивается ошибкой. Правило не может быть создано, если оно дублирует уже существующее, и правило не может быть сконфигурировано с порядковым номером, который уже используется для другого правила. Например, если пользователь добавляет новое правило ACL к ACL без указания номера последовательности, оно помещается в нижней части списка. Изменив номер последовательности, пользователь может перемещать правило ACL в другое положение в ACL.
[dscp *dscp*]	Задает значение DSCP, которое должно соответствовать правилу IPv6.

flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	***Примечание.*** Эта опция доступна только в случае, если правило настраивается для протокола TCP Когда +<tcpflagname> указан, совпадение имеет место, если указанный флаг <tcpflagname> установлен в TCP-заголовке. Когда -<tcpflagname> указан, совпадение имеет место, если указанный флаг <tcpflagname> не установлен в TCP-заголовке. Если указано ключевое слово established, совпадение происходит, если указанные RST или ACK-биты установлены в заголовке TCP. В системе устанавливается два правила.
[icmp-type *icmp-type [*icmp-code *icmp-code]* | icmp- message *icmp-message*]	***Примечание.*** Эта опция доступна только в случае, если правило настраивается для протокола ICMPv6. Указывает условие соответствия для пакетов ICMP. При указании *icmp-type* правило IPv6 ACL задаёт допустимый тип ICMPv6-сообщения, значением от 0 до 255. При указании *icmp-code* правило IPv6 ACL задаёт допустимый код ICMPv6-сообщения, значением от 0 до 255 Указание *icmp-message* означает, что указаны параметры icmp-type и icmp-code. Поддерживаются следующие ICMP-сообщения: *destination-unreachable*, *echo-reply*, *echo-request*, *header*, *hop-limit*, *mld-query*, *mld- reduction*, *mld-report*, *nd-na*, *nd-ns*, *next-header*, *no- admin*, *no-route*, *packet-too-big*, *port-unreachable*, *router-solicitation*, *router-advertisement*, *router- renumbering*, *time-exceeded*, and *unreachable*.
Fragments	Указывает, что правило IPv6 ACL совпадает с фрагментированными пакетами IPv6 (пакеты, в которых поле заголовка установлено как 44).
Routing	Указывает, что правило IPv6 ACL совпадает с IPv6-пакетами, в которых есть заголовки расширенной маршрутизации (следующее поле заголовка установлено как 43).
Log	Указывает, что это правило должно быть записано в журнал.
time-range *time-range-name*	Позволяет применять ограничение времени к правилу ACL, как это определено параметром *time-range-name*. Если временной диапазон с указанным именем не существует и ACL, содержащий это правило, применяется к интерфейсу или к VLAN, правило ACL применяется немедленно. Если временной диапазон с указанным именем существует и ACL, содержащий это правило, применяется к интерфейсу или к VLAN, правило ACL применяется, если временной диапазон с указанным именем становится активным. Правило ACL игнорируется, если временной диапазон с указанным именем становится неактивным.
assign-queue *queue-id*	Определяет связанную очередь, т. е. идентификатор очереди, к которой пакеты, соответствующие этому правилу, назначаются.
{mirror | redirect} *unit/slot/port*	Определяет mirror или redirect-интерфейс unit/slot/port, к которому пакеты, соответствующие этому правилу, копируются или пересылаются соответственно.
rate-limit *rate burst-size*	Определяет допустимую скорость передачи в соответствии с заданной скоростью в Кбит/с и с пиковым размером буфера в килобайтах.
rate-limit *rate burst-size*	Определяет допустимую скорость передачи в соответствии с заданной скоростью в Кбит/с и с пиковым размером буфера в килобайтах.

no sequence-number

Используйте эту команду для удаления правила ACL с указанным порядковым номером из ACL.

Формат: no *sequence-number*

Режим ввода команд: конфигурирование IPv6 Access-list

IPv6 traffic-filter

Эта команда либо закрепляет определенный IPv6 ACL, идентифицируемый по параметру *name,* к интерфейсу или набору интерфейсов, либо связывает его с VLAN ID в заданном направлении. Параметр *name* должен быть именем существующего IPv6 ACL.

Необязательный порядковый номер может быть указан, чтобы указать порядок этого IPv6 ACL по отношению к другим IPv6 ACL, уже назначенным этому интерфейсу и направлению. Меньшее значение указывает на более высокий приоритет. Если порядковый номер уже используется для этого интерфейса и направления, расширенный IPv6 ACL заменяет список, использующий этот порядковый номер. Если порядковый номер для этой команды не определен, будет использоваться порядковый номер, который на единицу больше, чем самый высокий порядковый номер для этого интерфейса и направления.

Эта команда, выполненная в режиме конфигурирования интерфейса, действует только на один интерфейс, в то время как в режиме глобальной конфигурации применяется для всех интерфейсов. Ключевое слово vlan действует только в режиме глобальной конфигурации.

Опция *control-plane* задается, чтобы применить ACL на порте CPU. Пакеты управления IPv6, такие как IGMPv6, также отбрасываются из-за подразумеваемого присутствия правила *deny all* в конце списка. Для того, чтобы это изменить, требуется добавить разрешающие правила, которые позволят передавать IPv6-пакеты управления.

Ключевое слово *control-plane* доступно только в режиме глобальной конфигурации.

Формат: IPv6 traffic-filter *name* {{control-plane |in|out}|vlan *vlan-id* {in|out}} [sequence *1-4294967295*]

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

no IPv6 traffic-filter

Эта команда удаляет IPv6 ACL, идентифицируемый по параметру *name* из интерфейса (ов), в заданном направлении.

Формат: no IPv6 traffic-filter <*name*{{control-plane | in | out} | vlan <*vlan-id*> {in|out}}

Режим ввода команд: глобальная конфигурация

конфигурирование интерфейса

show IPv6 access-lists

Эта команда отображает краткую информацию из всех списков доступа IPv6. Используйте параметр *name* для списка контроля доступа для отображения подробной информации о конкретном IPv6 ACL.

Эта команда отображает информацию об атрибутах icmp-type, icmp-code, fragments, routing, tcp flags, а также диапазоны портов L4 для источника и цели. Он отображает пакеты committed rate, committed burst size и ACL rule hit count, соответствующие настроенному правилу внутри ACL. При достижении максимального значения счетчик начинает дальнейший отсчет с нуля. Существует специальный счетчик для каждого правила ACL. Счетчики ACL не взаимодействуют с PBR-счетчиками.

Для ACL с несколькими правилами, когда совпадение происходит в каком-либо одном конкретном правиле, увеличиваются только счетчики, связанные с этим правилом.

Для счетчиков ACL, если не настроено правило RATE-LIMIT, значение счетчика является количеством переадресованных/отброшенных пакетов. (К примеру, если на интерфейс получено 100 пакетов, значение счетчика увеличится на 100).

Если правило ACL настроено с RATE LIMIT, значение счетчика будет отражать количество пакетов попадающих под правило, независимо от ограничения скорости. Если входящая скорость передачи трафика превышает установленный предел, счетчики все равно будут расти(несмотря на то, что они отбрасываются при превышении установленных ограничений, поскольку критерий соответствия выполняется). Счетчики ACL не взаимодействуют с политиками DiffServ.

Формат: `show IPv6 access-lists` *`[name]`*

Режим ввода команд: привилегированный

Вывод команды изменяется в зависимости от критериев соответствия, настроенных в рамках правил в ACL.

Термин	***Значение***
Rule Number	Идентификатор номера для каждого правила, которое определяется для IPv6 ACL.
Action	Действие, связанное с каждым правилом. Возможные значения: Permit или Deny.
Match All	Указывает, применяется ли этот список доступа к каждому пакету. Возможные значения: True или False.
Protocol	Протокол фильтрации.
Committed Rate	Гарантированная скорость, определяется атрибутом *rate limit*.
Committed Burst Size	Указанный размер буфера, определяется атрибутом *rate limit*.
Source IP Address	IP-адрес источника для этого правила.
Source L4 Port Keyword	L4-порт источника для этого правила.
Destination IP Address	IP-адрес назначения для этого правила.
Destination L4 Port Keyword	L4-порт назначения для этого правила.
IP DSCP	Значение, указанное для IP DSCP.
Flow Label	Значение, указанное для IPv6 Flow Label.
Log	Показывает, включено ли ведение журнала для правила.
Assign Queue	Идентификатор очереди, с которой связаны пакеты, соответствующие этому правилу.
Mirror Interface	*unit/slot/port,* к которому пакеты, соответствующие этому правилу, копируются.

Redirect Interface	*unit/slot/port,* к которому пакеты, соответствующие этому правилу, пересылаются.
Time Range Name	Отображает имя временного диапазона, если правило IP ACL ссылается на диапазон времени.
Rule Status	Статус правила IPv6 ACL (Активный/Неактивный).
ACL Hit Count	Счетчик выполнения правила ACL для пакетов, соответствующих настроенному правилу ACL внутри ACL.

15.10 Команды управления функцией Management Access Control and Administration List

В целях обеспечения безопасности функций управления коммутатора администратор может настроить список ACL для задач управления. Функция Management Access Control and Administration List (MACAL) используется для обеспечения контроля удаленного управления коммутатором через сеть TCP/IP только с известных и надежных устройств.

MACAL может быть применена только к стандартным портам, к сервисному порту эта функция не применима.

management access-list

Используйте эту команду для создания списка MACAL и входа в режим конфигурирования ACL, где требуется определить запрещенные или разрешенные условия доступа с помощью команд deny и permit. Если никакие критерии соответствия не определены, значение по умолчанию — deny. Если вы повторно вводите условия для ACL, новые правила будут добавлены в конец списка. Значение *name* может быть длиной до 32 символов.

Формат: `management access-list` *name*

Режим ввода команд: глобальная конфигурация

no management access-list

Данная команда удаляет MACAL, идентифицируемый параметром *name,* из системы.

Формат: `no management access-list` *name*

Режим ввода команд: глобальная конфигурация

{deny | permit} (Management ACAL)

Эта команда создает новое правило для текущего списка MACAL. Правило может либо запретить, либо разрешить трафик в соответствии с указанными полями классификации. Правила с параметрами ethernet, vlan и port-channel будут действовать только если IP-адрес определяется на соответствующем интерфейсе. Каждое правило должно иметь уникальный приоритет.

Формат:
`{deny | permit} [ethernet` *interface-number* `| vlan` *vlan-id* `| port-channel` *number*`] [service` *service*`] [priority` *priority-value*`]`
`{deny | permit} ip-source` *ip-address* `[mask` *mask* `|` *prefix-length*`] [ethernet` *interface- number* `| vlan` *vlan-id* `| port-channel` *number*`] [service` *service*`] [priority` *priority- value*`]`

Режим ввода команд: конфигурирование MACAL

Параметр	*Описание*
ethernet	Номер порта Ethernet.
ip-source	IP-адрес источника.
port-channel	Номер агрегированного интерфейса.
priority	Приоритет правила.
service	Состояние типа сервиса, которое может выражаться одним из следующих ключевых слов: • java • tftp • telnet • ssh • http • https • snmp • sntp • any
vlan	Номер VLAN.
mask	Сетевая маска IP-адреса источника (0–32).
prefix-length	Число битов, которые составляют префикс IP-адреса источника. Перед длиной префикса ставится косая черта (/).

management access-class

Используйте эту команду, чтобы выбрать активный список контроля доступа. Активный список MACAL не может быть обновлен или удален. Ключевое слово console-only указывает, что устройство может управляться только с консоли.

Формат: `management access-class {console-only | name}`

Режим ввода команд: глобальная конфигурация

no management access-class

Эта команда отключает ограничения управления.

Формат: `no management access-class`

Режим ввода команд: глобальная конфигурация

show management access-list

Данная команда отображает списки MACAL.

Формат: `show management access-list [name]`

Режим ввода команд: привилегированный

show management access-class

Эта команда отображает информацию об активном списке MACAL.

Формат: `show management access-class [name]`

Режим ввода команд: привилегированный

15.11 Команды настройки временного диапазона для ACL с ограничением по времени

ACL с ограничением по времени позволяют одному или нескольким правилам внутри ACL работать в зависимости от текущего времени. Каждое правило ACL, за исключением неявного *deny all*, может быть сконфигурировано на активное выполнение только в течение определенного периода времени. Команды временного диапазона позволяют указать определенное время дня и недели для того, чтобы реализовать ACL с ограничением по времени. Временной диапазон идентифицируется по имени. После этого на него можно ссылаться в рамках правил ACL.

time-range

Используйте эту команду, чтобы глобально включить работу временных интервалов.

Формат: `time-range`

Режим ввода команд: глобальная конфигурация

no time-range

Эта команда глобально выключает работу временных интервалов.

Формат: `no time-range`

Режим ввода команд: глобальная конфигурация

time-range name

Используйте эту команду, чтобы создать временной диапазон, определяемый параметром *name*, состоящим из одной абсолютной записи времени и/или одной или нескольких периодических записей времени. Параметр *name* представляет собой буквенно-цифровую строку длиной от 1 до 31 символа с учетом регистра и однозначно идентифицирует временной диапазон. Буквенно-цифровая строка определяется как состоящая только из буквенных символов, цифровых, тире, подчеркивания или символов пробела.

Если временной диапазон с этим именем уже существует, команда входит в режим конфигурирования временного диапазона, чтобы обновить соответствующую запись.

Если вы успешно выполнили эту команду, то режим CLI изменяется в режим Time-Range Config.

Формат: `time-range` *name*

Режим ввода команд: глобальная конфигурация

no time-range

Эта команда удаляет тайм-диапазон, идентифицируемый по параметру *name*.

Формат: `no time-range` *name*

Режим ввода команд: глобальная конфигурация

15.12 Команды Auto-Voice over IP

В этом разделе описаны команды, используемые для настройки функции Auto-Voice over IP (VoIP). Функция Auto-VoIP явно соответствует VoIP-потокам в коммутаторах Ethernet и обеспечивает им более высокий класс обслуживания, чем для обычного трафика. При включении функции Auto-VoIP на интерфейсе интерфейс сканирует входящий трафик для следующих протоколов управления вызовами:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

Когда протокол управления вызовами определен, коммутатор назначает трафик соответствующей сессии в CoS-очередь самого высокого уровня, которая используется для трафика, чувствительного к скорости.

auto-voip

Используйте эту команду, чтобы настроить режим Auto-VoIP. Поддерживаются режимы protocol-based и oui-based. Auto-VoIP на основе протокола устанавливает приоритет голосовых данных информации на основе layer 4, используемого для голосовой сессии. Auto-VoIP на основе OUI отдает приоритет трафику, основанного на известном OUI телефона.

Когда оба режима включены, подключенный OUI телефона является одним из настроенных OUI, и приоритет для голосовых данных назначается с помощью OUI Auto VoIP, в противном случае приоритет для голосовых данных устанавливается на основе протокола Auto VoIP.

Если Auto VoIP на порту выключен, активные сессии удаляются.

Значение по умолчанию: на основе oui

Формат: `auto-voip [protocol-based | oui-based]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no auto-voip

Используйте **no**-форму команды, чтобы установить режим по умолчанию.

Формат: `auto-voip [protocol-based | oui-based]`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

auto-voip oui

Используйте эту команду, чтобы настроить OUI для Auto VoIP. Трафик соответствующий настроенному OUI получит наивысший приоритет по отношению к другому трафику. Параметр *oui-prefix* является уникальным OUI, который идентифицирует производителя устройства или поставщика. OUI определяется в трех значениях октета (каждый октет представлен в виде двух шестнадцатеричных цифр), разделенных двоеточием. Параметр *string* представляет собой описание OUI, которое идентифицирует связанного производителя или поставщика.

Значение по умолчанию: список известных OUI присутствует.

Формат: `auto-voip oui` *`oui-prefix`* `oui-desc` *`string`*

Режим ввода команд: глобальная конфигурация

no auto-voip oui

Используйте **no**-форму команды, чтобы удалить настроенный OUI-префикс.

Формат: `no auto-voip oui` *`oui-prefix`*

Режим ввода команд: глобальная конфигурация

auto-voip oui-based priority

Используйте эту команду для настройки глобального приоритета VoIP на основе OUI. Если OUI телефона соответствует одному из настроенных OUI, то приоритет трафика с телефона меняется на приоритет OUI, настраиваемый с помощью этой команды. Параметр *priority-value* 802.1p используется для трафика, который соответствует значению в известном списке OUI.

Значение по умолчанию: максимальный приоритет (7)

Формат: `auto-voip oui-based priority` *`priority-value`*

Режим ввода команд: глобальная конфигурация

no auto-voip oui-based priority

Используйте **no**-форму команды, чтобы вернуть глобальный приоритет VoIP в значение по умолчанию.

Формат: `no auto-voip oui` *`oui-prefix`*

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

auto-voip protocol-based

Используйте эту команду для настройки приоритета или класса трафика Auto VoIP на основе протокола. Если приоритет для замечаний настроен, голосовые данные в этой сессии отмечаются приоритетом с помощью данной команды.

Значение *remark priority* является приоритетом 802.1p, используемым для маркирования трафика VoIP. Если интерфейс определяет протокол управления вызовами, устройство помечает указанным значением приоритета 802.1p голосовой трафик, для гарантированного наивысшего приоритета по всему сетевому пути.

Значение traffic-class *tc* является классом трафика (CoS). Если интерфейс определяет протокол управления вызовами, устройство связывает голосовой трафик с соответствующим CoS. Очередь CoS, связанная с указанным классом трафика, должна быть настроена с соответствующим распределением полосы пропускания для передачи приоритетного трафика VoIP.

Требуется включить тегирование для портов с автоматическим VoIP, чтобы отличать голосовые данные на выходе.

Значение по умолчанию: Traffic Class 7

Формат: `auto-voip protocol-based {remark` *`remark-priority`* `| traffic-class` *`tc`*`}`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

no auto-voip protocol-based

Используйте эту команду для сброса автоматически назначаемого приоритета или класса трафика VoIP в значение по умолчанию.

Формат: `no auto-voip protocol-based {remark` *`remark-priority`* `| traffic-class` *`tc`*`}`

Режим ввода команд: глобальная конфигурация
конфигурирование интерфейса

auto-voip vlan

Используйте эту команду, чтобы настроить глобальный Auto VoIP VLAN ID. Режим VLAN зависит от режима Auto VoIP. Auto-VoIP VLAN является VLAN, используемой для разделения VoIP-трафика от другого не голосового трафика. Трафик VoIP, который соответствует значению в известном списке OUI, получает назначение в VoIP VLAN.

Значение по умолчанию: отсутствует

Формат: `auto-voip vlan` *`vlan-id`*

Режим ввода команд: глобальная конфигурация

no auto-voip vlan

Используйте **no**-форму команды для сброса Auto-VoIP VLAN ID в значение по умолчанию.

Формат: `no auto-voip vlan`

Режим ввода команд: глобальная конфигурация

show auto-voip

Используйте эту команду, чтобы отобразить параметры VoIP на интерфейсе или интерфейсе коммутатора.

Формат: `show auto-voip {protocol-based|oui-based} interface {`*`unit/slot/port`*`|all}`

Режим ввода команд: привилегированный

Поле	*Описание*
VoIP VLAN ID	Глобальный VoIP VLAN ID.
Prioritization Type	Тип приоритетов используемого голосового трафика.
Class Value	• Если **Prioritization Type** сконфигурирован как traffic-class, это значение равно значению очереди. • Если **Prioritization Type** сконфигурирован как remark, это значение является приоритетом 802.1p, используемым для маркировки голосового трафика.
Priority	Приоритет 802.1p. Это поле действительно для OUI Auto VoIP.
AutoVoIP Mode	Состояние Auto VoIP на интерфейсе.

show auto-voip oui-table

Используйте эту команду для отображения информации о OUI-таблице VoIP.

Формат: `show auto-voip oui-table`

Режим ввода команд: привилегированный

Параметр	*Описание*
OUI	OUI MAC-адреса источника.
Status	По умолчанию или настроенный.
OUI Description	Описание OUI.

15.13 Команды оптимизации iSCSI

В этом разделе описаны команды, используемые для мониторинга iSCSI-сессий и приоритизации пакетов iSCSI. Оптимизация iSCSI обеспечивает QoS-обработку трафика между инициатором и целевой системой iSCSI. Это достигается за счет мониторинга трафика для обнаружения пакетов, используемых iSCSI-станциями для создания iSCSI-сессий и соединений. Данные такого обмена используются для создания правил классификации. Пакеты в потоке будут поставлены в очередь и запланированы на выходе на порт назначения на основе этих правил.

iscsi aging time

Эта команда устанавливает aging time для сессий iSCSI. Схема поведения при смене aging time следующая.

- Если aging time увеличивается, текущие сессии будут приостановлены в соответствии с новым значением.
- Если aging time уменьшается, любые сессии, которые были в таблице в течение времени, превышающего новые настройки, будут немедленно удалены. Все остальные сессии будут продолжать существовать в зависимости от нового значения aging time.

Значение по умолчанию: 10 минут

Формат: `iscsi aging time` *`time`*

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
time	Количество минут сессии, в течение которых она должна быть неактивна для удаления. Диапазон: 1–43200.

no iscsi aging time

Используйте no-форму команды для сброса значения aging time в значение по умолчанию.

Формат: `no iscsi aging time`

Режим ввода команд: глобальная конфигурация

iscsi cos

Эта команда устанавливает профиль качества обслуживания, который будет применен к потокам iSCSI. Потоки iSCSI назначены по умолчанию на наивысший VPT/DSCP, отображенный на самой высокой доступной очереди. Необходимо также позаботится о настройке соответствующих параметров класса обслуживания для очереди.

Настройка VPT/DSCP устанавливает профиль QoS, который определяет очередь выхода. Настройка планирования очередей коммутатора по умолчанию для исходящего трафика является Weighted Round Robin (WRR).

Вы можете осуществить настройки QoS с помощью настройки соответствующих портов для работы в других режимах планирования и управления очередью через настройки CoS. CoS может включать в себя строгий приоритет очереди, используемой для iSCSI-трафика. Недостатком строгого планирования приоритетов является то, что при определенных обстоятельствах (при большом количестве трафика с высоким приоритетом) другие, более низкие приоритеты трафика могут пострадать. В WRR очередь, к которой назначается поток, может быть настроена для получения необходимого процента пропускной способности.

Формат: `iscsi cos {vpt vpt | dscp dscp} [remark]`

Режим ввода команд: глобальная конфигурация

Параметр	***Описание***
vpt/dscp	VLAN Priority Tag или DSCP для назначения пакетов iSCSI-сессии.
remark	Маркирует кадры iSCSI с настроенным VPT/DSCP на выходе из коммутатора.

no iscsi cos

Используйте no-форму команды, чтобы вернуться к значению по умолчанию.

Формат: `no iscsi cos`

Режим ввода команд: глобальная конфигурация

iscsi enable

Эта команда глобально включает определение iSCSI.

Значение по умолчанию: выключено

Формат: `iscsi enable`

Режим ввода команд: глобальная конфигурация

no iscsi enable

Эта команда отключает определение iSCSI. При использовании команды no iscsi enable iSCSI-ресурсы будут освобождены.

Формат: `no iscsi enable`

Режим ввода команд: глобальная конфигурация

iscsi target port

Эта команда настраивает целевой порт iSCSI и при необходимости IP-адрес целевой системы и имя IQN. При работе с частными портами iSCSI (не портами 3260/860, назначенными IANA), рекомендуется также указать целевой IP-адрес, чтобы коммутатор отслеживал только кадры со значением TCP-порта из числа заданных и с IP-адресом назначения, совпадающим с целевым адресом. Таким образом, процессор не будет ошибочно загружен для неисполнения iSCSI-потоков (если случайно другие приложения также решили использовать эти незарезервированные порты).

Когда порт уже определен и не привязан к IP-адресу, и необходимо привязать его к IP-адресу, то следует удалить его, используя no-форму этой команды, а затем добавить его снова, на этот раз вместе с соответствующим IP-адресом.

Целевые имена отображаются только при использовании команды **show iscsi**. Эти имена не используются для сопоставления с информацией о iSCSI-сессии.

Максимум 16 портов TCP могут быть настроены либо привязаны к IP или нет.

Значение по умолчанию: известные iSCSI-порты 3260 и 860 настроены по умолчанию, но могут быть удалены, как и любые другие, настроенная вручную.

Формат: `iscsi target port` *`tcp-port-1 [tcp-port-2...tcp-port-16]`* `[address` *`ip-address]`* `[name` *`targetname`*`]`

Режим ввода команд: глобальная конфигурация

Параметр	*Описание*
tcp-port-n	Номер порта TCP или список номеров портов TCP, на котором целевой iSCSI прослушивает запросы. До 16 портов TCP могут быть определены в системе в одной команде или с помощью нескольких команд.
ip-address	IP-адрес целевого устройства. Когда ни одна из форм этой команды не используется и TCP-порт, который будет удален, привязан к определенному IP-адресу, поле адреса должно присутствовать.
targetname	iSCSI-имя целевого устройства. Имя может быть статически сконфигурировано. Тем не менее, оно может быть получено из iSNS или из ответа SendTargets. Инициатор должен представить и собственное iSCSI-имя, и iSCSI-имя целевого устройства, к которому он хочет подключиться, в первом запросе авторизации новой сессии или соединения.

no iscsi target port

Используйте no-форму команды, чтобы удалить целевой порт iSCSI, адрес и имя.

show iscsi

Эта команда отображает параметры iSCSI.

Формат: `show iscsi`

Режим ввода команд: привилегированный

show iscsi sessions

Эта команда отображает сессии iSCSI.

Значение по умолчанию: если не указано, сеансы отображаются в режиме short (не подробно).

Формат: `show iscsi sessions [detailed]`

Режим ввода команд: привилегированный

16 СИСТЕМНЫЕ СООБЩЕНИЯ

В данном разделе описаны основные сообщения системного журнала и причины их появления. Сообщениям в журнале нельзя назначать какие-либо действия. При диагностировании проблемы проверьте сообщения в журнале событий, что, в совокупности со знанием конфигурации системы и особенностей данной проблемы, поможет определить главную причину возникновения проблемы. Последние зарегистрированные сообщения отображаются в первую очередь.

В данном разделе перечислены не все сообщения системного журнала.

16.1 База

Системные сообщения BSP

Компонент	*Сообщение*	*Причина*
BSP	Event(0xaaaaaaaa)	Перезагрузка коммутатора.
BSP	Starting code...	Инициализация BSP завершена, начало работы ПО.

Системные сообщения NIM

Компонент	*Сообщение*	*Причина*
NIM	NIM: L7_ATTACH out of order for interface unit x slot x port x	Некорректно создан интерфейс.
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	Отсутствует маппинг между USP и номером интерфейса.
NIM	NIM: L7_DETACH out of order for interface unit x slot x port x	Некорректно создан интерфейс.
NIM	NIM: L7_DELETE out of order for interface unit x slot x port x	Некорректно создан интерфейс.
NIM	NIM: event(x),intf(x),component(x), in wrong phase	Событие NIM произошло в неверную фазу конфигурации (вероятно, фазу 1,2 или WMU).
NIM	NIM: Failed to notify users of interface change	Событие не было распространено по системе.
NIM	NIM: failed to send message to NIM message Queue	Очередь сообщений NIM заполнена или не существует.
NIM	NIM: Failed to notify the components of L7_CREATE event	Интерфейс не создан.
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	Компонент инициировал событие интерфейса во время неверной фазы инициализации.
NIM	NIM: incorrect phase for operation	Вызов API сделан во время неверной фазы инициализации.
NIM	NIM: Component(x) failed on event(x) for interface	Компонент вернул неверную индикацию для события интерфейса.

NIM	NIM: Timeout event(x), interface remainingMask = xxxx	Компонент не ответил NIM до истечения времени.

Системное сообщение SIM

Компонент	*Сообщение*	*Причина*
SIM	IP address conflict on service port/network port for IP address x.x.x.x. Conflicting host MAC address is xx:xx:xx:xx:xx:xx	Конфликт адресов в сети LAN (IP-адрес служебного/сетевого порта).

Системные сообщения System

Компонент	*Сообщение*	*Причина*
SYSTEM	Configuration file system.cfg size is 0 (zero) bytes	Файл конфигурации не может быть прочитан. На системе отсутствует или стерта конфигурация.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	Файл конфигурации не может быть прочитан. На системе отсутствует или стерта конфигурация.
SYSTEM	Building defaults for file *file name* version *version num*	Конфигурация для заданной опции или файла отсутствует или не может быть прочитана. Будут использованы значения по умолчанию. Имя и версия файла указаны.
SYSTEM	File *filename*: same version (*version num*) but the sizes (*version size* – *expected version size*) differ	Загруженный файл конфигурации отличается по размеру номера версии от ожидаемого. Требуется перевести файл конфигурации на номер версии, соответствующей данному образу кода. Сообщение может появиться после обновления образа кода до более новой версии продукта.
SYSTEM	Migrating config file *filename* from version *version num* to *version num*	Идентифицированный файл конфигурации был переведен с предыдущего номера версии. Заданы как старая, так и новая версии. Сообщение может появиться после обновления образа кода до более новой версии продукта.
SYSTEM	Building Defaults	Конфигурация для заданной опции отсутствует или не может быть прочитана. Будут использованы настройки по умолчанию.
SYSTEM	sysapiCfgFileGet failed size = *expected size of file* version = *expected version*	Конфигурация для заданной опции отсутствует или не может быть прочитана. За данным сообщением, как правило, следует сообщение, что будут использованы настройки конфигурации по умолчанию.

16.2 Утилиты

Системные сообщения менеджера трапов (Trap Mgr)

Компонент	*Сообщение*	*Причина*
Trap Mgr	Link Up/Down: unit/slot/port	Изменено состояние канала связи на интерфейсе.

Системные сообщения фильтрации DHCP (DHCP Filtering)

Компонент	*Сообщение*	*Причина*
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Невозможно создать семафор для структуры конфигурации фильтрации dhcp.
DHCP Filtering	Failed to register with nv Store	Невозможно зарегистрировать функции сохранения и восстановления для сохранения конфигурации.
DHCP Filtering	Failed to register with NIM	Невозможно зарегистрироваться в NIM для функций обратного вызова интерфейса.
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Ошибка при попытке сохранения конфигурации.

Системные сообщения NVStore

Компонент	*Сообщение*	*Причина*
NVStore	Building defaults for file XXX	Файл конфигурации компонента отсутствует или контрольная сумма файла неверна, используется файл конфигурации по умолчанию.
NVStore	Error on call to osapiFsWrite routine on file XXX	Файл не может быть открыт или устройство ввода-вывода операционной системы вернуло ошибку при попытке записи в файл.
NVStore	Error on call to osapiFsWrite routine on file XXX	Рассчитанная контрольная сумма файла конфигурации компонента в файловой системе не совпадает с контрольной суммой в памяти.
NVStore	Migrating config file XXX from version Y to Z	Обнаружено несовпадение версии файла конфигурации, начат переход файла конфигурации.

Системные сообщения RADIUS

Компонент	*Сообщение*	*Причина*
RADIUS	RADIUS: Invalid data length - xxx	Клиентом RADIUS получено недействительное сообщение с сервера.
RADIUS	RADIUS: Failed to send the request	Проблема соединения с сервером RADIUS.
RADIUS	RADIUS: Failed to send all of the request	Проблема во время обмена данными с сервером RADIUS.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Проблема выделения ресурсов клиент-сервиса RADIUS.

RADIUS	RADIUS: Buffer is too small for response processing	Клиент RADIUS превысил лимит ресурсов при создании ответа.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Проблема выделения ресурсов клиент-сервиса RADIUS.
RADIUS	RADIUS: Could not allocate requestInfo	Проблема выделения ресурсов клиент-сервиса RADIUS.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Ошибка при попытке прочесть данные с сервера RADIUS.
RADIUS	RADIUS: Accounting-Response failed to validate, id = xxx	Клиентом RADIUS получено недействительное сообщение с сервера.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	Получен непредвиденный вызов для сконфигурированного пользователя.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Проблема выделения ресурсов клиент-сервиса RADIUS.
RADIUS	RADIUS: Access-Challenge failed to validate, id = xxx	Клиентом RADIUS получено недействительное сообщение с сервера.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	Клиентом RADIUS получено недействительное сообщение с сервера.
RADIUS	RADIUS: Access-Accept failed to validate, id = xxx	Клиентом RADIUS получено недействительное сообщение с сервера.
RADIUS	RADIUS: Invalid packet length – xxx	Клиентом RADIUS получено недействительное сообщение с сервера.
RADIUS	RADIUS: Response is missing Message-Authenticator, id = xxx	Клиентом RADIUS получено недействительное сообщение с сервера.
RADIUS	RADIUS: Server address doesn't match configured server	Клиентом RADIUS получен ответ с не сконфигурированного сервера.

Системные сообщения TACACS+

Компонент	*Сообщение*	*Причина*
TACACS+	TACACS+: authentication error, no server to contact	Требуется запрос TACACS+, но нет сконфигурированных серверов.
TACACS+	TACACS+: connection failed to server x.x.x.x	Не получено ответа на запрос TACACS+, отправленный на сервер x.x.x.x.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	Не сконфигурирован ключ для заданного сервера.
TACACS+	TACACS+: received invalid packet type from server	Тип полученного пакета не поддерживается.
TACACS+	TACACS+: invalid major version in received packet	Несоответствие старшей версии.
TACACS+	TACACS+: invalid minor version in received packet	Несоответствие младшей версии.

Системное сообщение LLDP

Компонент	*Сообщение*	*Причина*
LLDP	lldpTask(): invalid message type:xx.xxxxxx:xx	Получен неподдерживаемый пакет LLDP.

Системное сообщение SNTP

Компонент	*Сообщение*	*Причина*
SNTP	SNTP: system clock synchronized on %s UTC	Протокол SNTP успешно синхронизирован со временем модуля сервера.

Системные сообщения клиента DHCPv6

Компонент	*Сообщение*	*Причина*
DHCP6 Client	ip6Map dhcp add failed.	Сбой обновления IP-адреса, арендованного DHCP, для IP6Map.
DHCP6 Client	osapiNetAddrV6Add failed on interface xxx	Сбой обновления IP-адреса, арендованного DHCP, для IP-стека (IP Stack) ядра.
DHCP6 Client	Failed to add DNS Server xxx to DNS Client	Сбой обновления адреса сервера DNS6 Server, сообщенного сервером DHCPv6 Server клиенту DNS6 Client.
DHCP6 Client	Failed to add Domain name xxx to DNS Client	Сбой обновления информации об имени домена DNS6 Domain, предоставленной сервером DHCPv6 Server клиенту DNS6 Client.

Системные сообщения клиента DHCPv4

Компонент	*Сообщение*	*Причина*
DHCP4 Client	Unsupported subOption (xxx) in Vendor Specific Option in received DHCP pkt	Получено сообщение DHCP-сервера с неподдерживаемой опцией производителя (Vendor Option).
DHCP4 Client	Failed to acquire an IP address on xxx; DHCP Server did not respond	Сбой аренды DHCP-клиентом IP-адреса, полученного с DHCP-сервера.
DHCP4 Client	DNS name server entry add failed	Сбой обновления информации по серверу имени домена DNS, полученной клиентом DNS от сервера DHCP.
DHCP4 Client	DNS domain name list entry addition failed	Сбой обновления информации о списке имен доменов DNS, полученной клиентом DNS от сервера DHCP.
DHCP4 Client	Interface xxx Link State is Down. Connect the port and try again.	При конфигурации сетевого протокола с DHCP отсутствуют активные каналы связи в управляющей VLAN.

16.3 Управление

Системное сообщение SNMP

Компонент	*Сообщение*	*Причина*
SNMP	EDB Callback: Unit Join: x	К стеку присоединено новое устройство.

Системные сообщения EmWeb

Компонент	*Сообщение*	*Причина*
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	Попытка установить соединение через telnet при достигнутом максимуме активных сессий telnet.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	Попытка установить соединение через SSH при достигнутом максимуме активных сессий SSH.
EmWeb	Handle table overflow	Соединение невозможно, все доступные дескрипторы соединений EmWeb уже используются.
EmWeb	*ConnectionType EmWeb socket accept() failed: errno*	Сокет не подходит заданному типу соединения.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection	Сбой получения сокета.
EmWeb	EmWeb: connection allocation failed	Сбой выделения памяти для нового соединения.
EmWeb	EMWEB TransmitPending: EWOULDBLOCK error sending data	Ошибка сокета при отправлении данных.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	Недопустимый индекс-дескриптор EmWeb.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	Достигнут лимит буфера приема. Неверный запрос или DoS-атака.
EmWeb	EmWeb accept: XXXX	Сбой функции доступа для нового соединения SSH. XXXX – информация об ошибке.

Системные сообщения CLI_UTIL

Компонент	*Сообщение*	*Причина*
CLI_UTIL	Telnet Send Failed errno = 0x%x	Не удалось отправить текстовую строку клиенту telnet.
CLI_UTIL	osapiFsDir failed	Не удалось получить информацию о каталоге из каталога тома.

Системные сообщения WEB

Компонент	*Сообщение*	*Причина*
Web	Max clients exceeded	Превышено максимальное количество соединений java-клиентов с коммутатором.
Web	Error on send to sockfd XXXX, closing connection	Не удалось отправить данные java-клиентам через данный сокет.
Web	# (XXXX) Form Submission Failed. No Action Taken.	Не удалось представить форму, действий не предпринято. XXXX – имя файла.
Web	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Неизвестная ошибка при загрузке файла с web-интерфейса через протокол TFTP.
Web	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Неизвестная ошибка при выгрузке файла с web-интерфейса через протокол TFTP.
Web	Web UI Screen with unspecified access attempted to be brought up	Не удалось получить дескриптор авторизации приложения для

		EmWeb/Server в ewsAuthRegister(). Заданная web-страница будет выведена в режиме «только для чтения».

Системные сообщения CLI_WEB_MGR

Компонент	*Сообщение*	*Причина*
CLI_WEB_MGR	File size is greater than 2K	Размер файла баннера превышает 2 килобайта.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	Количество строк превышает допустимый максимум.

Системные сообщения SSHD

Компонент	*Сообщение*	*Причина*
SSHD	SSHD: Unable to create the global (data) semaphore	Не удалось создать семафор для защиты глобальных данных.
SSHD	SSHD: Msg Queue is full, event = XXXX	Не удалось отправить сообщение события XXXX в очередь сообщений SSHD, очередь сообщений заполнена.
SSHD	SSHD: Unknown UI event in message, event = XXXX	Не удалось скоординировать сообщение UI с подходящей функцией SSHD, событие XXXX недопустимо.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd	Не удалось отправить сообщение в очередь сообщений SSHD.

Системные сообщения SSLT

Компонент	*Сообщение*	*Причина*
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Превышен максимум разрешенных соединений SSLT.
SSLT	SSLT: Error creating Secure server socket6	Не удалось создать сокет защищенного сервера для IPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Не удалось открыть соединения с незащищенным сервером. XXXX – адрес сокета незащищенного сервера. YYYY – результат, возвращенный при попытке соединения. ZZZZ – код ошибки.
SSLT	SSLT: Msg Queue is full, event = XXXX	Не удалось отправить полученное сообщение в очередь сообщений SSLT, очередь заполнена. XXXX – событие.
SSLT	SSLT: Unknown UI event in message, event = XXXX	Не удалось скоординировать сообщение пользовательского интерфейса (UI) с подходящей функцией SSLT, событие XXXX недопустимо.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd	Не удалось отправить сообщение в очередь сообщений SSLT.
SSLT	SSLT: Error loading certificate from file XXXX	Не удалось загрузить сертификат SSL из файла XXXX.
SSLT	SSLT: Error loading private key from file	Не удалось загрузить приватный ключ для соединения SSL.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Ошибка настройки списка шифров.

SSLT	SSLT: Could not delete the SSL semaphores	Не удалось удалить SSL семафоры при очистке всех ресурсов семафоров OpenSSL Locking.

Системные сообщения User_Manager

Компонент	*Сообщение*	*Причина*
User_Manager	User Login Failed for XXXX	Не удалось аутентифицировать пользователя при авторизации. XXXX – имя пользователя.
User_Manager	Access level for user XXXX could not be determined. Setting to Level 1	Недопустимый уровень доступа для пользователя. Установлен на уровень 1. XXXX – имя пользователя.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults	Не удалось перевести файл конфигурации. XXXX – имя файла конфигурации. YYYY – номер старой версии, ZZZZ – номер новой версии.

16.4 Коммутация

Системные сообщения защищенных портов (Protected Ports)

Компонент	*Сообщение*	*Причина*
Protected Ports	Protected Port: failed to save configuration	Невозможно сохранить конфигурацию защищенного порта.
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protected Port	Сбой protectedPortCfgRWLock
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	Сбой nimRegisterIntfChange для VLAN.
Protected Ports	Cannot add interface xxx to group yyy	Невозможно добавить интерфейс в заданную группу.
Protected Ports	unable to set protected port group	Сбой вызова DTL на добавление маски интерфейса на уровне драйвера.
Protected Ports	Cannot delete interface xxx from group yyy	Сбой вызова DTL на удаление интерфейса из группы.
Protected Ports	Cannot update group YYY after deleting interface XXX	Сбой обновления группы после удаления интерфейса.
Protected Ports	Received an interface change callback while not ready to receive it	Обратный вызов об изменении интерфейса получен до готовности компонента защищенного порта принять его.

Системные сообщения сетей VLAN IP-подсети (IP subnet VLANs)

Компонент	*Сообщение*	*Причина*
IP subnet VLANs	ERROR vlanIpSubnetSubnetValid:Invalid subnet	CLI вернул недопустимую пару подсети и сетевой маски.
IP subnet VLANs	IP Subnet Vlans: failed to save configuration	Не удалось сохранить конфигурацию vlan подсети.
IP subnet VLANs	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	Сбой создания блокировки чтения-записи.

IP subnet VLANs	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	Невозможно зарегистрировать данный компонент в уведомлениях об изменении vlan.
IP subnet VLANs	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	Сбой удаления семафора данного компонента.
IP subnet VLANs	vlanIpSubnetDtlVlanCreate: Failed	Вызову DTL не удалось добавить запись в таблицу.
IP subnet VLANs	vlanIpSubnetSubnetDeleteApply: Failed	DTL не удалось удалить запись из таблицы.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	DTL не удалось добавить запись для события уведомления о добавлении vlan.
IP subnet VLANs	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	DTL не удалось удалить запись для события уведомления об удалении vlan.

Системные сообщения сетей VLAN с MAC-адресацией (MAC based VLANs)

Компонент	*Сообщение*	*Причина*
MAC based VLANs	MAC VLANs: Failed to save configuration	Не удалось сохранить конфигурацию vlan с MAC-адресацией.
MAC based VLANs	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	Сбой создания блокировки чтения-записи.
MAC based VLANs	Unable to register for VLAN change callback	Невозможно зарегистрировать данный компонент в уведомлениях об изменении vlan.
MAC based VLANs	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	Сбой удаления семафора данного компонента.
MAC based VLANs	vlanMacAddApply: Failed to add an entry	DTL не удалось добавить запись в таблицу.
MAC based VLANs	vlanMacDeleteApply: Unable to delete an Entry	DTL не удалось удалить запись из таблицы.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to add an entry	DTL не удалось добавить запись для события уведомления о добавлении vlan.
MAC based VLANs	vlanMacVlanChangeCallback: Failed to delete an entry	DTL не удалось удалить запись для события уведомления об удалении vlan.

Системные сообщения 802.1X

Компонент	*Сообщение*	*Причина*
802.1X	*function*: Failed calling dot1xIssueCmd	Очередь сообщений 802.1X переполнена.
802.1X	*function:* EAP message not received from server	Сервер RADIUS не отправил требуемое сообщение EAP.
802.1X	*function*: Out of System buffers	802.1X не может обработать/передать сообщение, недостаток внутренних буферов.
802.1X	*function*: could not set state to *authorized/unauthorized*, intf xxx	Сбой вызова DTL при определении состояния авторизации порта.
802.1X	dot1xApplyConfigData: Unable to *enable/disable* dot1x in driver	Сбой DTL при включении/отключении 802.1X.
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Сбой отправки сообщения на сервер RADIUS.

802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex = xxx	Не удалось отправить начало учета на сервер RADIUS.
802.1X	*function*: failed sending terminate cause, intf xxx	Не удалось отправить окончание учета на сервер RADIUS.

Системные сообщения IGMP Snooping

Компонент	*Сообщение*	*Причина*
IGMP Snooping	*function*: osapiMessageSend failed	Очередь сообщений IGMP Snooping переполнена.
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Не удалось установить режим глобального IGMP-отслеживания (IGMP Snooping), очередь сообщений переполнена.
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Не удалось установить режим IGMP Snooping для интерфейса, очередь сообщений переполнена.
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Не удалось установить режим многоадресного ретранслятора интерфейса, очередь сообщений IGMP-отслеживания переполнена.
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Не удалось установить режим VLAN IGM Snooping , очередь сообщений переполнена.
IGMP Snooping	Failed to set igmp mrouter mode%d for interface xxx on Vlan yyy	Не удалось установить режим многоадресного ретранслятора VLAN, очередь сообщений IGMP-отслеживания переполнена.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Невозможно выделить буферы для IGMP-пакетов малого размера.
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Невозможно выделить буферы для IGMP-пакетов большого размера.

Системные сообщения GARP/GVRP/GMRP

Компонент	*Сообщение*	*Причина*
GARP/GVRP/GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	Очередь garpQueue переполнена сообщениями (номера внутренних интерфейсов, типы сообщений и др.).
GARP/GVRP/GMRP	GarpSendPDU: QUEUE SEND FAILURE	Очередь garpPduQueue переполнена сообщениями (GPDU, номера внутренних интерфейсов, vlan id, дескрипторы буферов и др.).
GARP/GVRP/GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	Отсутствует конфигурация по умолчанию для данного интерфейса. Вероятно, создан новый интерфейс, не имеющий предварительной конфигурации.
GARP/GVRP/GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Отслеживание состояния очереди сообщений, определение нагрузки на GARP.
GARP/GVRP/GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Несовпадение gmd (базы данных GMRP) и MFDB.
GARP/GVRP/GMRP	gmd_create_entry**:** GMRP failure adding	Таблица MFDB переполнена.

	MFDB entry: vlan %d and address %s	

Системные сообщения 802.3ad

Компонент	*Сообщение*	*Причина*
802.3ad	dot3adReceiveMachine: received default event %x	LAG PDU получен с задержкой, приемное устройство RX игнорирует данный LAGPDU.
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	Событие, отправленное на NIM, не было успешно завершено.

Системное сообщение FDB

Компонент	*Сообщение*	*Причина*
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Невозможно установить лимит жизни на уровне аппаратного обеспечения.

Системное сообщение тега Double VLAN

Компонент	*Сообщение*	*Причина*
Double VLAN Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	Отсутствует конфигурация по умолчанию для данного интерфейса. Вероятно, создан новый интерфейс, не имеющий предварительной конфигурации.

Системное сообщение инициализации IPv6 (IPv6 Provisioning)

Компонент	*Сообщение*	*Причина*
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	Отсутствует конфигурация по умолчанию для данного интерфейса. Вероятно, создан новый интерфейс, не имеющий предварительной конфигурации.

Системные сообщения MFDB

Компонент	*Сообщение*	*Причина*
MFDB	mfdbTreeEntryUpdate: entry does not exist	Попытка обновить несуществующую запись.

Системные сообщения 802.1Q

Компонент	*Сообщение*	*Причина*
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	Очередь dot1qMsgQueue переполнена.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range	Использован зарезервированный идентификатор vlan.
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	Отсутствует конфигурация по умолчанию для данного интерфейса. Вероятно, создан новый интерфейс, не имеющий предварительной конфигурации.

802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Очистка Vlan и конфигурации.
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	Если информация о данной сети vlan получена через GVRP, управление членством в ней недоступно.
802.1Q	dtl failure when adding ports to vlan id %d - portMask = %s	Не удалось добавить порты в запись VLAN на уровне аппаратного обеспечения.
802.1Q	dtl failure when deleting ports from vlan id %d - portMask = %s	Не удалось удалить порты в запись VLAN на уровне аппаратного обеспечения.
802.1Q	dtl failure when adding ports to tagged list for vlan id %d - portMask = %s	Не удалось добавить порт в список с теговой организацией на уровне аппаратного обеспечения.
802.1Q	dtl failure when deleting ports from tagged list for vlan id %d - portMask = %s"	Не удалось удалить порт из списка с теговой организацией на уровне аппаратного обеспечения.
802.1Q	dot1qTask: unsuccessful return code on receive from dot1qMsgQueue: %08x"	Не удалось получить сообщение dot1q от очереди сообщений dot1q.
802.1Q	Unable to apply VLAN creation request for VLAN ID %d, Database reached MAX VLAN count!	Не удалось создать идентификатор VLAN, база данных VLAN переполнена.
802.1Q	Attempt to create a vlan (%d) that already exists	Создание уже существующего динамического идентификатора VLAN.
802.1Q	DTL call to create VLAN %d failed with rc %d"	Не удалось создать идентификатор сети VLAN на уровне аппаратного обеспечения.
802.1Q	Problem unrolling data for VLAN %d	Не удалось удалить VLAN из базы данных после сбоя создания VLAN на уровне аппаратного обеспечения.
802.1Q	VLan %d does not exist	Не удалось удалить запись VLAN.
802.1Q	VLan %d requestor type %d does not exist	Не удалось удалить динамический идентификатор сети VLAN, недопустимый запросчик.
802.1Q	Can not delete the VLAN, Some unknown component has taken the ownership!	Не удалось удалить сеть, ресурс используется неизвестным компонентом.
802.1Q	Not valid permission to delete the VLAN %d requestor %d	Не удалось удалить идентификатор VLAN, несовпадение запросчика и состояния записи VLAN.
802.1Q	VLAN Delete Call failed in driver for vlan %d	Не удалось удалить VLAN с аппаратного обеспечения.
802.1Q	Problem deleting data for VLAN %d	Не удалось удалить идентификатор VLAN из базы данных VLAN.
802.1Q	Dynamic entry %d can only be modified after it is converted to static	Не удалось изменить фильтр групп VLAN.
802.1Q	Cannot find vlan %d to convert it to static	Не удалось сконвертировать динамическую сеть VLAN в статичную VLAN. Отсутствует VLAN.
802.1Q	Only Dynamically created VLANs can be converted	Ошибка при попытке конвертации статически созданной VLAN в статич-
802.1Q	Cannot modify tagging of interface %s to non existence vlan %d"	Ошибка при попытке данного интерфейса установить теги для всех сетей VLAN в маске vlan.

802.1Q	Error in updating data for VLAN %d in VLAN database	Не удалось добавить запись VLAN в базу данных VLAN
802.1Q	DTL call to create VLAN %d failed with rc %d	Не удалось создать запись VLAN на уровне аппаратного обеспечения.
802.1Q	Not valid permission to delete the VLAN %d	Не удалось удалить статичный VLAN ID. Недопустимый запрос.
802.1Q	Attempt to set access vlan with an invalid vlan id %d	Недопустимый идентификатор VLAN.
802.1Q	Attempt to set access vlan with (%d) that does not exist	Отсутствует идентификатор VLAN.
802.1Q	VLAN create currently underway for VLAN ID %d	Попытка создания VLAN, уже находящейся в процессе создания.
802.1Q	VLAN ID %d is already exists as static VLAN	Попытка создания уже существующей статичной VLAN.
802.1Q	Cannot put a message on dot1q msg Queue, Returns:%d	Не удалось отправить сообщение Dot1q в очередь сообщений Dot1q.
802.1Q	Invalid dot1q Interface: %s	Не удалось добавить VLAN к элементу порта.
802.1Q	Cannot set membership for user interface %s on management vlan %d	Не удалось добавить VLAN к элементу порта.
802.1Q	Incorrect tagmode for vlan tagging. tagmode: %d Interface: %s	Неверный режим тегирования VLAN.
802.1Q	Cannot set tagging for interface %d on non existent VLAN %d"	Отсутствует идентификатор VLAN.
802.1Q	Cannot set tagging for interface %d which is not a member of VLAN %d	Сбой в настройке конфигурации тегирования для интерфейса в диапазоне VLAN
802.1Q	VLAN create currently underway for VLAN ID %d"	Попытка создания идентификатора VLAN, уже находящегося в процессе
802.1Q	VLAN ID %d already exists	Попытка создания уже существующей VLAN.
802.1Q	Failed to delete, Default VLAN %d cannot be deleted	Попытка удаления VLAN по умолчанию.
802.1Q	Failed to delete, VLAN ID %d is not a static VLAN	Попытка удаления динамической VLAN из CLI.
802.1Q	Requestor %d attempted to release internal VLAN %d: owned by %d	-

Системные сообщения 802.1S

Компонент	***Сообщение***	***Причина***
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	Очередь сообщений переполнена.

Системные сообщения 802.1S

Компонент	***Сообщение***	***Причина***
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	Невозможно обработать BPDU в текущих условиях (запрещен порт или не завершена обработка предыдущего BPDU на том же интерфейсе.
802.1S	dot1sBpduTransmit(): could not get a buffer	Превышение ресурса системных буферов.

Системное сообщение блокировки портов по MAC-адресам (Port Mac Locking)

Компонент	*Сообщение*	*Причина*
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	Отсутствует конфигурация по умолчанию для данного интерфейса. Вероятно, создан новый интерфейс, не имеющий предварительной конфигурации.

Системные сообщения сетей VLAN на основе протоколов (Protocol-based VLANs)

Компонент	*Сообщение*	*Причина*
Protocol based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Сбой при попытке nimRegisterIntfChange зарегистрировать pbVlan для изменений состояния канала связи.
Protocol based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with VLANs	Сбой при попытке VLANRegisterForChange зарегистрировать обратный вызов pbVlan для изменений VLAN.
Protocol based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Сбой при попытке nvStoreRegister зарегистрировать функции сохранения и восстановления для сохранения конфигурации.

16.5 Качество обслуживания

Системные сообщения ACL

Компонент	*Сообщение*	*Причина*
ACL	Total number of ACL rules (x) exceeds max (y) on intf i	Количество требуемых правил, порождаемых совокупностью всех ACL, применяемых к интерфейсу, превосходит возможности платформы.
ACL	ACL *name*, rule *x*: This rule is not being logged	В результате конфигурирования ACL требуется зарегистрировать больше правил, чем позволяет платформа. За исключением регистрации заданное правило выполняется в полном объеме.
ACL	aclLogTask: error logging ACL rule trap for correlator *number*	Система не может отправить трап SNMP с атрибутом записи для данного правила ACL.
ACL	IP ACL *number*: Forced truncation of one or more rules during config migration	При обработке сохраненной конфигурации система столкнулась с ACL, содержащим большее количество правил, чем поддерживается текущей версией. Возможная причина: программный код обновлен до версии, поддерживающей меньшее количество процедур, чем предыдущая версия.

Системное сообщение CoS

Компонент	*Сообщение*	*Причина*
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	Компоненту COS не удалось применить сохраненную конфигурацию, использованы заводские настройки.

Системные сообщения DiffServ

Компонент	*Сообщение*	*Причина*
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	Не удалось очистить текущую конфигурацию: ошибка очистки текущих настроек. Это может привести к нестабильной работе системы, рекомендуется переустановка.
DiffServ	Policy invalid for service intf: policy *name*, interface *x*, direction *y*	Определение политики DiffServ несопоставимо с возможностями заданного интерфейса. Для получения информации об ограничениях конфигурации ознакомьтесь с примечанием к версии платформы.

16.6 Маршрутизация/Маршрутизация IPv6

Системные сообщения ретрансляции DHCP (DHCP Relay)

Компонент	*Сообщение*	*Причина*
DHCP Relay	REQUEST hops field more than config value	Агент DHCP Relay обработал DHCP-запрос со значением поля пересылок (HOPS), превышающим сконфигурированное максимальное значение. Агент не будет отправлять сообщение со значением счетчика пересылок, превышающим 4.
DHCP Relay	Request's seconds field less than the config value	Агент DHCP Relay обработал DHCP-запрос со значением поля секунд (SECS), превышающим сконфигурированный минимум разрешенного времени ожидания.
DHCP Relay	processDhcpPacket: invalid DHCP packet type: %u\n	Агент DHCP Relay обработал недопустимый DHCP-пакет. Такие пакеты отвергаются агентом.

Системные сообщения OSPFv2

Компонент	*Сообщение*	*Причина*
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 регистрируется в менеджере таблицы маршрутизации IPv4 (RTO) для получения уведомлений об изменениях наилучшего маршрута. Если OSPFv2 пытается сняться с учета более одного раза, происходит сбой второго снятия. Сбой безвреден.

OSPFv2	XX_Call() failure in _checkTimers for thread 0x869bcc0	Таймер OSPFv2 сработал, но очередь сообщений для данного события переполнена. Критическая ошибка.
OSPFv2	Warning: OSPF LSDB is 90% full (22648 LSAs).	OSPFv2 ограничивает количество LSA (Link State Advertisements), хранимых в LSDB (Link State Database). При степени заполнения базы данных свыше 90 или 95 процентов OSPFv2 выводит данное предупреждение. Текущий объем базы данных указан в предупреждении.
OSPFv2	The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation	Данное сообщение выводится OSPFv2 при заполнении базы данных OSPFv2 LSDB. OSPFv2 повторно запускает LSA маршрутизатора с максимальной метрикой всех неответвленных каналов связи, чтобы другие маршрутизаторы рассчитали пути в обход перегруженного маршрутизатора.
OSPFv2	Dropping the DD packet because of MTU mismatch	OSPFv2 игнорирует DD-пакеты (Database Description packets) с максимальным размером MTU, превышающим IP MTU на интерфейсе, где был получен DD-пакет.
OSPFv2	LSA Checksum error in LsUpdate, dropping LSID 1.2.3.4 checksum 0x1234.	OSPFv2 игнорирует полученное LSA с неверной контрольной суммой.

Системные сообщения OSPFv3

Компонент	*Сообщение*	*Причина*
OSPFv3	Best route client deregistration failed for OSPFv3 Redist	OSPFv3 регистрируется в менеджере таблицы маршрутизации IPv6 (RTO6) для получения уведомлений об изменениях наилучшего маршрута. Если OSPFv3 пытается сняться с учета более одного раза, происходит сбой второго снятия. Сбой безвреден.
OSPFv3	Warning: OSPF LSDB is 90% full (15292 LSAs)	OSPFv3 ограничивает количество LSA (Link State Advertisements), хранимых в базе LSDB (Link State Database). При степени заполнения базы данных свыше 90 или 95 процентов OSPFv3 выводит данное предупреждение. Текущий объем базы данных указан в предупреждении.
OSPFv3	The number of LSAs, 16992, in the OSPF LSDB has exceeded the LSDB memory allocation.	Данное сообщение выводится OSPFv3 при заполнении базы данных OSPFv3 LSDB. OSPFv3 повторно запускает LSA маршрутизатора с R-битом, указывающим на перегрузку маршрутизатора.
OSPFv3	LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	OSPFv3 периодически сверяет контрольную сумму каждого LSA с

		памятью. При несовпадении OSPFv3 выводит данное сообщение.

Системные сообщения менеджера таблицы маршрутизации (RTO)

Компонент	*Сообщение*	*Причина*
RTO	RTO is no longer full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes.	Если количество наилучших маршрутов падает ниже полного объема, RTO выводит данное уведомление. Количество неудачных добавлений может содержать указание на количество добавлений маршрутов, неудавшихся из-за того, что таблица была заполнена, но на рост данного показателя могут влиять и другие причины.
RTO	RTO is full. Routing table contains xxx best routes, xxx total routes, xxx reserved local routes. The routing table manager stores a limited number of best routes. The count of total routes includes alternate routes, which are not installed in hardware.	Менеджер таблицы маршрутизации (“RTO”) хранит ограниченное количество наилучших маршрутов, основанное на возможностях аппаратного обеспечения. RTO выводит данное предупреждение при заполнении таблицы маршрутизации. Счетчик общего количества маршрутов включает альтернативные маршруты, не прописанные на аппаратном уровне.

Системные сообщения VRRP

Компонент	*Сообщение*	*Причина*
VRRP	VRRP packet of size xxx dropped. Min VRRP packet size is xxx; Max VRRP packet size is xxx.	Лавинообразное распространение VRRP-сообщений в данной сети.
VRRP	VR xxx on interface xxx started as xxx	Виртуальный маршрутизатор запустился как главный (Master) или резервный (Backup).
VRRP	This router is the IP address owner for virtual router xxx on interface xxx. Setting the virtual router priority to xxx.	Обновление принадлежности адреса для заданного VR. Если данному маршрутизатору принадлежит адрес VR, приоритет VR устанавливается на максимум (согласно стандарту RFC 3768). Если адрес более не принадлежит маршрутизатору, приоритет обнуляется.

Системное сообщение ARP

Компонент	*Сообщение*	*Причина*
ARP	IP address conflict on interface xxx for IP address yyy. Conflicting host MAC address is zzz.	Обнаружен конфликт адреса на коммутаторе во время принятия ARP-пакета от другого хоста или маршрутизатора.

Системное сообщение RIP

Компонент	*Сообщение*	*Причина*
RIP	RIP: discard response from xxx via unexpected interface	Ответ RIP получен с исходным адресом, не совпадающим с подсетью исходящего интерфейса.

16.7 Многоадресная рассылка

Системные сообщения IGMP/MLD

Компонент	*Сообщение*	*Причина*
IGMP/MLD	MGMD Protocol Heap Memory Init Failed; Family – xxx.	Сбой инициализации динамической памяти MGMD (MGMD Heap memory) для семейства с заданным адресом. Сообщение выводится при попытке запуска MGMD.
IGMP/MLD	MGMD Protocol Heap Memory De-Init Failed; Family – xxx.	Сбой деинициализации динамической памяти MGMD (MGMD Heap memory) для семейства с заданным адресом. Сообщение выводится при попытке отключения MGMD (IGMP/MLD). Последующие попытки запуска/отключения MGMD также вернут ошибку.
IGMP/MLD	MGMD Protocol Initialization Failed; Family – xxx.	Сбой последовательности инициализации протокола MGMD. Может быть вызвано недоступностью ресурсов. Сообщение выводится при попытке запуска MGMD.
IGMP/MLD	MGMD All Routers Address - xxx Set to the DTL Mcast List Failed; Mode – xxx, intf – xxx	Сообщение выводится при попытке запуска MGMD.
IGMP/MLD	MGMD All Routers Address - xxx Add to the DTL Mcast List Failed.	Не удалось добавить MGMD All Routers Address в локальный список многоадресного вещания. Многоадресные MGMD-пакеты не будут приниматься приложением.
IGMP/MLD	MGMD All Routers Address – xxx Delete from the DTL Mcast List Failed	Не удалось удалить MGMD All Routers Address из локального списка многоадресного вещания. Многоадресные MGMD-пакеты по-прежнему будут приниматься приложением, несмотря на то, что MGMD отключен.
IGMP/MLD	MLDv2 GroupAddr-[FF02::16] Enable with Interpeak Stack Failed; rtrIfNum - xxx, intf – xxx.	Не удалось зарегистрировать адрес группы (Group Address) в межпиковом стеке (Interpeak stack). Пакеты MLDv2 не будут приниматься приложением.
IGMP/MLD	MGMD Group Entry Creation Failed; grpAddr - xxx, rtrIfNum – xxx.	Не удалось зарегистрировать заданный групповой адрес (Group Address) на заданном интерфейсе маршрутизатора.
IGMP/MLD	MGMD Socket Creation/Initialization Failed for addrFamily – xxx.	Не удалось создать/инициализировать сокет MGMD (сбой MGMD Socket Creation/options Set).

		Контрольные MGMD-пакеты не могут быть отправлены интерфейсом.

16.8 Стекирование

Системное сообщение EDB

Компонент	*Сообщение*	*Причина*
EDB	EDB Callback: Unit Join: *num*.	Устройство *num* присоединилось к стеку.

16.9 Технологии

Сообщения об ошибках

Компонент	*Сообщение*	*Причина*
Broadcom	Invalid USP unit = x, slot = x, port = x	Не удалось преобразовать порт во время приема.
Broadcom	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Не удалось добавить адрес 2-го уровня (L2) в таблицу MAC-адресов. Причины: хэш-коллизия или переполненная таблица.
Broadcom	Failed installing mirror action - rest of the policy applied successfully	Ранее сконфигурированный тестовый порт не используется в данной политике. В примечании к версии указано, что может быть сконфигурирован только один тестовый порт.
Broadcom	Policy x does not contain rule x	Процедура не была включена в политику из-за превышения количества процедур для данной политики. Также сообщение может выводиться при модификации старой процедуры, не входящей в политику.
Broadcom	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x	Возможно дублирование хэша, не удалось установить политику.
Broadcom	ACL x not found in internal table	Попытка удаления несуществующего списка ACL.
Broadcom	ACL internal table overflow	Попытка добавить ACL в переполненную таблицу.
Broadcom	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Попытка сконфигурировать неподдерживаемую ширину полосы пропускания.
Broadcom	USL: failed to put sync response on queue	Ответ на запрос sync не был поставлен в очередь. Возможно, предыдущий запрос был получен с запаздыванием.
Broadcom	USL: failed to sync ipmc table on unit = x	Сбой передачи или потеря сообщения.
Broadcom	usl_task_ipmc_msg_send(): failed to send with x	Сбой передачи или потеря сообщения.
Broadcom	USL: No available entries in the STG table	Таблица групп STG USL переполнена.
Broadcom	USL: failed to sync stg table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены

Broadcom	USL: A Trunk doesn't exist in USL	Попытка модификации отсутствующей магистрали.
Broadcom	USL: A Trunk being created by bcmx already existed in USL	Возможна проблема синхронизации приложения, аппаратного обеспечения и уровня синхронизации.
Broadcom	USL: A Trunk being destroyed doesn't exist in USL	Возможна проблема синхронизации приложения, аппаратного обеспечения и уровня синхронизации.
Broadcom	USL: A Trunk being set doesn't exist in USL	Возможна проблема синхронизации приложения, аппаратного обеспечения и уровня синхронизации.
Broadcom	USL: failed to sync trunk table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.
Broadcom	USL: Mcast entry not found on a join	Возможна проблема синхронизации приложения, аппаратного обеспечения и уровня синхронизации.
Broadcom	USL: Mcast entry not found on a leave	Возможна проблема синхронизации приложения, аппаратного обеспечения и уровня синхронизации.
Broadcom	USL: failed to sync dVLAN data on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.
Broadcom	USL: failed to sync policy table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.
Broadcom	USL: failed to sync VLAN table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.
Broadcom	Invalid LAG id x	Вероятно, проблема синхронизации драйвера BCM и HAPI.
Broadcom	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Преобразователь портов (Uport) недопустим для драйвера BCM.
Broadcom	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	Невозможно считать USP с события для драйвера BCM.
Broadcom	Unable to insert route R/P	Маршрут R с префиксом P не может быть введен в таблицу маршрутов аппаратного обеспечения. Последует повторная попытка.
Broadcom	Unable to Insert host H	Хост H не может быть введен в таблицу хостов аппаратного обеспечения. Последует повторная попытка.
Broadcom	USL: failed to sync L3 Intf table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.
Broadcom	USL: failed to sync L3 Host table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.
Broadcom	USL: failed to sync L3 Route table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.

Broadcom	USL: failed to sync initiator table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены
Broadcom	USL: failed to sync terminator table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.
Broadcom	USL: failed to sync ip-multicast table on unit = x	Не удалось синхронизировать устройство x: сбой передачи или API на удаленном устройстве. Попытки синхронизации будут продолжены.

16.10 Поддержка ОС

Системное сообщение Linux BSP

Компонент	*Сообщение*	*Причина*
Linux BSP	rc = 10	Второе сообщение, регистрируемое при загрузке ОС, сразу после *Starting code…. Always (Запуск кода… Без изменений)*.

Системные сообщения OSAPI Linux

Компонент	*Сообщение*	*Причина*
OSAPI Linux	osapiNetLinkNeighDump: could not open socket! - or – ipstkNdpFlush: could not open socket! – or – osapiNetlinkDumpOpen: unable to bind socket! errno = XX	Невозможно открыть сокет NetLink®. Убедитесь, что “Поддержка ARP-демона ” (CONFIG_ARPD) разрешена для ядра Linux, если не используется двоичная система обращения к ядру.
OSAPI Linux	ipstkNdpFlush: sending delete failed	Сбой команды ядру на удаление точки входа из таблицы соседей (некорректное сообщение).
OSAPI Linux	unable to open /proc/net/ipv6/conf/default/hop_limit	Объекты IPv6 MIB прочитаны, но не установлена файловая система /proc либо действующее ядро не поддерживает IPV6.
OSAPI Linux	osapimRouteEntryAdd, errno XX adding 0xYY to ZZ – or – osapimRouteEntryDelete, errno XX deleting 0xYY from ZZ	Ошибка при добавлении или удалении маршрута IPv4 (указан в шестнадцатеричном формате как YY), на данном интерфейсе ZZ с установленной ОС Linux. Код ошибки содержится в errno.h.
OSAPI Linux	l3intfAddRoute: Failed to Add Route – or – l3intfDeleteRoute: Failed to Delete Route	Ошибка при создании или удалении шлюза по умолчанию в/из таблицы маршрутизации ядра (функция osapiRawMRouteAdd()/Delete()).
OSAPI Linux	osapiNetIfConfig: ioctl on XX failed: addr: 0xYY, err: ZZ – or – osapiNetIPSet: ioctl on XX failed: addr: 0x%YY	Сбой при попытке присвоения IP-адреса (в шестнадцатеричном формате как YY) интерфейсу с установленной ОС Linux, данный интерфейс отсутствует. Иногда эта ошибка безвредна для работы системы (к примеру, попытка присвоить адрес 0 во время обработки протоколом DHCP

		сетевого порта (dtl0) при начальной загрузке до создания тест-порта).
OSAPI Linux	ping: sendto error	Проблема при отправке с пользовательского интерфейса пакета эхо-запроса ICMP при выполнении команды ping. Возможно, отсутствует маршрут к данной сети
OSAPI Linux	Failed to Create Interface	Недостаточно памяти, идет инициализация системы.
OSAPI Linux	TAP Unable to open XX	Отсутствует файл /dev/tap или, если не используется двоичная система обращения к ядру, у ядра отсутствует “Поддержка универсального драйвера устройств TUN/TAP” (CONFIG_TUN).
OSAPI Linux	Tap monitor task is spinning on select failures – then – Tap monitor select failed: XX.	Проблема чтения устройства /dev/tap: ознакомьтесь с сообщением ошибки XX для получения дополнительной информации.
OSAPI Linux	Log_Init: log file error - creating new log file	Во флеш-памяти отсутствует файл “event log” во флеш-памяти, либо его контрольная сумма неверна.
OSAPI Linux	Log_Init: Flash (event) log full; erasing	Файл журнала событий был очищен во время загрузки.
OSAPI Linux	Log_Init: Corrupt event log; erasing	В файле журнала событий запись следует за «пустой» записью, сбой организации данных.
OSAPI Linux	Failed to Set Interface IP Address – or – IP Netmask – or – Broadcast Address – or – Flags – or – Hardware Address – or – Failed to Retrieve Interface Flags	Ошибка при добавлении IP- или MAC-адреса протокола VRRP интерфейсу сети Linux.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации программного обеспечения ООО «Русьтелетех» можно обращаться в Сервисный центр компании:

Российская Федерация,115419, г. Москва, ул. Орджоникидзе, дом 11, стр. 40.

Телефон: +7(495) 234-9777

E-mail: support@rusteletech.ru

Официальный сайт компании: rusteletech.ru