НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ ПОЛИГОН

450000, Россия
г.Уфа, а/я 1262
Телефон/факс: (347)-292-09-90
E-mail: info@plgn.ru
URL: www.plgn.ru

Аппаратура Акманай-2ххх

Руководство по эксплуатации. Часть II

БЛПА.465255.076РЭ1

Подп. и дат.	Инв. № дубл.	Взам. инв. №.	Подп. и дата.	Инв. № подл.

2025

Содержание

1 Введение 24
1.1 Основные характеристики коммутатора 24
1.2 Заводские настройки 26
2 Подключение к коммутатору 30
2.1 Требования к ПК 30
2.2 Порядок действий для организации управления через порт «F» 32
2.3 Порядок действий для организации управления по протоколу Telnet 33
3 Описание интерфейса командной строки 34
3.1 Использование интерфейса командной строки 34
3.2 Контекстная помощь и автодополнение команд 34
3.3 Проверка синтаксиса команд 35
3.4 Список используемых клавиш 35
3.5 Описание синтаксиса команд 36
3.6 Описание обозначений интерфейсов и портов 37
4 Управление коммутатором 38
4.1 Вывод общей информации о коммутаторе 38
4.1.1 Общие положения 38
4.1.2 show debug action 38
4.1.3 show hostname 39
4.1.4 show idprom interface 39
4.1.5 show inventory 40
4.1.6 show location 40
4.1.7 show logging 40
4.1.8 show logging boot 41
4.1.9 show terminal 41
4.1.10 show version 42
4.1.11 show system mtu 42
4.2 Управление учетными записями пользователей 43
4.2.1 Разграничение доступа 43
4.2.2 username 43
4.2.3 username sshkey 44
4.2.4 show users 44
4.2.5 show user 45
4.3 Настройка времени и даты 46
4.3.1 Общие положения 46
4.3.2 clock set 46
4.3.3 clock summer-time 47
4.3.4 clock timezone 48

4.3.5 ntp authenticate 48
4.3.6 ntp authentication-key 48
4.3.7 ntp master 49
4.3.8 ntp server 50
4.3.9 ntp trusted-key 50
4.3.10 show clock 51
4.3.11 show ntp 51
4.3.12 show ntp status 51
4.4 Настройка общих параметров 53
4.4.1 Общие положения 53
4.4.2 configure terminal 54
4.4.3 copy 54
4.4.4 clear log 56
4.4.5 clear service-log 56
4.4.6 clear debug files 56
4.4.7 clear boot log 56
4.4.8 clear ssh hosts 57
4.4.9 clear ssh host 57
4.4.10 debug action 57
4.4.11 debug core-dumps 58
4.4.12 delete 58
4.4.13 dir 59
4.4.14 mkdir 60
4.4.15 echo 60
4.4.16 end 61
4.4.17 exit 61
4.4.18 hostname 62
4.4.19 ip http server 62
4.4.20 ip http secure-server 62
4.4.21 ip telnet server 63
4.4.22 locator-led 63
4.4.23 logging host 63
4.4.24 logging console 64
4.4.25 logout 64
4.4.26 more 65
4.4.27 ntp server 65
4.4.28 ping 66
4.4.29 port jumbo-frame 66
4.4.30 reload 67
4.4.31 rename 67
4.4.32 run-script 68
4.4.33 serdes reference clock 68
4.4.34 ssh 69

4.4.35 system mtu 70
4.4.36 terminal session-timeout 70
4.4.37 terminal type 70
4.4.38 traceroute 71
4.4.39 telnet 71
4.4.40 tls config 72
4.4.41 show processes cpu history 72
4.4.42 show cpu utilization 73
4.4.43 show locator-led 73
4.4.44 show logging hosts 74
4.4.45 show port jumbo-frame 74
4.4.46 show reload 74
4.4.47 show tcp brief 75
4.4.48 show tls config 75
4.4.49 show serdes reference clock 75
4.5 Создание макрокоманд 77
4.5.1 Общие положения 77
4.5.2 macro apply 77
4.5.3 macro description 77
4.5.4 macro global 78
4.5.5 macro global description 78
4.5.6 macro name 79
4.5.7 show parser macro 79
4.5.8 show parser macro description 80
4.6 Управление конфигурациями 81
4.6.1 Наборы настроек коммутатора 81
4.6.2 boot config-file 81
4.6.3 show running-config 82
4.6.4 show startup-config 83
4.7 Сетевые настройки 84
4.7.1 Общие положения 84
4.7.2 arp 84
4.7.3 ip proxy-arp static 84
4.7.4 ip address 85
4.7.5 ip proxy-arp 86
4.7.6 ip default-gateway 86
4.7.7 ip name-server 87
4.7.8 renew dhcp 88
4.7.9 show hosts 88
4.7.10 show ip redirects 88
4.7.11 show arp 89
4.8 Настройка SSH 90

4.8.1 Общие положения 90
4.8.2 ip ssh authentication-retries 90
4.8.3 ip ssh timeout 90
4.8.4 ssh server 91
4.8.5 ssh key 91
4.8.6 show ssh 92
4.8.7 show ssh key 92
4.9 Мониторинг температуры и системы электропитания 93
4.9.1 Общие положения 93
4.9.2 system env fanspeed-control manual 93
4.9.3 show env 93
4.10 Обновление программного обеспечения 95
4.10.1 Комплекты обновления программного обеспечения 95
4.10.2 archive download-sw 95
4.10.3 archive upload-sw 96
4.10.4 boot system 98
4.10.5 show bootvar 98
4.11 Специальные команды CLI 99
4.11.1 Общие положения 99
4.11.2 clear cli history 99
4.11.3 cli alias name 99
4.11.4 cli var name 100
4.11.5 show cli alias 100
4.11.6 show cli history 100
4.11.7 show cli variables 101
4.12 Автоматизация конфигурации 102
4.12.1 Общие положения 102
4.12.2 for 102
5 Функции портов 104
5.1 Настройка PoE 104
5.1.1 Общие положения 104
5.1.2 power inline consumption mode dynamic 105
5.1.3 logging event power-inline-status 106
5.1.4 power inline 106
5.1.5 show power inline 108
5.2 Настройка портов RS-232/RS-485 109
5.2.1 Общие положения 109
5.2.2 controllers 109
5.2.3 baudrate 110
5.2.4 databits 110
5.2.5 default 110
5.2.6 description 111

5.2.7 duplex 111
5.2.8 parity 111
5.2.9 state 112
5.2.10 stopbits 112
5.2.11 termination-state 112
5.2.12 virtual-port 113
5.2.13 show rs232-port 114
5.3 Настройка параметров интерфейсов Ethernet 115
5.3.1 Общие положения 115
5.3.2 default 116
5.3.3 clear counters 117
5.3.4 duplex 117
5.3.5 flowcontrol 117
5.3.6 interface 118
5.3.7 interface range 119
5.3.8 description (настройка интерфейса) 119
5.3.9 logging event 119
5.3.10 logging event transceiver 120
5.3.11 mdix auto 121
5.3.12 media-type 121
5.3.13 shutdown 122
5.3.14 speed 122
5.3.15 storm-control 123
5.3.16 rate-limit 123
5.3.17 storm-control action 124
5.3.18 switchport block 124
5.3.19 errdisable recovery cause 125
5.3.20 errdisable recovery interval 126
5.3.21 show errdisable 126
5.3.22 show flowcontrol 126
5.3.23 show interfaces 127
5.3.24 show interfaces description 127
5.3.25 show interfaces status 128
5.3.26 show interfaces summary 128
5.3.27 show interfaces counters 129
5.3.28 show idprom 131
5.3.29 show interfaces transceiver 132
5.3.30 show storm-control 133
5.4 Рефлектометрический тест кабеля 134
5.4.1 Общие положения 134
5.4.2 test cable-diagnostics tdr interface 134
5.4.3 show cable-diagnostics tdr 134

6 Аутентификация, авторизация и аккаунтинг 136
6.1 Настройка AAA (аутентификации, авторизации и учета) 136
6.1.1 aaa authentication login 136
6.1.2 aaa authentication dot1x 136
6.1.3 ip http authentication 137
6.1.4 line 138
6.1.5 login authentication 138
6.1.6 show authentication methods 139
6.2 Настройка RADIUS и TACACS+ 140
6.2.1 debug radius 140
6.2.2 debug tacacs 140
6.2.3 radius-server attribute 4 140
6.2.4 radius-server deadtime 141
6.2.5 radius-server host 142
6.2.6 radius-server key 143
6.2.7 radius-server retransmit 144
6.2.8 radius-server timeout 144
6.2.9 tacacs-server host 145
6.2.10 tacacs-server key 146
6.2.11 tacacs-server timeout 146
6.2.12 test aaa server radius 147
6.2.13 show radius-servers 148
6.2.14 show tacacs 148
6.3 Настройка 802.1X 149
6.3.1 aaa authorization 149
6.3.2 aaa server radius dynamic-author 149
6.3.3 auth-type 150
6.3.4 authentication command bounce-port ignore 151
6.3.5 authentication command disable-port ignore 151
6.3.6 authentication event fail 152
6.3.7 authentication order 152
6.3.8 clear dot1x statistics 153
6.3.9 client 153
6.3.10 debug aaa coa 154
6.3.11 debug aaa pod 155
6.3.12 debug dot1x 155
6.3.13 dot1x guest-vlan 155
6.3.14 dot1x guest-vlan supplicant 157
6.3.15 dot1x re-authenticate 157
6.3.16 dot1x system-auth-control 158
6.3.17 dot1x host-mode 158
6.3.18 dot1x max-req 159

6.3.19 dot1x port-control 160
6.3.20 dot1x reauthentication 160
6.3.21 dot1x timeout quiet-period 161
6.3.22 dot1x timeout reauth-period 162
6.3.23 dot1x timeout server-timeout 162
6.3.24 dot1x timeout supp-timeout 163
6.3.25 dot1x timeout tx-period 163
6.3.26 port 164
6.3.27 show aaa server radius 165
6.3.28 show authentication sessions 165
6.3.29 show dot1x 167
6.3.30 show dot1x statistics 170
6.3.31 show dot1x users 171
6.4 802.1X: поддержка загружаемых ACL (DACL) 173
6.4.1 Общие положения 173
6.4.2 clear ip device tracking 174
6.4.3 ip device tracking probe 174
6.4.4 ip device tracking maximum 175
6.4.5 show ip device tracking 175
7 Функции VLAN 177
7.1 Настройка VLAN 177
7.1.1 Общие положения 177
7.1.2 interface vlan 178
7.1.3 switchport access 178
7.1.4 switchport customer 178
7.1.5 switchport mode 179
7.1.6 switchport protected 179
7.1.7 switchport protected-port 180
7.1.8 switchport community 180
7.1.9 switchport trunk native 181
7.1.10 switchport trunk allowed 181
7.1.11 switchport general pvid 182
7.1.12 switchport general allowed 182
7.1.13 switchport general map 183
7.1.14 vlan 184
7.1.15 name 184
7.1.16 state 185
7.1.17 map 185
7.1.18 vlan dot1q tag native 186
7.1.19 shutdown vlan 187
7.1.20 show interfaces protected 187
7.1.21 show interfaces protected-ports 188

7.1.22 show interfaces switchport 188
7.1.23 show interfaces trunk vlan 188
7.1.24 show interfaces vlan 189
7.1.25 show vlan 189
7.2 Настройка Voice VLAN 191
7.2.1 Общие положения 191
7.2.2 mls qos trust device ip-phone 193
7.2.3 switchport voice vlan 193
7.2.4 show interfaces voice-vlan 194
7.3 Настройка GVRP 195
7.3.1 Общие положения 195
7.3.2 gvrp global 195
7.3.3 gvrp timer 196
7.3.4 gvrp vlan create 197
7.3.5 show gvrp interface 197
7.3.6 show gvrp summary 197
7.4 Настройка Selective Q-in-Q 199
7.4.1 Общие положения 199
7.4.2 vlan mapping 199
7.4.3 switchport vlan mapping 200
7.4.4 switchport trunk allowed 201
7.4.5 show interfaces vlan mapping 202
8 QoS 203
8.1 Настройка качества обслуживания QoS 203
8.1.1 Общие положения 203
8.1.2 mls qos 204
8.1.3 mls qos map 204
8.1.4 mls qos trust 205
8.1.5 priority-queue out num-of-queues 205
8.1.6 traffic-shape 205
8.1.7 traffic-shape queue 206
8.1.8 qos wrr-queue wrtd 207
8.1.9 wrr-queue bandwidth 207
8.1.10 show mls qos 208
8.1.11 show mls qos interface 208
8.1.12 show mls qos maps 208
9 ACL 210
9.1 Настройка списков контроля доступа (ACL) 210
9.1.1 Общие положения 210
9.1.2 clear access-lists counters 216
9.1.3 access-list logging interval 216
9.1.4 ip access-list 217

9.1.5 ipv6 access-list 219
9.1.6 mac access-list 219
9.1.7 service-acl input 220
9.1.8 service-acl output 221
9.1.9 permit (настройка IPv4 ACL) 223
9.1.10 deny (настройка IPv4 ACL) 226
9.1.11 permit (настройка IPv6 ACL) 229
9.1.12 deny (настройка IPv6 ACL) 233
9.1.13 permit (настройка MAC ACL) 236
9.1.14 deny (настройка MAC ACL) 238
9.1.15 show access-lists 239
9.1.16 show interfaces access-lists 239
9.1.17 show interfaces access-lists counters 241
9.1.18 show interfaces access-lists vlan 241
9.2 Ограничение управления устройством (Management ACL) 243
9.2.1 management access-list 243
9.2.2 management access-class 243
9.2.3 deny 244
9.2.4 permit 245
9.2.5 show management access-list 246
9.2.6 show management access-class 246
10 Spanning tree и резервирование соединений 249
10.1 Настройка протоколов Spanning Tree 249
10.1.1 Общие положения 249
10.1.2 clear spanning-tree statistics 259
10.1.3 debug spanning-tree 259
10.1.4 spanning-tree bpdufilter 259
10.1.5 spanning-tree bpduguard 260
10.1.6 spanning-tree cost 260
10.1.7 spanning-tree forward-time 261
10.1.8 spanning-tree hello-time 261
10.1.9 spanning-tree link-type 262
10.1.10 spanning-tree portfast 262
10.1.11 spanning-tree max-age 263
10.1.12 spanning-tree mode 263
10.1.13 spanning-tree port-priority 264
10.1.14 spanning-tree priority 264
10.1.15 spanning-tree transmit hold-count 265
10.1.16 spanning-tree mst max-hops 265
10.1.17 spanning-tree mst priority 266
10.1.18 spanning-tree mst configuration 266
10.1.19 abort (настройка MST) 266

10.1.20 commit (настройка MST) 267
10.1.21 exit (настройка MST) 267
10.1.22 instance (настройка MST) 267
10.1.23 name (настройка MST) 268
10.1.24 revision (настройка MST) 268
10.1.25 spanning-tree guard 269
10.1.26 spanning-tree mst hello-time 269
10.1.27 spanning-tree mst cost 270
10.1.28 spanning-tree mst port-priority 270
10.1.29 spanning-tree vlan 270
10.1.30 show current 271
10.1.31 show pending 272
10.1.32 show spanning-tree 272
10.1.33 show spanning-tree mst 274
10.1.34 show spanning-tree mst configuration 276
10.1.35 show spanning-tree statistics 276
10.2 Настройка ERPS 277
10.2.1 clear erps 277
10.2.2 erps command 277
10.2.3 erps guard 278
10.2.4 erps holdoff 278
10.2.5 erps major 279
10.2.6 erps mep 280
10.2.7 erps revertive 280
10.2.8 erps rpl 281
10.2.9 erps sub 282
10.2.10 erps topology-change propagate 283
10.2.11 erps version 283
10.2.12 erps vlan 284
10.2.13 show erps 284
10.3 Настройка обнаружения петель в сети 286
10.3.1 set interface active 286
10.3.2 loopback-detection enable (глобальная настройка) 286
10.3.3 loopback-detection logging 286
10.3.4 loopback-detection mode 287
10.3.5 loopback-detection interval 287
10.3.6 loopback-detection enable (конфигурация интерфейса) 288
10.3.7 show loopback-detection 288
10.4 Настройка UDLD 290
10.4.1 debug udld 290
10.4.2 udld reset 290
10.4.3 udld enable 290

10.4.4 udld message 291
10.4.5 udld port 291
10.4.6 show udld 291
11 Зеркалирование портов 293
11.1 Настройка зеркалирования 293
11.1.1 monitor session 293
11.1.2 source 293
11.1.3 destination 294
11.1.4 shutdown 295
11.1.5 show monitor session 296
11.1.6 remote-span 297
12 Агрегация интерфейсов 298
12.1 Агрегация интерфейсов 298
12.1.1 channel-group 298
12.1.2 port-channel load-balance 299
12.2 Агрегация с помощью LACP 300
12.2.1 debug lacp 300
12.2.2 lacp system-priority 300
12.2.3 lacp port-priority 301
12.2.4 lacp timeout 301
12.2.5 show lacp 302
12.2.6 show lacp port-channel 304
13 Туннелирование 305
13.1 Настройка PPPoE Intermediate-Agent 305
13.1.1 Общая информация 305
13.1.2 Настройка PPPoE-IA 306
13.1.3 clear pppoe intermediate-agent statistics 307
13.1.4 pppoe intermediate-agent 307
13.1.5 pppoe intermediate-agent format-type 308
13.1.6 pppoe intermediate-agent 309
13.1.7 pppoe intermediate-agent format-type 310
13.1.8 pppoe intermediate-agent trust 310
13.1.9 pppoe intermediate-agent limit rate 311
13.1.10 pppoe intermediate-agent vendor-tag strip 311
13.1.11 show pppoe intermediate-agent info 312
13.1.12 show pppoe intermediate-agent statistics 312
14 DHCP 314
14.1 Настройка DHCP-сервера 314
14.1.1 clear ip dhcp binding 314
14.1.2 debug ip dhcp client 314
14.1.3 debug ip dhcp server 314
14.1.4 ip dhcp excluded-address 315

14.1.5 ip dhcp pool host 316
14.1.6 ip dhcp pool network 316
14.1.7 ip dhcp server 317
14.1.8 address (настройка пулов хостов) 317
14.1.9 client-name 318
14.1.10 address (настройка пулов сетей) 318
14.1.11 lease 319
14.1.12 default-router 320
14.1.13 dns-server 320
14.1.14 domain-name 321
14.1.15 next-server 322
14.1.16 bootfile 322
14.1.17 option 323
14.1.18 show ip dhcp 324
14.1.19 show ip dhcp binding 324
14.1.20 show ip dhcp excluded-address 325
14.1.21 show ip dhcp pool host 325
14.1.22 show ip dhcp pool network 326
14.2 Настройка IPv6 DHCP-сервера 327
14.2.1 ipv6 dhcp server 327
14.2.2 address (настройка пулов сетей) 327
14.2.3 dns-server 328
14.2.4 clear ipv6 dhcp binding all 328
14.2.5 show ipv6 dhcp binding 328
14.3 Настройка IPv6 DHCP-клиента 330
14.3.1 ipv6 address dhcp 330
14.3.2 show ipv6 route 330
14.4 Настройка DHCP Relay 331
14.4.1 Общие положения 331
14.4.2 debug ip dhcp relay 333
14.4.3 ip dhcp information option 334
14.4.4 ip dhcp information option format remote-id 334
14.4.5 ip dhcp relay enable 334
14.4.6 ip dhcp relay address 335
14.4.7 ip dhcp information option format circuit-id 336
14.4.8 ip dhcp relay enable 336
14.4.9 ip dhcp relay address 337
14.4.10 show ip dhcp relay 337
14.5 Настройки IPv6-адресации 339
14.5.1 ipv6 address 339
15 Функции безопасности 340
15.1 Настройка DHCP Snooping 340

15.1.1 debug ip dhcp snooping 340
15.1.2 clear ip dhcp snooping database 340
15.1.3 ip dhcp snooping 340
15.1.4 ip dhcp snooping vlan 341
15.1.5 ip dhcp snooping trust 341
15.1.6 ip dhcp snooping limit rate 342
15.1.7 ip dhcp snooping information option allowed-untrusted 342
15.1.8 ip dhcp snooping verify 343
15.1.9 ip dhcp snooping database 343
15.1.10 ip dhcp snooping database update-freq 344
15.1.11 ip dhcp snooping binding 345
15.1.12 show ip dhcp snooping 346
15.1.13 show ip dhcp snooping binding 346
15.2 Настройка безопасности на интерфейсах (Port Security) 348
15.2.1 clear port-security 348
15.2.2 switchport port-security 348
15.2.3 switchport port-security mac-address 349
15.2.4 switchport port-security maximum 350
15.2.5 switchport port-security mode 350
15.2.6 switchport port-security violation 351
15.2.7 show port-security 352
15.3 Настройка IP Source Guard 353
15.3.1 Общие положения 353
15.3.2 ip source-guard 356
15.3.3 ip source-guard binding 356
15.3.4 ip source-guard vlan 357
15.3.5 ip source-guard 358
15.3.6 show ip source-guard configuration 358
15.3.7 show ip source-guard status 359
15.3.8 show ip source-guard inactive 359
15.3.9 show ip source-guard statistics 360
15.4 Настройка таблицы MAC-адресов 361
15.4.1 Общие положения 361
15.4.2 clear mac address-table dynamic 361
15.4.3 mac address-table aging-time 362
15.4.4 mac address-table static 362
15.4.5 mac address-table static drop 363
15.4.6 show mac address-table 363
15.4.7 show mac address-table address 364
15.4.8 show mac address-table aging-time 364
15.4.9 show mac address-table count 365
15.4.10 show mac address-table dynamic 365

15.4.11 show mac address-table interface 366
15.4.12 show mac address-table static 366
15.4.13 show mac address-table vlan 367
15.5 Настройка Dynamic ARP Inspection 368
15.5.1 Общие положения 368
15.5.2 clear ip arp inspection statistics 374
15.5.3 debug ip arp inspection 374
15.5.4 ip arp inspection 374
15.5.5 ip arp inspection debug interval 375
15.5.6 ip arp inspection list assign 375
15.5.7 ip arp inspection list create 376
15.5.8 ip arp inspection logging interval 376
15.5.9 ip arp inspection validate 377
15.5.10 ip arp inspection vlan 378
15.5.11 ip arp inspection trust 378
15.5.12 ip mac 379
15.5.13 show ip arp inspection interface 379
15.5.14 show ip arp inspection list 380
15.5.15 show ip arp inspection statistics 380
15.6 Настройка защиты от DoS-атак (автоматизированная защита от SYN/SYN-ACK Flooding) 382
15.6.1 Общее положение: 382
15.6.2 ip tcp 382
16 Маршрутизация 384
16.1 Команды, независимые от протокола маршрутизации IP 384
16.1.1 key chain 384
16.1.2 key 384
16.1.3 accept-lifetime 385
16.1.4 key-string 387
16.1.5 send-lifetime 387
16.1.6 show key chain 389
16.2 Статическая маршрутизация 390
16.2.1 ip route 390
16.2.2 show ip route 390
16.3 Настройка RIP 392
16.3.1 Общие положения 392
16.3.2 debug ip rip 393
16.3.3 router rip 394
16.3.4 authentication key-chain 394
16.3.5 authentication mode 395
16.3.6 ip rip offset 396
16.3.7 ip rip shutdown 396

16.3.8 ip rip ttl-security 397
16.3.9 network 397
16.3.10 redistribute (RIP) 398
16.3.11 shutdown 400
16.3.12 show ip rip 400
16.3.13 show ip rip statistics 401
16.3.14 loadbalance 401
16.4 Настройка RIPng 402
16.4.1 router rip 402
16.4.2 network 402
16.4.3 redistribute (RIPng) 403
16.4.4 aggregate-address 403
16.4.5 default-information originate 404
16.4.6 default-metric 404
16.4.7 offset-list 405
16.4.8 passive-interface 406
16.4.9 route 406
16.4.10 timers basic 407
16.4.11 ipv6 ripng split-horizon 407
16.4.12 show ipv6 ripng 408
16.4.13 show ipv6 ripng status 408
16.5 Настройка OSPFv2 410
16.5.1 Общие положения 410
16.5.2 clear ip ospf process 412
16.5.3 debug ip ospf 412
16.5.4 router ospf 413
16.5.5 area authentication 414
16.5.6 area default-cost 414
16.5.7 area nssa 415
16.5.8 area range 416
16.5.9 area shutdown 417
16.5.10 area stub 418
16.5.11 compatible rfc1583 418
16.5.12 max-metric router-lsa 419
16.5.13 network area 420
16.5.14 no area 421
16.5.15 passive-interface 421
16.5.16 redistribute 422
16.5.17 router-id 424
16.5.18 ip ospf authentication 424
16.5.19 ip ospf authentication-key 425
16.5.20 ip ospf authentication key-chain 426

16.5.21 ip ospf cost 426
16.5.22 ip ospf dead-interval 427
16.5.23 ip ospf hello-interval 428
16.5.24 ip ospf mtu-ignore 428
16.5.25 ip ospf passive-interface 429
16.5.26 ip ospf priority 429
16.5.27 ip ospf retransmit-interval 430
16.5.28 ip ospf shutdown 431
16.5.29 ip ospf ttl-security 431
16.5.30 show ip ospf 432
16.5.31 show ip ospf database 432
16.5.32 show ip ospf interface 433
16.5.33 show ip ospf neighbor 433
16.5.34 loadbalance 434
16.6 Настройка OSPFv3 435
16.6.1 Общие положения 435
16.6.2 clear ip ospf6 process 437
16.6.3 router ospf6 437
16.6.4 area authentication 438
16.6.5 area default-cost 439
16.6.6 area nssa 439
16.6.7 area range 440
16.6.8 area shutdown 441
16.6.9 area stub 442
16.6.10 max-metric router-lsa 442
16.6.11 network area 443
16.6.12 no area 444
16.6.13 passive-interface 445
16.6.14 redistribute 445
16.6.15 router-id 447
16.7 Настройка IS-IS 448
16.7.1 Общие положения 448
16.7.2 clear isis neighbor 450
16.7.3 router isis 451
16.7.4 area password 451
16.7.5 default-information originate 452
16.7.6 domain password 452
16.7.7 hostname dynamic 453
16.7.8 is-type 453
16.7.9 log-adjacency-changes 454
16.7.10 lsp-gen-interval 454
16.7.11 lsp-mtu 455

16.7.12 lsp-refresh-interval 455
16.7.13 max-lsp-lifetime 456
16.7.14 metric-style 456
16.7.15 net 457
16.7.16 redistribute 458
16.7.17 set-overload-bit 459
16.7.18 mpls-te 460
16.7.19 spf-delay-ietf 460
16.7.20 spf-interval 461
16.7.21 isis circuit-type 462
16.7.22 isis csnp-interval 462
16.7.23 isis hello 463
16.7.24 isis hello-interval 463
16.7.25 isis hello-multiplier 464
16.7.26 isis metric 465
16.7.27 isis network point-to-point 465
16.7.28 isis passive 466
16.7.29 isis password 466
16.7.30 isis priority 467
16.7.31 isis psnp-interval 467
16.7.32 ip router isis 468
16.7.33 show isis 468
16.8 Настройка BFD 470
16.8.1 Общие положения 470
16.8.2 bfd 470
16.8.3 peer 470
16.8.4 profile 471
16.8.5 detect-multiplier 471
16.8.6 receive-interval 472
16.8.7 transmit-interval 472
16.8.8 echo receive-interval 473
16.8.9 echo transmit-interval 473
16.8.10 echo-mode 474
16.8.11 shutdown 474
16.8.12 passive-mode 474
16.8.13 profile 475
16.8.14 ip ospf bfd 475
16.8.15 neighbor bfd 476
16.8.16 show bfd peer 476
16.8.17 show bfd peers 477
16.9 Настройка BGP 479
16.9.1 debug ip bgp 479

16.9.2 router bgp 479
16.9.3 bgp always-compare-med 480
16.9.4 bgp bestpath as-path ignore 481
16.9.5 bgp cluster-id 481
16.9.6 bgp default local-preference 482
16.9.7 bgp deterministic-med 482
16.9.8 bgp ebgp-requires-policy 483
16.9.9 neighbor local-as 483
16.9.10 neighbor maximum-prefix 484
16.9.11 neighbor next-hop-self 485
16.9.12 neighbor password 486
16.9.13 neighbor remote-as 486
16.9.14 neighbor route-map 487
16.9.15 neighbor route-reflector-client 487
16.9.16 neighbor route-server-client 488
16.9.17 neighbor timers 489
16.9.18 neighbor transport 489
16.9.19 neighbor ttl-security 490
16.9.20 network 491
16.9.21 redistribute 492
16.9.22 show ip bgp 493
16.9.23 show ip bgp route 493
16.9.24 show ip bgp summary 494
16.9.25 show ip bgp detail 494
16.10 Настройка VRRP 496
16.10.1 Общие положения 496
16.10.2 clear vrrp statistics 501
16.10.3 vrrp authentication 502
16.10.4 vrrp debug 503
16.10.5 vrrp debug interval 504
16.10.6 vrrp delay 504
16.10.7 vrrp description 505
16.10.8 vrrp ip 505
16.10.9 vrrp preempt 506
16.10.10 vrrp priority 507
16.10.11 vrrp shutdown 508
16.10.12 vrrp timers advertise 508
16.10.13 vrrp version 509
16.10.14 show vrrp 510
16.11 Настройка Route-Map 514
16.11.1 Общие положения 514
16.11.2 route-map 514

16.11.3 match access-group 515
16.11.4 set metric 515
16.11.5 set next-hop 516
16.11.6 service-route-policy 516
16.11.7 show route-map 516
17 Многоадресная рассылка 518
17.1 Настройка IGMP Snooping 518
17.1.1 Общие положения 518
17.1.2 clear ip igmp group 519
17.1.3 ip igmp profile 519
17.1.4 ip igmp snooping 520
17.1.5 ip igmp snooping last-member-query-count 520
17.1.6 ip igmp snooping last-member-query-interval 521
17.1.7 ip igmp snooping vlan mrouter 522
17.1.8 ip igmp snooping querier 523
17.1.9 ip igmp snooping query-interval 524
17.1.10 ip igmp snooping query-max-response-time 525
17.1.11 ip igmp snooping robustness-variable 525
17.1.12 ip igmp snooping startup-query-count 526
17.1.13 ip igmp snooping startup-query-interval 527
17.1.14 ip igmp snooping vlan static 527
17.1.15 ip igmp snooping version 528
17.1.16 ip igmp filter 529
17.1.17 ip igmp immediate-leave 529
17.1.18 ip igmp max-groups 530
17.1.19 ip igmp max-groups action 531
17.1.20 ip igmp snooping report-suppression 532
17.1.21 deny 533
17.1.22 permit 534
17.1.23 show ip igmp profile 534
17.1.24 show ip igmp snooping 535
17.1.25 show ip igmp snooping groups 535
17.1.26 show ip igmp snooping mrouter 536
17.1.27 show ip igmp snooping querier 537
17.2 Настройка MLD Snooping 538
17.2.1 Общие положения 538
17.2.2 ipv6 mld snooping 539
17.2.3 ipv6 mld snooping querier vlan 539
17.2.4 ipv6 mld snooping version 540
17.2.5 ipv6 mld snooping query-interval 541
17.2.6 ipv6 mld snooping query-max-response-time 541
17.2.7 ipv6 mld snooping robustness-variable 542

17.2.8 ipv6 mld snooping startup-query-count 543
17.2.9 ipv6 mld snooping startup-query-interval 543
17.2.10 ipv6 mld snooping last-member-query-count 544
17.2.11 ipv6 mld snooping last-member-query-interval 545
17.2.12 show ipv6 mld snooping 546
17.2.13 show ipv6 mld snooping groups 547
17.2.14 show ipv6 mld snooping querier 547
17.3 Настройка MVR 548
17.3.1 mvr 548
17.3.2 mvr group 548
17.3.3 mvr mode 549
17.3.4 mvr querytime 550
17.3.5 mvr vlan 550
17.3.6 mvr type 551
17.3.7 mvr vlan 551
17.3.8 mvr immediate 552
17.3.9 show mvr 553
17.3.10 show mvr interface 553
17.3.11 show mvr members 553
18 Стекирование устройств 555
18.1 Общие положения 555
18.2 Порядок действий для организации стека 555
18.3 session 556
18.4 switch stack id 556
18.5 show switch 556
19 Статистика и подсчет трафика 558
19.1 Вывод статистики 558
19.1.1 Общие положения 558
19.1.2 show controllers cpu-interface 558
19.1.3 show controllers ethernet-controller 559
19.1.4 show controllers utilization 559
19.2 Настройка sFlow 561
19.2.1 Общие положения 561
19.2.2 Порядок настройки 562
19.2.3 clear sflow statistics 563
19.2.4 sflow flow-sampling mode 563
19.2.5 sflow receiver 563
19.2.6 sflow flow-sampling 564
19.2.7 sflow counters-sampling 565
19.2.8 show sflow configuration 566
19.2.9 show sflow statistics 566

20 Управление, мониторинг и контроль сетевой инфраструктуры 568
20.1 Настройка LLDP 568
20.1.1 Общие положения 568
20.1.2 clear lldp table 568
20.1.3 debug lldp 569
20.1.4 clear lldp statistics 569
20.1.5 lldp hold-multiplier 569
20.1.6 lldp med fast-start repeat-count 570
20.1.7 lldp med network-policy (глобальная настройка) 570
20.1.8 lldp reinit 572
20.1.9 lldp run 572
20.1.10 lldp timer 573
20.1.11 lldp tx-delay 573
20.1.12 lldp management-address 574
20.1.13 lldp med-select-tlv 574
20.1.14 lldp med location 575
20.1.15 lldp med network-policy (настройка интерфейса) 576
20.1.16 lldp select-tlv 577
20.1.17 lldp receive 578
20.1.18 lldp transmit 578
20.1.19 show lldp configuration 579
20.1.20 show lldp local 580
20.1.21 show lldp med configuration 581
20.1.22 show lldp neighbors 582
20.1.23 show lldp statistics 583
20.2 Настройка CFM OAM 584
20.2.1 ethernet cfm domain 584
20.2.2 service instance ethernet 584
20.2.3 service 585
20.2.4 continuity-check 586
20.2.5 cfm mep domain 587
20.2.6 show ethernet cfm errors 587
20.3 Настройка SNMP 589
20.3.1 Общие положения 589
20.3.2 snmp-server community 590
20.3.3 snmp-server contact 590
20.3.4 snmp-server context 590
20.3.5 snmp-server engineid 591
20.3.6 snmp-server host 591
20.3.7 snmp-server location 592
20.3.8 snmp-server protocol enable 592
20.3.9 snmp-server protocol version 592

20.3.10 snmp-server source-interface 593
20.3.11 snmp-server traps 593
20.3.12 snmp-server user 594
20.3.13 show snmp 595
20.4 Управление и мониторинг по протоколу SNMP 596
20.4.1 Общие положения 596
20.4.2 Подготовка к управлению и мониторингу по протоколу SNMP . . 596
20.4.3 Управление общей информацией о системе 599
20.4.4 Получение информации об интерфейсах системы 599
20.4.5 Настройка портов RS-232/485 600
20.4.6 Настройка интерфейсов Ethernet 601
20.4.7 Описание SNMP-ловушек 602
20.4.8 Получение информации о счетчиках статистики RMON 602
21 Обновление программного обеспечения через TFTP-сервер 603
21.1 Настройка TFTP-сервера 603
21.2 Порядок настройки tftpd32: 603
21.3 Загрузка программного обеспечения 604
Приложение А Таблицы преобразований Cos – Prio, DSCP – Prio 606
Приложение Б Типы и формат журналируемых событий 607

1 Введение

В данном руководстве описывается конфигурация ПО.

1.1 Основные характеристики коммутатора

Настоящая часть РЭ содержит сведения, необходимые для контроля и управления аппаратурой Акманай-2xxx (далее «коммутатор»), имеющей версию программного обеспечения не ниже 1.1.17.

К работе с коммутатором допускаются лица, изучившие части I и II настоящего РЭ.

Меры безопасности при работе с коммутатором описаны в части I настоящего РЭ.

В таблице 1 приведены основные характеристики коммутатора.

Таблица 1 – Основные характеристики Акманай-2xxx

Характеристики	Значение
Таблица MAC-адресов	16K
Максимальный размер пакета	10000
Поддержка IP v4 и IP v6	+
Стекирование	
Количество устройств	5
Управление	
SNMP	+
Telnet	+
SSH	+
DHCP-сервер	+
DHCP Relay	+
VLAN	
Tag-based VLANs, поддержка «двойного тега» (Double Tagging/QinQ)	+
Количество статических групп VLANs (802.1Q VLANs)	4K
Количество динамических групп VLANs (802.1Q Dynamic VLANs)	4K
Private VLAN Edge/Lite	+
Voice VLAN	+

Продолжение таблицы 1

Характеристики	Значение
QoS	
QoS 802.1p Priority. 8 очередей на порт, поддержка 802.1 Tagged Frames, IPv4 ToS (Type of Service), IPv4 DS (Differentiated Service/DiffServ), IPv6 TC (Traffic Class), 802.1Q VID (Идентификатор VLAN)	+
Поддержка очередей SPQ, SDWRR	+
STP	
802.1D STP (Spanning Tree)	+
802.1w RSTP (Rapid Spanning Tree)	+
802.1s MSTP (Multiple Spanning Tree)	+
Loopback Detection Protocol	+
PoE	
IEEE 802.3af	+
IEEE 802.3at	+
Маршрутизация	
Статическая	+
BGP	+
RIP	+
OSPFv2	+
OSPFv3	+
Дополнительно	
IGMP Snooping	+
GARP/GVRP	+
Задание статических MAC-адресов	+
Ограничение входящего трафика на портах	+
Передача данных с портов RS-232/RS-485	+

1.2 Заводские настройки

Заводские настройки, устанавливаемые производителем при поставке аппаратуры, представлены в таблице 2.

Таблица 2 – Заводские настройки

Тип настройки	Название	Значение
Настройки часового пояса	Часовой пояс	YEKT, смещение 5 часов 0 минут
	Переход на летнее время	Последнее воскресенье марта в 3:00
	Переход на зимнее время	Последнее воскресенье октября в 3:00
Настройки управления	Управление по SSH	Включено, версия 2
	Управление по Telnet	Включено
	Управление по SNMP	Включено, все версии
	Таймаут управления по SSH и Telnet	5 минут
	Тип терминала	xterm
Сетевые настройки	IP-адрес шлюза	0.0.0.0
	IP-адреса DNS-серверов	Отсутствуют
Общие настройки	Имя коммутатора	«Switch»
	Приоритет коммутатора	1
	Пороговая температура включения вентилятора, градусы Цельсия	40
Настройки интерфейсов Ethernet	Максимальный размер поля данных в фрейме Ethernet	1500
	Режим дуплекса	auto
	Режим скорости	auto
	Режим управления потоком	desired
	Режим автокроссирования	auto
	Текстовое описание	«interface gigabitethernet0/N», «interface tengigabitethernet0/N»
	Защита от мультикастового и широковещательного шторма	Выключена
	Блокирование обычного и мультикастового трафика с неизвестным адресом назначения	Выключено
	Журналирование событий	Включено для всех событий

Продолжение таблицы 2

Тип настройки	Название	Значение
Настройки Spanning Tree Protocol	Режим фильтрации BPDU	Выключен на всех интерфейсах
	Режим контроля прихода BPDU	Выключен на всех интерфейсах
	Режим STP	rstp
	Интервал отправки сообщений hello, секунды	2
	Время перехода интерфейсов в режим «FORWARDING», секунды	15
	Ограничение по управляющему трафику	6
	Время старения информации, секунды	20
	Приоритет моста	36384
	Тип подключения	auto
	Приоритет интерфейса	128
	Стоимость пути для интерфейса	20 000 для gigabitethernet, 2 000 для tengigabitethernet
	Режим быстрого перехода в состояние «FORWARDING»	Выключен
	Число прыжков (hops) в MST-регионе перед тем, как пакет BPDU будет удален	20
	Приоритет устройства для указанного поддерева Spanning Tree	32768
	Номер поддерева MST	0
	Имя конфигурации MST	Пустая строка
	Версия конфигурации MST	0
	Режим Root Guard	Выключен
	Режим Topology Change Guard	Выключен
	Интервал отправки BPDU, сек	2
	Приоритет порта	128
Настройки QoS	Режим QoS	Выключен
	Режим классификации приоритета пакетов по параметрам CoS (802.1p) и DSCP (IP)	Выключен
	Правила преобразования DSCP-Prio (внутренний приоритет)	См. таблицу А.2 Приложения А

Продолжение таблицы 2

Тип настройки	Название	Значение
	Правила преобразования CoS-Prio (внутренний приоритет)	См. таблицу А.1 Приложения А
Настройки IGMP Snooping	Режим работы	Выключен
	Таймер «leave», миллисекунды	1000
	Режим IGMP querier	Выключен на всех интерфейсах
	Режим немедленного выхода из мультикастовой группы	Выключен
	Интерфейс мультикастового маршрутизатора	Отсутствует
	Статические мультикастовые группы	Отсутствуют
Настройки VLAN	Номер VLAN управления	1
	Режим работы интерфейсов	access
	Номер access VLAN для интерфейса	1
	Номер native VLAN для интерфейса	1
	Режим защищенного порта (protected)	Выключен
	Режим тегирования native VLAN	Выключен
	Таблица VLAN	VLAN №1, членами которого являются все интерфейсы
	Private VLAN Edge	Выключен
Настройки Voice VLAN	Voice VLAN	Выключен
	Проверка подключения IP-телефона	Выключена
Настройки GVRP	Режим работы	Выключен
	Режим создания динамических VLAN	Выключен
Настройки таблицы MAC-адресов	Время старения, секунды	300
	Статические MAC-адреса	Отсутствуют
Настройки SNMP	Режим работы	Включен для всех версий (v1, v2c, v3)
	Имена сообществ для чтения	«public»

Продолжение таблицы 2

Тип настройки	Название	Значение
	Контактная информация	«no contact»
	Имя системы	«no name»
	Расположение системы	«no location»
	Имя контекста	«»
	Имя движка SNMP	«80:00:3A:25:03», дополненное текстовым представлением MAC-адреса коммутатора
	Имена пользователей SNMPv3	Отсутствуют
	IP-адреса SNMP-менеджеров для отправки ловушек	Отсутствуют
Настройки Syslog	Список syslog-серверов	Не задан
Настройки NTP	Список NTP-серверов	Не задан
Настройки DHCP Relay	DHCP Relay	Выключен
	Значение подопции Remote ID опции 82	MAC-адрес устройства в шестнадцатеричном формате (текстовом)
	IP-адрес DHCP-сервера	Отсутствует
	Значение подопции Circuit ID опции 82	«vlanN», где N – идентификатор VLAN (номер)
Настройки DHCPсервера	Режим работы	Выключен
	Пулы сетей	Отсутствуют
	Пулы хостов	Отсутствуют
	Исключенные адреса	Отсутствуют
Настройки PoE	Режим подсчета потребления мощности	По классу
	Журналирование событий	Включено
	Режим работы на интерфейсе	auto, максимальная мощность 30 Вт
Настройки маршрутизации	Статические маршруты	Отсутствуют
	BGP	Отсутствуют
	RIP	Отсутствуют
	OSPFv2	Отсутствуют
	OSPFv3	Отсутствуют

2 Подключение к коммутатору

2.1 Требования к ПК

Для управления коммутатором через порт «F» необходимо наличие ПК с портом RS-232 или USB (кабель должен быть оснащен переходником USB-COM, так же на моделях -SR управление коммутатором происходит через порт консоли, в этом случае необходимо использовать кабель miniUSB-USB) и программы типа PuTTY 0.60 или старше. Программа PuTTY доступна по адресу:

https://www.chiark.greenend.org.uk/ sgtatham/putty/latest.html.

Настройки программы-терминала для подключения к коммутатору через порт «F» приведены в таблице 3.

Таблица 3 – Настройки программы-терминала

Название параметра	Значение
Скорость COM-порта [бит/с]	115 200
Количество бит данных	8
Количество стоповых бит	1
Режим проверки четности	нет
Тип терминала	xterm

Примечание – Пользователи операционной системы Linux для управления коммутатором могут использовать программу, подобную kermit. Информация по настройке программы kermit доступна по команде «**man kermit**».

Пример настройки программы PuTTY 0.60 для подключения к коммутатору через порт «F» приведен на рисунках 1 и 2.

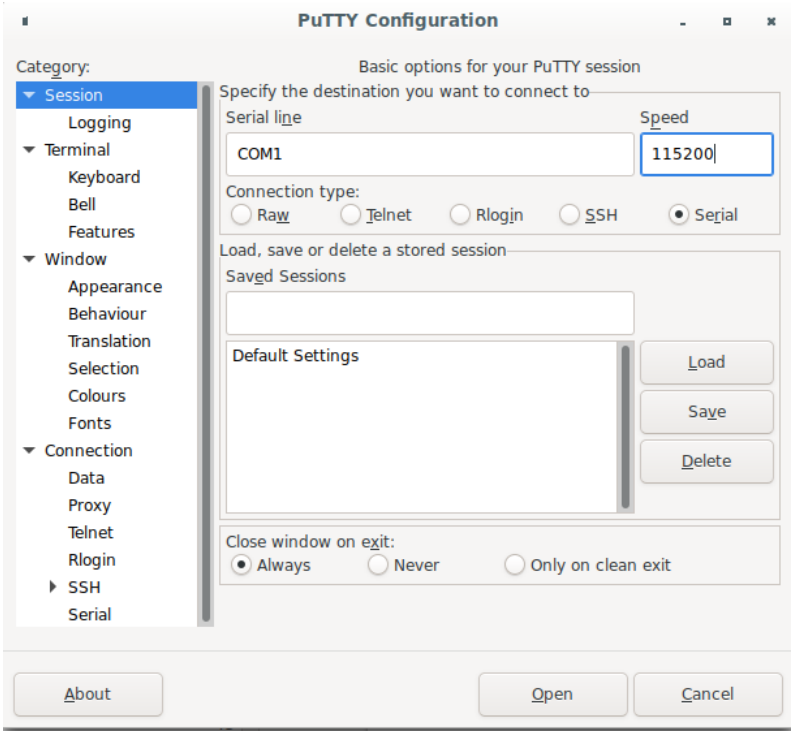

Рисунок 1 – Настройка COM-порта

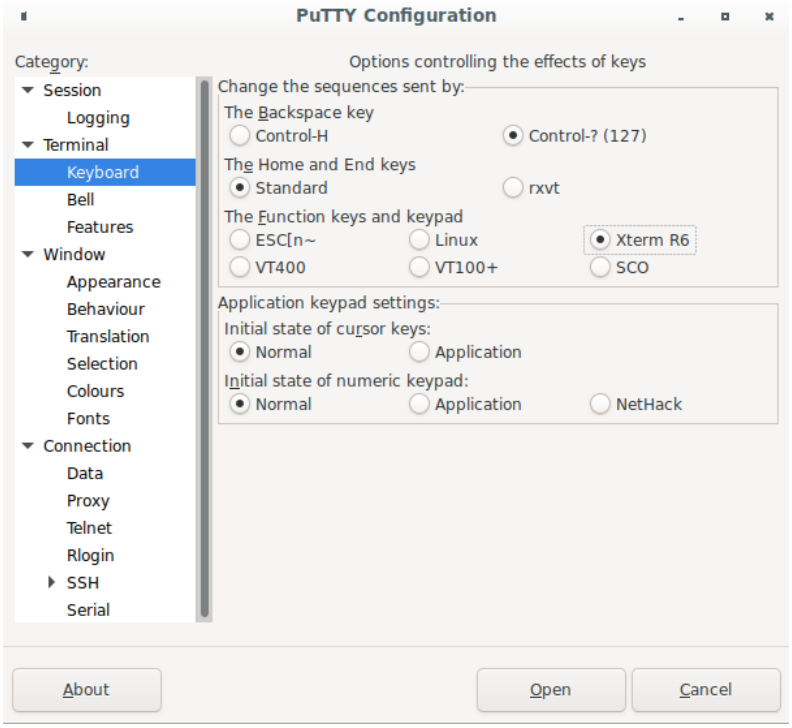

Рисунок 2 – Настройка режимов эмуляции

Для управления коммутатором по протоколу Telnet или SSH рекомендуется использование программы PuTTY 0.60 или старше. Пример настроек программы PuTTY 0.60 для управления по протоколу Telnet приведен на рисунках 2 и 3.

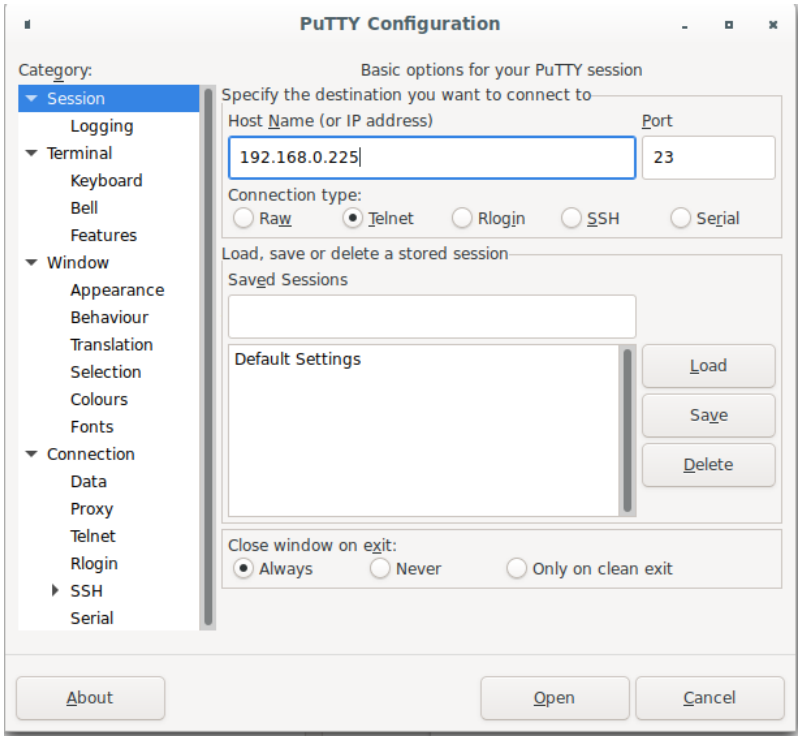

Рисунок 3 – Настройка сессии PuTTY

Примечание – Пользователи операционной системы Linux для управления коммутатором по протоколу Telnet могут использовать программу PuTTY. Подключение к коммутатору осуществляется с помощью команды «**telnet IP**», где «IP» – IP-адрес коммутатора.

В АО НПП «Полигон» выполнена проверка возможности управления коммутатором через программу PuTTY.

2.2 Порядок действий для организации управления через порт «F»

1. Рекомендуется обесточить коммутатор и подключаемое оборудование при подключении кабелей.
2. Подключить кабель управления к COM-порту ПК.
3. Подключить кабель управления к порту «F» коммутатора.
4. Настроить программу-терминал в соответствии с вышеуказанными параметрами.
5. Включить коммутатор (если коммутатор уже включен, то этот и следующий пункт можно пропустить).
6. Дождаться окончания загрузки ПО коммутатора (вывода приглашения для ввода имени пользователя и пароля).

7. Ввести имя пользователя и пароль. Заводские настройки для доступа: имя пользователя – “admin”, пароль – “admin”. Вводимый пароль не отображается на экране терминала.

2.3 Порядок действий для организации управления по протоколу Telnet

1. Подключить ПК к локальной сети.
2. Подключить коммутатор к локальной сети (через порт 10/100/1000BASE-T).
3. Настроить программу-терминал в соответствии с вышеуказанными параметрами.
4. Включить коммутатор (если коммутатор уже включен, то этот и следующий пункт можно пропустить).
5. Дождаться окончания загрузки ПО коммутатора (около 4 минут).
6. В CLI коммутатора включить доступ к управлению по протоколу telnet (команда «**ip telnet server**») и настроить IP-адрес.

   Настройка IP-адреса осуществляется следующим образом:

   ```
   configure terminal
   interface vlan 1
   ip address xxx.xxx.xxx.xxx/y
   ```

   где xxx.xxx.xxx.xxx – IP-адрес, задаваемый устройству; y – маска подсети.
7. Подключиться к коммутатору через программу-терминал.
8. Ввести имя пользователя и пароль. Заводские настройки для доступа: имя пользователя – “admin”, пароль – “admin”. Вводимый пароль не отображается на экране терминала.

3 Описание интерфейса командной строки

3.1 Использование интерфейса командной строки

Интерфейс командной строки (далее «CLI») поддерживает две роли доступа:

- роль обычного пользователя, для которого доступен только ограниченный набор команд;
- роль привилегированного пользователя (администратора), обладающего правами для выполнения всех команд.

Тип роли текущего пользователя отображается в приглашении командной строки. Для обычного пользователя приглашение имеет следующий вид (user – имя текущего пользователя): «user@Switch>».

Для администратора приглашение имеет следующий вид (admin – имя текущего пользователя): «admin@Switch#».

Команды пользователя организованы в иерархическую структуру:

1. Фундаментальные команды доступны из любого режима CLI.
2. Команды глобальных настроек доступны после перехода в режим глобальной настройки по команде «**configure terminal**». Приглашение CLI принимает следующий вид: «admin@Switch(config)#».
3. Команды настроек интерфейсов доступны после перехода из режима глобальной настройки в режим настройки интерфейсов по команде «**interface**». Приглашение CLI принимает следующий вид: «admin@Switch(config-if)#».
4. Команды настроек для группы интерфейсов доступны после перехода из режима глобальной настройки в режим настройки группы интерфейсов по команде «**interface range**». Приглашение CLI принимает следующий вид: «admin@Switch(config-if-range)#».
5. Команды настроек VLAN доступны после перехода из режима глобальной настройки в режим настройки VLAN по команде «**vlan**». Приглашение CLI принимает следующий вид: «admin@Switch(config-vlan)#».

CLI позволяет хранить в памяти до 200 последних введенных команд.

3.2 Контекстная помощь и автодополнение команд

Интерфейс командной строки предоставляет контекстную помощь по командам. Для вывода помощи необходимо нажать на комбинацию клавиш «Shift+?». Контекстная помощь позволяет вывести:

- общий список команд;
- список команд, начинающихся с последовательности символов, введенных пользователем;

– список аргументов и ключевых слов команд.

Вывод общего списка команд:

```
Switch> ?
  clear cli clock configure copy delete
...
```

Вывод списка команд, начинающихся с «cl»:

```
Switch> cl?
  clear cli clock
```

Вывод контекстной помощи для команды «clock»:

```
Switch> clock ?
  set    set current clock time and date
  timezone set clock timezone
```

CLI поддерживает автодополнение команд по нажатию на клавишу «Tab». Если введенному сочетанию символов соответствует несколько команд, то на экране терминала отобразится список из соответствующих команд.

```
Switch> cl <Tab>
  clear cli clock
```

3.3 Проверка синтаксиса команд

Если команда введена неправильно, то на экране терминала отобразится сообщение об ошибке:

```
Switch> clock tamezone
          ^
% Invalid input detected at '^' marker.
```

Если при вводе команды пропущены ключевые слова, то на экране терминала отобразится сообщение об ошибке:

```
Switch> show controllers

% Incomplete command.
```

Интерфейс CLI распознает команды при их неполном вводе. Необходимо ввести часть команды, достаточную для ее идентификации. В противном случае будет выведено сообщение об ошибке:

```
Switch> i
% Ambiguous command.
```

3.4 Список используемых клавиш

CLI поддерживает набор клавиш и их сочетаний, представленный в таблице 4.

Таблица 4 – Набор клавиш и их сочетаний

Клавиша или сочетание клавиш	Назначение
Символьные клавиши	Ввод команд и их аргументов
«Вверх», «Ctrl-P»	Вывод предыдущей команды из памяти команд
«Вниз», «Ctrl-N»	Вывод следующей команды из памяти команд
«Влево», «Ctrl-B»	Перемещение на один символ влево в командной строке
«Вправо», «Ctrl-F»	Перемещение на один символ вправо в командной строке
«Ctrl-A»	Перемещение в начало строки
«Ctrl-E»	Перемещение в конец строки
«Alt-B»	Перемещение на одно слово влево
«Alt-F»	Перемещение на одно слово вправо
«Tab»	Автодополнение команды
«?»	Вывод контекстной помощи
«Ctrl-D», «Delete»	Удаление символа справа от курсора
«Backspace»	Удаление символа слева от курсора
«Alt-D»	Удаление слова или его части справа от курсора с сохранением удаленного слова в буфере обмена
«Ctrl-W», «Alt-Backspace»	Удаление слова или его части слева от курсора с сохранением удаленного слова в буфере обмена
«Alt-W»	Сохранение части командной строки слева от курсора в буфере обмена
«Ctrl-K»	Очистка введенной строки справа от курсора с сохранением удаленного слова в буфере обмена
«Ctrl-Y»	Вставка сохраненного текста из буфера обмена

3.5 Описание синтаксиса команд

Команды и ключевые слова выделяются **жирным** шрифтом. Например: «**configure terminal**».

Параметры команд выделяются *наклонным* шрифтом. Например: «**system mtu** *bytes*».

Необязательные параметры заключаются в квадратные скобки. Например: «**vlan** *vlan-id* [**name** *vlan-name*]».

Перечисление возможных значений параметров заключается в фигурные скобки. Между значениями параметров ставится вертикальная черта. Например: «**spanning-tree mode {stp | rstp}**».

3.6 Описание обозначений интерфейсов и портов

Обозначения интерфейсов Ethernet выполняются в следующем виде: «тип интерфейса номер_устройства/номер_интерфейса» (например, «gigabitethernet0/1»).

Коммутатор поддерживает следующие типы интерфейса: «gigabitethernet» для интерфейсов 10/100/1000BASE-T и 1000BASE-X, «tengigabitethernet» для интерфейса 10GBASE-SR/LR (в зависимости от исполнения).

4 Управление коммутатором

4.1 Вывод общей информации о коммутаторе

4.1.1 Общие положения

Коммутатор обеспечивает:

- вывод имени устройства по команде «**show hostname**»;
- вывод информации о производителе и авторских правах по команде «**show copyright**»;
- вывод информации о местоположении устройства по команде «**show location**»;
- вывод информации об устройстве по команде «**show inventory**»;
- вывод информации о версии ПО по команде «**show version**»;
- вывод сообщений из журнала событий с указанием даты, времени и типа события по команде «**show logging**»;
- вывод сообщений из журнала загрузки ПО с указанием даты и времени загрузки ПО по команде «**show logging boot**»;
- вывод информации об SFP-модулях на портах 1000BASE-X/10G BASE-X по команде «**show idprom**»;
- вывод информации о настройках терминала по команде «**show terminal**»;
- вывод информации о коммутаторе по команде «**show switch**».

4.1.2 show debug action

Команда доступна из любого режима. Вывод информации о состоянии специальных диагностических действий.

Синтаксис команды:

show debug action {**reload-on-crash** | **save-crash-dump**}

Параметры команды:

reload-on-crash	информация о состоянии режима перезагрузки оборудования при возникновении критической ошибки в ПО
save-crash-dump	информация о состоянии режима сохранения аварийных дампов в постоянной памяти оборудования

Примеры команды:

```
admin@Switch# show debug action reload-on-crash

Switch0:
  reload-on-crash: true

admin@Switch#
```

```
admin@Switch# show debug action save-crash-dump

Switch0:
  save-crash-dump: false
  crash-dump location:

admin@Switch#
```

4.1.3 show hostname

Фундаментальная команда. Вывод имени устройства. Имя устройства отображается в приглашении CLI.

Синтаксис команды:

show hostname

Пример команды:

```
admin@Switch# show hostname
Hostname: Switch
admin@Switch#
```

4.1.4 show idprom interface

Фундаментальная команда. Вывод информации об SFP-модулях для определённых портов 1000BASE-X / 10G BASE-X.

Синтаксис команды:

show idprom interface *interface-id*

Использование команды:

- если модуль подключен – выводит информацию об SFP-модулях;
- если модуль не подключен – **no sfp in requested port**;
- указан интерфейс, на котором нет модуля - **wrong interface**;
- указан id несуществующего устройства - **remote device not found**.

Параметры команды:

interface-id	идентификатор интерфейса

Пример команды:

```
admin@Switch# show idprom interface tengigabitethernet 0/1
Base ID fields:
Identifier: 0x03 (SFP or SFP+)
Extended Identifier: 0x04
Connector: 0x07 (LC)
Compliance codes: 0x00 0x00 0x00 0x40 0x00 0x00 0x00 0x00
Encoding: 0x01
Bit-rate Nominal: 1300 Mbps
Rate Identifier: 0x00
Length: 20 km
Vendor Name: PLGN
Vendor OUI: 0x00
Vendor Part Number: SFP-PLGN-GE-SM-1
Vendor Revision: 1.0
Laser Wavelength: 1310 nm
Reserved: 0x00
[output truncated]
```

4.1.5 show inventory

Фундаментальная команда. Вывод информации об устройстве.

Синтаксис команды:

show inventory

Пример команды:

```
admin@Switch# show inventory
Switch0:
Device ID: Акманай-2xxx
Hardware version: 2.0 12.10.2012
Chip1 revision: C0
Serial number: 916531
```

4.1.6 show location

Фундаментальная команда. Вывод общей информации о местоположении устройства. Выводит значение параметра, устанавливаемого командой «**snmp-server location**».

Синтаксис команды:

show location

Пример команды:

```
admin@Switch# show location
Location: Ufa, Russia
admin@Switch#
```

4.1.7 show logging

Фундаментальная команда. Вывод сообщений из журнала событий с указанием даты, времени и типа события. Журналирование до 5120 записей или не больше 320КБ. Типы и формат журналируемых событий приведены в Приложении Б.

Синтаксис команды:
show logging [**boot** | **hosts**]
Параметры команды:

boot	вывод информации о загрузке прошивок с указанием даты, времени и информации о прошивке
hosts	вывод информации о работе настроенных серверов

Пример команды:

```
admin@Switch# show logging
Date                  Event
--------------------  --------------------------------
11.01.2021 05:02:39   %SYS-6-STARTED: Device initialization complete
11.01.2021 05:07:27   %AAA-6-SUCCESS: Authentication successful for admin using rs232
11.01.2021 05:07:57   %CFG-4-CHANGED: Configuration changed by admin
11.01.2021 23:43:44   %SYS-5-REBOOT: Device 1 is going to reboot
admin@Switch#
```

4.1.8 show logging boot

Фундаментальная команда. Вывод сообщений из журнала загрузки ПО с указанием даты и времени загрузки ПО.

Синтаксис команды:
show logging boot *unit-id*
Параметры команды:

unit-id	выбор определенного члена стека, для которого необходимо отобразить журнал загрузки ПО

Пример команды:

```
admin@Switch# show logging boot
Date                  Event
--------------------  --------------------
20.12.2020 16:30:18   Device 0: Loading Image-2
20.12.2020 17:40:25   Device 0: Loading Image-2
```

4.1.9 show terminal

Фундаментальная команда. Вывод информации о настройках терминала.

Синтаксис команды:
show terminal
Пример команды:

```
admin@Switch# show terminal
Terminal information:
--------------------
Height: 51 line(s)
Width: 80 column(s)
Session-timeout: not set
Terminal type: vt102
admin@Switch#
```

4.1.10 show version

Команда, доступная из любого режима. Вывод информации о версии программного обеспечения и аппаратной части.

Синтаксис команды:

show version

Использование команды:

Команда «**show version**» используется для вывода информации о версии программного обеспечения и аппаратной части.

Пример команды:

```
admin@Switch# show version

Switch: 0

Software version: 1.1.2
Hardware version: 2.0
----------------------
Uptime: 0 days, 0 hours, 34 minutes
```

4.1.11 show system mtu

Фундаментальная команда. Вывод информации о максимальном размере MTU (Maximum Transmission Unit).

Синтаксис команды:

show system mtu

Пример команды:

```
admin@Switch# show system mtu
System MTU size is 1600 bytes
```

4.2 Управление учетными записями пользователей

4.2.1 Разграничение доступа

Учетные записи пользователей предназначены для разграничения прав доступа пользователей коммутатора.

Система управления коммутатора поддерживает два типа прав пользователей:

- «Администратор» – пользователь с данными правами может просматривать и изменять значения параметров коммутатора;
- «Пользователь» – пользователь с данными правами может просматривать значения параметров и состояний коммутатора (включая записи в журнале событий), а также изменять собственный пароль.

Изначально коммутатор содержит только одну встроенную учетную запись с правами администратора “admin” с паролем “admin”. Общее количество пользователей не ограничено.

При подключении к коммутатору необходимо провести авторизацию пользователя, то есть ввести имя и пароль пользователя.

Права учетной записи пользователя определяют видимость команд, т.е. команды, недоступные пользователю, не будут видны (в ответ на такие команды будет выдаваться сообщение об их отсутствии).

Для добавления, удаления и смены пароля учетных записей применяется команда «**username**».

Вывод списка учетных записей пользователей осуществляется с помощью команды «**show users**».

4.2.2 username

Команда глобальной настройки. Добавление, удаление и смена пароля учетных записей пользователей.

Синтаксис команды:

username *user-name* **[password** *password***] [role {user | admin}]**

no username *user-name*

Команда с приставкой «**no**» удаляет учетную запись пользователя.

Параметры команды:

user-name	имя пользователя в виде текстовой строки
password *password*	пароль пользователя в виде текстовой строки. Если пароль пользователя не задан, то он будет пустым
role {user | admin}	роль (права) пользователя («user» – пользователь, «admin» – администратор). Если права пользователя не заданы, то пользователю присваиваются права «user»

Использование команды:

Учетная запись «admin» не может быть удалена.

Пользователь учетной записи с правами «admin» может менять пароль любой учетной записи, для этого необходимо ввести команду с указанием имени пользователя и нового пароля.

Пользователь учетной записи с правами «user» может менять пароль только собственной учетной записи.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# username ivan password navi role admin
admin@Switch(config)# end
admin@Switch#
```

4.2.3 username sshkey

Команда глобальной настройки. Установка ключа SSH для существующей учетной записи пользователя.

Синтаксис команды:

username *user-name* **sshkey** {**ssh-dss** | **ssh-rsa** | **ssh-ed25519**} *key*

Параметры команды:

user-name	имя пользователя в виде текстовой строки
sshkey {**ssh-dss** | **ssh-rsa** | **ssh-ed25519**}	выбор типа SSH-ключа
key	ввод SSH-ключа

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# username user sshkey ssh-dss 12345678
admin@Switch(config)# end
admin@Switch#
```

4.2.4 show users

Фундаментальная команда. Вывод списка учетных записей пользователей.

Синтаксис команды:

show users

Пример команды:

```
admin@Switch# show users
User name   Role   Key
---------   -----  --------
admin       admin  no
User        user   ssh-dss

admin@Switch#
```

4.2.5 show user

Фундаментальная команда. Вывод основной информации для отдельной учетной записи.

Синтаксис команды:

show user *username*

Параметры команды:

username имя пользователя в виде текстовой строки

Пример команды:

```
admin@Switch# show user admin

Login: admin
Role: admin
Public key: no

admin@Switch#
```

4.3 Настройка времени и даты

4.3.1 Общие положения

Коммутатор обеспечивает:

- установку системного времени и даты с помощью команды «**clock set**»;
- установку часового пояса и смещения относительно нулевого меридиана в часах и минутах с помощью команды «**clock timezone**»;
- установку времени и даты перехода на летнее или зимнее время с помощью команды «**clock summer-time**»;
- включение аутентификации трафика, принятого от серверов NTP, с помощью команды «**ntp authenticate**»;
- установку ключа аутентификации для протокола NTP с помощью команды «**ntp authentication-key**»;
- установку номера ключа аутентификации для сервера NTP с помощью команды «**ntp trusted-key**»;
- вывод списка NTP-серверов с помощью команды «**show ntp**»;
- вывод информации о состоянии NTP-серверов с помощью команды «**show ntp status**».

Вывод текущего времени и даты, а также настроек часового пояса и параметров перехода на зимнее или летнее время осуществляется с помощью команды «**show clock detail**».

4.3.2 clock set

Фундаментальная команда. Установка значения системного времени.
Синтаксис команды:
clock set *time day month year*
Параметры команды:

time	время в формате: ЧЧ:ММ:СС
day	день месяца в диапазоне от 1 до 31
month	месяц года: January, February, March, April, May, June, July, August, September, October, November, December
year	год в диапазоне от 2000 до 2037

Пример команды:

```
admin@Switch# clock set 18:00:00 20 December 2020
admin@Switch#
```

4.3.3 clock summer-time

Команда глобальной настройки. Установка времени и даты перехода на летнее или зимнее время.

Синтаксис команды:

clock summer-time *zone-name start-week start-day start-month start-time endweek end-day end-month end-time offset-minutes*

no clock summer-time

Команда с приставкой «**no**» устанавливает параметры по умолчанию.

Параметры команды:

zone-name	аббревиатура часового пояса в виде текстовой строки
start-week	номер недели месяца для перехода на летнее время в диапазоне от 1 до 5. Номер недели, равный 5, означает последнюю неделю месяца
start-day	день недели для перехода на летнее время из списка: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
start-month	месяц для перехода на летнее время из списка: January, February, March, April, May, June, July, August, September, October, November, December
start-time	время для перехода на летнее время в формате ЧЧ:ММ
end-week	номер недели месяца для перехода на зимнее время в диапазоне от 1 до 5. Номер недели, равный 5, означает последнюю неделю месяца
end-day	день недели для перехода на зимнее время из списка: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
end-month	месяц для перехода на зимнее время из списка: January, February, March, April, May, June, July, August, September, October, November, December
end-time	время для перехода на зимнее время в формате ЧЧ:ММ
offset-minutes	количество минут смещения времени в диапазоне от 1 до 1440

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# clock summer-time YEKT 5 Saturday March 5 Saturday October 300
admin@Switch(config)# end
admin@Switch#
```

4.3.4 clock timezone

Команда доступна из любого режима. Установка часового пояса и смещения относительно нулевого меридиана в часах и минутах.

Синтаксис команды:

clock timezone *zone-name offset-hours offset-minutes*

no clock timezone

Команда с приставкой «**no**» устанавливает значение часового пояса «YEKT», смещение в часах, равное 5, смещение в минутах, равное 0.

Параметры команды:

zone-name	аббревиатура часового пояса в виде строки: «PST», «EST»
offset-hours	смещение в часах относительно UTC в диапазоне от -23 до 23
offset-minutes	смещение в минутах относительно UTC в диапазоне от 0 до 59

Пример команды:

```
admin@Switch# clock timezone YEKT 5 0
admin@Switch#
```

4.3.5 ntp authenticate

Команда глобальной настройки. Включение аутентификации трафика, принятого от серверов NTP.

Синтаксис команды:

ntp authenticate

no ntp authenticate

Команда с приставкой «**no**» отключает функцию.

Значение по умолчанию:

По умолчанию аутентификация отключена.

Использование команды:

Команда применима как к обычному, так и широковещательному трафику.

Пример команды:

```
admin@Switch(config)# ntp authenticate
admin@Switch(config)# ntp authentication-key 8 md5 ClkKey
admin@Switch(config)# ntp trusted-key 8
```

4.3.6 ntp authentication-key

Команда глобальной настройки. Установка ключа аутентификации для протокола NTP (Network Time Protocol).

Синтаксис команды:
ntp authentication-key *key-number* **md5** *key-value*
no ntp authentication-key *key-number*
no ntp authentication-keys
Команда с приставкой «**no**» удаляет ключ аутентификации для протокола NTP.
Параметры команды:

key-number	номер ключа в диапазоне от 1 до 65535
key-value	значение ключа длиной до 8 символов

Значение по умолчанию:
По умолчанию ключи аутентификации отсутствуют.
Пример команды:

```
admin@Switch(config)# ntp authentication-key 8 md5 ClkKey
admin@Switch(config)# ntp trusted-key 8
admin@Switch(config)# ntp authenticate
```

4.3.7 ntp master

Команда глобальной настройки. Используйте команду «**ntp master**» для включения режима работы NTP в качестве сервера. Эта функция позволяет сократить обмен пакетами NTP по вышестоящему каналу передачи данных и уменьшить нагрузку на вышестоящий сервер NTP.
Синтаксис команды:
ntp master [*stratum*]
no ntp master
Используйте команду с приставкой «**no**» для отключения функции.
Параметры команды:

stratum	(опционально) номер уровня в иерархии. Диапазон значений от 1 до 15. По умолчанию равен 8

Значение по умолчанию:
Устройство не работает в режиме сервера NTP.
По умолчанию номер уровня в иерархии равен 8.
Использование команды:
Будьте осторожны при установке уровня иерархии в случае, если клиенты синхронизируются от нескольких серверов NTP. Установка высокого уровня иерархии может привести к тому, что клиенты будут выбирать менее точный источник (локальное устройство) в качестве сервера синхронизации.
Пример команды:
Следующий пример показывает, как включить режим работы NTP в качестве сервера:

```
admin@Switch# configure terminal
admin@Switch(config)# ntp master
admin@Switch(config)#
```

4.3.8 ntp server

Команда глобальной настройки. Добавление сервера NTP.

Синтаксис команды:

ntp server *ip-address* [**trusted-key** *key-number*]

no ntp server *ip-address* [**trusted-key** *key-number*]

Используйте команду с приставкой «**no**» для отключения функции. Команда «**no ntp servers**» удаляет все ntp сервера.

Параметры команды:

ip-address	IP-адрес сервера
trusted-key *key-number*	номер ключа аутентификации в диапазоне от 1 до 65535. Если ключ аутентификации не задан, то сервер может быть подключен без аутентификации

Значение по умолчанию:

По умолчанию сервер не назначен.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ntp server 192.168.10.100 trusted-key 1
admin@Switch(config)#
```

4.3.9 ntp trusted-key

Команда глобальной настройки. Установка номера ключа аутентификации для сервера NTP.

Синтаксис команды:

ntp trusted-key *key-number*

ntp trusted-keys *key-number* | *key list* | *key range*

no ntp trusted-key *key-number*

no ntp trusted-keys [*key-number* | *key list* | *key range*]

Команда «**no ntp trusted-key** *key-number*» удаляет номер ключа аутентификации для сервера NTP. Команда «**no ntp trusted-keys**» удаляет все номера ключей аутентификации для сервера NTP.

Параметры команды:

key-number	номер ключа аутентификации в диапазоне от 1 до 65535
key list	список ключей аутентификации в диапазоне от 1 до 65535 (1,5)
key range	диапазон ключей аутентификации от 1 до 65535 (1-10)

Значение по умолчанию:

По умолчанию ключи аутентификации не заданы.

Пример команды:

```
admin@Switch(config)# ntp trusted-key 8
admin@Switch(config)# ntp authentication-key 8 md5 ClkKey
admin@Switch(config)# ntp trusted-key 8
admin@Switch(config)# ntp authenticate
```

4.3.10 show clock

Фундаментальная команда. Вывод текущего времени и даты.
Синтаксис команды:
show clock [**detail**]
Параметры команды:

detail вывод текущего часового пояса и настроек перехода на летнее/зимнее время

Пример команды:

```
admin@Switch# show clock detail
17:04:00 YEKT Dec 20 2020
Timezone: YEKT +5:00
Summer time: Sunday, last week March, 3:00
Winter time: Sunday, last week October, 3:00
admin@Switch#
```

4.3.11 show ntp

Команда, доступная из любого режима. Вывод настроек NTP.
Синтаксис команды:
show ntp
Пример команды:

```
admin@Switch#
Local device is not NTP master.

NTP servers:
-----------
192.168.1.100

NTP Authentication
Use authentication: disable
Authentication keys:
Number   Key Value
------   ---------
1         abcdef
Trusted key: 1
```

4.3.12 show ntp status

Фундаментальная команда. Вывод информации о состоянии NTP-серверов.
Синтаксис команды:
show ntp status

Пример команды:

```
admin@Switch# show ntp status
remote          refid        st  t  when  poll  reach  delay  offset  jitter
==============================================================================
*192.168.0.10   91.209.94.10  2   u  33    64    377 0.188  -0.402  0.300

ind  assid   status  conf  reach  auth   condition  last_event  cnt
===========================================================================
1    37167   966a    yes   yes none   sys.peer   sys_peer    6
```

- **remote** – адрес ntp сервера;
- **refid** – показывает откуда этот сервер берет время;
- **st** (Stratum) – слой в котором работает данный сервер, число от 1 до 16 указывающее удаление от источника синхронизации. Слой данного сервера на 1 больше слоя сервера, по которому идет синхронизация;
- **t** – тип удаленного сервера (local, unicast, multicast or broadcast);
- **when** – сколько секунд назад был получен последний пакет от данного сервера;
- **poll** – период опроса сервера в секундах;
- **reach** – восьмеричное представление массива из 8-ми бит, в котором фиксируется 8 последних попыток синхронизации. Если попытка была успешной, то устанавливается 1. Значение 377 говорит о том, что все 8 последних попыток были удачными;
- **delay** – вычисленная задержка ответов от сервера в миллисекундах;
- **offset** – разница во времени между локальным и удаленным сервером в миллисекундах;
- **jitter** – дисперсия отклонения удаленных часов относительно локальных, вычисленная по нескольким последним запросам в миллисекундах.

4.4 Настройка общих параметров

4.4.1 Общие положения

Коммутатор обеспечивает:

- вход в режим глобальной настройки с помощью команды «**configure terminal**»;
- возврат в предыдущий режим CLI с помощью команды «**end**»;
- копирование файлов с помощью команды «**copy**»;
- удаление файлов с помощью команды «**delete**»;
- вывод списка файлов в каталоге с помощью команды «**dir**»;
- вывод различного текста с помощью команды «**echo**»;
- установку имени устройства, отображаемого в приглашении командной строки, с помощью команды «**hostname**»;
- добавление syslog-сервера для журналирования событий с помощью команды «**logging host**»;
- завершение сеанса управления и отображение запроса имени пользователя и пароля с помощью команды «**logout**»;
- добавление NTP-сервера с помощью команды «**ntp server**»;
- отправку ICMP-запросов на определенный IP-адрес или доменное имя с помощью команды «**ping**»;
- включение передачи фреймов длиной до 10000 байт (jumbo-frame) с помощью команды «**port jumbo-frame**»;
- перезагрузку с помощью команды «**reload**»;
- переименование файла настроек с помощью команды «**rename**»;
- запуск скрипта из файла на исполнение с помощью команды «**run-script**»;
- установку таймаута неактивности пользователя, после которого происходит автоматическое завершение сессии управления, с помощью команды «**terminal session-timeout**»;
- установку типа используемого эмулятора терминала с помощью команды «**terminal type**»;
- трассировку маршрута до сетевого устройства с помощью команды «**traceroute**»;
- подключение к хосту по протоколу Telnet с помощью команды «**telnet**»;
- подключение к хосту по протоколу SSH с помощью команды «**ssh**»;
- вывод информации об использовании CPU с помощью команды «**show cpu utilization**»;
- вывод списка syslog-серверов с помощью команды «**show logging hosts**»;

– вывод текущего значения настройки передачи фреймов длиной до 10000 байт (jumbo-frame) с помощью команды «**show port-jumbo frame**».

4.4.2 configure terminal

Команда фундаментального режима. Вход в режим глобальной настройки. Данную команду необходимо вводить только в режиме фундаментальных команд.

Синтаксис команды:
configure terminal
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)#
```

4.4.3 copy

Команда фундаментального режима. Копирование файлов конфигурации во внутреннюю память устройства или на внешние носители информации, включая внешние серверы.

Синтаксис команды:
copy *src-url dest-url*
Параметры команды:

src-url URL источника

dest-url URL назначения

В качестве префиксов URL могут выступать:

usb0:// копирование файлов конфигурации с внешнего носителя или на внешний носитель, подключенный к разъему USB № 1.
Синтаксис: **usb0**://[*directory*/]*filename*

usb1:// копирование файлов конфигурации с внешнего носителя или на внешний носитель, подключенный к разъему USB № 2.
Синтаксис: **usb1**://[*directory*/]*filename*

tftp:// копирование файлов конфигурации на внешний сервер TFTP или с внешнего сервера. Префикс не может одновременно использоваться в URL источника и URL назначения.
Синтаксис: **tftp**://[*location*/][*directory*/]*filename*

ftp:// копирование файлов конфигурации на внешний сервер FTP или с внешнего сервера.
Синтаксис:
tftp://[*username*[:*password*]@]*location*/[*directory*/]*filename*
Если имя учетной записи «*username*» и пароль «*password*» не указаны, то устройство производит анонимное подключение. Если пароль не указан, то он равен пустой строке

scp:// копирование файлов конфигурации на внешний сервер или с внешнего сервера по протоколу SCP.
Синтаксис:
scp://[*username*[:*password*]@]*location*/[*directory*/]*filename*
Если пароль не указан, то он равен пустой строке

Зарезервированные слова команды:

running-config копирование текущей конфигурации. Может использоваться только в качестве URL источника

startup-config копирование в файл и из файла конфигурации, используемого при загрузке

crash-dump копирование файла аварийного дампа

service-log копирование файла журнала диагностики внутренних сервисов

Использование команды:

Команда «**copy**» используется для копирования файлов конфигурации во внутреннюю память устройства или на внешние носители информации, включая внешние серверы. Если префикс URL не задан, то копирование производится во внутреннюю память.

Форматы URL:

Устройство позволяет копировать файлы конфигурации с внешних источников, таких как TFTP-сервер и накопитель данных, подключенный через один из разъемов USB. При копировании файлов конфигурации из внешних источников устройство не проверяет их правильность, поэтому вся ответственность лежит целиком на пользователе. Если копирование невозможно из-за отсутствия свободного места на носителе информации, будет выведено сообщение: «Copy failed: not enough free space».

Если при копировании по протоколу SCP устройство обнаруживает, что у удаленного сервера изменился ключ SSH, то устройство выводит сообщение об ошибке и завершает работу команды. Если удаленный сервер является легитимным хостом, но его ключ изменился по какой-либо причине, удалите старый SSH-ключ хоста с помощью команды «**clear ssh hosts**».

Внешние носители USB могут быть недоступны для некоторых модификаций устройства.

Примеры команды:

```
admin@Switch# copy running-config my.conf
admin@Switch#
```

```
admin@Switch# copy my.conf usb0://my.conf
admin@Switch#
```

```
admin@Switch# copy tftp://192.168.0.1/my.conf startup-config
admin@Switch#
```

4.4.4 clear log

Команда фундаментального режима. Очистка журнала событий.

Синтаксис команды:

clear log

Использование команды:

Команда «**clear log**» используется для очистки журнала событий. События из журнала будут удалены перманентно.

Пример команды:

```
admin@Switch# clear log
admin@Switch#
```

4.4.5 clear service-log

Команда фундаментального режима. Очистка файла журнала диагностики внутренних сервисов.

Синтаксис команды:

clear service-log

Использование команды:

Команда «**clear service-log**» используется для очистки журнала диагностики внутренних сервисов. События из журнала будут удалены перманентно.

Пример команды:

```
admin@Switch# clear service-log
admin@Switch#
```

4.4.6 clear debug files

Команда фундаментального режима. Очистка журнала диагностики.

Синтаксис команды:

clear debug files

Использование команды:

Команда «**clear debug files**» используется для очистки журнала диагностики. Журнал будет удален перманентно.

Пример команды:

```
admin@Switch# clear debug files
admin@Switch#
```

4.4.7 clear boot log

Команда фундаментального режима. Очистка журнала загрузки ПО.

Синтаксис команды:

clear boot log *unit-id*

Параметры команды:

unit-id	выбор определенного члена стека, на котором будет удален журнал загрузки ПО.

Использование команды:

Команда «**clear boot log**» используется для очистки журнала загрузки ПО. Журнал будет удален перманентно.

Пример команды:

```
admin@Switch# clear boot log
admin@Switch#
```

4.4.8 clear ssh hosts

Команда фундаментального режима. Удаление всех открытых ключей SSH посещенных хостов.

Синтаксис команды:

clear ssh hosts

Пример команды:

```
admin@Switch# clear ssh hosts
admin@Switch#
```

4.4.9 clear ssh host

Команда фундаментального режима. Удаление открытых ключей SSH указанных хостов.

Синтаксис команды:

clear ssh host [*ip-address* | *hostname*]

Параметры команды:

ip-address IP-адрес хоста

hostname доменное имя хоста

Использование команды:

Команда «**clear ssh host**» используется для удаления открытых ключей SSH посещенных хостов.

При подключении к хосту по протоколу SSH с помощью команды «**ssh**» устройство автоматически сохраняет открытый ключ SSH хоста для дальнейшего использования. При повторной генерации ключа SSH на хосте (в частности, при физической замене оборудования хоста) старый и новый ключи не будут совпадать, что приведет к невозможности подключения к хосту по протоколу SSH. Удалите старый ключ хоста с помощью команды «**clear ssh host**», и устройство автоматически сохранит новый ключ при подключении к хосту.

Пример команды:

```
admin@Switch# clear ssh hosts 192.168.10.10
admin@Switch#
```

4.4.10 debug action

Команда фундаментального режима. Включение специальных диагностических действий.

Синтаксис команды:
debug action {reload-on-crash | save-crash-dump}
no debug action reload-on-crash
no debug action save-crash-dump
Команда с приставкой «**no**» отключает специальные диагностические действия.
Параметры команды:

reload-on-crash перезагрузка оборудования при возникновении критической ошибки в ПО

save-crash-dump сохранение аварийных дампов в постоянной памяти оборудования

Значение по умолчанию:
По умолчанию включен режим «**debug action reload-on-crash**».
Пример команды:

```
admin@Switch# debug action save-crash-dump
admin@Switch#
```

4.4.11 debug core-dumps

Команда фундаментального режима. Включение диагностики ядра ОС Linux.
Синтаксис команды:
debug core-dumps
no debug core-dumps
Команда с приставкой «**no**» отключает данную функцию.
Пример команды:

```
admin@Switch# debug core-dumps
admin@Switch#
```

4.4.12 delete

Команда фундаментального режима. Удаление файлов конфигурации и директорий.
Синтаксис команды:
delete *file-url*
Параметры команды:

file-url URL файла (директории), который нужно удалить

В качестве префиксов URL могут выступать:

usb0:// удаление файлов конфигурации на внешнем носителе, подключенном к разъему USB №1. Данный аргумент поддерживается не на всех версиях устройства

usb1:// удаление файлов конфигурации на внешнем носителе, подключенном к разъему USB №2. Данный аргумент поддерживается не на всех версиях устройства

Зарезервированные слова команды:

startup-config удаление файла конфигурации, используемого при загрузке

Использование команды:

Команда «**delete**» используется для удаления файлов конфигурации и директорий во внутренней памяти коммутатора или на внешних носителях информации. Если префикс URL не задан, то производится удаление файлов во внутренней памяти.

Коммутатор не выводит дополнительного запроса на подтверждение об удалении файла. Будьте внимательны при вводе команды удаления.

Пример команды:

```
admin@Switch# delete my.conf
admin@Switch#
```

4.4.13 dir

Команда фундаментального режима. Вывод содержимого директорий файловой системы.

Синтаксис команды:

dir {config | tls | *directory-url***}**

Параметры команды:

config вывод списка файлов конфигурации, находящихся во внутренней памяти устройства

tls вывод содержимого директории с сертификатом TLS

directory-url URL директории, информацию о которой необходимо отобразить

В качестве префиксов URL могут выступать:

usb0:// вывод содержимого директорий внешнего носителя, подключенного к разъему USB №1. Данный аргумент поддерживается не на всех версиях устройства

usb1:// вывод содержимого директорий внешнего носителя, подключенного к разъему USB №2. Данный аргумент поддерживается не на всех версиях устройства

debug-files:// вывод содержимого директорий с диагностической информацией

Использование команды:

Команда «**dir**» используется для вывода содержимого директорий файловой системы во внутренней памяти коммутатора или на внешних носителях информации. Если URL директории не задан, то выводится содержимое внутренней директории коммутатора, в которой хранятся файлы конфигурации.

Пример команды:

```
admin@Switch# dir config
startup.conf
admin@Switch#
```

4.4.14 mkdir

Команда фундаментального режима. Создание директории на внешних носителях.

Синтаксис команды:

mkdir *directory-url*

Параметр команды:

directory-url URL директории, которую необходимо создать

В качестве префиксов URL могут выступать:

usb0:// вывод содержимого директорий внешнего носителя, подключенного к разъему USB №1. Данный аргумент поддерживается не на всех версиях устройства

usb1:// вывод содержимого директорий внешнего носителя, подключенного к разъему USB №2. Данный аргумент поддерживается не на всех версиях устройства

Использование команды:

Команда «**mkdir**» используется для создания директории на внешних носителях. При создании вложенной директории необходимо, чтобы директории, расположенные выше по иерархии, существовали на момент выполнения команды.

Если директорию создать невозможно по какой-либо причине, то будет выведено сообщение об ошибке: «Can not create directory».

Пример команды:

```
admin@Switch# mkdir usb0://test
admin@Switch#
```

4.4.15 echo

Команда фундаментального режима. Вывод различного текста.

Синтаксис команды:

echo [backslash-interpret] [*text*]

Параметры команды:

backslash-interpret интерпретация символов после «\» как управляющих символов

text текст для отображения. Текст может включать обращение к переменным окружения

Использование команды:
Опции форматирования:

\b	удаление символа
\c	удаление символа перевода строки в конце текста
\f	вставка символа Form Feed
\n	перевод строки
\r	возврат каретки
\t	вставка горизонтальной табуляции
\v	вставка вертикальной табуляции
\\	вставка символа «\»
\nnn	вставка ASCII-символа с восьмеричным кодом «nnn»

Пример команды:

```
admin@Switch# echo backslash-interpret text\n\r
text
admin@Switch#
```

4.4.16 end

Команда фундаментального режима. Возврат в предыдущий режим CLI.
Синтаксис команды:
end
Использование команды:
Реакция на ввод данной команды зависит от текущего режима работы CLI:

- режим фундаментальных команд: команда игнорируется (для выхода из CLI используется команда «**exit**»);
- режим глобальной настройки: переход в режим фундаментальных команд;
- режим настройки интерфейсов: переход в режим глобальной настройки;
- режим настройки VLAN: переход в режим глобальной настройки.

Пример команды:

```
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

4.4.17 exit

Команда фундаментального режима. Выход из CLI.
Синтаксис команды:
exit

Пример команды:

```
admin@Switch# exit

Connection closed by foreign host.
```

4.4.18 hostname

Команда глобальной настройки. Установка имени устройства, отображаемого в приглашении командной строки.

Синтаксис команды:

hostname *name*

no hostname

Команда с приставкой «**no**» устанавливает значение по умолчанию «Switch».

Параметры команды:

name	имя устройства, которое будет отображаться в приглашении командной строки

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# hostname Akmanay

Hostname changed
admin@Akmanay(config)#
```

4.4.19 ip http server

Команда глобальной настройки. Включение управления по протоколу HTTP.

Синтаксис команды:

ip http server

no ip http server

Команда с приставкой «**no**» отключает управление по протоколу HTTP.

Значение по умолчанию:

Управление по протоколу HTTP отключено.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip http server
admin@Switch(config)#
```

4.4.20 ip http secure-server

Команда глобальной настройки. Включение управления по протоколу HTTPS.

Синтаксис команды:

ip http secure-server

no ip http secure-server

Команда с приставкой «**no**» отключает управление по протоколу HTTPS.

Значение по умолчанию:

Управление по протоколу HTTPS отключено.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip http secure-server
admin@Switch(config)#
```

4.4.21 ip telnet server

Команда глобальной настройки. Включение управления по протоколу Telnet.

Синтаксис команды:

ip telnet server

no ip telnet server

Команда с приставкой «**no**» отключает управление по протоколу Telnet.

Значение по умолчанию:

Управление по протоколу Telnet отключено.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip telnet server
admin@Switch(config)#
```

4.4.22 locator-led

Команда фундаментального режима. Включение кнопок-индикатора на корпусе устройства (светодиода ID).

Синтаксис команды:

locator-led {*unit-id*}

no locator-led {*unit-id*}

Команда с приставкой «**no**» отключает кнопку-индикатора на корпусе устройства (светодиод ID).

Параметры команды:

init-id (опционально) идентификатор устройства в стеке. Если параметр не задан, то команда применяется для текущего устройства

Пример команды:

```
admin@Switch# locator-led
admin@Switch#
admin@Switch# no locator-led
admin@Switch#
```

4.4.23 logging host

Команда глобальной настройки. Добавление syslog-сервера для журналирования событий.

Синтаксис команды:

logging host *ip-address*

no logging host *ip-address*

Команда с приставкой «**no**» удаляет syslog-сервер из списка.

Параметры команды:

ip-address IP-адрес хоста

Значение по умолчанию:
По умолчанию syslog-серверы не заданы.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# logging host 192.168.1.1
```

4.4.24 logging console

Команда глобальной настройки. Включение вывода сообщений системного журнала в консоль.

Синтаксис команды:
logging console *level*
no logging console
Команда с приставкой «**no**» отключает вывод сообщений в консоль.
Параметры команды:

level уровень выводимых сообщений:

0 – emergencies

1 – alerts

2 – critical

3 – errors

4 – warnings

5 – notifications

6 – informational

7 – debugging

Значение по умолчанию:
По умолчанию установлен 5 уровень сообщений.
Команда «**logging console**» без параметра устанавливает значение по умолчанию.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# logging console 3
admin@Switch(config)#
```

4.4.25 logout

Команда фундаментального режима. Завершение сеанса управления и отображение запроса имени пользователя и пароля.

Синтаксис команды:
logout
Пример команды:

```
admin@Switch# logout
Switch login:
```

4.4.26 more

Команда фундаментального режима. Отображение содержимого указанного файла.

Синтаксис команды:
more {startup-config | *path-url*}
Параметры команды:

startup-config отображение содержимого конфигурации, используемого при загрузке коммутатора

В качестве префиксов path-url могут выступать:

config:// путь до файла конфигурации

debug-files:// путь до файла отладки

usb0:// путь до файла на внешнем носителе, подключенному к разъему USB №1

usb1:// путь до файла на внешнем носителе, подключенному к разъему USB №2

Пример команды:

```
admin@Switch# more debug-files://manager-logs/0
rm: can't remove '/var/tmp/manager.stopped': No such file or directory
Erlang/OTP 20 [erts-9.0] [source-a464e5f] [async-threads:10] [kernel-poll:false]
=progress report==== 1-jan-1970::0:1:59 ===
  supervisor: {local,sasl_safe_sup}
   started: [{pid,<0.1288.0>},
    {id,alarm_handler},
    {mfargs,{alarm_handler,start_link,[]}},
    {restart_type,permanent},
    {shutdown,2000},
    {child_type,worker}]
[output truncated]
```

4.4.27 ntp server

Команда глобальной настройки. Добавление NTP-сервера с адресом «ip-address».

Синтаксис команды:
ntp server *ip-address*
no ntp server *ip-address*

Команда с приставкой «**no**» удаляет NTP-сервер с адресом «ip-address».

Параметры команды:

ip-address IP-адрес NTP-сервера

Значение по умолчанию:

По умолчанию NTP-серверы не заданы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ntp server 192.168.1.100
```

4.4.28 ping

Команда фундаментального режима. Отправка ICMP эхо-запросов на определенный IP-адрес или доменное имя.

Синтаксис команды:

ping {*dest-ipv4-address* | *hostname*} **[count** {*number* | **unlimited**}] **[packet-size** *bytes*] **[source vlan** *vlan-id*]

Параметры команды:

dest-ipv4-address	IP-адрес назначения
hostname	доменное имя назначения
count	установка количества эхо-запросов для отправки
number	количество эхо-запросов для отправки в диапазоне от 1 до $(2^{32} – 1)$. По умолчанию равно 5
packet-size *bytes*	установка размера пакета в диапазоне от 1 до 75468. По умолчанию размер пакета – 56 байт
source vlan *vlan-id*	использовать IP-адрес с интерфейса VLAN, имеющего идентификатор «*vlan-id*»

Пример команды:

```
admin@Switch# ping 192.168.0.1 count 2
PING 192.168.0.1 (192.168.0.1) 56 data bytes
64 bytes from 192.168.0.1: seq=0 ttl=64 time=2.646 ms

64 bytes from 192.168.0.1: seq=1 ttl=64 time=0.577 ms
-- 192.168.0.1 ping statistics --
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.577/1.611/2.646 ms
admin@Switch#
```

4.4.29 port jumbo-frame

Команда глобальной настройки. Включение передачи фреймов длиной до 10000 байт (jumbo-frame).

Синтаксис команды:

port jumbo-frame

no port jumbo-frame

Команда с приставкой «**no**» отключает передачу фреймов длиной до 10000 байт (jumbo-frame).

Значение по умолчанию:

По умолчанию данная настройка выключена.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# port jumbo-frame
```

4.4.30 reload

Команда фундаментального режима. Перезагрузка устройства.

Синтаксис команды:

reload [slot *slot-id* **] [{at** *time day month year* **| in** *interval* **}] [cancel]**

Параметры команды:

slot *slot-id*	номер члена стека в диапазоне от 1 до 5
at	выполнение отложенной перезагрузки устройства в определенную дату и время
time	время в формате “ЧЧ:ММ:СС”
day	день месяца в диапазоне от 1 до 31
month	месяц года из списка: January, February, March, April, May, June, July, August, September, October, November, December
year	год в диапазоне от 2000 до 2037
in	выполнение отложенной перезагрузки через определенный интервал времени
interval	интервал времени в формате “ЧЧ:ММ:СС”
cancel	отмена запланированной перезагрузки устройства

Значение по умолчанию:

Отложенная перезагрузка отключена.

Использование команды:

Команда «**reload**» используется для перезагрузки устройства. Если команда введена без аргументов «**at**» или «**in**», то перезагрузка производится немедленно.

Если команда введена на стеке устройств и номер члена стека не указан, то происходит перезагрузка всех членов стека одновременно.

Примеры команды:

```
admin@Switch# reload at 00:00:01 1 January 2021
admin@Switch#
```

```
admin@Switch# reload in 00:01:00
admin@Switch#
```

4.4.31 rename

Команда фундаментального режима. Изменение имени файла конфигурации.

ВНИМАНИЕ

Использование имен «**default-config**», «**running-config**», «**startup-config**» недопустимо.

Синтаксис команды:
rename {running-config | *old-filename***}** *new-filename*
Параметры команды:

running-config	файл текущей конфигурации
old-filename	старое имя файла конфигурации
new-filename	новое имя файла конфигурации

Пример команды:

```
admin@Switch# rename myconfig.conf hisconfig.conf
admin@Switch#
```

4.4.32 run-script

Команда фундаментального режима. Запуск скрипта из файла на исполнение. На скрипт накладываются те же ограничения и правила, что и на обычные команды пользователя.

Синтаксис команды:
run-script *filename*
Параметры команды:

filename	имя файла скрипта

Пример команды:

```
admin@Switch# run-script myscript
Executing command: configure terminal ... ok
Executing command: gvrp global ... ok
Executing command: gvrp vlan create ... ok
<output truncated>
admin@Switch#
```

4.4.33 serdes reference clock

Команда фундаментального режима. Настройка источника синхронизации SERDES.

Синтаксис команды:
serdes reference clock {external-125-diff | internal-125}
no serdes reference clock
Команда с приставкой «**no**» выставляет значение по умолчанию (default).
Параметры команды:

external-125-diff	установка внешнего источника синхронизации
internal-125	установка внутреннего источника синхронизации

Пример команды:

```
admin@Switch# serdes reference clock external-125-diff
admin@Switch#
```

4.4.34 ssh

Команда фундаментального режима. Подключение по протоколу SSH к удаленному хосту.

Синтаксис команды:

ssh [-c *cipher* **] [-l** *username***] [-m** *mac***] [-p** *port***] {***ip-address* **|** *hostname***} [***command***]**

Параметры команды:

cipher — список алгоритмов шифрования сессии, разделенных запятой. Поддерживаемые алгоритмы шифрования:

– 3des-cbc;

– aes128-cbc;

– aes256-cbc;

– aes128-ctr;

– aes256-ctr

username — имя пользователя, от имени которого производить подключение. По умолчанию устройство использует имя пользователя из текущей сессии CLI

mac — список алгоритмов хэширования сессии, разделенных запятой. Поддерживаемые алгоритмы хэширования:

– hmac-sha1;

– hmac-sha1-96;

– hmac-sha2-256;

– hmac-sha2-512;

– hmac-md5

port — номер порта TCP для подключения в диапазоне от 1 до 75535. По умолчанию порт равен 22

ip-address — IP-адрес хоста

hostname — доменное имя хоста

command — команда CLI, которую необходимо выполнить на хосте. После выполнения команды соединение с хостом автоматически завершается

Использование команды:

Команда «**ssh**» используется для подключения по протоколу SSH к удаленному хосту.

При подключении к хосту по протоколу SSH с помощью команды «**ssh**» устройство автоматически сохраняет открытый ключ SSH хоста для дальнейшего использования. При повторной генерации ключа SSH на хосте (в частности, при физической замене оборудования хоста) старый и новый ключи не будут совпадать, что приведет к невозможности подключения к хосту по протоколу SSH. Удалите старый ключ хоста с помощью команды «**clear ssh host**», и устройство автоматически сохранит новый ключ при подключении к хосту.

Пример команды:

```
admin@Switch# ssh 192.168.10.10
Somehost login:
```

4.4.35 system mtu

Команда глобальной настройки. Устанавливает максимальное значение MTU.

Синтаксис команды:

system mtu *bytes*

Параметр команды:

bytes значение MTU в байтах. Параметр принимает значения только 1500 или 1600 байт

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# system mtu 1500
admin@Switch(config)#
```

4.4.36 terminal session-timeout

Команда фундаментального режима. Установка таймаута неактивности пользователя, после которого происходит автоматическое завершение сессии управления.

Синтаксис команды:

terminal session-timeout *minutes*

terminal no session-timeout

Команда «**terminal no session-timeout**» устанавливает таймаут неактивности пользователя, равный 5 минутам.

Параметры команды:

minutes количество минут в диапазоне от 0 до 2147483647. Значение, равное 0, отключает таймаут неактивности пользователя

Пример команды:

```
admin@Switch# terminal session timeout 5
admin@Switch#
```

4.4.37 terminal type

Команда фундаментального режима. Установка типа используемого эмулятора терминала.

Синтаксис команды:
terminal type *type*
terminal no type
Команда «**terminal no type**» устанавливает значение «xterm».
Параметры команды:

type	тип эмулятора терминала в виде текстовой строки. Например, vt100, xterm

Пример команды:

```
admin@Switch# terminal type xterm
admin@Switch#
```

4.4.38 traceroute

Команда фундаментального режима. Трассировка маршрута до сетевого устройства.

Синтаксис команды:
traceroute {*dest-ipv4-addr* | *hostname*} [**source vlan** *vlan-id*]
Параметры команды:

dest-ipv4-addr	IP-адрес сетевого устройства
hostname	доменное имя сетевого устройства
source vlan *vlan-id*	использовать IP-адрес с интерфейса VLAN, имеющего идентификатор «*vlan-id*»

Пример команды:

```
admin@Switch# traceroute www.plgn.ru
traceroute to www.plgn.ru (217.23.159.76), 30 hops max, 40 byte packets 1
proxyserver.polygon.local (192.168.0.2) 0.761 ms 0.281 ms 0.256ms 2 195.239.220.61
(195.239.220.61) 1.717 ms 2.706 ms 1.218 ms 3 cisco3.ufa.gldn.net (195.218.138.9)
1.436 ms 1.021 ms 0.993 ms 4 cat02.moscow.gldn.net (194.186.157.125) 20.457 ms 21.412
ms22.132 ms 5 cat02.moscow.gldn.net (194.186.157.125) 20.599 ms 20.488 ms20.649 ms
6 m9-cr01-te2-3.msk.stream-internet.net (195.34.36.121) 20.801 ms20.974 ms 20.798
ms 7 m9-cr02- po1.msk.stream-internet.net (195.34.59.54) 20.987 ms21.605 ms 20.828
ms 8 caravan-m9.msk.stream-internet.net (195.34.36.142) 21.540 ms20.584 ms 20.637
ms 9 v701.office-1.caravan.ru (212.158.172.147) 20.985 ms 20.974 ms20.908 ms10
polygon-group.ru (217.23.159.76) 21.081 ms 20.987 ms 20.929 ms
admin@Switch#
```

4.4.39 telnet

Команда фундаментального режима. Подключение к хосту по протоколу Telnet.
Синтаксис команды:
telnet *ip-address* [*port*]
Параметры команды:

ip-address	IP-адрес хоста
port	номер порта TCP. Если порт не указан, то производится подключение на порт 23

Значение по умолчанию:
Порт 23.
Использование команды:
Команда «**telnet**» позволяет подключиться к хосту по протоколу Telnet.
Для перехода в режим ввода специальных команд Telnet используется сочетание клавиш <Ctrl>-]. Этот режим может понадобиться для принудительного завершения сессии подключения по протоколу Telnet в случае зависания подключения к хосту.
Пример команды:

```
admin@Switch# telnet 176.213.10.50
```

4.4.40 tls config

Команда глобальной настройки. Добавление конфигурации TLS.
Синтаксис команды:
tls config *name ca* {*ourcrt ourkey password*}
no tls config *name*
Команда с приставкой «**no**» удаляет выбранную конфигурацию TLS.
Параметры команды:

name	название конфигурации TLS
ca	выбор файла CA-сертификата
ourcrt	выбор файла OUR-сертификата
ourkey	выбор файла с ключом
password	установка пароля

Пример команды:

```
admin@Switch#configure terminal
admin@Switch(config)# tls config TLSname CA.crt OUR.crt OUR.key password
admin@Switch(config)#
```

4.4.41 show processes cpu history

Команда доступна из любого режима. Вывод истории загрузки CPU за последнюю минуту, последний час и последние 72 часа.
Синтаксис команды:
show processes cpu history
Использование команды:
Команда “**show processes cpu history**” выводит историю загрузки CPU за последнюю минуту, последний час и последние 72 часа. В выводе команды эти данные отображается в виде диаграммы. Строки отображают загрузку в процентах. Столбцы отображают временной интервал (значения времени необходимо читать сверху вниз). За последнюю минуту интервал разделен на каждые 5 секунд. За последний час на каждую минуту. За последние 72 часа в столбце указывается каждый час. Звездочкой

(*) отображается максимальное значение загрузки CPU; решеткой (#) – среднее значение загрузки CPU.

Пример команды:

```
admin@Switch# show processes cpu history

Switch 0:
655443322110
50505050505
------
100
90
80
70
60
50
40
30 *
20 **************
10 **************
CPU% per second (last 60 seconds)
6,55555555554444E+059
9,87654321098766E+058
-----------------
100
90
80
70
60
50
40
30 *** * ** *** ** ** ** ** ** * ******** ** ** * * *** *
20 ############################################################
10 ############################################################
CPU% per minute (last 60 minutes)
* - maximum CPU% # - average CPU%
[output truncated]
```

4.4.42 show cpu utilization

Команда фундаментального режима. Вывод информации об использовании CPU.

Синтаксис команды:

show cpu utilization

Пример команды:

```
admin@Switch# show cpu utilization
CPU utilization
-----------------------------
Switch 0:
five seconds: 20.2%; one minute: 21.6%; five minutes: 21.6%
admin@Switch#
```

4.4.43 show locator-led

Команда, доступная из любого режима. Вывод состояния кнопок-индикаторов.

Синтаксис команды:
show locator-led
Использование команды:
Команда «**show locator-led**» используется для вывода состояния кнопок индикаторов. Если команда введена на коммутаторе стека, то выводится информация о состоянии кнопок-индикаторов на всех членах стека.
Пример команды:

```
admin@Switch# show locator-led
Switch  Locator LED Status
------  ----------------
1       Off
2       Off
3       On
4       Off
```

4.4.44 show logging hosts

Команда фундаментального режима. Вывод списка syslog-серверов.
Синтаксис команды:
show logging hosts
Пример команды:

```
admin@Switch# show logging hosts
Logging hosts:
192.168.1.1
admin@Switch#
```

4.4.45 show port jumbo-frame

Команда фундаментального режима. Вывод текущего состояния функции передачи фреймов длиной до 10000 байт.
Синтаксис команды:
show port jumbo-frame
Пример команды:

```
admin@Switch# show port jumbo-frame
Jumbo-frames are enabled
```

4.4.46 show reload

Команда фундаментального режима. Вывод настроек отложенной перезагрузки.
Синтаксис команды:
show reload
Пример команды:

```
admin@Switch# show reload
Switch0:
Reload scheduled at 00:00:01 1 January 2021
admin@Switch#
```

4.4.47 show tcp brief

Команда доступна из любого режима. Вывод установленных TCP соединений.

Синтаксис команды:

show tcp brief {all | numeric}

Параметры команды:

all для каждого TCP соединения отображать доменное имя, если известно

numeric для каждого TCP соединения отображать ip-адрес

Пример команды:

```
admin@Switch(config)# show tcp brief all
Inode        Local address                Foreign address              State
-----        ----------------------       -------------------------    -----------
34745        localhost.localdomain:1488   localhost.localdomain:41746  ESTABLISHED
34744        localhost.localdomain:41746  localhost.localdomain:1488   ESTABLISHED
admin@Switch#
```

4.4.48 show tls config

Команда доступна из любого режима. Отображение установленных конфигураций TLS.

Синтаксис команды:

show tls config *name*

Параметры команды:

name название конфигурации TLS

Использование команды:

Команда без аргументов выводит полный список установленных конфигураций TLS.

Команда не выводит заданные пароли.

Пример команды:

```
admin@Switch(config)# show tls config

Name         CA_cert      Our_cert     Our_key
-------      -------      --------     -------
TLSname      CA.crt       OUR.crt      OUR.key

admin@Switch(config)#
```

4.4.49 show serdes reference clock

Команда доступа из любого режима. Вывод установленного значения для источника синхронизации SERDES.

Синтаксис команды:

show serdes reference clock

Пример команды:

```
admin@Switch# show serdes reference clock

external-125-diff
admin@Switch#
```

4.5 Создание макрокоманд

4.5.1 Общие положения

Коммутатор поддерживает создание макрокоманд глобальной настройки и настройки интерфейсов. Макрокоманда глобальной настройки представляет собой набор команд глобальной настройки. Макрокоманда настройки интерфейсов представляет собой набор команд настройки интерфейсов.

Выполнение или трассировка макрокоманды настройки интерфейса осуществляется по команде «**macro apply**».

Ввод описания для макрокоманд, примененных к интерфейсу, производится по команде «**macro description**».

Выполнение или трассировка макрокоманды глобальной настройки осуществляется по команде «**macro global**».

Ввод описания для макрокоманд глобальной настройки, примененных к коммутатору, производится по команде «**macro global description**».

Создание макрокоманды с именем “macro-name” осуществляется по команде «**macro name**».

4.5.2 macro apply

Команда настройки интерфейса. Выполнение или трассировка макрокоманды настройки интерфейса.

Синтаксис команды:

macro {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

Параметры команды:

apply	выполнение макрокоманды
trace	трассировка макрокоманды
macro-name	имя макрокоманды
parameter {*value*}	название и значение параметра макрокоманды, например, «$VID 5». В приведенном примере все вхождения параметра «$VID» в макрокоманде при выполнении будут заменены на значение 5

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet0/1
admin@Switch(config-if)# macro apply vlans $VID 5
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

4.5.3 macro description

Команда настройки интерфейса. Ввод описания для макрокоманд, примененных к интерфейсу.

Синтаксис команды:
macro description *text*
no macro description
Команда с приставкой «**no**» удаляет описание.
Параметры команды:
text описание примененных макрокоманд

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# macro description default vlans
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

4.5.4 macro global

Команда глобальной настройки. Выполнение или трассировка макрокоманд глобальной настройки.

Синтаксис команды:
macro global {apply | trace} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

Параметры команды:

apply	выполнение макрокоманды
trace	трассировка макрокоманды
macro-name	имя макрокоманды
parameter {*value*}	название и значение параметра макрокоманды, например, «$MTU 1600». В приведенном примере все вхождения параметра «$MTU» в макрокоманде при выполнении будут заменены на значение 1600

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# macro sysmtu $MTU 1600
admin@Switch(config)# end
admin@Switch#
```

4.5.5 macro global description

Команда глобальной настройки. Ввод описания для примененных макрокоманд глобальной настройки.

Синтаксис команды:
macro global description *text*
no macro global description
Команда с приставкой «**no**» удаляет описание для примененных макрокоманд глобальной настройки.

Параметры команды:

text описание примененных макрокоманд

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# macro global description sysmtu 1600
admin@Switch(config)# end
admin@Switch#
```

4.5.6 macro name

Команда глобальной настройки. Создание макрокоманды и переход в режим ввода макрокоманды. Завершение ввода макрокоманды производится с помощью команды «**end**».

Синтаксис команды:

macro name *macro-name*

no macro name *macro-name*

Команда с приставкой «**no**» удаляет макрокоманду.

Параметры команды:

macro name имя макрокоманды

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# macro name sysmtu
system-mtu $MTU
end
admin@Switch(config)# end
admin@Switch#
```

4.5.7 show parser macro

Команда доступна из любого режима. Вывод информации о созданных макросах.

Синтаксис команды:

show parser macro [brief | name *name***]**

Параметры команды:

brief отображение только имен макросов

name *name* отображение информации о выбранном макросе

Пример команды:

```
admin@Switch# show parser macro
Total number of macros = 2
--------------
Macro name: test
macro global apply test
--------------
Macro name: test_routing
  interface vlan 2
    ip address 172.16.0.1 255.255.255.0
  end
  interface gigabitethernet 0/2
    switchport access vlan 2
end
  ip route 192.168.0.0 /24 172.16.0.2
```

4.5.8 show parser macro description

Команда доступна из любого режима. Вывод описания для созданных макросов.
Синтаксис команды:
show parser macro description
Пример команды:

```
admin@Switch# show parser macro descriptoin
description
admin@Switch#
```

4.6 Управление конфигурациями

4.6.1 Наборы настроек коммутатора

Управление конфигурациями коммутатора реализовано на базе следующих наборов настроек:

- текущие настройки коммутатора, которые имеют специальное имя «running-config»;
- дополнительные наборы пользовательских настроек коммутатора;
- заводские настройки коммутатора, которые имеют специальное имя «default-config»;
- настройки, загружаемые при запуске коммутатора, которые имеют специальное имя «startup-config».

Сохранение настроек в файле, используемом при запуске коммутатора, производится с помощью команды «**copy running-config startup-config**». Автоматическое сохранение настроек отсутствует. При необходимости пользователь может сохранять текущую конфигурацию под другими именем.

Заводские настройки имеют статус «только для чтения» и не могут быть перезаписаны.

Коммутатор обеспечивает возможность загрузки и выгрузки файлов конфигурации по протоколу TFTP, FTP и SCP.

Файл настроек коммутатора – текстовый. Структура файла предполагает возможность его формирования пользователем вне коммутатора с помощью текстового редактора.

Проверка корректности файла конфигурации происходит при его загрузке как текущей конфигурации. В случае обнаружения ошибки номер строки, содержащей ошибку, выдается на консоль.

Выбор файла конфигурации, используемого при загрузке устройства, осуществляется по команде «**boot config-file**».

Вывод содержимого файла текущей конфигурации осуществляется по команде «**show running-config**». Файл конфигурации содержит команды, которые необходимо ввести, чтобы получить текущую конфигурацию коммутатора.

Вывод содержимого файла конфигурации, используемого при загрузке устройства, осуществляется по команде «**show startupconfig**».

4.6.2 boot config-file

Команда глобальной настройки. Выбор файла конфигурации, используемого при загрузке устройства.

Синтаксис команды:
boot config-file {running-config | *filename***}**
no boot config-file
Команда с приставкой «**no**» отключает использование файла конфигурации.
Параметры команды:

filename	имя файла конфигурации
running-config	выбор текущей конфигурации

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# boot config-file myconf.conf
admin@Switch(config)# end
admin@Switch#
```

4.6.3 show running-config

Команда, доступная из любого режима. Вывод текущей конфигурации устройства (файла текущей конфигурации в памяти).
Синтаксис команды:
show running-config [all | *interface-id* **] [xml]**
Параметры команды:

all	вывод значений всех параметров
interface-id	идентификатор интерфейса, для которого необходимо вывести конфигурацию
xml	вывод конфигурации в формате XML

Использование команды:
Команда «**show running-config**» используется для вывода текущей конфигурации устройства (файла текущей конфигурации в памяти).
Файл конфигурации представляет собой набор команд, которые необходимо выполнить для получения текущих настроек устройства.
Если команда введена без аргументов, то выводятся только изменения относительно конфигурации по умолчанию. Аргумент «**all**» используется для вывода всех параметров.
Примеры команды:

```
admin@Switch# show running-config

Current configuration:
-----------
configure terminal

interface gigabitethernet 0/1
  location Ufa
  duplex full
  speed 100
exit

interface vlan 1
  ip address 192.168.0.10 255.255.255.0
exit
```

```
admin@Switch# show running-config xml

<rpc-reply xmlns:plgnos="http://xml.plgn.ru/plgnos/3.0.0/plgnos»
 <configuration plgnos:commit-localtime="2016-01-01 00:00:01 UTC"plgnos:commit-user="admin»
  <version>3.0.0</version>
  <interfaces>
   <interface>
    <name>gigabitethernet0/1</name>
    <location>Ufa</location>
    <duplex>full</duplex>
     <speed>100</speed>
   </interface>
   <interface>
    <name>vlan 1</name>
    <ip-address>192.168.0.10/24</ip-address>
   </interface>
  </interfaces>
 </configuration>
</rpc-reply>
```

4.6.4 show startup-config

Фундаментальная команда. Вывод содержимого файла конфигурации, используемого при загрузке устройства. Файл конфигурации представляет собой набор команд, которые необходимо выполнить для получения настроек коммутатора после применения файла конфигурации.

Синтаксис команды:

show startup-config

Пример команды:

```
admin@Switch# show startup-config

configure terminal
vlan 1-2
end
interface vlan 1-2
  ip address 192.168.10.1 255.255.255.0
end
end
admin@Switch#
```

4.7 Сетевые настройки

4.7.1 Общие положения

Коммутатор позволяет устанавливать локальный IP-адрес, маску подсети, IP-адрес шлюза и IP-адреса DNS-серверов. Для установки сетевых настроек необходимо перейти в режим глобальной настройки с помощью команды «**configure terminal**».

Установка локального IP-адреса и маски подсети осуществляется с помощью команды «**ip address**». Для установки сетевых настроек необходимо перейти в режим настройки интерфейса VLAN с помощью команды «**interface vlan <vlan-id>**».

Установка IP-адреса шлюза осуществляется с помощью команды «**ip default-gateway**». Коммутатор поддерживает только один шлюз, поэтому установка нового значения заменяет старое.

Установка IP-адресов DNS-серверов осуществляется с помощью команды «**ip name-server**». Команда позволяет установить до 10 IP-адресов DNS-серверов, отображаемых в виде списка. Коммутатор отправляет запросы к DNS-серверам в порядке следования их IP-адресов в списке (слева направо).

Вывод списка DNS-серверов и списка доменных имен, для которых найдены IP-адреса, осуществляется с помощью команды «**show hosts**».

Вывод IP-адреса шлюза и IP-адресов, для которых получены ICMP-сообщения «redirect», осуществляется с помощью команды «**show ip redirects**».

4.7.2 arp

Команда настройки интерфейса (Ethernet). Добавление статической записи в таблицу ARP.

Синтаксис команды:

arp *ip-address hardware*

no arp *ip-address hardware-address*

Команда с приставкой «**no**» удаляет статическую запись из таблицы ARP.

Параметры команды:

ip-address	IP-адрес хоста
hardware-address	MAC-адрес хоста в шестнадцатеричном формате (например, “00:1B:28:11:22:33”)

Значение по умолчанию:

Статические записи ARP отсутствуют.

Пример команды:

```
admin@Switch(config)# arp 10.0.0.1 00:1B:28:11:22:33
```

4.7.3 ip proxy-arp static

Команда глобальной настройки. Включение или отключение режима статических записей в ARP-таблице коммутатора.

Синтаксис команды:
ip proxy-arp static
no ip proxy-arp static
Команда с приставкой «**no**» отключает режим статических записей в ARP-таблице коммутатора.
Значение по умолчанию:
Записи в ARP-таблице динамические.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip proxy-arp static
admin@Switch(config)#
```

4.7.4 ip address

Команда настройки интерфейса (VLAN). Установка IP-адреса на VLAN.
Синтаксис команды:
ip address *ip-address* **{***subnet-mask* **|** *prefix-length***} [secondary]**
no ip address *ip-address* **{***subnet-mask* **|** *prefix-length***} [secondary]**
Команда с приставкой «**no**» удаляет IP-адрес с VLAN.
Параметры команды:

ip-address	IP-адрес в формате “xxx.xxx.xxx.xxx”
subnet-mask	маска подсети в формате “xxx.xxx.xxx.xxx”
prefix-length	длина префикса адреса в битах. Префикс представляет собой альтернативный способ указания маски сети клиента. Значению длины префикса должен предшествовать символ “косая черта” (“/”)
secondary	добавление или удаление дополнительного IP-адреса

Значение по умолчанию:
На VLAN 1 установлен IP-адрес 192.168.0.225 с маской подсети 255.255.255.0.
Использование команды:
Команда «**ip address**» используется для установки IP-адреса на VLAN.
Ограничения команды:

1. Устройство поддерживает один основной IP-адрес на интерфейсе;
2. При вводе команды с новым значением основного IP-адреса, происходит замена основного адреса;
3. При удалении основного IP-адреса дополнительные адреса остаются в конфигурации, но при этом обработка IP-трафика на этом интерфейсе прекращается (включая маршрутизацию).
4. Дополнительные адреса нельзя вводить при отсутствии основного IP-адреса.

Если на VLAN устройствах включено получение IP-адреса от DHCP-сервера, то устройство отправляет сообщение: “DHCPDISCOVER” для того, чтобы заявить о себе DHCP-серверу сети.

При вводе команды «**no ip address**» устройство освобождает полученный IP-адрес и отправляет сообщение “DHCPRELEASE” (если адрес был получен по протоколу DHCP).

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip address 192.168.0.10 255.255.255.0
admin@Switch(config-if-vlan)#
```

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip address 10.0.0.10 255.255.255.0 secondary
admin@Switch(config-if-vlan)#
```

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip address 192.168.1.1 /24
admin@Switch(config-if-vlan)#
```

4.7.5 ip proxy-arp

Команда настройки интерфейса (VLAN). Добавление интерфейса VLAN к числу объединяемых с помощью Proxy-ARP.

Синтаксис команды:

ip proxy-arp

no ip proxy-arp

Команда с приставкой «**no**» исключает интерфейс VLAN из числа объединяемых с помощью Proxy-ARP.

Значение по умолчанию:

ip proxy-arp отключен для всех VLAN.

Использование команды:

Минимальное количество интерфейсов для объединения – 2, максимальное – 10. Объединяемым интерфейсам VLAN должны быть назначены IP-адреса.

Команда «**no ip proxy-arp**» выключает Proxy-ARP на данном интерфейсе VLAN (как только число объединяемых интерфейсов станет меньше 2, Proxy-ARP завершит работу).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 2
admin@Switch(config-if-vlan)# ip proxy-arp
admin@Switch(config-if-vlan)#
```

4.7.6 ip default-gateway

Команда глобальной настройки. Установка IP-адреса шлюза по умолчанию.

Синтаксис команды:

ip default-gateway *ip-address*

no ip default-gateway

Команда с приставкой «**no**» удаляет IP-адрес шлюза по умолчанию.

Параматеры команды:

ip-address IP-адрес шлюза по умолчанию

Значение по умолчанию:

IP-адрес шлюза по умолчанию отсутствует.

Использование команды:

Команда «**ip default-gateway**» используется для установки IP-адреса шлюза по умолчанию. При повторной настройке новое значение заменяет старое.

В случае необходимости отправки пакетов на другое устройство, локальное устройство проверяет возможность прямой отправки пакета через один из IP-адресов, настроенных на VLAN. Если прямая отправка невозможна, то есть IP-адрес назначения находится в сети, для которой не настроен IP-адрес на устройстве, устройство проверяет таблицу маршрутизации (статической и динамической). Если в таблице маршрутизации отсутствует маршрут до искомой сети, то используется шлюз по умолчанию (маршрут по умолчанию).

Команда «**ip default-gateway**» является алиасом команды «**ip route 0.0.0.0 /0**». То есть, например, ввод команды «**ip default-gateway 192.168.0.2**» приводит к выполнению команды «**ip route 0.0.0.0 /0 192.168.0.2**».

Команда «**show ip route**» используется для вывода списка маршрутов в таблице маршрутизации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip default-gateway 192.168.0.2
admin@Switch(config)#
```

4.7.7 ip name-server

Команда глобальной настройки. Установка и удаление IP-адресов DNS-серверов.

Синтаксис команды:

ip name-server *server-address1* **[***server-address2...server-address10***]**

no ip name-server *server-address1* **[***server-address2...server-address10***]**

Команда с приставкой «**no**» с указанием списка IP-адресов удаляет соответствующие им DNS-серверы.

Параметр команды:

server-address список IP-адресов DNS-серверов в формате «xxx.xxx.xxx.xxx»

Использование команды:

При вводе больше 10 IP-адресов DNS серверов, будут записаны только последние 10.

ВНИМАНИЕ

Количество DNS-серверов не должно превышать 10.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip name-server 192.168.0.1
admin@Switch(config)# end
admin@Switch#
```

4.7.8 renew dhcp

Команда глобальной настройки. Обновление IP-адреса, который был получен от DHCP-сервера для указанного интерфейса.

Синтаксис команды:

renew dhcp vlan *vlan-id*

Параметры команды:

vlan-id номер VLAN в диапазоне от 1 до 4094

Использование команды:

Необходимо учитывать, что команда не включает DHCP на интерфейсе. Если DHCP не включен на необходимом интерфейсе, то выводится сообщение об ошибке.

Если DHCP включен на интерфейсе и IP-адрес был уже получен, то команда осуществит попытку обновления данного IP-адреса.

Если DHCP включен на интерфейсе и IP-адрес еще не получен, то команда отправит запрос DHCP.

Пример команды:

```
admin@Switch# configure terminal

admin@Switch(config)# renew dhcp vlan 19
```

4.7.9 show hosts

Фундаментальная команда. Вывод списка DNS-серверов и списка доменных имен, для которых найдены IP-адреса.

Синтаксис команды:

show hosts

Пример команды:

```
admin@Switch# show hosts
Name servers:
--------------
1   192.168.0.1
2   192.168.0.2
3   192.168.0.3
admin@Switch#
```

4.7.10 show ip redirects

Фундаментальная команда. Вывод IP-адреса шлюза и IP-адресов, для которых получены ICMP-сообщения «redirect».

Синтаксис команды:
show ip redirects
Пример команды:

```
admin@Switch# show ip redirects
Default gateway is 192.168.0.2
admin@Switch#
```

4.7.11 show arp

Команда, доступная из любого режима. Вывод ARP-таблицы на устройстве.
Синтаксис команды:
show arp [*entry-type*] [*ip-address* [*mask*]] [**vlan** *vlan-id*]
Параметры команды:

entry-type — тип записи:

- **dynamic** – вывод только динамических записей;
- **static** – вывод только статических записей;
- **incomplete** – вывод только записей, для которых определение IP-адреса не завершено

ip-address [mask] — IP-адрес и маска подсети для хоста. Вместо маски подсети допускается использование длины префикса. Если маска подсети не задана, то маска подсети определяется как маска для классовой сети (RFC791)

vlan-id — идентификатор интерфейса, на котором определены записи ARP

Использование команды:
Команда «**show arp**» используется для вывода ARP-таблицы на устройстве.
Пример команды:

```
admin@Switch# show arp
IP Address         Hardware Address   Type         Interface
-------------      ----------------   -------      ---------
192.168.0.101      00:1B:28:00:00:01  dynamic      VLAN 1
192.168.0.102      00:1B:28:00:00:02  static       VLAN 2
192.168.0.103      --                 incomplete   VLAN 3
```

4.8 Настройка SSH

4.8.1 Общие положения

SSH – сетевой протокол сеансового уровня, который позволяет осуществлять удаленное управление.

Коммутатор обеспечивает:

- включение/выключение SSH-сервера с помощью команды «**ssh server**»;
- генерацию SSH-ключа сервера с помощью команды «**ssh key**».

Отображение открытых ключей сервера и их отпечатков (md5 хэш) осуществляется с помощью команды «**show ssh key**».

Досрочно завершить SSH-сессию можно с помощью сочетания клавиш «Ctrl-D».

4.8.2 ip ssh authentication-retries

Команда глобальной настройки. Настройка количества попыток аутентификации по протоколу SSH.

Синтаксис команды:

ip ssh authentication-retries *count*

no ip ssh authentication-retries

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметр команды:

count количество попыток аутентификации по протоколу SSH. Доступна установка значения в диапазоне от 1 до 10

Значение по умолчанию:

По умолчанию количество попыток равно 5.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip ssh authentication-retries 10
admin@Switch(config)#
```

4.8.3 ip ssh timeout

Команда глобальной настройки. Устанавливает время, через которое должен произойти обрыв SSH сессии.

Синтаксис команды:

ip ssh timeout *time*

no ip ssh timeout

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметр команды:

time время, через которое должен произойти обрыв SSH сессии (доступна установка значения в диапазоне от 10 до 300 секунд)

Значение по умолчанию:

По умолчанию время разрыва сессии SSH равно 30.

Пример команды:

```
admin@Switch(config)# ip ssh timeout 140
admin@Switch(config)#
```

4.8.4 ssh server

Команда глобальной настройки. Включение/выключение SSH-сервера.

Синтаксис команды:

ssh server enable

no ssh server enable

Использование команды:

Прежде чем включить SSH-сервер, необходимо сгенерировать SSH-ключ сервера с помощью команды «**ssh key**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ssh server enable
admin@Switch(config)# end
admin@Switch#
```

4.8.5 ssh key

Команда глобальной настройки. Генерация SSH-ключа сервера.

Синтаксис команды:

ssh key{**dsa** [**force**] | **rsa** [*bits*] [**force**] | **ed25519** [**force**]}

no ssh key [dsa | rsa | ed25519]

Команда с приставкой «**no**» отменяет генерацию SSH-ключа сервера.

Параметры команды:

dsa	генерация ключа DSA
rsa	генерация ключа RSA
ed25519	генерация ключа ed25519
bits	количество бит, используемых при генерации RSA-ключа, в диапазоне от 512 до 4096 бит (по умолчанию используется значение «1024 бит»). Данное значение кратно восьми
force	замена существующего ключа

Использование команды:

Если отсутствует RSA-ключ, генерируется новый RSA-ключ длиной 1024 бит (значение по умолчанию).

Если отсутствует DSA-ключ, генерируется новый DSA-ключ.

Если отсутствует ed25519-ключ, генерируется новый ed25519-ключ.

Если отсутствуют все ключи, генерируются все ключи.

Выполнение команды может занять продолжительное время в зависимости от размера ключа.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ssh key rsa 2048 force
admin@Switch(config)# end
admin@Switch#
```

4.8.6 show ssh

Команда доступна из любого режима. Вывод информации о текущих SSH сессиях.

Синтаксис команды:

show ssh

Пример команды:

```
admin@Switch# show ssh
Connection   Version   Encryption   State     Username
----------   -------   ----------   -------   --------
2            2.0       aes128-ctr   Started   admin
```

4.8.7 show ssh key

Команда фундаментального режима. Отображение открытых ключей сервера и их отпечатков (md5 хэш).

Синтаксис команды:

show ssh key [dsa | rsa | ed25519]

Параметры команды:

dsa отображение ключа DSA

rsa отображение ключа RSA

ed25519 отображение ключа ed25519

Пример команды:

```
admin@Switch# show ssh key
RSA
public key:
AAAAB3NzaC1yc2EAAAADAQABAAAAgwDHYMosHNNfshxbQBvdnPsjLjgRNkd964bbcojF3fA+qFUGI/
lC5FajPOVXzo3JDeNW5tHqfjjrKOTJFtR6ufHw1hurQP3xEcgkupeuXZ2Lhx7ac6Z7vc/AcB5oSH/
xxplXXxjLrmZB7ZAv9lLOpkHfFnZ1KscTBkHipPqpyT8Or3MHFingerprint:
75:26:65:6f:f6:45:1a:c5:16:c3:91:df:04:99:e7:bcDSA key not found
admin@Switch#
```

4.9 Мониторинг температуры и системы электропитания

4.9.1 Общие положения

Коммутатор оборудован датчиком температуры и управляемыми вентиляторами. С помощью интерфейса управления пользователь может настроить режим работы вентиляторов:

1. Автоматический режим (по умолчанию): скорость вращения вентиляторов автоматически регулируется коммутатором в зависимости от температуры.
2. Ручной режим: пользователь вручную задает фиксированную скорость вращения вентиляторов в процентах от максимальной.

Для мониторинга температуры используется команда «**show env**».

4.9.2 system env fanspeed-control manual

Команда глобальной настройки. Используется для включения ручного режима управления вентиляторами и установки фиксированной скорости их вращения.

Синтаксис команды:

system env fanspeed-control manual *percent*

no system env fanspeed-control manual

Команда с приставкой «**no**» отключает ручной режим и возвращает управление вентиляторами в автоматический режим.

Параметры команды:

percent	скорость вращения вентиляторов в процентах от максимальной (диапазон значений от 40 до 100)

Значение по умолчанию:

Команда выключена. Включен автоматический режим работы вентиляторов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# system env fanspeed-control manual 40
admin@Switch(config)#
```

4.9.3 show env

Команда фундаментального режима. Вывод информации о температуре воздуха внутри корпуса коммутатора.

Синтаксис команды:

show env {temperature | fanspeed-control}

Параметры команды:

temperature	вывод информации о температуре
fanspeed-control	вывод информации о режиме работы вентиляторов, а также о пороговых значениях температуры, при которых происходит включение/выключение вентиляторов

Пример команды:

```
admin@Switch(config)# show env fanspeed-control

Fan Speed Control Information
-----------------------------
Mode: manual
Speed: 40%
```

4.10 Обновление программного обеспечения

4.10.1 Комплекты обновления программного обеспечения

Коммутатор поддерживает установку новых версий ПО по протоколам SCP, FTP, TFTP. Загрузка новой версии ПО осуществляется с помощью команды «**archive download-sw**».

На время обновления ПО коммутатор должен быть обеспечен гарантированным бесперебойным питанием. Ответственность за любые неполадки, возникшие в результате пропадания питания в процессе обновления ПО коммутатора, возлагаются на пользователя.

Отправка архива текущей версии ПО на сервер осуществляется с помощью команды «**archive upload-sw**».

Выбор образа ПО, загружаемого при запуске устройства, осуществляется с помощью команды «**boot system**».

Вывод информации об установленных образах ПО осуществляется с помощью команды «**show bootvar**».

4.10.2 archive download-sw

Команда фундаментального режима. Установка образов программного обеспечения с внешних носителей данных или серверов.

Синтаксис команды:

archive download-sw *src-url*

Параметры команды:

src-url URL источника

В качестве префиксов URL могут выступать:

usb0:// установка образа ПО с внешнего носителя, подключенного к разъему USB № 1.

Синтаксис: **usb0**://[*directory*/]*filename*

usb1:// установка образа ПО с внешнего носителя, подключенного к разъему USB № 2.

Синтаксис: **usb1**://[*directory*/]*filename*

tftp:// установка образа ПО с внешнего TFTP-сервера.

Синтаксис: **tftp**://[*location*/][*directory*/]*filename*

scp:// установка образа ПО с внешнего сервера по протоколу SCP.

Синтаксис:

scp://*username*[:*password*]@*location*/[*directory*/]*filename*

Если пароль не указан, то он равен пустой строке

ftp:// установка образа ПО с внешнего FTP-сервера.

Синтаксис:

ftp://[*username*[:*password*]@]*location*/[*directory*/]*filename*

Если имя учетной записи «*username*» и пароль «*password*» не указаны, то устройство производит анонимное подключение. Если пароль не указан, то он равен пустой строке

Использование команды:

Команда «**archive download-sw**» используется для установки образов программного обеспечения с внешних носителей данных или серверов.

При установке образа ПО на устройство проверка корректности образа будет произведена автоматически после окончания копирования. Если образ ПО корректен, то устройство автоматически будет его использовать при следующей загрузке. В случае обнаружения ошибок в образе ПО будет выведено сообщение: «Copy failed: invalid image».

Если при копировании по протоколу SCP устройство обнаруживает, что у удаленного сервера изменился ключ SSH, то устройство выводит сообщение об ошибке и завершает работу команды. Если удаленный сервер является легитимным хостом, но его ключ изменился по какой-либо причине, удалите старый SSH-ключ хоста с помощью команды «**clear ssh hosts**».

Внешние носители USB могут быть недоступны для некоторых модификаций устройства.

Пример команды:

```
admin@Switch# archive download-sw tftp://192.168.0.1/image.pol
downloading ok
check version ok
installing ok
admin@Switch#
```

4.10.3 archive upload-sw

Команда фундаментального режима. Копирование установленных образов программного обеспечения на внешние носители данных или серверы.

Синтаксис команды:

archive upload-sw {**image-1** | **image-2** } *dest-url*

Параметры команды:

image-1	копирование первого образа ПО на внешний носитель или сервер
image-2	копирование второго образа ПО на внешний носитель или сервер
dest-url	URL назначения

В качестве префиксов URL могут выступать:

usb0:// копирование образов ПО на внешний носитель, подключенный к разъему USB № 1.

Синтаксис: **usb0**://[*directory*/]*filename*

usb1:// копирование образов ПО на внешний носитель, подключенный к разъему USB № 2.

Синтаксис: **usb1**://[*directory*/]*filename*

tftp:// копирование образов ПО на внешний TFTP-сервер.

Синтаксис: **tftp**://[*location*/][*directory*/]*filename*

ftp:// копирование образов ПО на внешний FTP-сервер.

Синтаксис:

ftp://[*username*[:*password*]@]*location*/[*directory*/]*filename*

Если имя учетной записи «*username*» и пароль «*password*» не указаны, то устройство производит анонимное подключение. Если пароль не указан, то он равен пустой строке

scp:// копирование образов ПО по протоколу SCP.

Синтаксис:

scp://*username*[:*password*]@*location*/[*directory*/]*filename*

Если пароль не указан, то он равен пустой строке

Использование команды:

Команда «**archive upload-sw**» используется для копирования установленных образов программного обеспечения на внешние носители данных или серверы.

Если копирование невозможно из-за отсутствия свободного места на носителе информации, будет выведено сообщение «Copy failed: not enough free space».

Если при копировании по протоколу SCP устройство обнаруживает, что у удаленного сервера изменился ключ SSH, то устройство выводит сообщение об ошибке и завершает работу команды. Если удаленный сервер является легитимным хостом, но его ключ изменился по какой-либо причине, удалите старый SSH-ключ хоста с помощью команды «**clear ssh hosts**».

Внешние носители USB могут быть недоступны для некоторых модификаций устройства.

Примеры команды:

```
admin@Switch# archive upload-sw image-1 tftp://192.168.0.1/image.pol
admin@Switch#
```

```
admin@Switch# archive upload-sw image-2 usb0://image.pol
admin@Switch#
```

4.10.4 boot system

Команда фундаментального режима. Выбор образа ПО, загружаемого при запуске устройства.

Синтаксис команды:

boot system {**image-1** | **image-2**}

Параметры команды:

image-1	при следующем запуске устройства будет загружен первый образ ПО
image-2	при следующем запуске устройства будет загружен второй образ ПО

Использование команды:

Команда «**boot system**» используется для выбора образа ПО, загружаемого при запуске устройства.

Команда «**show bootvar**» используется для вывода информации об установленных образах ПО.

Пример команды:

```
admin@Switch# boot system image-1
admin@Switch#
```

4.10.5 show bootvar

Фундаментальная команда. Вывод информации об установленных образах ПО.

Синтаксис команды:

show bootvar

Пример команды:

```
admin@Switch# show bootvar
Switch0:
Image   Version   Status       Default   MDS
-----   -------   ----------   --------  --------------------------------
1       1.1.2     Not active             67824afc1548a12408f137c50f368a2b
2       1.1.2     Active        *        a007b08b277d1f92050b66f2475403b9
```

4.11 Специальные команды CLI

4.11.1 Общие положения

Специальные команды CLI предназначены для упрощения работы пользователя путем создания собственных синонимов команд и переменных окружения, используемых для хранения промежуточных данных (различные константы).

Очистка истории введенных команд осуществляется с помощью команды «**clear cli history**».

Добавление синонима для команды CLI осуществляется с помощью команды «**cli alias name**».

Добавление переменной окружения осуществляется с помощью команды «**cli var name**».

Вывод синонимов команд CLI производится с помощью команды «**show cli alias**».

Вывод списка введенных команд с указанием времени и даты ввода команды осуществляется с помощью команды «**show cli history**».

Вывод переменных окружения осуществляется с помощью команды «**show cli variables**».

4.11.2 clear cli history

Команда фундаментального режима. Очистка истории введенных команд. Коммутатор позволяет хранить до 200 последних введенных команд.

Синтаксис команды:

clear cli history

Пример команды:

```
admin@Switch# clear cli history
admin@Switch#
```

4.11.3 cli alias name

Команда глобальной настройки. Добавление синонима для команды CLI.

Синтаксис команды:

cli alias name *alias-name alias-text*

no cli alias name *alias-name*

Команда с приставкой «**no**» удаляет синоним для команды CLI.

Параметры команды:

alias-name	имя синонима команды CLI. Имя может содержать только буквы английского алфавита, цифры и символ подчеркивания
alias-text	команда CLI, для которой устанавливается синоним

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# cli alias name showmac show mac address-table
admin@Switch(config)#
```

4.11.4 cli var name

Команда фундаментального режима. Добавление переменной окружения. Переменные окружения сохраняются только в пределах текущего сеанса управления.

Синтаксис команды:

cli var name *variable-name variable-text*

cli no var name *variable-name*

Параметры команды:

variable-name	имя переменной окружения в виде текстовой строки. Имя переменной может содержать только буквы английского алфавита, цифры и символ подчеркивания
variable-text	значение переменной окружения в виде текстовой строки, которое может содержать в себе любые данные, включая зарезервированные слова и команды

ВНИМАНИЕ

Доступ к значению переменной производится с использованием следующего синтаксиса: $(variable-name).

Пример команды:

```
admin@Switch# cli var name Myvar 15
admin@Switch# $(Myvar)15
admin@Switch#
```

4.11.5 show cli alias

Команда фундаментального режима. Вывод синонимов команд CLI. Команда без параметра выводит список всех синонимов и закрепленных за ними команд.

Синтаксис команды:

show cli alias [name *alias-name***]**

Параметры команды:

name *alias-name*	вывод синонима с определенным именем

Пример команды:

```
admin@Switch# show cli alias
CLI alias commands
--------------------
showmac = ‘‘show mac address-table’’
```

4.11.6 show cli history

Команда фундаментального режима. Вывод списка введенных команд с указанием времени и даты ввода команды.

Синтаксис команды:
show cli history [*lines***] [unformatted]**
Параметры команды:

lines	количество последних введенных команд для вывода
unformatted	вывод без указания времени и даты ввода команды

Пример команды:

```
admin@Switch# show cli history 3
#    Time/Date               Command
--   -------------------     -------------------------
56   16:28:08 18.06.2010     show cli alias name shmac
57   16:28:31 18.06.2010     show cli history
58   16:29:12 18.06.2010     show cli history 3
admin@Switch#
```

4.11.7 show cli variables

Команда фундаментального режима. Вывод переменных окружения.
Синтаксис команды:
show cli variables
Пример команды:

```
admin@Switch# show cli variables
CLI variables
-------------
myvar = "5"
admin@Switch#
```

4.12 Автоматизация конфигурации

4.12.1 Общие положения

Коммутатор обеспечивает автоматизацию настройки параметров с помощью циклов:

- выполнение одной команды с различными значениями параметров с помощью команды «**for**»;
- выполнение вложенных циклов для создания комбинаций параметров с помощью команды «**for**» с вложенной конструкцией.

Циклы позволяют значительно сократить время конфигурации оборудования при необходимости выполнения однотипных операций с изменяющимися параметрами.

4.12.2 for

Команда выполнения цикла. Используется для многократного выполнения одной или нескольких команд с изменяющимися параметрами.

Синтаксис команды:

for *переменная* **in** *значение1 значение2 ... значениеN;* **do** *команды;* **done**
или
for *переменная* **in** [*начальное_значение..конечное_значение;*] **do** *команды;* **done**

Параметры команды:

переменная	имя переменной, которая будет принимать значения из списка или диапазона
значение1...N	список значений, разделенных пробелами, которые будет принимать переменная на каждой итерации
[*начальное_значение..конечное_значение*]	диапазон принимаемых значений
команда	команда или набор команд для выполнения в цикле. Значения в команду подставляются с помощью символа доллара и имени переменной ($переменная)

Использование команды:

Вложенные циклы используются, когда необходимо сгенерировать комбинации параметров. Внешний цикл выполняется полностью для каждого значения внутреннего цикла.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# for a in 1 2 3; do for b in 1 2 3; do ip route 10.$a.$b.0 /24
1.1.1.1; done; done
admin@Switch(config)# end
admin@Switch#
```

Результат выполнения команды:

```
ip route 10.1.1.0 /24 1.1.1.1
ip route 10.1.2.0 /24 1.1.1.1
ip route 10.1.3.0 /24 1.1.1.1
ip route 10.2.1.0 /24 1.1.1.1
ip route 10.2.2.0 /24 1.1.1.1
ip route 10.2.3.0 /24 1.1.1.1
ip route 10.3.1.0 /24 1.1.1.1
ip route 10.3.2.0 /24 1.1.1.1
ip route 10.3.3.0 /24 1.1.1.1
```

5 Функции портов

5.1 Настройка PoE

На коммутаторах, не поддерживающих PoE, команды, описанные в данном подразделе, отсутствуют.

5.1.1 Общие положения

Power over Ethernet (PoE) – технология, позволяющая передавать удаленному устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet.

Коммутатор поддерживает следующие режимы PoE:

1. «**auto**» – коммутатор автоматически определяет, является ли подключенное устройство питаемым. Если коммутатор обнаруживает питаемое устройство, подключенное к порту, при наличии достаточной мощности он выделяет питание, обновляет бюджет питания и подает питание на порт на основе принципа «первым прибыл, первым обслужен».

   При отключении питаемого устройства коммутатор автоматически обнаруживает отключение и прекращает подачу питания на порт. Имеется возможность подключения непитаемого устройства без его повреждения.

   Режим «**auto**» может быть использован для любого PoE-порта. Данный режим используется по умолчанию.

2. «**static**» – коммутатор предварительно выделяет питание для порта (даже если питаемое устройство не подключено) и гарантирует доступность питания для него. Коммутатор выделяет питание в соответствии с установленным значением максимальной мощности, и данное значение не может быть изменено согласно классу IEEE через питаемое устройство. Поскольку питание предварительно выделяется, любое питаемое устройство, потребляющее не больше максимального значения мощности, гарантированно обеспечивается питанием в случае подключения к порту в режиме «static». В данном режиме порт уже не участвует в модели «первым прибыл, первым обслужен».

   Однако, если мощность потребления по классу IEEE питаемого устройства выше, чем установленное значение максимальной мощности, то коммутатор не подает питание на данное устройство.

   Если значение мощности не задано, то коммутатор выделяет питание согласно максимально возможному значению. Коммутатор подает питание на порт, только если обнаружит питаемое устройство. Режим «static» используется для высокоприоритетного интерфейса.

3. «**never**» – коммутатор отключает функцию обнаружения питаемого устройства и никогда не подает питание на PoE-порт, даже если подключено непитаемое устройство. Данный режим следует использовать для обеспечения гарантии

отсутствия питания на PoE-порту, чтобы использовать его только для передачи данных.

Коммутатор обеспечивает настройку следующих параметров PoE:

- включение режима динамического подсчета суммарного потребления мощности с помощью команды «**power inline consumption mode dynamic**»;
- включение журналирования событий PoE с помощью команды «**logging event power-inline-status**»;
- установку режима PoE на PoE-портах с помощью команды «**power inline**»;
- вывод информации о состоянии PoE для указанного PoE-порта или для всех PoE-портов с помощью команды «**show power inline**».

5.1.2 power inline consumption mode dynamic

Команда глобальной настройки. Включение режима динамического подсчета суммарного потребления мощности.

Синтаксис команды:

power inline consumption mode dynamic

no power inline consumption mode

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Значение по умолчанию:

Потребление мощности подсчитывается согласно классу устройства.

Использование команды:

Для питаемых устройств IEEE, когда коммутатор запрашивает информацию о питании, он регулирует потребляемую мощность согласно классификации IEEE питаемых устройств. Если питаемое устройство относится к классу 0 (неизвестный класс) или классу 3, коммутатор выделяет 15,4 Вт для устройства, независимо от действительно необходимой мощности. Если питаемое устройство сообщает о более высоком классе, чем его фактический уровень потребления, или если устройство не поддерживает классификацию по питанию (класс 0), коммутатор может обеспечить питанием меньшее количество устройств, т.к. для мониторинга распределения общей мощности он использует информацию о классах по IEEE.

ВНИМАНИЕ

Чтобы избежать повреждения коммутатора, необходимо тщательно планировать распределение питания. При вводе команды глобальной настройки **«power inline consumption mode dynamic»** может появиться следующее сообщение: «CAUTION: Misconfiguring the power consumption may cause damage to the switch and void your warranty. Take precaution not to oversubscribe the power supply».

Пример команды:

```
Switch(config)# power inline consumption mode dynamic
CAUTION: Misconfiguring the power consumption may cause damage to the switch and void
your warranty. Take precaution not to oversubscribe the power supply.
```

5.1.3 logging event power-inline-status

Команда настройки интерфейса. Включение журналирования событий PoE.
Синтаксис команды:
logging event power-inline-status
no logging event power-inline-status
Команда с приставкой «**no**» отключает журналирование событий PoE.
Значение по умолчанию:
По умолчанию журналирование событий PoE включено.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# logging event power-inline-status
admin@Switch(config-if)#
```

5.1.4 power inline

Команда настройки интерфейса. Установка режима PoE на PoE-портах.
Синтаксис команды:
power inline {auto [max *max-wattage*] **| never | static [max** *max-wattage*]}
no power inline
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

auto	включение функции обнаружения питаемого устройства. При наличии достаточной мощности питание автоматически подается на PoE-порт после обнаружения устройства
max *max-wattage*	ограничение мощности, подаваемой на порт, в диапазоне от 4 до 30 Вт. Если данный параметр не задан, то устанавливается максимальное значение
never	отключение функции обнаружения питаемого устройства и подачи питания на порт
static	включение функции обнаружения питаемого устройства. Производится предварительное резервирование питания для порта перед обнаружением коммутатором питаемого устройства

Значение по умолчанию:

По умолчанию устанавливается значение «**auto**».

Максимальная мощность составляет 30 Вт.

Использование команды:

Параметр «**max** *max-wattage*» используется для запрета подачи питания на питаемые устройства с высокой мощностью потребления. Если максимальное значение мощности по классу питаемого устройства выше, чем установленное значение, коммутатор не подает питание на данное устройство.

В случае если коммутатор не подает питание на питаемое устройство (максимальная мощность по классу IEEE выше, чем установленная максимальная мощность), PoE-порт находится в состоянии «power-deny». Коммутатор при этом генерирует системное сообщение и в столбце «Oper» в выводе команды «**show power inline**» отображается запись «power-deny».

Команда «**power inline static max** *max-wattage*» используется для назначения порту высокого приоритета. Коммутатор выделяет питание PoE для порта, находящегося в режиме «static» перед выделением питания для порта, находящегося в режиме «auto». Коммутатор резервирует питание для порта в режиме «static» при его настройке, а не при обнаружении устройства. Коммутатор резервирует питание для порта в режиме «static», даже если нет подключенного к нему устройства, и вне зависимости от того, включен порт или нет.

В случае если коммутатор не может выделить питание для порта в режиме «static» (например, из-за того, что общая мощность уже перераспределена по другим портам, находящимся в режиме «auto» или «static»), появляется следующее сообщение: «Can not pre-allocate power budget: power not available». Настройка порта остается без изменений.

При настройке порта с помощью команды настройки интерфейса «**power inline auto**» или «**power inline static**» порт проводит автосогласование, используя установленные настройки скорости и дуплекса. Это необходимо для определения требований по питанию подключенного устройства (является ли оно питаемым устройством). После определения требований по питанию коммутатор настраивает интерфейс, используя установленные настройки скорости и дуплекса без перезагрузки интерфейса.

При настройке порта с помощью команды «**power inline never**» порт возвращается к установленным настройкам скорости и дуплекса.

Примеры команды:

```
Switch(config)# interface tengigabitethernet 0/1
Switch(config-if)# power inline auto
```

```
Switch(config)# interface tengigabitethernet 0/1
Switch(config-if)# power inline auto max 7000
```

```
Switch(config)# interface tengigabitethernet 0/1
Switch(config-if)# power inline never
```

5.1.5 show power inline

Фундаментальная команда. Вывод информации о состоянии PoE для указанного PoE-порта или для всех PoE-портов.

Синтаксис команды:

show power inline [*interface-id* **| consumption]**

Параметры команды:

interface-id — вывод информации о питании PoE для указанного интерфейса

consumption — вывод информации о распределении питания PoE по устройствам, подключенным к PoE-портам

Пример команды:

```
admin@Switch# show power inline
Available:370.0(w) Used:80.6(w) Remaining:289.4(w)
Interface  Admin   Oper         Power   Device                  Class   Max
                   (Watts)
---------  -----   ----------   -----   --------------------    -----   ----
te0/1      auto    on           6.3     IEEE powered device     0       30.0
te0/2      static  off          15.4    n/a                     n/a     30.0
te0/3      static  power-deny   10.0    n/a                     n/a     10.0
<output truncated>
```

Описание полей примера представлено в таблице 5.

Таблица 5 – Описание полей примера

Поле	Описание
Admin	Режим управления: auto, off, static
Oper	Режим работы: – on – питаемое устройство обнаружено; питание подается; – off – питание PoE не подается; – faulty – ошибка обнаружения устройства или неисправность питаемого устройства; – power-deny – обнаружено питаемое устройство, но питание PoE недоступно, либо максимальная мощность превышает максимальное значение для обнаруженного типа питаемого устройства
Power	Мощность подаваемого питания PoE, Вт
Device	Тип устройства: n/a, unknown, IEEE powered device
Class	Класс IEEE: n/a, Class 0-4
Available	Суммарная мощность питания PoE в системе
Used	Мощность питания PoE, распределенная по портам
Remaining	Мощность питания PoE в системе, не распределенная по портам

5.2 Настройка портов RS-232/RS-485

5.2.1 Общие положения

Устройство передает данные от портов RS-232/RS-485 по тракту Ethernet с использованием протокола TCP/IP. Устройство поддерживает только соединения типа «точка-точка». Переход в режим настройки соответствующего контроллера порта осуществляется с помощью команды «**controllers**».

Устройство обеспечивает:

- установку скорости работы порта с помощью команды «**baudrate**»;
- установку количества битов данных с помощью команды «**databits**»;
- установку настроек в значения по умолчанию с помощью команды «**default**»;
- установку текстового описания порта с помощью команды «**description**»;
- установку режима проверки четности с помощью команды «**parity**»;
- установку режима работы порта с помощью команды «**state**»;
- установку количества стоповых бит с помощью команды «**stopbits**»;
- установку режима работы терминирующих резисторов для порта RS-485 с помощью команды «**termination-state**».

Вывод настроек портов RS-232 и RS-485 осуществляется с помощью команды «**show rs232-port**».

5.2.2 controllers

Команда глобальной настройки. Переход в режим настройки контроллеров портов RS-232/RS-485.

Синтаксис команды:

controllers rs232 *interface-path-id*

Параметры команды:

interface-path-id	идентификатор контроллера порта в формате «устройство/порт»

Использование команды:

Номер порта 1 соответствует порту RS-232, номер порта 2 соответствует порту RS-485.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)#
```

5.2.3 baudrate

Команда настройки портов RS-232/RS-485. Установка скорости работы порта в бит/с.

Синтаксис команды:

baudrate *rate*

Параметры команды:

rate	скорость работы порта из списка: 75, 100, 200, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200. По умолчанию используется значение «115200»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# baudrate 115200
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.4 databits

Команда настройки портов RS-232/RS-485. Установка количества битов данных.

Синтаксис команды:

databits *bits*

Параметры команды:

bits	количество битов данных из списка: 5, 6, 7, 8. По умолчанию используется значение «8»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# databits 8
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.5 default

Команда настройки портов RS-232/RS-485. Установка настроек в значения по умолчанию.

Синтаксис команды:

default

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# default
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.6 description

Команда настройки портов RS-232/RS-485. Установка текстового описания порта.

Синтаксис команды:

description *text*

no description

Команда с приставкой «**no**» устанавливает текстовое описание «RS232 interface N» или «RS485 interface N» (в зависимости от типа порта), где «N» номер порта.

Параметры команды:

text	текстовая строка

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# description rs232-modem
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.7 duplex

Команда настройки портов RS-232/RS-485. Установка режима дуплекса для порта RS-485.

Синтаксис команды:

duplex {full | half}

Параметры команды:

full	режим полного дуплекса
half	режим полудуплекса

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# duplex full
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.8 parity

Команда настройки портов RS-232/RS-485. Установка режима проверки четности.

Синтаксис команды:

parity *mode*

Параметры команды:

mode	режим проверки четности из списка: even, odd, mark, space, none. По умолчанию используется значение «none»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# parity odd
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.9 state

Команда настройки портов RS-232/RS-485. Установка режима работы порта.

Синтаксис команды:

state *state*

Параметры команды:

state режим работы порта: enabled, disabled. По умолчанию используется значение «enabled»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# state enabled
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.10 stopbits

Команда настройки портов RS-232/RS-485. Установка количества стоповых бит.

Синтаксис команды:

stopbits *bits*

Параметры команды:

bits количество стоповых бит: 1; 1,5; 2. Количество стоповых бит «1,5» используется только для количества битов данных, равных 5. Количество стоповых бит «2» используется только для количества битов данных, равных 6, 7 или 8. По умолчанию используется значение «1»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# stopbits 1
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.11 termination-state

Команда настройки портов RS-232/RS-485. Установка режима работы терминирующих резисторов для порта RS-485. Терминирующие резисторы необходимо включать на оконечных устройствах для длинных линий RS-485.

Синтаксис команды:
termination-state *state*
Параметры команды:

state	режим работы терминирующих резисторов: open (отключены), connected (включены). По умолчанию используется значение «open»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# termination-state open
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.12 virtual-port

Команда настройки портов RS-232/RS-485. Установка режима работы канала передачи данных.

Синтаксис команды:
virtual-port mode {tcpclient *ip-address* **| tcpserver | rfc2217 }** [*port*]
Параметры команды:

tcpclient	режим работы канала передачи данных TCP-клиент, то есть устройство подключается к указанному IP-адресу. В этом режиме передаются только данные RX/TX
tcpserver	режим работы канала передачи данных TCP-сервер. В этом режиме передаются только данные RX/TX
rfc2217	режим работы канала передачи данных RFC2217. В этом режиме передаются данные RX/TX и информация о состоянии управляющих линий. Режим RFC2217 поддерживает удаленную настройку параметров порта RS232/RS-485
ip-address	IP-адрес для подключения в режиме «tcpclient»
port	номер порта для подключения

Использование команды:
Режим TCP-сервер применяется в двух случаях:

1. Создание окончания для виртуального COM-порта на ПК. В этом случае на ПК необходимо создать виртуальный COM-порт с помощью ПО ArlanComManager или аналогичного; в параметрах виртуального COM-порта необходимо указать IP-адрес устройства и номер порта TCP канала передачи данных;
2. Создание канала передачи данных между портами RS-232/485 двух устройств. В этом случае на втором устройстве необходимо использовать режим TCP-клиент. В настройках канала передачи данных второго устройства необходимо указать IP-адрес и номер порта TCP канала передачи данных первого устройства.

Режим TCP-клиент применяется для создания канала передачи данных между портами RS-232/485 двух устройств, а также для подключения к серверам и устройствам сторонних производителей. В настройках канала передачи данных устройства необходимо указать IP-адрес и номер порта TCP для подключения к серверу.

Режим RFC2217 применяется для создания окончания виртуального COM-порта на ПК. Режим RFC2217 предоставляет возможность удаленной настройки параметров порта RS-232/485 через виртуальный COM-порт. В этом случае на ПК необходимо создать виртуальный COM-порт с помощью ПО ArlanComManager или аналогичного, в параметрах виртуального COM-порта необходимо указать IP-адрес устройства и номер порта TCP канала передачи данных.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# controllers rs232 0/1
admin@Switch(config-rs232)# virtual-port mode rfc2217 6000
admin@Switch(config-rs232)# end
admin@Switch(config)# end
admin@Switch#
```

5.2.13 show rs232-port

Фундаментальная команда. Вывод настроек портов RS-232 и RS-485.

Синтаксис команды:

show rs232-port { *portnum* | **summary** }

Параметры команды:

portnum	номер порта
summary	вывод таблицы настроек для всех портов

Примеры команды:

```
admin@Switch# show rs232-port 0/1
Description: "RS232 interface 0/1"
State:   enable
Baudrate:   115200
Databits:   8
Stopbits:   1
Parity:   none
Termination state: -
Duplex:   -
Virtual port:
  Mode:   TCP-server
  Port:   6001
admin@Switch#
```

```
admin@Switch# show rs232-port summary
Port    State   Baudrate  Databits  Stopbits  Duplex  Parity  TermState
----    -----   --------  --------  --------  ------  ------  ---------
1       enable  115200    8         1         -       none    -
2       enable  115200    8         1         full    none    open
admin@Switch#
```

5.3 Настройка параметров интерфейсов Ethernet

5.3.1 Общие положения

Коммутатор поддерживает настройку как группы интерфейсов, так и каждого интерфейса в отдельности. Часть команд настройки относится к глобальным командам, которые доступны после перехода в режим глобальной настройки с помощью команды «**configure terminal**».

Для настройки отдельного интерфейса необходимо сначала перейти в режим глобальной настройки с помощью команды «**configure terminal**», а затем в режим настройки интерфейса с помощью команды «**interface**» (в качестве аргумента команды должен использоваться идентификатор интерфейса, например, «tengigabitethernet 0/1»).

Для настройки группы интерфейсов необходимо сначала перейти в режим глобальной настройки с помощью команды «**configure terminal**», а затем в режим настройки группы интерфейсов с помощью команды «**interface range**» (в качестве аргумента команды должен использоваться диапазон идентификаторов интерфейсов, например, «tengigabitethernet 0/1-5»).

Коммутатор обеспечивает установку следующих настроек параметров интерфейсов Ethernet:

1. Максимальный размер поля данных фрейма Ethernet: 1500 или 1600 байтов. Установка максимального размера поля данных фрейма Ethernet осуществляется для всех интерфейсов Ethernet одновременно с помощью команды «**system mtu**». Максимальный размер фрейма равен 1518 (1522) и 1632 байтам.
2. Режим дуплекса: автоматическое определение, полудуплекс, полный дуплекс. Установка режима дуплекса осуществляется с помощью команды «**duplex**».
3. режим скорости интерфейса: автоматическое определение, 10 Мбит/с, 100 Мбит/с, 1000 Мбит/с, 10000 Мбит/с. Установка режима скорости осуществляется с помощью команды «**speed**».
4. Режим управления потоком: включено/выключено. Управление потоком поддерживается только для входящего направления (отправка фреймов паузы). Установка режима управления потоком осуществляется с помощью команды «**flowcontrol**».
5. Режим кроссирования линий (только для интерфейсов 10/100BASE-T и 10/100/1000BASE-T): автоматическое кроссирование, режим MDI-X. Установка режима кроссирования линий осуществляется с помощью команды «**mdix auto**».
6. Текстовое описание интерфейса, которое настраивается с помощью команды «**description**».
7. Режим ограничения мультикастового и широковещательного трафика, который настраивается с помощью команды «**storm-control**».

8. Режим блокировки мультикастового и обычного трафика с неизвестным адресом назначения, который настраивается с помощью команды «**switchport block**».

Коммутатор предоставляет следующие дополнительные возможности по настройке и управлению интрефейсами Ethernet:

1. Режим журналирования событий изменения состояний интерфейса, состояния STP. Установка режима журналирования событий осуществляется с помощью команды «**logging event**».
2. Административное отключение интерфейса, осуществляемое с помощью команды «**shutdown**». Административное включение интерфейса осуществляется с помощью команды «**no shutdown**».
3. Создание и применение макрокоманд, которое осуществляется с помощью команд «**macro**» (режим глобальной настройки) и «**macro apply**». Дополнительно можно настроить описание для последней примененной макрокоманды с помощью команды «**macro description**».

Коммутатор обеспечивает следующие возможности вывода состояний настроек и счетчика статистики:

1. Вывод состояний и настроек интерфейсов с помощью команды «**show interfaces**».
2. Вывод статистики интерфейсов с помощью команды «**show interfaces counters**».
3. Вывод настроек управления потоком с помощью команды «**show flowcontrol**».
4. Вывод максимального размера поля данных Ethernet, пропускаемого коммутатором, с помощью команды «**show system mtu**».

5.3.2 default

Команда глобальной настройки. Сброс настроек на интерфейсе в значения по умолчанию.

Синтаксис команды:
default *interface-id*
Параметр команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:
Команда «**default**» используется для сброса настроек на интерфейсе до значений по умолчанию.

Пример команды:

```
admin@Switch(config)# default tengigabitethernet 1/1
```

5.3.3 clear counters

Команда фундаментального режима. Сброс счетчиков статистики на интерфейсе.
Синтаксис команды:
clear counters [*interface-id*]
Параметр команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**clear counters**» используется для сброса счетчиков статистики на интерфейсе. Если команда введена без аргументов, то она применяется для всех интерфейсов.

Пример команды:

```
admin@Switch# clear counters tengigabitethernet 1/1
```

5.3.4 duplex

Команда настройки интерфейса. Установка режима дуплекса на интерфейсе.
Синтаксис команды:
duplex {auto | full | half}
no duplex
Команда с приставкой «**no**» устанавливает режим автосогласования.
Параметры команды:

auto режим автосогласования

full режим полного дуплекса

half режим полудуплекса

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# duplex auto
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.5 flowcontrol

Команда настройки интерфейса. Установка режима управления потоком на интерфейсе.
Синтаксис команды:
flowcontrol receive {desired | off | on}
Параметры команды:

receive установка режима для входящего направления

desired | off | on установка режима: автоматический, выключен, включен

Использование команды:

Управление потоком применяется для ограничения входящего трафика, если скорость на двух интерфейсах, через которые проходит трафик, не одинакова. Например, трафик входит в 1000 Мбит/с интерфейс и выходит через 100 Мбит/с интерфейс, в данном случае входящий трафик может быть больше пропускной способности исходящего интерфейса. Для исключения потерь пакетов необходимо включить управление потоком на интерфейсе 1000 Мбит/с.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# flowcontrol receive off
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.6 interface

Команда глобальной настройки. Переход в режим настройки интерфейса «config-if».

Синтаксис команды:

interface *interface-id*

Параметры команды:

interface-id идентификатор интерфейса. Формат идентификатора для интерфейсов Ethernet: “Тип” “Номер устройства” “/” “Номер интерфейса”. Типы интерфейсов Ethernet (поддерживаемые типы зависят от конкретной модели устройства):

1. **gigabitethernet** – 1 Гбит/с интерфейс Ethernet;
2. **tengigabitethernet** – 10 Гбит/с интерфейс;
3. **mgmt** – выделенный интерфейс управления Ethernet.

Формат идентификатора для loopback-интерфейсов: loopback “Номер интерфейса”, где номер интерфейса – целое число в диапазоне от 1 до 32

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface mgmt 0/1
admin@Switch(config-if)#
```

Следующий пример показывает, как перейти в режим настройки выделенного интерфейса управления mgmt 0/1:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)#
```

5.3.7 interface range

Команда глобальной настройки. Переход в режим настройки набора интерфейсов «config-if-range». В данном режиме настройки применяются сразу для всего набора интерфейсов.

Синтаксис команды:

interface range *if-range*

no interface range *if-range*

Команда с приставкой «**no**» позволяет выйти из режима настройки набора интерфейсов.

Параметры команды:

if-range диапазон интерфейсов вида: «tengigabitethernet 0/1-5, 12»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface range tengigabitethernet 0/1-5, 12
admin@Switch(config-if-range)#
```

5.3.8 description (настройка интерфейса)

Команда настройки интерфейса. Ввод текстового описания для интерфейса. Как правило, используется для описания местоположения интерфейса (линии связи, подключенной к интерфейсу).

Синтаксис команды:

description *text*

no description

Команда с приставкой «**no**» удаляет описание интерфейса.

Параметры команды:

text описание интерфейса в виде текстовой строки

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# description Ufa
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.9 logging event

Команда настройки интерфейса. Установка режима журналирования событий для интерфейса.

Синтаксис команды:

logging event {link-status | power-inline-status | spanning-tree}

Команда с приставкой «**no**» отключает журналирование соответствующих событий.

Параметры команды:

link-status	журналирование изменений состояния интерфейса
power-inline-status	журналирование событий подсистемы PoE
spanning tree	журналирование событий протокола STP

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# logging event spanning-tree
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.10 logging event transceiver

Команда настройки интерфейса (Ethernet). Включение журналирования событий, связанных с SFP-модулями.

Синтаксис команды:

logging event transceiver [alarm] [warning] [detection] [crc-error]

no logging event transceiver [alarm] [warning] [detection] [crc-error]

Команда с приставкой «no» отключает журналирование.

Параметры команды:

alarm	включение или отключение журналирования событий, возникающих при выходе контролируемых параметров за “красную” границу
warning	включение или отключение журналирования событий, возникающих при выходе контролируемых параметров за “желтую” границу
detection	включение или отключение журналирования событий, возникающих при установке или удалении SFP-модуля
crc-error	включение или отключение журналирования событий, возникающих при обнаружении ошибок CRC в параметрах SFP-модуля

Значение по умолчанию:

Устройство журналирует все события, связанные с SFP-модулями.

Использование команды:

Команда «**logging event transceiver**» используется для включения журналирования событий, связанных с SFP-модулями. Команда без параметров включает журналирование всех поддерживаемых событий.

Журналирование событий, связанных с выходом контролируемых параметров за границы допустимых значений, доступно только для SFP-модулей, поддерживающих DDM.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# logging event transceiver
admin@Switch(config-if)#
```

5.3.11 mdix auto

Команда настройки интерфейса. Включение автоматического определения приемных и передающих линий на интерфейсе (автокроссирование). Данная команда работает только для интерфейсов 10/100BASE-T и 10/100/1000BASE-T.

Синтаксис команды:

mdix auto

no mdix auto

Команда «**no mdix auto**» отключает автоматическое определение приемных и передающих линий на интерфейсе и устанавливает режим MDI-X (перекрестное расположение линий).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# mdix auto
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.12 media-type

Команда настройки интерфейса. Выбор приоритетного подключения.

Синтаксис команды:

media-type {rj45 | sfp} auto-failover

no media-type auto-failover

Команда с приставкой «**no**» назначает приоритет той среде, на которой раньше появилась связь.

Параметры команды:

rj45 назначение приоритета медному кабелю

sfp назначение приоритета оптическому кабелю

Значение по умолчанию:

По умолчанию приоритет отдается оптическому соединению.

Использование команды:

Ограничения по применению:

1. При установке SFP-модуля, рассчитанного на 100 Мбит/с или 1 Гбит/с, медный разъем COMBO-порта отключается.
2. При одновременном подключении медного и оптического (SFP) разъемов индикация соединения производится на оптическом разъеме.

3. Данная команда применима к коммутаторам, имеющим COMBO-порты.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# media-type rj45 auto-failover
admin@Switch(config-if)#
```

5.3.13 shutdown

Команда настройки интерфейса. Команда «**shutdown**» отключает интерфейс. Команда «**no shutdown**» включает интерфейс.

Синтаксис команды:

shutdown

no shutdown

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# shutdown
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.14 speed

Команда настройки интерфейса. Установка режима скорости на интерфейсе.

Синтаксис команды:

speed {10 | 100 | 1000 | 10000 | auto [10 | 100 | 1000]}

no speed

Команда с приставкой «**no**» устанавливает автоматическое согласование скорости.

Параметры команды:

10	скорость 10 Мбит/с
100	скорость 100 Мбит/с
1000	скорость 1000 Мбит/с
10000	скорость 10000 Мбит/с
auto	режим автосогласования

Примечание – В качестве дополнительного параметра для режима автосогласования можно указать список анонсируемых скоростей. Например, автосогласование с анонсированием только скорости 1000 Мбит/с: «speed auto 1000».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# speed 1000
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.15 storm-control

Команда настройки интерфейса. Установка ограничения для входящего широковещательного (broadcast), мультикастового (multicast) и обычного (unicast) трафика в битах в секунду.

Синтаксис команды:

storm control [action {shutdown | trap}] {broadcast | multicast | unicast} level bps *bps*

Команда с приставкой «**no**» отключает ограничение трафика.

Параметры команды:

action shutdown	при получении ограниченного трафика выключить порт
action trap	при получении ограниченного трафика уничтожить пакет
broadcast	ограничение широковещательного трафика
multicast	ограничение широковещательного и мультикастового трафика (вычисляется суммарный трафик)
unicast	ограничение широковещательного, мультикастового и обычного трафика (вычисляется суммарный трафик)
level bps *bps*	ограничение трафика в диапазоне от 64 000 до 256 000 000 бит/с

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# storm-control broadcast level bps 128000
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# storm-control action trap
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.16 rate-limit

Команда настройки интерфейса (Ethernet). Установка ограничения входящего трафика на интерфейсе.

Синтаксис команды:

rate-limit [*bps***]**

no rate-limit

Команда с приставкой «no» отключает ограничение входящего трафика на интерфейсе.

Параметры команды:

bps	ограничение трафика (в бит/с) в диапазоне от 1 000 000 бит/с до максимальной скорости порта (в бит/с)

Значение по умолчанию:

Ограничение входящего трафика отключено.

Использование команды:

Команда «**rate-limit**» используется для установки ограничения входящего трафика на интерфейсе.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# rate-limit 1000000
admin@Switch(config-if)#
```

5.3.17 storm-control action

Команда настройки интерфейса (Ethernet). Выбор действия, которое необходимо совершить устройству при превышении установленного ограничения на входящий трафик.

Синтаксис команды:

storm control action {shutdown | trap}

no storm control action

Команда с приставкой «**no**» отключает данную функцию.

Параметры команды:

action shutdown	при превышении ограничения выключить порт
action trap	при превышении ограничения уничтожить пакет

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# storm-control action trap
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.18 switchport block

Команда настройки интерфейса. Включение блокировки мультикастового или обычного трафика с неизвестным адресом назначения. Данная команда применима, только если используемые MAC-адреса внесены в таблицу как статические.

Синтаксис команды:

switchport block {multicast | unicast}

no switchport block {multicast | unicast}

Команда с приставкой «**no**» отключает блокировку мультикастового или обычного трафика с неизвестным адресом назначения.

Параметры команды:

multicast мультикастовый трафик

unicast обычный трафик

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport block multicast
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

5.3.19 errdisable recovery cause

Команда глобальной настройки. Включение автоматической реактивации интерфейса после его отключения из-за возникновения ошибки («Err-Disable»).

Синтаксис команды:

errdisable recovery cause {**all | dhcp-rate-limit | loopback-detection | psecure-violation | stp-bpdu-guard | stp-self-loop | udld**}

Команда с приставкой «**no**» отключает автоматическую реактивацию.

Параметры команды:

all включение механизма восстановления после отключения интерфейса любой из функций

dhcp-rate-limit включение механизма восстановления после отключения интерфейса при превышении лимита, установленного командой «**ip dhcp snooping limit rate**»

loopback-detection включение механизма восстановления после отключения интерфейса функцией обнаружения петель в сети

psecure-violation включение механизма восстановления после отключения интерфейса функцией безопасности на портах

stp-bpdu-guard включение механизма восстановления после отключения интерфейса функцией **bpdu guard**

stp-self-loop включение механизма восстановления после отключения интерфейса протоколом STP при обнаружении петель в сети

udld включение механизма восстановления после отключения интерфейса протоколом UDLD

Значение по умолчанию:

Автоматическая реактивация отключена.

Использование команды:

Команда «**errdisable recovery cause**» используется для включения автоматической реактивации интерфейса после его отключения из-за возникновения ошибки

(“Err-Disable”).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# errdisable recovery cause loopback-detection
admin@Switch(config)#
```

5.3.20 errdisable recovery interval

Команда глобальной настройки. Установка тайм-аута для восстановления после ошибок.

Синтаксис команды:

errdisable recovery interval *seconds*

no errdisable recovery interval

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	тайм-аут для восстановления после ошибок в диапазоне от 30 до 86400 секунд

Значение по умолчанию:

По умолчанию используется значение «30 секунд».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# errdisable recovery interval 600
```

5.3.21 show errdisable

Команда фундаментального режима. Отображение информации о динамическом отключении интерфейсов из-за возникновения ошибки (Err-Disable).

Синтаксис команды:

show errdisable

Использование команды:

Состояние «**enable**» означает, что возникла ошибка и интерфейс был отключен. Состояние «**disable**» – ошибок нет.

Пример команды:

```
admin@Switch# show errdisable
Errdisable cause   State
----------------   -------
loopback-detection disable
psecure-violation  disable
dhcp-rate-limit    disable
stp-bpdu-guard     disable
udld               disable
stp-self-loop      disable
```

5.3.22 show flowcontrol

Команда фундаментального режима. Вывод информации о настройках управления потоком интерфейсов Ethernet для определенного интерфейса.

Синтаксис команды:
show flowcontrol [interface *interface-id***]**
Параметры команды:

interface *interface-id* идентификатор интерфейса

Пример команды:

```
admin@Switch# show flowcontrol
Port                      Receive flow control    Rx pause     TX pause
----------------------    --------------------    --------     --------
tengigabitethernet 0/1    desired                 0            0
tengigabitethernet 0/2    desired                 0            0
tengigabitethernet 0/3    desired                 0            0
tengigabitethernet 0/4    desired                 0            0
tengigabitethernet 0/5    desired                 0            0
<output truncated>
admin@Switch#
```

5.3.23 show interfaces

Команда фундаментального режима. Вывод информации обо всех интерфейсах или об определенном интерфейсе.

Синтаксис команды:
show interfaces [*interface-id* **| vlan** *vlan-id***]**
Параметры команды:

interface-id идентификатор интерфейса

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# show interfaces gigabitethernet 0/1
Interface gigabitethernet 0/1
-----------------------------
Interface is UP
MAC-address: 00:01:02:03:04:24
IP-address: 192.168.0.170 Mask: 255.255.255.0
Speed: auto, duplex: auto
STP settigns:
  BPDU filter: disable, BPDU guard: disable
  Cost: auto, priority: 128
  Link type: auto
Switchport settings:
  Mode: access, vlan 1
  Block multicast: disable, unicast: disable
  Protected: disable
MLS QoS trust Cos: not trusted, DSCP: not trusted
Description:
```

5.3.24 show interfaces description

Команда, доступная из любого режима. Вывод описания интерфейсов и их текущего состояния.

Синтаксис команды:

show interfaces [*interface-id* **] description**

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show interfaces description**» используется для вывода описания интерфейсов и их текущего состояния.

Пример команды:

```
admin@Switch# show interfaces description
Interface  Status  Description
---------  ------  -----------
gi0/1      Up      Server
gi0/2      Up      Localnet
gi0/3      EDis    Localnet2
gi0/4      Down    Unused
```

5.3.25 show interfaces status

Команда, доступная из любого режима. Вывод общей информации о состоянии интерфейсов.

Синтаксис команды:

show interfaces status

Использование команды:

Команда «**show interfaces status**» используется для вывода общей информации о состоянии интерфейсов.

Пример команды:

```
admin@Switch# show interfaces status
Port       Type                    Link    Speed   Duplex  Port VLAN
------     ------------------      ----    ------  ------  ---------
gi 0/1     10/100/1000BASE-T       Up      a-1000  a-full  1
gi 0/2     10/100/1000BASE-T       Down    auto    auto    2
gi 0/3     No transceiver          Down    1000    full    3
gi 0/4     1000BASE-X              Up      1000    full    4
```

5.3.26 show interfaces summary

Команда фундаментального режима. Вывод общей информации о загрузке интерфейсов.

Синтаксис команды:

show interfaces summary [*interface-id***]**

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Примеры команды:

```
admin@Test# show interfaces summary
Port       RX bps     TX bps     RX pps     TX pps
-----      ------     ------     ------     ------
gi0/1      26000      0          34         0
gi0/2      0          0          0          0
gi0/3      0          0          0          0
gi0/4      0          0          0          0
gi0/5      0          0          0          0
gi0/6      0          0          0          0
gi0/7      0          0          0          0
gi0/8      0          0          0          0
gi0/9      0          0          0          0
gi0/10     0          0          0          0
gi0/11     0          0          0          0
gi0/12     0          0          0          0
gi0/13     0          0          0          0
gi0/14     0          0          0          0
gi0/15     0          0          0          0
gi0/16     0          0          0          0
gi0/17     0          0          0          0
gi0/18     0          0          0          0
gi0/19     0          0          0          0
te0/1      0          0          0          0
te0/2      0          0          0          0
te0/3      0          0          0          0
te0/4      0          0          0          0
```

```
admin@Test# show interfaces summary gigabitethernet 0/1
Port       RX bps     TX bps     RX pps     TX pps
-----      ------     ------     ------     ------
gi0/1      19528      0          35         0
```

5.3.27 show interfaces counters

Команда фундаментального режима. Вывод счетчиков статистики на интерфейсах.

Синтаксис команды:

show interfaces counters [*interface-id***]**

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Примеры команды:

```
admin@Test# show interfaces counters
Port      InUcastPkts  InMcastPkts  InBcastPkts  InOctets
-----     -----------  -----------  -----------  --------
gi0/1     126          270          3034         284843
gi0/2     0            0            0            0
gi0/3     0            0            0            0
gi0/4     0            0            0            0
gi0/4     0            0            0            0
gi0/5     0            0            0            0
gi0/6     0            0            0            0
gi0/7     0            0            0            0
gi0/8     0            0            0            0
gi0/9     0            0            0            0
gi0/10    0            0            0            0
gi0/11    0            0            0            0
gi0/12    0            0            0            0
gi0/13    0            0            0            0
gi0/14    0            0            0            0
gi0/15    0            0            0            0
gi0/16    0            0            0            0
gi0/17    0            0            0            0
gi0/18    0            0            0            0
gi0/19    0            0            0            0
gi0/20    0            0            0            0
gi0/21    0            0            0            0
gi0/22    0            0            0            0
gi0/23    0            0            0            0
te0/1     0            0            0            0
te0/2     0            0            0            0
te0/3     0            0            0            0
te0/4     0            0            0            0

Port      OutUcastPkts OutMcastPkts OutBcastPkts OutOctets
-----     ------------ ------------ ------------ ---------
gi0/1     13           18           1            2260
gi0/2     0            0            0            0
gi0/3     0            0            0            0
gi0/4     0            0            0            0
gi0/4     0            0            0            0
gi0/5     0            0            0            0
gi0/6     0            0            0            0
gi0/7     0            0            0            0
gi0/8     0            0            0            0
gi0/9     0            0            0            0
gi0/10    0            0            0            0
gi0/11    0            0            0            0
gi0/12    0            0            0            0
gi0/13    0            0            0            0
gi0/14    0            0            0            0
gi0/15    0            0            0            0
gi0/16    0            0            0            0
gi0/17    0            0            0            0
gi0/18    0            0            0            0
```

```
gi0/19    0           0           0           0
gi0/20    0           0           0           0
gi0/21    0           0           0           0
gi0/22    0           0           0           0
gi0/23    0           0           0           0
gi0/24    0           0           0           0
te0/1     0           0           0           0
te0/2     0           0           0           0
te0/3     0           0           0           0
te0/4     0           0           0           0
```

```
admin@Test# show interfaces counters gigabitethernet 0/1
Port             InUcastPkts  InMcastPkts       InBcastPkts  InOctets
--------         -----------  -----------       -----------  --------
gi0/1            128          291               3302         306708

Port             OutUcastPkts OutMcastPkts      OutBcastPkts OutOctets
--------         ------------ ------------      ------------ ---------
gi0/1            14           19                1            2402
Rx pause         0            Tx pause                       0
Rx fcs err       0            Tx fcs err                     0
Rx frames 64     2977         Tx collisions                  0
Rx frames 127    529          Tx multiple                    0
Rx frames 255    158          Tx excessive                   0
Rx frames 511    61           Tx late collision              0
Rx frames 1023   19           Tx deferred                    0
Rx frames max    11
Rx bad octets    0
Rx undersize     0
Rx fragments     0
Rx oversize      0
Rx jabber        0
Rx mac rcv err   0
```

5.3.28 show idprom

Команда, доступная из любого режима. Вывод информации об установленных SFP.

Синтаксис команды:

show idprom [interface *interface-id*] **[summary]**

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

summary вывод общей информации

Использование команды:

Команда «**show idprom**» используется для вывода информации об установленных SFP.

Примеры команды:

```
admin@Switch# show idprom interface gigabitethernet 0/1
Base ID fields:
Identifier:                  0x03 (SFP or SFP+)
Extended Identifier:         0x04
Connector:                   0x07 (LC)
Compliance Codes:            0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Encoding                     : 0x00
Bit-rate Nominal:            1000 Mbps
Rate Identifier:             0x00
Length:                      10 km
Vendor name:                 POLYGON
Vendor OUI:                  0x001B28
Vendor Part Number:          SFP-PLGN
Vendor Revision:             01
Laser Wavelength:            0x05 0x1E
Reserved:                    0x00
```

```
Extended ID fields:
Options:                     0x00 0x00
Bit-rate Max (%):            0
Bit-rate Min (%):            0
Vendor Serial Number:        12345
Manufacturing Date Code:     2005092800
Diagnostic Monitoring Type:  0x60 (supported)
Enhanced Options:            0x00
SFF-8472 Compliance:         0x05

Vendor Specific:
0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

```
admin@Switch# show idprom interface gigabitethernet 0/1 summary
            Bit-rate     Laser                  Diagnostic
            Nominal      Wavelength   Length    Monitoring
Port        (Mbps)       (nm)         (km)      Type
------      --------     ----------   ------    ----------
gi 0/1      1000         1310         10        Supported
```

5.3.29 show interfaces transceiver

Команда, доступная из любого режима. Вывод параметров цифрового диагностического мониторинга (DDM) SFP-модуля на интерфейсе.

Синтаксис команды:

show interfaces [*interface-id***] transceiver [detail]**

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)
detail	вывод детальной информации, которая включает в себя значения допустимых границ (warning / alarm thresholds), при выходе из которых устройство выводит предупреждающее сообщение

Использование команды:

Команда «**show interfaces transceiver**» используется для вывода параметров цифрового диагностического мониторинга (DDM) SFP-модуля на интерфейсе. Команда без параметров выводит общую информацию для всех интерфейсов.

Примеры команды:

```
admin@Switch# show interfaces gigabitethernet0/1 transceiver
                              Optical         Optical
        Temperature  Voltage   Transmit Power  Receive Power
Port    (Celsius)    (Volts)   (dBm)           (dBm)
------  -----------  -------   --------------  --------
gi 0/1  32.81        3.23      -2.16           -inf
```

```
admin@Switch# show interfaces gigabitethernet0/1 transceiver detail

                              High Alarm   High Warn    Low Warn     Low Alarm
             Temperature      Threshold    Threshold    Threshold    Threshold
Port         (Celsius)        (Celsius)    (Celsius)    (Celsius)    (Celsius)
-----        -----------      ----------   ---------    --------     ---------
Gi0/1        28.69            110.00       95.00        -42.00       -45.00
                              High Alarm   High Warn    Low Warn     Low Alarm
             Voltage          Threshold    Threshold    Threshold    Threshold
Port         (Volts)          (Volts)      (Volts)      (Volts)      (Volts)
-----        -----------      ----------   ---------    --------     ---------
Gi0/1        3.23             3.60         3.50         3.05         3.00
             Optical          High Alarm   High Warn    Low Warn     Low Alarm
             Transmit Power   Threshold    Threshold    Threshold    Threshold
Port         (dBm)            (dBm)        (dBm)        (dBm)        (dBm)
-----        -----------      ----------   ---------    --------     ---------
Gi0/1        -2.16            2.00         1.00         -6.00        -7.00
             Optical          High Alarm   High Warn    Low Warn     Low Alarm
             Recieve Power    Threshold    Threshold    Threshold    Threshold
Port         (dBm)            (dBm)        (dBm)        (dBm)        (dBm)
-----        -----------      ----------   ---------    --------     ---------
Gi0/1        -inf             -2.00        -3.00        -19.00       -20.00
```

5.3.30 show storm-control

Команда доступна из любого режима. Отображение настроек ограничения для входящего трафика на интерфейсах.

Синтаксис команды:

show storm-control

Пример команды:

```
admin@Switch# show storm-conrol
Interface    Mode         Level
---------    ---------    -----
Fa0/1        broadcast    64000
Fa0/2        multicast    128000
Fa0/3        unicast      256000
[output truncated]
```

5.4 Рефлектометрический тест кабеля

5.4.1 Общие положения

Рефлектометр для кабельных линий (Time Domain Reflectometer) предназначен для выявления дефектов в кабельных линиях локационным (рефлектометрическим) методом.

Рефлектометр предоставляет следующую информацию:

1. Длина каждой витой пары в кабеле;
2. Тип дефекта для каждой витой пары в кабеле:

- дефект отсутствует (normal);
- короткое замыкание (short);
- разрыв в кабеле (open).

3. Несоответствие волнового сопротивления (impedance mismatch);
4. Время и дата проведения последнего измерения.

5.4.2 test cable-diagnostics tdr interface

Команда глобальной настройки. Запуск рефлектометрического теста кабеля на определенном интерфейсе.

Синтаксис команды:

test cable-diagnostics tdr interface *interface-id*

Параметры команды:

interface-id	идентификатор интерфейса Ethernet

Использование команды:

Команда «**test cable-diagnostics tdr interface**» используется для запуска рефлектометрического теста кабеля на определенном интерфейсе. Для вывода результатов теста используется команда «**show cable-diagnostics tdr**».

Устройство может поддерживать рефлектометрический тест кабеля только на части интерфейсов Ethernet.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# test cable-diagnostics tdr interface gigabitethernet 0/1
admin@Switch(config)#
```

5.4.3 show cable-diagnostics tdr

Команда, доступная из любого режима. Вывод результатов рефлектометрического теста кабеля.

Синтаксис команды:

show cable-diagnostics tdr interface *interface-id*

Параметры команды:

interface-id (опционально) идентификатор интерфейса Ethernet

Использование команды:

Команда «**show cable-diagnostics tdr**» используется для вывода результатов рефлектометрического теста кабеля. Если интерфейс не задан, то выводятся результаты для всех интерфейсов.

Пример команды:

```
admin@Switch# show cable-diagnostics tdr interface gigabitethernet 1/1
Port    Pair   Length   Status   Last update
-----   ----   ------   ------   ---------------
gi0/1   1-2    < 50     Normal    March 5 10:22:06
        3-4    < 50     Normal
        5-6    < 50     Normal
        7-8    < 50     Short
```

6 Аутентификация, авторизация и аккаунтинг

6.1 Настройка AAA (аутентификации, авторизации и учета)

6.1.1 aaa authentication login

Команда глобальной настройки. Установка порядка методов аутентификации пользователя.

Синтаксис команды:

aaa authentication login {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication login {**default** | *list-name*}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

list-name	имя списка методов аутентификации пользователя. Рекомендуемая длина: от 1 до 12 символов
method1 [*method2...*]	список методов аутентификации пользователя из следующих вариантов (каждый вариант может быть задан только один раз): **local** – локальная база учетных записей пользователей; **none** – отключение аутентификации; **radius** – аутентификация на сервере RADIUS; **tacacs** – аутентификация на сервере TACACS+

Значение по умолчанию:

Аутентификация с помощью локальной базы учетных записей пользователей.

Использование команды:

Команда «**aaa authentication login**» используется для используется для установки порядка методов аутентификации пользователя.

Каждый последующий метод аутентификации в списке задействуется, только если предыдущий метод не может быть использован. Например, если задать порядок “radius local”, то локальная база задействуется, только если все серверы RADIUS недоступны или список RADIUS-серверов пустой. Локальная база всегда доступна, поэтому не имеет смысла задавать другие методы после “local”.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa authentication login authen-list radius local
admin@Switch(config)#
```

6.1.2 aaa authentication dot1x

Команда глобальной настройки. Установка списка методов аутентификации 802.1X.

Синтаксис команды:

aaa authentication dot1x default *method1* [*method2...*]

no aaa authentication dot1x

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

method1	основной метод, используемый для аутентификации: **none** – отключение аутентификации; **radius** – аутентификация на сервере RADIUS
method2...	дополнительные методы, используемые для аутентификации. Каждый последующий метод используется, только если предыдущие методы были завершены неуспешно

Значение по умолчанию:

Аутентификация на серверах RADIUS.

Использование команды:

Команда «**aaa authentication dot1x**» используется для используется для установки списка методов аутентификации 802.1X.

Команда позволяет указать аутентификацию на серверах RADIUS, отсутствие аутентификации или оба метода одновременно.

В случае необходимости успешного завершения аутентификации, даже если сервер RADIUS недоступен или вернул сообщение об ошибке, необходимо указать «**none**» в качестве последнего метода аутентификации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa authentication dot1x default radius
admin@Switch(config)#
```

6.1.3 ip http authentication

Команда глобальной настройки. Установка порядка методов аутентификации пользователя для доступа к серверу HTTP.

Синтаксис команды:

ip http authentication aaa login-authentication *list-name*

no ip http authentication aaa login-authentication

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

list-name	имя списка методов аутентификации пользователя. Рекомендуемая длина: от 1 до 12 символов

Значение по умолчанию:

Значение по умолчанию соответствует значению команды «**aaa authentication login default**».

Использование команды:

Команда «**ip http authentication**» используется для установки порядка методов аутентификации пользователя для аутентификации на сервере HTTP.

Команда используется для доступа к серверам HTTP и HTTPS. Каждый последующий метод аутентификации в списке задействуется, только если предыдущий метод не может быть использован. Например, если задать порядок “tacacs local”, то локальная база задействуется, только если все серверы TACACS+ недоступны или список TACACS+-серверов пустой. Локальная база всегда доступна, поэтому не имеет смысла задавать другие методы после “local”.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip http authentication aaa login-authentication tacacs local
admin@Switch(config)#
```

6.1.4 line

Команда глобальной настройки. Переход в режим настройки линии (протокола) управления.

Синтаксис команды:

line {**console** | **telnet** | **ssh**}

Параметры команды:

console	управление через консоль
telnet	управление по протоколу Telnet
ssh	управление по протоколу SSH

Использование команды:

Команда «**line**» используется для перехода в режим настройки линии (протокола) управления.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# line ssh
admin@Switch(config-line)#
```

6.1.5 login authentication

Команда настройки конфигурации протоколов управления. Установка порядка методов аутентификации для протоколов управления.

Синтаксис команды:

login authentication {**default** | *list-name*}

no login authentication

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

list-name имя списка методов аутентификации пользователя

Значение по умолчанию:

Значение по умолчанию соответствует значению команды «**aaa authentication login default**».

Использование команды:

Команда «**login authentication**» используется для установки порядка методов аутентификации для протоколов управления.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa authentication login authen-list radius local
admin@Switch(config)# line console
admin@Switch(config-line)# login authentication authen-list
admin@Switch(config-line)#
```

6.1.6 show authentication methods

Команда, доступная из любого режима. Вывод информации об используемых методах аутентификации.

Синтаксис команды:

show authentication methods

Использование команды:

Команда «**show authentication methods**» используется для вывода информации об используемых методах аутентификации.

Пример команды:

```
admin@Switch# show authentication methods
Login Authentication Method Lists
---------------------------------
Default: tacacs, radius, local
Console_login: local

Dot1x Authentication Method Lists
---------------------------------
radius, none

Line      Login Method List
-------   -----------------
Console    Console_login
Telnet     Default
SSH        Default
HTTP:      radius, local
HTTPS:     radius, local
```

6.2 Настройка RADIUS и TACACS+

6.2.1 debug radius

Команда фундаментального режима. Включение отладки RADIUS.
Синтаксис команды:
debug radius {**authentication brief** | **events**}
no debug radius {**authentication brief** | **events**}
Команда с приставкой «**no**» отключает отладку RADIUS.
Параметры команды:

authentication brief	вывод краткой информации о пакетах авторизации
events	вывод информации о событиях RADIUS

Пример команды:

```
admin@Switch# debug radius events
admin@Switch#
```

6.2.2 debug tacacs

Команда фундаментального режима. Включение отладки TACACS+.
Синтаксис команды:
debug tacacs {**events** | **packets brief**}
no debug tacacs {**events** | **packets brief**}
Команда с приставкой «**no**» отключает отладку TACACS+.
Параметры команды:

events	вывод информации только о событиях TACACS+
packets brief	вывод информации только о полученных/отправленных пакетах, без отображения содержимого пакетов

Пример команды:

```
admin@Switch# debug tacacs
admin@Switch#
```

6.2.3 radius-server attribute 4

Команда глобальной настройки. Установка NAS (Network Attached Storage) IP, используемого при обмене с серверами RADIUS.
Синтаксис команды:
radius-server attribute 4 *ip-address*
no radius-server attribute 4
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

ip-address	IP-адрес, подставляемый в параметр NAS IP. По умолчанию устройство определяет NAS IP автоматически

Значение по умолчанию:

По умолчанию устройство определяет NAS IP автоматически по следующему алгоритму:

1. При запуске устройство находит первый VLAN с IP-адресом, начиная с VLAN 1, и устанавливает NAS IP равным IP-адресу на этом VLAN.
2. При изменении IP-адреса на выбранном VLAN, NAS IP также изменяется.
3. При удалении IP-адреса на выбранном VLAN, устройство повторяет алгоритм из пункта 1.

Использование команды:

Команда «**radius-server attribute 4**» используется для установки NAS IP, используемого при обмене с серверами RADIUS.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# radius-server attribute 4 10.0.0.1
admin@Switch(config)#
```

6.2.4 radius-server deadtime

Команда глобальной настройки. Установка интервала времени, в течение которого недоступный (не отвечающий) RADIUS-сервер отслеживается на наличие ответной реакции.

Синтаксис команды:

radius-server deadtime *deadtime*

no radius-server deadtime

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

deadtime	интервал времени, в течение которого недоступный (не отвечающий) RADIUS-сервер отслеживается на наличие ответной реакции, в диапазоне от 0 до 2000 минут

Значение по умолчанию:

По умолчанию команда отключена.

Использование команды:

Команда «**radius-server deadtime**» используется для установки интервала времени, в течение которого недоступный (не отвечающий) RADIUS-сервер отслеживается на наличие ответной реакции.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# radius-server deadtime 10
admin@Switch(config)#
```

6.2.5 radius-server host

Команда глобальной настройки. Добавление сервера RADIUS.

Синтаксис команды:

radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**priority** *priority*] [**udp**] [**tls** *name*]

no radius-server host {*ip-address* | *hostname*}

Команда с приставкой «**no**» удаляет сервер RADIUS.

Параметры команды:

ip-address	IP-адрес сервера RADIUS
hostname	доменное имя сервера RADIUS. Рекомендуемая длина каждого поддомена: до 63 символов
auth-port-number	порт, используемый для аутентификации, в диапазоне от 0 до 65535. Значение равное нулю, означает, что сервер не будет использоваться для аутентификации. Если параметр не задан, то используется значение 1812
timeout	время ожидания ответа от сервера в диапазоне от 1 до 30 секунд. Если параметр не задан, то используется глобальное значение, задаваемое командой «**radius-server timeout**»
retries	количество попыток отправки запроса аутентификации в случае отсутствия ответа от сервера в диапазоне от 1 до 15. Если параметр не задан, то используется глобальное значение, задаваемое командой «**radius-server retransmit**»
deadtime	интервал времени, на которое сервер RADIUS исключается из опроса, если он не ответил на все попытки запроса аутентификации, в диапазоне от 0 до 2000 минут. Если параметр не задан, то используется глобальное значение, задаваемое командой «**radius-server deadtime**»
key-string	ключ аутентификации и шифрования длиной от 0 до 128 символов. Для настройки пустого ключа используются двойные скобки «()». Если параметр не задан, то используется глобальное значение, задаваемое командой «**radius-server key**».

priority	приоритет, определяющий порядок перебора серверов в диапазоне от 0 до 65535. Нулевое значение означает максимальный приоритет. Если параметр не задан, то используется значение 0
udp	выбор протокола UDP
tls	выбор протокола TLS
name	имя конфигурации TLS

Значение по умолчанию:

Серверы RADIUS не заданы.

Использование команды:

Команда «**radius-server host**» используется для добавления сервера RADIUS.

Команда «**aaa authentication login**» используется для установки порядка методов аутентификации пользователя.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# radius-server host 192.168.0.1
admin@Switch(config)#
```

6.2.6 radius-server key

Команда глобальной настройки. Установка ключа аутентификации и шифрования, используемого для взаимодействия с серверами RADIUS.

Синтаксис команды:

radius-server key *key-string*

no radius-server key

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

key-string	ключ аутентификации и шифрования длиной от 0 до 128 символов. Для настройки пустого ключа используются двойные скобки «()».

Значение по умолчанию:

По умолчанию используется пустая строка.

Использование команды:

Команда «**radius-server key**» используется для установки ключа аутентификации и шифрования, используемого для взаимодействия с серверами RADIUS. Ключ аутентификации и шифрования можно переопределить для каждого сервера RADIUS.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# radius-server key The_Key
admin@Switch(config)#
```

6.2.7 radius-server retransmit

Команда глобальной настройки. Установка количества попыток отправки запроса аутентификации в случае отсутствия ответа от сервера RADIUS.

Синтаксис команды:

radius-server retransmit *retries*

no radius-server retransmit

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

retries	количество попыток отправки запроса аутентификации в случае отсутствия ответа от сервера в диапазоне от 1 до 15

Значение по умолчанию:

По умолчанию количество попыток отправки запроса аутентификации равно 3.

Использование команды:

Команда «**radius-server retransmit**» используется для установки количества попыток отправки запроса аутентификации в случае отсутствия ответа от сервера RADIUS.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# radius-server retransmit 2
admin@Switch(config)#
```

6.2.8 radius-server timeout

Команда глобальной настройки. Установка времени ожидания ответа от сервера RADIUS.

Синтаксис команды:

radius-server timeout *timeout*

no radius-server timeout

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

timeout	время ожидания ответа от сервера в диапазоне от 1 до 30 секунд

Значение по умолчанию:

Устройство ожидает ответа от сервера 3 секунды.

Использование команды:

Команда «**radius-server timeout**» используется для установки времени ожидания ответа от сервера RADIUS.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# radius-server timeout 2
admin@Switch(config)#
```

6.2.9 tacacs-server host

Команда глобальной настройки. Добавление сервера TACACS+.

Синтаксис команды:

tacacs-server host {*ip-address* | *hostname*} [**single-connection**] [**tacport** *port-number*] [**timeout** *timeout*] [**key** *key-string*] [**priority** *priority*]

no tacacs-server host {*ip-address* | *hostname*}

Команда с приставкой «**no**» удаляет сервер TACACS+.

Параметры команды:

ip-address	IP-адрес сервера TACACS+
hostname	доменное имя сервера TACACS+. Рекомендуемая длина каждого поддомена: до 63 символов
single-connection	устройство будет использовать одно постоянное подключение к серверу. Если параметр не задан, то устройство будет открывать отдельное подключение для каждого запроса
port-number	порт, используемый для аутентификации, в диапазоне от 0 до 65535. Значение, равное нулю, означает, что сервер не будет использоваться для аутентификации. Если параметр не задан, то используется значение 49
timeout	время ожидания ответа от сервера в диапазоне от 1 до 30 секунд. Если параметр не задан, то используется глобальное значение, задаваемое командой «**tacacs-server timeout**»
key-string	ключ аутентификации и шифрования длиной от 0 до 128 символов. Для настройки пустого ключа используются двойные скобки «()». Если параметр не задан, то используется глобальное значение, задаваемое командой «**tacacs-server key**».
priority	приоритет, определяющий порядок перебора серверов в диапазоне от 0 до 65535. Нулевое значение означает максимальный приоритет. Если параметр не задан, то используется значение 0

Значение по умолчанию:

Серверы TACACS+ не заданы.

Использование команды:

Команда «**tacacs-server host**» используется для добавления сервера TACACS+.

Команда «**aaa authentication login**» используется для установки порядка методов аутентификации пользователя.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# tacacs-server host 192.168.0.1
admin@Switch(config)#
```

6.2.10 tacacs-server key

Команда глобальной настройки. Установка ключа аутентификации и шифрования, используемого для взаимодействия с серверами TACACS+.

Синтаксис команды:

tacacs-server key *key-string*

no tacacs-server key

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

key-string	ключ аутентификации и шифрования длиной от 0 до 128 символов. Для настройки пустого ключа используются двойные скобки «()».

Значение по умолчанию:

Пустая строка.

Использование команды:

Команда «**tacacs-server key**» используется для установки ключа аутентификации и шифрования, используемого для взаимодействия с серверами TACACS+. Ключ аутентификации и шифрования можно переопределить для каждого сервера TACACS+.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# tacacs-server key The_Key
admin@Switch(config)#
```

6.2.11 tacacs-server timeout

Команда глобальной настройки. Установка времени ожидания ответа от сервера TACACS+.

Синтаксис команды:

tacacs-server timeout *timeout*

no tacacs-server timeout

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

timeout	время ожидания ответа от сервера в диапазоне от 1 до 30 секунд

Значение по умолчанию:

Устройство ожидает ответа от сервера 5 секунд.

Использование команды:

Команда «**tacacs-server timeout**» используется для установки времени ожидания ответа от сервера TACACS+.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# tacacs-server timeout 2
admin@Switch(config)#
```

6.2.12 test aaa server radius

Команда фундаментального режима. Отправка тестового запроса на сервер RADIUS.

Синтаксис команды:

test aaa server radius {*ip-address* | *hostname*} *username password*

Параметры команды:

ip-address	IP-адрес сервера RADIUS
hostname	доменное имя сервера RADIUS
username	имя пользователя, используемое в запросе
password	пароль пользователя, используемый в запросе

Использование команды:

Команда «**test aaa server radius**» используется для отправки тестового запроса на сервер RADIUS. Сервер должен существовать в конфигурации устройства.

После выполнения команды устройство выводит сообщение об успешной или неуспешной аутентификации следующего формата:

“%AAA-6-TEST: Test request to RADIUS server <IP> with username <USER> and password <PASS>: <RESULT>”.

Варианты значений результата “<RESULT>”:

- “server is not configured” – запрос не был отправлен, так как сервер отсутствует в конфигурации устройства;
- “server is not alive” – запрос не был отправлен, так как сервер помечен флагом “вышедший из строя”;
- “server not responding” – сервер не ответил на запрос;
- “authentication success” – сервер ответил, что указанные имя и пароль пользователя корректны;
- “authentication fail” – сервер ответил, что указанные имя и пароль пользователя некорректны;
- “internal error” – при обработке запроса возникла ошибка.

Пример команды:

```
admin@Switch# test aaa server radius 10.0.0.1 user pass
%AAA-6-TEST: Test request to RADIUS server 10.0.0.1 with username 'user' and password
'pass': authentication success
admin@Switch#
```

6.2.13 show radius-servers

Команда, доступная из любого режима. Вывод настроек серверов RADIUS.

Синтаксис команды:

show radius-servers

Использование команды:

Команда «**show radius-servers**» используется для вывода настроек серверов RADIUS.

Параметр «Dead till» показывает время (в минутах), которое осталось до исключения сервера из списка мертвых. Если время равно нулю, то сервер жив.

Пример команды:

```
admin@Switch# show radius-servers
IP address    PortAuth  TimeOut  Retransmision  Deadtime  Priority  Dead till
----------    --------  -------  -------------  --------  --------  ---------
10.0.0.1      1812      global   global         global    1         0
radius.local  1812      5        2              10        2         4

Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
```

6.2.14 show tacacs

Фундаментальная команда. Вывод настроек серверов TACACS+.

Синтаксис команды:

show tacacs

Использование команды:

Команда «**show tacacs**» используется для вывода настроек серверов TACACS+.

Пример команды:

```
admin@Switch# show tacacs

IP address   Status         Port  Single Connection  TimeOut  Priority
-----------  -------------  ----  -----------------  -------  --------
192.168.0.1  Connected      49    No                 global   1
tacacs.local Not connected  49    No                 global   2

Global values
------------
TimeOut: 5
```

6.3 Настройка 802.1X

6.3.1 aaa authorization

Команда глобальной настройки. Установка метода авторизации.

Синтаксис команды:

aaa authorization network default *method*

no aaa authorization network default

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

network	авторизация сетевых функций
default	установка списка, используемого по умолчанию
method1 [*method2...*]	метод авторизации:
	– **if-authenticated** – разрешение авторизации, если клиент прошел аутентификацию на сервере RADIUS;
	– **none** – отключение авторизации;
	– **radius** – авторизация на сервере RADIUS

Значение по умолчанию:

Авторизация отключена (эквивалентно указанию параметра «**none**»).

Использование команды:

Команда «**aaa authorization**» используется для установки метода авторизации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa authorization network default radius
admin@Switch(config)#
```

6.3.2 aaa server radius dynamic-author

Команда глобальной настройки. Включение на устройстве сервера аутентификации, авторизации и аккаунтинга, взаимодействующего с внешними серверами политик.

Синтаксис команды:

aaa server radius dynamic-author

no aaa server radius dynamic-author

Команда с приставкой «**no**» отключает функцию.

Значение по умолчанию:

Устройство не обеспечивает функции сервера при взаимодействии с внешними серверами политик.

Использование команды:

Команда «**aaa server radius dynamic-author**» используется для включения на устройстве сервера аутентификации, авторизации и аккаунтинга, взаимодействующего с внешними серверами политик. При вводе команды происходит переход в режим настройки сервера динамической авторизации.

Стандартный режим RADIUS предполагает инициацию действий со стороны сетевого устройства, которое генерирует запрос к серверам авторизации. Серверы авторизации, в свою очередь, возвращают ответ на запрос. Устройство поддерживает динамический режим авторизации, описанный в RFC 5176. В динамическом режиме авторизации серверы аутентификации, авторизации и аккаунтинга могут инициировать смену параметров сессии на сетевом устройстве.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa server radius dynamic-author
admin@Switch(config-locsvr-da-radius)#
```

6.3.3 auth-type

Команда настройки сервера динамической аутентификации. Установка типа авторизации клиентов RADIUS.

Синтаксис команды:

auth-type {**all** | **any**}

no auth-type

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

all	все атрибуты сообщения должны соответствовать сессии
any	любой атрибут сообщения должен соответствовать сессии

Значение по умолчанию:

Все атрибуты сообщения должны соответствовать сессии.

Использование команды:

Команда «**auth-type**» используется для установки типа авторизации клиентов RADIUS.

Стандартный режим RADIUS предполагает инициацию действий со стороны сетевого устройства, которое генерирует запрос к серверам авторизации. Серверы авторизации, в свою очередь, возвращают ответ на запрос. Устройство поддерживает динамический режим авторизации, описанный в RFC 5176. В динамическом режиме авторизации серверы аутентификации, авторизации и аккаунтинга могут инициировать смену параметров сессии на сетевом устройстве.

Устройство идентифицирует сессию аутентификации по атрибутам Calling-Station-ID и Acct-Session-ID. Параметр «**all**» указывает, что если в сообщении присутствует более одного из указанных атрибутов, то все они должны соответствовать одной и той же сессии. Если в команде «**auth-type**» указан параметр «**any**», то устройство по порядку обрабатывает атрибуты на предмет соответствия какой-либо

сессии и применяет необходимые действия к первой найденной сессии.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa server radius dynamic-author
admin@Switch(config-locsvr-da-radius)# auth-type any
admin@Switch(config-locsvr-da-radius)#
```

6.3.4 authentication command bounce-port ignore

Команда глобальной настройки. Включение игнорирования команды сброса интерфейса RADIUS CoA.

Синтаксис команды:

authentication command bounce-port ignore

no authentication command bounce-port ignore

Команда с приставкой «**no**» отключает функцию.

Значение по умолчанию:

Функция отключена.

Использование команды:

Команда «**authentication command bounce-port ignore**» используется для включения игнорирования команды сброса интерфейса RADIUS CoA.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# authentication command bounce-port ignore
admin@Switch(config)#
```

6.3.5 authentication command disable-port ignore

Команда глобальной настройки. Включение игнорирования команды отключения интерфейса RADIUS CoA.

Синтаксис команды:

authentication command disable-port ignore

no authentication command disable-port ignore

Команда с приставкой «**no**» отключает функцию.

Значение по умолчанию:

Функция отключена.

Использование команды:

Команда «**authentication command disable-port ignore**» используется для включения игнорирования команды отключения интерфейса RADIUS CoA.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# authentication command disable-port ignore
admin@Switch(config)#
```

6.3.6 authentication event fail

Команда настройки интерфейса (Ethernet). Установка действия, применяемого в случае неудачной попытки аутентификации клиента на интерфейсе из-за некорректных учетных данных.

Синтаксис команды:

authentication event fail [**retry** *retry-count*] **action** {**authorize vlan** *vlan-id* | **next-method**}

no authentication event fail

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

retry *retry-count*	количество повторных попыток аутентификации, после которых применяется действие. Диапазон значений от: 1 до 10
authorize vlan *vlan-id*	перевод интерфейса в неаутентифицированный VLAN, заданный параметром «*vlan-id*». Диапазон значений: от 1 до 4094. Неаутентифицированный VLAN не может быть равен Voice VLAN
next-method	использование следующего метода аутентификации. Порядок методов определяется командой «**authentication order**»

Значение по умолчанию:

Устройство выполняет две повторные попытки аутентификации, после которых используется следующий метод аутентификации, заданный командой «**authentication order**».

Использование команды:

Команда «**authentication event fail**» используется для установки действия, применяемого в случае неудачной попытки аутентификации клиента на интерфейсе из-за некорректных учетных данных.

Клиенты, которые не проходят аутентификацию, остаются в неаутентифицированном VLAN до попытки повторной аутентификации (если включено на интерфейсе). Если аутентификация завершается неудачно, то интерфейс остается в неаутентифицированном VLAN. Если аутентификация завершается успешно, то интерфейс переходит либо в Access VLAN, либо в VLAN, предоставленный сервером RADIUS.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# authentication event fail retry 3 action authorize vlan 10
admin@Switch(config-if)#
```

6.3.7 authentication order

Команда настройки интерфейса (Ethernet). Установка порядка методов аутентификации для клиентов, подключенных к интерфейсу.

Синтаксис команды:

authentication order {**dot1x** [**mab**] | **mab** [**dot1x**]}

no authentication order

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

dot1x	аутентификация по стандарту IEEE 802.1X
mab	аутентификация по MAC-адресу (MAC Based Authentication)

Значение по умолчанию:

По умолчанию порядок методов аутентификации: dot1x, mab.

Использование команды:

Команда «**authentication order**» используется для установки порядка методов аутентификации для клиентов, подключенных к интерфейсу.

Каждый метод аутентификации может быть указан только один раз. Устройство переходит к следующему методу аутентификации, только если предыдущий метод завершился неудачно.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# authentication order mab dot1x
admin@Switch(config-if)#
```

6.3.8 clear dot1x statistics

Команда фундаментального режима. Очистка статистики 802.1X на всех или конкретном интерфейсе.

Синтаксис команды:

clear dot1x statistics [*interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Значение по умолчанию:

Не применимо.

Использование команды:

Команда «**clear dot1x statistics**» используется для очистки статистики 802.1X на всех или конкретном интерфейсе. Если команда введена без аргументов, то производится очистка статистики 802.1X для всех интерфейсов Ethernet.

Пример команды:

```
admin@Switch# clear dot1x statistics tengigabitethernet 0/1
admin@Switch#
```

6.3.9 client

Команда настройки сервера динамической маршрутизации. Добавление клиента RADIUS, от которого устройство может принимать запросы смены авторизации (RADIUS CoA) и завершения сессии.

Синтаксис команды:
client {*hostname* | *ip-address*} [**server-key** *string*]
no client {*hostname* | *ip-address*}
Команда с приставкой «**no**» удаляет клиента.
Параметры команды:

hostname	имя хоста клиента RADIUS
ip-address	IP-адрес хоста клиента RADIUS
string	ключ аутентификации и шифрования длиной от 0 до 128 символов. Повторный ввод команды без указания ключа позволяет установить пустой ключ. По умолчанию используется пустой ключ

Значение по умолчанию:
Клиенты RADIUS не заданы.
Использование команды:
Команда «**client**» используется для добавления клиента RADIUS, от которого устройство может принимать запросы смены авторизации (RADIUS CoA) и завершения сессии.

Стандартный режим RADIUS предполагает инициацию действий со стороны сетевого устройства, которое генерирует запрос к серверам авторизации. Серверы авторизации, в свою очередь, возвращают ответ на запрос. Устройство поддерживает динамический режим авторизации, описанный в RFC 5176. В динамическом режиме авторизации серверы аутентификации, авторизации и аккаунтинга могут инициировать смену параметров сессии на сетевом устройстве.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa server radius dynamic-author
admin@Switch(config-locsvr-da-radius)# client 10.0.0.1 server-key polygon123
admin@Switch(config-locsvr-da-radius)#
```

6.3.10 debug aaa coa

Команда фундаментального режима. Включение отладки получения пакетов RADIUS CoA (Change of Authorization).
Синтаксис команды:
debug aaa coa
no debug aaa coa
Команда с приставкой «**no**» отключает отладку.
Использование команды:
Команда «**debug aaa coa**» используется для включения отладки получения пакетов RADIUS CoA (Change of Authorization).
Пример команды:

```
admin@Switch# debug aaa coa
admin@Switch#
```

6.3.11 debug aaa pod

Команда фундаментального режима. Включение отладки получения пакетов RADIUS PoD (Packet of Disconnect).

Синтаксис команды:

debug aaa pod

no debug aaa pod

Команда с приставкой «**no**» отключает отладку.

Использование команды:

Команда «**debug aaa pod**» используется для включения отладки получения пакетов RADIUS PoD (Packet of Disconnect).

Пример команды:

```
admin@Switch# debug aaa pod
admin@Switch#
```

6.3.12 debug dot1x

Команда фундаментального режима. Включение отладки IEEE 802.1X.

Синтаксис команды:

debug dot1x {**all** | **packets** | **events**}

no debug dot1x {**all** | **packets** | **events**}

Команда с приставкой «**no**» отключает отладку IEEE 802.1X.

Параметры команды:

all	вывод всех отладочных событий (включает / выключает все ключи отладки)
packets	вывод содержимого пакетов EAPoL в шестнадцатеричном формате (отдельно заголовок и данные)
events	вывод событий

Значение по умолчанию:

Отладка отключена.

Использование команды:

Команда «**debug dot1x**» используется для включения отладки IEEE 802.1X.

Пример команды:

```
admin@Switch# debug dot1x all
admin@Switch#
```

6.3.13 dot1x guest-vlan

Команда настройки интерфейса (Ethernet). Установка номера гостевого VLAN на интерфейсе.

Синтаксис команды:

dot1x guest-vlan *vlan-id*

no dot1x guest-vlan

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Гостевой VLAN отсутствует.

Использование команды:

Команда «**dot1x guest-vlan**» используется для установки номера гостевого VLAN на интерфейсе.

Guest VLAN (гостевой VLAN) предназначен для предоставления ограниченных функций для клиентов, которые не поддерживают аутентификацию IEEE 802.1X или нуждаются в выполнении каких-либо задач перед аутентификацией (например, загрузка ПО с сервера).

Если на интерфейсе уже был настроен гостевой VLAN, то устройство переводит интерфейс в неавторизованное состояние и начинает процесс аутентификации.

Ограничения гостевого VLAN:

- гостевой VLAN не может быть равен Voice VLAN;
- гостевой VLAN не поддерживается в режиме сессий «**multi-sessions**». Таким образом, попытка настройки Guest VLAN при режиме сессий «**multi-sessions**» или попытка установки режима сессий «**multi-sessions**» при настроенном Guest VLAN приведет к выводу сообщения об ошибке.

Если на интерфейсе включен гостевой VLAN, то устройство действует по следующему алгоритму:

1. При появлении соединения на интерфейсе (link up) устройство отправляет запрос EAPOL. Если клиент не отвечает на запрос (не отправляет пакет EAPOL), устройство переводит интерфейс в гостевой VLAN (Access VLAN заменяется на гостевой VLAN) и разрешает прием и передачу пакетов.

   Пока на интерфейсе не получен ни один пакет EAPOL, интерфейс остается в гостевом VLAN.

2. Если на интерфейсе получен пакет EAPOL, то, по умолчанию, устройство исключает интерфейс из Guest VLAN, блокирует прием и передачу на нем и начинает процесс аутентификации. Устройство запоминает, что на интерфейсе есть клиент IEEE 802.1X и больше не добавляет интерфейс в гостевой VLAN. Устройство поддерживает возможность блокировки данной подфункции.
3. При пропадании соединения на интерфейсе устройство забывает информацию о наличии клиента IEEE 802.1X.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x guest-vlan 20
admin@Switch(config-if)#
```

6.3.14 dot1x guest-vlan supplicant

Команда глобальной настройки. Разрешение доступа к гостевому VLAN со стороны клиентов IEEE 802.1X.

Синтаксис команды:

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

Команда с приставкой «**no**» запрещает доступа к гостевому VLAN со стороны клиентов IEEE 802.1X.

Значение по умолчанию:

Клиенты IEEE 802.1X не имеют доступа к гостевому VLAN.

Использование команды:

Команда «**dot1x guest-vlan supplicant**» используется для разрешения доступа к гостевому VLAN со стороны клиентов IEEE 802.1X.

Если этот параметр включен, то устройство не удаляет клиента IEEE 802.1X из гостевого VLAN во время аутентификации. Если от сервера аутентификации не получен атрибут назначения VLAN для клиента, то клиент IEEE 802.1X остается в гостевом VLAN и после успешной аутентификации. Если аутентификация завершена неуспешно и настроен неаутентифицированный VLAN, то клиент IEEE 802.1X попадает в неаутентифицированный VLAN.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# dot1x guest-vlan supplicant
admin@Switch(config)#
```

6.3.15 dot1x re-authenticate

Фундаментальная команда. Проведение повторной аутентификации на всех или конкретном интерфейсе.

Синтаксис команды:

dot1x re-authenticate [*interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Значение по умолчанию:

Не применимо.

Использование команды:

Команда «**dot1x re-authenticate**» используется для проведения повторной аутентификации на всех или конкретном интерфейсе. Если команда введена без аргументов, то она применяется для всех интерфейсов Ethernet.

Пример команды:

```
admin@Switch(config)# dot1x re-authenticate gigabitethernet 0/1
admin@Switch(config)#
```

6.3.16 dot1x system-auth-control

Команда глобальной настройки. Глобальное включение аутентификации IEEE 802.1X.

Синтаксис команды:

dot1x system-auth-control

no dot1x system-auth-control

Команда с приставкой «**no**» глобально отключает аутентификацию IEEE 802.1X.

Значение по умолчанию:

Аутентификация IEEE 802.1X отключена.

Использование команды:

Команда «**dot1x system-auth-control**» используется для глобального включения аутентификации IEEE 802.1X.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# dot1x system-auth-control
admin@Switch(config)#
```

6.3.17 dot1x host-mode

Команда настройки интерфейса (Ethernet). Установка режима сессий (аутентификации одного и множества хостов) на интерфейсе.

Синтаксис команды:

dot1x host-mode {**single-host | multi-host | multi-sessions | multi-auth**}

no dot1x host-mode

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

single-host	установка режима с одним хостом
multi-host	установка режима с множеством хостов
multi-sessions	установка режима с множеством сессий
multi-auth	установка режима двухдоменной аутентификации (VLAN данных и голосовой VLAN)

Значение по умолчанию:

Режим с множеством хостов.

Использование команды:

Команда «**dot1x host-mode**» используется для установки режима сессий (аутентификации одного и множества хостов) на интерфейсе.

В режиме с одним хостом аутентификация производится только для одного хоста. После успешной аутентификации хоста только этот хост получает доступ в сеть.

В режиме с множеством хостов, при успешной аутентификации любого из хостов доступ в сеть разрешен всем хостам, подключенным к интерфейсу. При завершении сессии доступ в сеть запрещен всем хостам, подключенным к интерфейсу.

В режиме с множеством сессий каждый хост должен пройти аутентификацию для доступа в сеть.

Необходимо иметь в виду, что пакеты не зашифрованы и после успешной аутентификации, фильтрация пакетов проводится только по MAC-адресу источника.

В режиме двухдоменной аутентификации аутентификация производится для одного хоста в VLAN данных и еще одного хоста в голосовой VLAN.

Рекомендуется включить повторную аутентификацию при работе в режиме с множеством сессий для обнаружения сессий, не завершенных корректно.

Режим безопасности на интерфейсе может быть включен, только если интерфейс находится в режиме «**multi-host**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x host-mode multi-sessions
admin@Switch(config-if)#
```

6.3.18 dot1x max-req

Команда настройки интерфейса (Ethernet). Установка максимального количества повторов при отправке фреймов Extensible Authentication Protocol (EAP) request/identity (в случае отсутствия ответов) клиенту перед перезапуском процесса аутентификации.

Синтаксис команды:

dot1x max-req *count*

no dot1x max-req

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

count	количество повторов при отправке фреймов EAP request/identity клиенту перед перезапуском процесса аутентификации в диапазоне от 1 до 10

Значение по умолчанию:

Количество повторов равно 2.

Использование команды:

Команда «**dot1x max-req**» используется для установки максимального количества повторов при отправке фреймов Extensible Authentication Protocol (EAP) request/identity (в случае отсутствия ответов) клиенту перед перезапуском процесса аутентификации.

Значение настройки рекомендуется изменять только в случае возникновения проблем из-за ненадежного подключения клиентов или проблем совместимости между клиентами и серверами аутентификации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x max-req 6
admin@Switch(config-if)#
```

6.3.19 dot1x port-control

Команда настройки интерфейса (Ethernet). Установка состояния аутентификации на интерфейсе.

Синтаксис команды:

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

auto	включение аутентификации 802.1X на интерфейсе. Состояние аутентификации на интерфейсе определяется обменом по протоколу 802.1X между устройством и клиентом
force-authorized	отключение аутентификации 802.1X и безусловное разрешение доступа на интерфейсе (прием и передача трафика)
force-unauthorized	отключение аутентификации 802.1X и безусловный запрет доступа на интерфейсе. Интерфейс игнорирует все попытки аутентификации и запрещает любой прием и передачу трафика через него

Значение по умолчанию:

Отключение аутентификации 802.1X и безусловное разрешение доступа на интерфейсе (прием и передача трафика).

Использование команды:

Команда «**dot1x port-control**» используется для установки состояния аутентификации на интерфейсе.

Рекомендуется отключить протоколы Spanning-Tree на интерфейсах в режиме «**auto**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x port-control auto
admin@Switch(config-if)#
```

6.3.20 dot1x reauthentication

Команда настройки интерфейса (Ethernet). Включение периодической (повторной) аутентификации клиентов.

Синтаксис команды:

dot1x reauthentication

no dot1x reauthentication

Команда с приставкой «**no**» отключает периодическую (повторную) аутентификацию клиентов.

Значение по умолчанию:

Периодическая (повторная) аутентификация клиентов отключена.

Использование команды:

Команда «**dot1x reauthentication**» используется для включения периодической (повторной) аутентификации клиентов.

Рекомендуется включить повторную аутентификацию при работе в режиме с множеством сессий для обнаружения сессий, не завершенных корректно.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x reauthentication
admin@Switch(config-if)#
```

6.3.21 dot1x timeout quiet-period

Команда настройки интерфейса (Ethernet). Установка интервала ожидания после неуспешной аутентификации.

Синтаксис команды:

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал ожидания после неуспешной аутентификации в диапазоне от 0 до 65535 секунд

Значение по умолчанию:

Интервал ожидания 60 секундам.

Использование команды:

Команда «**dot1x timeout quiet-period**» используется для установки интервала ожидания после неуспешной аутентификации.

В течение интервала ожидания устройство не принимает и не инициирует попытки аутентификации. Значение настройки рекомендуется изменять только в случае возникновения проблем из-за ненадежного подключения клиентов или проблем совместимости между клиентами и серверами аутентификации.

Интервал ожидания предназначен для уменьшения вероятности подбора пароля. Команда изменяет интервал ожидания только для аутентификации 802.1X.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x timeout quiet-period 10
admin@Switch(config-if)#
```

6.3.22 dot1x timeout reauth-period

Команда настройки интерфейса (Ethernet). Установка интервала периодической (повторной) аутентификации клиентов.

Синтаксис команды:

dot1x timeout reauth-period *seconds*

no dot1x timeout reauth-period

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds интервал периодической аутентификации клиентов в диапазоне от 300 до 4294967295 секунд

Значение по умолчанию:

Интервал периодической аутентификации клиентов равен 3600 секундам.

Использование команды:

Команда «**dot1x timeout reauth-period**» используется для установки интервала периодической (повторной) аутентификации клиентов.

Команда изменяет интервал периодической аутентификации клиентов только для аутентификации 802.1X.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x timeout reauth-period 5000
admin@Switch(config-if)#
```

6.3.23 dot1x timeout server-timeout

Команда настройки интерфейса (Ethernet). Установка интервала ожидания ответа от сервера аутентификации.

Синтаксис команды:

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds интервал ожидания ответа от сервера аутентификации в диапазоне от 1 до 65535 секунд

Значение по умолчанию:

Интервал ожидания равен 30 секундам.

Использование команды:

Команда «**dot1x timeout server-timeout**» используется для установки интервала ожидания ответа от сервера аутентификации.

В качестве реального интервала ожидания используется наименьшее число из двух: «**dot1x timeout server-timeout**» и произведения «**radius-server retransmit**» на «**radius-server timeout**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x timeout server-timeout 5
admin@Switch(config-if)#
```

6.3.24 dot1x timeout supp-timeout

Команда настройки интерфейса (Ethernet). Установка интервала ожидания ответа от клиента на запрос EAP (Extensible Authentication Protocol) перед повторной отправкой запроса.

Синтаксис команды:

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал ожидания ответа на запрос EAP от клиента перед повторной отправкой запроса в диапазоне от 1 до 65535 секунд

Значение по умолчанию:

Интервал ожидания равен 30 секундам.

Использование команды:

Команда «**dot1x timeout supp-timeout**» используется для установки интервала ожидания ответа от клиента на запрос EAP (Extensible Authentication Protocol) перед повторной отправкой запроса.

Значение настройки рекомендуется изменять только в случае возникновения проблем из-за ненадежного подключения клиентов или проблем совместимости между клиентами и серверами аутентификации.

Команда изменяет интервал ожидания только для аутентификации 802.1X.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x timeout supp-timeout 60
admin@Switch(config-if)#
```

6.3.25 dot1x timeout tx-period

Команда настройки интерфейса (Ethernet). Установка интервала ожидания ответа от клиента на запрос EAP (Extensible Authentication Protocol) request/identity перед повторной отправкой запроса.

Синтаксис команды:
dot1x timeout tx-period *seconds*
no dot1x timeout tx-period
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

seconds	интервал ожидания ответа на запрос EAP request/identity от клиента перед повторной отправкой запроса в диапазоне от 1 до 65535 секунд

Значение по умолчанию:
Интервал ожидания равен 30 секундам.
Использование команды:
Команда «**dot1x timeout tx-period**» используется для установки интервала ожидания ответа от клиента на запрос EAP (Extensible Authentication Protocol) request/identity перед повторной отправкой запроса.

Значение настройки рекомендуется изменять только в случае возникновения проблем из-за ненадежного подключения клиентов или проблем совместимости между клиентами и серверами аутентификации.

Команда изменяет интервал ожидания только для аутентификации 802.1X.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# dot1x timeout tx-period 60
admin@Switch(config-if)#
```

6.3.26 port

Команда настройки сервера динамической маршрутизации. Установка номера порта UDP, на котором устройство принимает запросы от клиентов RADIUS.
Синтаксис команды:
port *port-number*
no port
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

port-number	номер порта UDP в диапазоне от 1 до 65535, на котором устройство принимает запросы от клиентов RADIUS. По умолчанию равен 3799

Значение по умолчанию:
Устройство принимает запросы от клиентов RADIUS на порту 3799.
Использование команды:
Команда «**port**» используется для установки типа авторизации клиентов RADIUS.

Стандартный режим RADIUS предполагает инициацию действий со стороны сетевого устройства, которое генерирует запрос к серверам авторизации. Серверы авторизации, в свою очередь, возвращают ответ на запрос. Устройство поддерживает динамический режим авторизации, описанный в RFC 5176. В динамическом

режиме авторизации серверы аутентификации, авторизации и аккаунтинга могут инициировать смену параметров сессии на сетевом устройстве.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# aaa server radius dynamic-author
admin@Switch(config-locsvr-da-radius)# port 5000
admin@Switch(config-locsvr-da-radius)#
```

6.3.27 show aaa server radius

Команда, доступная из любого режима. Вывод настроек сервера динамической маршрутизации RADIUS.

Синтаксис команды:

show aaa server radius

Использование команды:

Команда «**show aaa server radius**» используется для вывода настроек сервера динамической маршрутизации RADIUS.

Пример команды:

```
admin@Switch# show aaa server radius
Bounce-port command is not ignored
Disable-port command is not ignored
Listening port is 5000
Authentication type is all

Clients:

N   IP/Hostname
-   -----------
1   10.0.0.1
2   10.0.0.2
```

6.3.28 show authentication sessions

Команда, доступная из любого режима. Вывод состояния сессий аутентификации на интерфейсах устройства.

Синтаксис команды:

show authentication sessions [**interface** *interface-id* | **mac** *mac-address* | **method** *method-name* **interface** *interface-id* | **session-id** *session-id*]

Параметры команды:

interface-id	идентификатор интерфейса
mac-address	MAC-адрес клиента. MAC-адрес необходимо указать в виде 6 пар шестнадцатеричных цифр, разделенных двоеточиями
method-name	имя метода аутентификации: **dot1x** – аутентификация по стандарту IEEE 802.1X, **mab** – аутентификация по MAC-адресу

session-id идентификатор сессии в виде 96-битного шестнадцатеричного числа

Использование команды:

Команда «**show authentication sessions**» используется для вывода состояния сессий аутентификации на интерфейсах устройства. Если команда введена без аргументов, то выводится сводная информация о состоянии всех сессий.

Примеры команды:

```
admin@Switch# show authentication sessions
Interface   MAC Address         Method   Status         Session ID
---------   -----------------   ------   ------------   ------------------------
gi0/1       00:1B:28:00:00:01   dot1x    Auth Success   C0A8016400000010000A271
gi0/2       00:1B:28:00:00:02   dot1x    Running        C0A8016400000040000A9F4
gi0/3       00:1B:28:00:00:03   mab      Auth Fail      C0A8016400000030000A799
gi0/4       00:1B:28:00:00:04   mab      Auth Success   C0A8016400000020000A414
```

```
admin@Switch# show authentication sessions gigabitethernet 0/1
Interface: gigabitethernet 0/1
  Oper Status: Authorized
  Oper Host Mode: single-host

Session ID: C0A80164000000010000A271
  MAC Address: 00:1B:28:00:00:01
  IPv4 Address: 192.168.1.100
  User-Name: testuser
  Status: Auth Success
  VLAN: 50
Domain: Data

Auth method status:
  Method   State
  ------   ------------
  dot1x    Auth Success
  mab      Not run
```

Методы аутентификации в списке «Auth method status» расположены в порядке, заданном командой «**authentication order**».

Таблица 6 – Описание полей примера команды «**show authentication sessions**»

Название	Описание
Oper Status	Текущее состояние авторизации на интерфейсе: – Authorized – интерфейс авторизован. Прием и передача пакетов включены – Unauthorized – интерфейс не авторизован. Прием и передача пакетов отключены

Продолжение таблицы 6

Название	Описание
Oper Host Mode	Режим сессий (см. команду «**dot1x host-mode**»): – single-host – режим с одним хостом – multi-host – режим с множеством хостов – multi-sessions – режим с множеством сессий
Session ID	Идентификатор сессии, который состоит из следующих составляющих: – наименьший по значению IP-адрес устройства – монотонно увеличивающееся 32-битное число – время начала сессии (32-битная временная метка, равная sysUpTime)
MAC Address	MAC-адрес клиента
IPv4 Address	IPv4-адрес клиента. Определяется из базы данных DHCP Snooping
Status	Текущее состояние аутентификации сессии: – Auth Success – аутентификация пройдена – Auth Fail – аутентификация не пройдена – Running – аутентификация в процессе выполнения – Idle – аутентификация в процессе подготовки выполнения (промежуточное состояние)
VLAN	Идентификатор VLAN, назначенный на интерфейс по атрибутам RADIUS (может быть “N/A”, если сервер RADIUS не предоставил соответствующих атрибутов)
Domain	Домен, к которому отнесен хост: Data или Voice
State	Текущее состояние метода аутентификации: – Auth Success – метод успешно завершил аутентификацию – Auth Fail – метод завершил аутентификацию не успешно – Fail over – метод завершил аутентификацию не успешно. Процесс аутентификации передан следующему методу. Данное значение может быть, только если для интерфейса включено более одного метода аутентификации – Running – аутентификация в процессе выполнения – Not run – метод не использовался для аутентификации (предыдущий метод успешно завершил аутентификацию)

6.3.29 show dot1x

Фундаментальная команда. Вывод настроек и состояния 802.1X всех или конкретного интерфейса.

Синтаксис команды:

show dot1x [*interface* **interface-id | detailed**]

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

detailed вывод информации для всех портов, включая отключенные

Использование команды:

Команда «**show dot1x**» используется для вывода настроек и состояния 802.1X всех или конкретного интерфейса. Если команда введена без аргументов, то она применяется для всех интерфейсов.

Пример команды «show dot1x detailed»:

```
admin@Switch# show dot1x detailed
802.1x is enabled

Port   Admin mode          Oper control   Reauth control   Reauth period  Username
-----  ----------------    ------------   --------------   -------------  --------
Gi0/1  Force-authorized    Authorized     Disable          3600           N/A
Gi0/2  Force-authorized    Authorized     Disable          3600           N/A
Gi0/3  Force-authorized    Authorized     Disable          3600           N/A
Gi0/4  Force-authorized    Authorized     Disable          3600           N/A
Te0/1  Force-authorized    Authorized     Disable          3600           N/A
Te0/2  Force-authorized    Authorized     Disable          3600           N/A
Te0/3  Force-authorized    Authorized     Disable          3600           N/A
Te0/4  Force-authorized    Authorized     Disable          3600           N/A
Te0/5  Force-authorized    Authorized     Disable          3600           N/A
Te0/6  Force-authorized    Authorized     Disable          3600           N/A
Te0/7  Force-authorized    Authorized     Disable          3600           N/A
Te0/8  Force-authorized    Authorized     Disable          3600           N/A
Te0/9  Force-authorized    Authorized     Disable          3600           N/A
Te0/10  Force-authorized    Authorized     Disable          3600           N/A
Te0/11  Auto/Single host    Authorized     Disable          3600           00:18:13:A0:9C:5E
Te0/12  Auto/Mult hosts     Unauthorized   Disable          3600           N/A
Te0/13  Auto/Mult ssns      Unauthorized   Enable           3600           0
Te0/14  Force-unauthorized  Unauthorized   Disable          3600           N/A
Te0/15  Force-authorized    Authorized     Disable          3600           N/A
Te0/16  Force-authorized    Authorized     Disable          3600           N/A
Te0/17  Force-authorized    Authorized     Disable          3600           N/A
Te0/18  Force-authorized    Authorized     Disable          3600           N/A
Te0/19  Force-authorized    Authorized     Disable          3600           N/A
Te0/20  Force-authorized    Authorized     Disable          3600           N/A
Te0/21  Force-authorized    Authorized     Disable          3600           N/A
Te0/22  Force-authorized    Authorized     Disable          3600           N/A
Te0/23  Force-authorized    Authorized     Disable          3600           N/A
Te0/24  Force-authorized    Authorized     Disable          3600           N/A
```

Пример команды «show dot1x interface tengigabitethernet 0/1»:

```
admin@Switch# show dot1x interface tengigabitethernet 0/1
802.1x is enabled
Port    Admin mode         Oper control   Reauth control   Reauth period  Username
-----   ----------------   ------------   --------------   -------------  --------
Fa0/1   Auto/Single host    Authorized     Disable          3600           00:26:18:A0:9C:5B

Quiet period:                       60 Seconds
Tx period:                          30 Seconds
Max req:                            2
Supplicant timeout:                 30 Seconds
Server timeout:                     30 Seconds
Auth Method list:                   radius
Session time:                       00:02:54
MAC Address:                        00:26:18:A0:9C:5B
Termination Cause:                  Session is not terminated yet
Authenticator State Machine State: authed
```

Пример команды «show dot1x interface tengigabitethernet 0/1»:

```
admin@Switch# show dot1x interface tengigabitethernet 0/1
802.1x is enabled
Port    Admin mode       Oper control   Reauth control   Reauth period  Username
-----   --------------   ------------   --------------   -------------  --------
Te0/1   Auto/Mult host   Unauthorized   Disable          3600           N/A

Quiet period:                       60 Seconds
Tx period:                          30 Seconds
Max req:                            2
Supplicant timeout:                 30 Seconds
Server timeout:                     30 Seconds
Auth Method list:                   radius
Session time:                       00:00:00
MAC Address:                        N/A
Termination Cause:                  No session
Authenticator State Machine State: unauthed
```

Описание полей примера представлено в таблице 7.

Таблица 7 – Описание полей примера

Поле	Описание
Port	Номер порта
Admin mode	Режим аутентификации на интерфейсе из списка: Forceauth, Forceunauth, Auto
Oper mode	Текущее состояние аутентификации на интерфейсе из списка: Authorized, Unautho-rized, Down
Reauth Control	Режим повторной аутентификации

Продолжение таблицы 7

Поле	Описание
Reauth Period	Интервал повторной аутентификации
Username	Имя пользователя, аутентифицированного на интерфейсе, если интерфейс находится в автоматическом режиме аутентификации. Если интерфейс аутентифицирован, то отображается имя текущего пользователя. Если интерфейс не аутентифицирован, то отображается имя последнего пользователя, аутентифицировавшегося на интерфейсе
Quiet period	Интервал ожидания после неуспешной аутентификации (например, клиент предоставил некорректный пароль)
Tx period	Интервал ожидания ответа на запрос EAP request/identity от клиента перед повторной отправкой запроса
Max req	Количество повторов при отправке фреймов EAP request/identity клиенту перед перезапуском процесса аутентификации
Supplicant timeout	Интервал ожидания ответа на запрос EAP от клиента перед повторной отправкой запроса
Server timeout	Интервал ожидания ответа от сервера аутентификации
Session Time	Время, прошедшее с начала сессии
MAC address	MAC-адрес клиента, аутентифицировавшегося на интерфейсе
Authentication Method	Метод аутентификации, использованный для установления сессии
Termination Cause	Причина завершения сессии

6.3.30 show dot1x statistics

Фундаментальная команда. Вывод статистики 802.1X на всех или конкретном интерфейсе.

Синтаксис команды:

show dot1x statistics [**interface** *interface-id*]

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show dot1x statistics**» используется для вывода статистики 802.1X на всех или конкретном интерфейсе. Если команда введена без аргументов, то она применяется для всех интерфейсов.

Пример команды:

```
admin@Switch# show dot1x statistics interface tengigabitethernet 0/1
tengigabitethernet0/1 802.1x Statistics:
EapolFramesRx: 5
EapolFramesTx: 4
EapolStartFramesRx: 2
EapolLogoffFramesRx: 0
EapolRespIdFramesRx: 2
EapolRespFramesRx: 1
EapolReqIdFramesTx: 2
EapolReqFramesTx: 2
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 2
LastEapolFrameSource: 00:26:18:A0:9C:5B
```

Описание полей примера представлено в таблице 8.

Таблица 8 – Описание полей примера

Поле	Описание
EapolFramesRx	Количество фреймов EAPOL, полученных на интерфейсе
EapolFramesTx	Количество фреймов EAPOL, отправленных с интерфейса
EapolStartFramesRx	Количество пакетов EAPOL-Start, полученных на интерфейсе
EapolLogoffFramesRx	Количество пакетов EAPOL-Logoff, полученных на интерфейсе
EapolRespIdFramesRx	Количество пакетов EAP Resp/Id, полученных на интерфейсе
EapolRespFramesRx	Количество пакетов EAP (кроме Resp/Id), полученных на интерфейсе
EapolReqIdFramesTx	Количество пакетов EAP Req/Id, отправленных с интерфейса
EapolReqFramesTx	Количество пакетов EAP (кроме Req/Id), отправленных с интерфейса
InvalidEapolFramesRx	Количество некорректных фреймов EAPOL, полученных на интерфейсе
EapLengthErrorFramesRx	Количество фреймов EAPOL с некорректной длиной тела пакета (Packet Body Length), полученных на интерфейсе
LastEapolFrameVersion	Версия EAPOL последнего фрейма EAPOL, полученного на интерфейсе
LastEapolFrameSource	MAC-адрес источника последнего фрейма EAPOL, полученного на интерфейсе

6.3.31 show dot1x users

Фундаментальная команда. Вывод списка пользователей 802.1X, аутентифицированных на интерфейсах.

Синтаксис команды:

show dot1x users [**username** *username*]

Параметры команды:

username	имя пользователя в виде текстовой строки длиной от 1 до 160 символов

Использование команды:

Команда «**show dot1x users**» используется для вывода списка пользователей 802.1X, аутентифицированных на интерфейсах. Если команда введена без аргументов, то она применяется для всех пользователей.

Пример команды:

```
admin@Switch(config)# show dot1x users
Port   Username            Session Time   Auth Method   MAC Address        Vlan
----   -----------------   ------------   -----------   -----------------   ---
Te0/1  00:26:18:A0:9C:5B   00:14:14       radius        00:26:18:A0:9C:5B   1
```

6.4 802.1X: поддержка загружаемых ACL (DACL)

6.4.1 Общие положения

Устройство поддерживает установку загружаемых ACL на интерфейсе для каждого отдельного пользователя IEEE 802.1X (MAB). Для работы этой функции необходимо выполнение следующих условий:

1. На интерфейсе включена аутентификация IEEE 802.1X.
2. Устройство имеет корректную конфигурацию RADIUS и IP-связность до сервера.
3. На устройстве включена авторизация с аргументом network.
4. Сервер RADIUS имеет корректные настройки загружаемых ACL.

Ограничения загружаемых ACL:

1. Функция поддерживается в режимах **single-host** и **multi-session** (в этом режиме DACL применяется только на Access VLAN).
2. Длина загружаемого ACL не может быть больше 4096 символов.
3. Загружаемый ACL замещает существующий статический ACL на интерфейсе. Если на интерфейсе назначен загружаемый ACL и администратор назначает статический ACL, то настройка будет применена только после удаления загружаемого ACL с интерфейса. Также будет выведено предупреждающее сообщение “%Static ACL will be temporarily disabled until DACL is being removed, i.e. due to IEEE 802.1X session close”.

Загружаемые ACL позволяют назначить различные уровни доступа к сети в зависимости от учетной записи пользователя IEEE 802.1X. При аутентификации пользователя IEEE 802.1X, подключенного к интерфейсу устройства, сервер RADIUS отправляет атрибуты ACL, связанные с учетной записью пользователя, на устройство. В свою очередь, устройство применяет полученные атрибуты на интерфейс. После завершения сессии аутентификации устройство автоматически удаляет ACL с интерфейса (включая потерю соединения на интерфейсе).

Устройство поддерживает получение загружаемых ACL и атрибута Cisco-IP-Downloadable-ACL(185) (Cisco AV Pair). Один атрибут содержит в себе одну строку ACL, то есть количество атрибутов Cisco-IP-Downloadable-ACL(185) равно количеству строк в ACL.

Если одна или несколько строк загружаемого ACL некорректны, то устройство игнорирует ACL целиком.

Устройство автоматически заменяет IP-адрес источника в ACL на IP-адрес хоста, прошедшего аутентификацию. Если хост впоследствии меняет IP-адрес, то устройство изменяет DACL в соответствии с новым IP-адресом хоста. Во избежание некорректного поведения каждый хост должен иметь только один IP-адрес, в противном случае устройство будет использовать IP-адрес хоста, обнаруженный первым.

6.4.2 clear ip device tracking

Команда фундаментального режима. Очистка таблиц обнаруженных хостов.

Синтаксис команды:

clear ip device tracking [interface *interface-id* **]**

Описание синтаксиса:

interface *interface-id* (опционально) идентификатор интерфейса (Ethernet, Port-channel)

Использование команды:

Используйте команду «**clear ip device tracking**» для очистки таблиц обнаруженных хостов. Если команда введена без аргументов, то происходит очистка таблиц на всех интерфейсах (Ethernet, Port-channel).

Пример команды:

```
admin@Switch# clear ip device tracking interface gigabitethernet 0/1
admin@Switch#
```

6.4.3 ip device tracking probe

Команда глобальной настройки. Установка параметров обнаружения устройств с помощью ARP-проб.

Синтаксис команды:

ip device tracking probe {count *number* **| delay** *seconds* **| interval** *seconds***}**

no ip device tracking probe {count *number* **| delay** *seconds* **| interval** *seconds***}**

Команда с приставкой «**no**» используется для установки значения по умолчанию.

Параметры команды:

count *number* количество отправляемых ARP-проб при отсутствии ответа на которые, устройство удаляет хост из таблицы. Диапазон значений от 1 до 255

delay *seconds* задержка отправки первой ARP-пробы в диапазоне от 1 до 120 секунд

interval *seconds* интервал отправки ARP-проб в диапазоне от 30 до 1814400 секунд

Значение по умолчанию:

Устройство отправляет до 3 ARP-проб с интервалом в 30 секунд. Задержка отправки отсутствует.

Указания по применению:

Используйте команду **ip device tracking probe** для установки параметров обнаружения устройств с помощью ARP-проб.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip device tracking probe interval 40
admin@Switch(config)#
```

6.4.4 ip device tracking maximum

Команда настройки интерфейса. Установка максимального количества хостов, обнаруживаемых на интерфейсе.

Синтаксис команды:

ip device tracking maximum *number*

no ip device tracking maximum

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

number	максимальное количество устройств, обнаруживаемых на интерфейсе, в диапазоне от 0 (функция отключена) до 65535

Значение по умолчанию:

Максимальное количество равно 0 (функция отключена).

Использование команды:

Используйте команду «**ip device tracking maximum**» для установки максимального количества хостов, обнаруживаемых на интерфейсе.

Примеры команды:

Следующий пример показывает, как установить максимальное количества хостов, обнаруживаемых на интерфейсе gigabitethernet 0/1, равным 5:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip device tracking maximum 5
admin@Switch(config-if)#
```

6.4.5 show ip device tracking

Команда, доступная из любого режима. Вывод таблиц хостов, обнаруженных на интерфейсах.

Синтаксис команды:

show ip device tracking {all count | interface *interface-id***}**

Параметры команды:

all count	вывод настроек и сводной информации о хостах, обнаруженных на интерфейсах
interface *interface-id*	идентификатор интерфейса (Ethernet, Port-channel)

Указания по применению:

Используйте команду «**show ip device tracking**» для вывода таблиц хостов, обнаруженных на интерфейсах.

Примеры команды:

Следующий пример показывает, как вывести настройки обнаружения и сводную информацию о хостах, обнаруженных на интерфейсах:

```
admin@Switch# show ip device tracking all count
Probe Count:       3
Probe Interval:    30

Interface          Count
---------          -----
gi0/1              4
gi0/2              0
gi0/3              1
gi0/4              2
```

Следующий пример показывает, как вывести информацию о хостах, обнаруженных на интерфейсе gigabitethernet 0/1:

```
admin@Switch# show ip device tracking interface gigabitethernet 0/1

Entry 1:
  IP: 10.0.0.11
  MAC: 00:1B:28:BE:EF:01

Entry 2:
  IP: 10.0.0.12
  MAC: 00:1B:28:BE:EF:02
```

7 Функции VLAN

7.1 Настройка VLAN

7.1.1 Общие положения

Коммутатор обеспечивает широкие возможности по настройке параметров VLAN (Virtual Local Area Network). Коммутатор поддерживает настройку всего диапазона VLAN (1–4094).

Переход в режим настройки интерфейса VLAN осуществляется с помощью команды «**interface vlan**».

Добавление VLAN в таблицу VLAN и переход в режим настройки VLAN осуществляется с помощью команды глобальной настройки «**vlan**».

В коммутаторе реализовано три режима работы VLAN для интерфейсов Ethernet: «access», «trunk» и «customer». Установка режима интерфейса осуществляется с помощью команды «**switchport mode**». Отличия режимов VLAN:

1. В режиме «access» интерфейс Ethernet принимает и передает пакеты без тега. На интерфейс коммутируются только пакеты с номером тега access-VLAN интерфейса Ethernet.
2. В режиме «trunk» интерфейс принимает и передает пакеты с тегом VLAN. Все входящие пакеты без тега маркируются тегом native-VLAN интерфейса Ethernet. Из исходящих пакетов производится удаление тега, если пакет содержит тег VLAN, равный тегу native-VLAN интерфейса Ethernet.
3. В режиме «customer» интерфейс Ethernet всегда добавляет тег в отправляемые пакеты и удаляет тег из принимаемых пакетов. На интерфейс коммутируются только пакеты с номером тега customer-VLAN интерфейса Ethernet. Тип протокола в добавляемом теге – 0x8100.

Установка uplink-порта для интерфейса осуществляется с помощью команды «**switchport protected**».

Коммутатор позволяет настроить режим «защищенного» (protected) интерфейса. Трафик от одного «защищенного» интерфейса не может попасть в другой «защищенный» интерфейс. Включение режима защищенного интерфейса осуществляется с помощью команды «**switchport protected-port**».

В целях упрощения настройки VLAN в сложных сетях рекомендуется включить протокол GVRP на коммутаторе. Протокол GVRP работает только на портах в режиме «trunk».

Отключение передачи трафика в указанном VLAN осуществляется с помощью команды «**shutdown vlan**».

Вывод информации о VLAN, настроенных на коммутаторе, осуществляется с помощью команды «**show vlan**».

7.1.2 interface vlan

Команда глобальной настройки. Переход в режим настройки интерфейса VLAN.

Синтаксис команды:

interface vlan *vlan-id*

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Использование команды:

Команда «**interface vlan**» используется для перехода в режим настройки интерфейса VLAN.

Интерфейс VLAN предоставляет возможность управления устройством, а также отвечает за работу функций L3.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)#
```

7.1.3 switchport access

Команда настройки интерфейса. Установка номера access-VLAN для интерфейса в режиме «access».

Синтаксис команды:

switchport access vlan *vlan-id*

no switchport access vlan

Команда с приставкой «**no**» устанавливает значение 1.

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# switchport access vlan 2
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

7.1.4 switchport customer

Команда настройки интерфейса. Установка номера VLAN для туннелирования интерфейса в режиме «customer».

Синтаксис команды:

switchport customer vlan *vlan-id*

no switchport customer vlan

Команда с приставкой «**no**» устанавливает значение 1.

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# switchport customer vlan 2
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

7.1.5 switchport mode

Команда настройки интерфейса. Установка режима интерфейса.

Синтаксис команды:

switchport mode {access | customer | trunk}

no switchport mode

Команда с приставкой «**no**» устанавливает режим «access».

Параметры команды:

access режим «access». Интерфейс принимает и передает пакеты без тега 802.1Q

customer режим «customer». Интерфейс предназначен для туннелирования трафика пользователя. Трафик с тегами 802.1Q, принятый на порты «customer», передается через порты «trunk» с двойным тегом 802.1Q

trunk режим «trunk». Интерфейс принимает и передает пакеты с тегом и без тега 802.1Q. Пакеты без тега классифицируются как принадлежащие native-VLAN интерфейса

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# switchport mode trunk
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

7.1.6 switchport protected

Команда настройки интерфейса. Используется для ограничения передачи трафика между определёнными портами в одном VLAN. Настройка не зависит от режима «**switchport protected-port**».

Синтаксис команды:

switchport protected *interface-id*

no switchport protected

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

interface-id идентификатор интерфейса вида «gigabitethernet 0/1»

Значение по умолчанию:

Порты не ограничивают передачу трафика в одном VLAN.

Использование команды:

Команда «**switchport protected**» используется для ограничения передачи трафика между определёнными портами в одном VLAN. Интерфейс, настроенный как защищённый от указанного порта, не сможет обмениваться с ним трафиком.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport protected gigabitethernet 0/2
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

7.1.7 switchport protected-port

Команда настройки интерфейса. Включение режима защищенного порта. Защищенные порты не могут передавать трафик между собой, даже если находятся в одном VLAN.

Синтаксис команды:

switchport protected-port

no switchport protected-port

Команда с приставкой «**no**» отключает режим защищенного порта.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# switchport protected-port
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

7.1.8 switchport community

Команда настройки интерфейса. Добавление защищенного порта к сообществу.

Синтаксис команды:

switchport community *community*

no switchport community

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

community номер сообщества в диапазоне от 1 до 30

Пример команды:

```
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport community 1
```

7.1.9 switchport trunk native

Команда настройки интерфейса. Установка номера native-VLAN для интерфейса в режиме «trunk». Фреймы Ethernet без тега классифицируются как принадлежащие native-VLAN.

Синтаксис команды:

switchport trunk native vlan *vlan-id*

no switchport trunk native vlan

Команда с приставкой «**no**» устанавливает значение 1.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# switchport trunk native vlan 2
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

7.1.10 switchport trunk allowed

Команда настройки интерфейса (Ethernet). Настройка списка VLAN, которые интерфейс будет передавать и принимать в режиме «Trunk».

Синтаксис команды:

switchport trunk allowed vlan {add | remove} {*vlan-list* **| all}**

Параметры команды:

add	добавление VLAN к существующему списку
remove	удаление VLAN из существующего списка
vlan-list	список VLAN (через запятую), которые необходимо добавить или удалить. Для задания диапазонов можно использовать знак «-» (минус), например: «1-5,10,12-14»
all	добавление или удаление всех существующих VLAN на коммутаторе, кроме Native VLAN для порта

Значение по умолчанию:

По умолчанию порты в режиме «Trunk» передают и принимают только Native VLAN.

Использование команды:

Команда «**switchport trunk allowed vlan**» используется для настройки списка VLAN, которые интерфейс будет передавать и принимать в режиме «Trunk».

Native VLAN на интерфейсе не может быть удален с помощью команды «**switchport trunk allowed vlan**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport trunk allowed vlan add 10-20
admin@Switch(config-if)#
```

7.1.11 switchport general pvid

Команда настройки VLAN по умолчанию для режима «General».

Синтаксис команды:

switchport general pvid *vlan-id*

no switchport general pvid

Команда с приставкой «**no**» устанавливает значение 1.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport general pvid 20
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

7.1.12 switchport general allowed

Команда настройки интерфейса (Ethernet). Настройка списков VLAN, которые интерфейс будет передавать и принимать в режиме «General» (как тегированные, так и нетегированные).

Синтаксис команды:

switchport general allowed vlan {add | remove} {*vlan-id* | *vlan-range*} **{tagged | untagged}**

Параметры команды:

add	добавление VLAN к существующему списку
remove	удаление VLAN из существующего списка
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
vlan-range	списки VLAN (через запятую), которые необходимо добавить или удалить. Для задания диапазонов можно использовать знак «-» (минус), например: «1-5,10,12-14»
tagged	список тегированных VLAN
untagged	список нетегированных VLAN

Значение по умолчанию:

По умолчанию порты в режиме «General» передают и принимают только PVID VLAN.

Использование команды:

Команда «**switchport general allowed**» используется для настройки списка VLAN, которые интерфейс будет передавать и принимать в режиме «General».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport general allowed vlan add 10-20 untagged
admin@Switch(config-if)#
```

7.1.13 switchport general map

Команда настройки интерфейса. Команда привязывает созданную группу к конкретному нетегированному VLAN.

Синтаксис команды:

switchport general map {macs-group | subnets-group | protocols-group} *group-id* **vlan** *vlan-id*

no switchport general map {macs-group | subnets-group | protocols-group} *group-id* **vlan** *vlan-id*

Команда с приставкой «**no**» удаляет привязку группы.

Параметры команды:

macs-group	список групп привязок по MAC-адресу
subnets-group	список групп привязок по IP-адресу
protocols-group	список групп привязок по протоколу
group-id	номер группы в диапазоне от 1 до 65535
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Использование команды:

Команда привязывает созданную группу к конкретному нетегированному VLAN. Привязка происходит в зависимости от созданной группы и может быть трех видов:

- по MAC-адресу источника пакета;
- по IP-адресу источника пакета;
- по типу протокола (ICMP/TCP/UDP).

Ограничения команды:

- две привязки одного типа и одной группы не могут быть одновременно назначены на интерфейс.

Пример команды:

```
admin@Switch#configure terminal
admin@Switch(config)# interface gigabitethernet0/1
admin@Switch(config-if)# switchport mode general
admin@Switch(config-if)# switchport general allowed vlan add 20 untagged
admin@Switch(config-if)# switchport general map macs-group 3226 vlan 20
admin@Switch(config-if)#
```

7.1.14 vlan

Команда глобальной настройки. Добавление VLAN в таблицу VLAN и переход в режим настройки VLAN.

Синтаксис команды:

vlan {*vlan-id* | *vlan-list*}

no vlan

Команда с приставкой «**no**» удаляет VLAN.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
vlan-list	список VLAN, через запятую, которые необходимо добавить или удалить. Для указания диапазонов можно использовать знак “-” (минус), например: “1-5,10,12-14”

Значение по умолчанию:

Создан VLAN 1, членами которого являются все интерфейсы.

Использование команды:

Команда «**vlan**» используется для добавления VLAN в таблицу VLAN и перехода в режим настройки VLAN.

При добавлении VLAN автоматически получает имя вида “VLANxxxx”, где “xxxx” – идентификатор VLAN с ведущими нулями, например “VLAN0050”.

Если в качестве аргумента команды задан список VLAN, то команды режима настройки VLAN применяются к списку VLAN. Команда режима настройки VLAN «**name**» при этом становится недоступна (команда «**no name**» доступна).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# vlan 10-20
admin@Switch(config-vlan)#
```

7.1.15 name

Команда настройки VLAN. Установка имени VLAN.

Синтаксис команды:

name *name*

no name

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

name	уникальное имя VLAN в виде текстовой строки. Рекомендуемая длина: до 32 символов

Значение по умоланию:

Имя вида “VLANxxxx”, где “xxxx” – идентификатор VLAN с ведущими нулями, например “VLAN0050”.

Использование команды:

Команда «**name**» используется для установки имени VLAN.

Если в качестве аргумента команды «**vlan**» задан список VLAN, то команда режима настройки VLAN «**name**» становится недоступна (команда «**no name**» доступна).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# vlan 2
admin@Switch(config-vlan)# name DataVLAN
admin@Switch(config-vlan)#
```

7.1.16 state

Команда настройки VLAN. Установка режима приема и передачи трафика на VLAN.

Синтаксис команды:

state {suspend | active}

no state

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

suspend	отключение передачи и приема трафика на VLAN
active	включение передачи и приема трафика на VLAN

Значение по умолчанию:

Передача и прием трафика включены.

Использование команды:

Команда «**state**» используется для установки режима приема и передачи трафика на VLAN.

Отключение и включение приема и передачи трафика на VLAN можно настроить также с помощью команды глобальной настройки «**shutdown vlan**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# vlan 2
admin@Switch(config-vlan)# state suspend
admin@Switch(config-vlan)#
```

7.1.17 map

Команда глобальной настройки. Команда map обеспечивает привязку нетегированного трафика на входящем направлении general-порта к нумерованной группе.

Синтаксис команды:

map mac *mac-address prefix_length_mac* **macs-group** *group-id*

no map mac *mac-address prefix_length*

map subnet *ip-address prefix_length_ip* **subnets-group** *group-id*

no map subnet *ip-address prefix_length_ip*

map protocol {icmp | tcp | udp} protocols-group *group-id*

no map protocol {icmp | tcp | udp}

Команды с приставкой «**no**» удаляют существующую группу.

Параметры команды:

mac	привязка по MAC-адресу
mac-address	MAC-адрес
prefix_length_mac	длина префикса в диапазоне от 0 до 48
macs-group	список групп привязок по MAC-адресу
group-id	номер группы в диапазоне от 1 до 65535
subnet	привязка по IP-адресу
ip-address	IP-адрес хоста или подсети
prefix_length_ip	длина префикса (значение от 0 до 32)
subnets-group	список групп привязок по IP-адресу
protocol	привязка по протоколу
icmp	протокол icmp
tcp	протокол tcp
udp	протокол udp
protocols-group	список групп привязок по протоколу

Использование команды:

Команда map обеспечивает привязку нетегированного трафика на входящем направлении general-порта к нумерованной группе. Команда настраивает автоматическое назначение номера VLAN в зависимости от какого-либо из трех признаков:

- MAC-адрес источника пакета;
- IP-адрес источника пакета;
- тип протокола (ICMP/TCP/UDP).

Ограничения команды:

- один и тот же адрес (протокол) не может быть назначен разным группам.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# map subnet 190.10.10.1 24 subnets-group 1
admin@Switch(config)#
```

7.1.18 vlan dot1q tag native

Команда глобальной настройки. Включение режима тегирования пакетов native-VLAN для интерфейсов в режиме «trunk».

Синтаксис команды:
vlan dot1q tag native
no vlan dot1q tag native

Команда с приставкой «**no**» отключает режим тегирования пакетов native-VLAN для интерфейсов в режиме «trunk».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# vlan dot1q tag native
admin@Switch(config)# end
admin@Switch#
```

7.1.19 shutdown vlan

Команда глобальной настройки. Отключение передачи трафика в указанном VLAN. Указанный VLAN должен быть предварительно настроен на коммутаторе.

Синтаксис команды:
shutdown vlan *vlan-id*
no shutdown vlan *vlan-id*

Команда с приставкой «**no**» включает передачу трафика в указанном VLAN.

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# shutdown vlan 2
admin@Switch(config)# end
admin@Switch#
```

7.1.20 show interfaces protected

Команда доступна из любого режима. Вывод списка всех портов и отображение изолированных портов. Для изолированных портов отображается uplink-порт.

Синтаксис команды:
show interfaces protected [*interface-id*]
Параметры команды:

interface-id идентификатор интерфейса Ethernet

Пример команды:

```
admin@Switch# show interfaces protected gigabitethernet 0/1
Interface  State      Uplink port
---------  ---------  -----------
gi0/1      Protected  gi0/2
admin@Switch#
```

7.1.21 show interfaces protected-ports

Команда фундаментального режима. Вывод параметров защищенных портов.

Синтаксис команды:

show interfaces protected-ports [*interface-id***]**

Параметры команды:

interface-id идентификатор интерфейса

Пример команды:

```
admin@Switch# show interfaces protected-ports
Interface  State       Community
---------  ---------   ---------
gi0/1      Protected   1
gi0/2      Protected   Isolated
gi0/3      Unprotected 20
gi0/4      Unprotected Isolated
```

7.1.22 show interfaces switchport

Команда доступна из любого режима. Отображение информации о настроенных режимах на всех портах коммутатора.

Синтаксис команды:

show interfaces switchport

Пример команды:

```
admin@Switch# show interfaces switchport

Name: fa0/1
Status: not connected
Operational Mode: access
Access Mode VLAN: 1
Voice VLAN: none
Trunking Native Mode VLAN : 1
Trunking VLANs enabled: 1
Customer Mode VLAN: 1
VLAN Mappings: none
Private VLAN Lite State: disable
Private VLAN Lite Community: isolated
[output truncated]
```

7.1.23 show interfaces trunk vlan

Команда доступна из любого режима. Отображает порты, настроенные как trunk, пропускающие пакеты определенного VLAN.

Синтаксис команды:

show interfaces trunk vlan *vlan-id*

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# show interfaces trunk vlan 1

VLANs allowed on trunk
fa0/1 1-15

VLANs allowed and active in management domain
fa0/1 1

VLANs in spannig tree forwarding state
admin@Switch#
```

7.1.24 show interfaces vlan

Команда доступна из любого режима. Вывод информации о настройках интерфейсов VLAN.

Синтаксис команды:

show interfaces vlan *vlan-id*

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# show interfaces vlan
VLAN    IP address    Netmask         Type
----    ----------    -------------   ------
1       10.0.0.1      255.255.255.0   Static
2       192.168.20.1  255.255.255.0   DHCP
```

7.1.25 show vlan

Команда фундаментального режима. Вывод информации о VLAN, настроенных на коммутаторе.

Синтаксис команды:

show vlan [brief | dot1q tag native | id *vlan-id* **| name** *vlan-name***]**

Параметры команды:

brief вывод краткой информации обо всех VLAN (номера, имени, состояния и списка интерфейсов, являющихся членами VLAN)

dot1q tag native вывод настройки режима тегирования для VLAN доступа интерфейсов в режиме «trunk»

id *vlan-id* вывод информации для определенного VLAN по его номеру

name *vlan-name* вывод информации для определенного VLAN по его имени

Пример команды:

```
admin@Switch# show vlan
VLAN    Name    Type    State   Ports
----    ----    ------  ------  ---------------
1               static  active  gigabitethernet0/1
                                gigabitethernet0/2
                                gigabitethernet0/3
                                gigabitethernet0/4
                                gigabitethernet0/5
                                gigabitethernet0/6
                                gigabitethernet0/7
                                gigabitethernet0/8
                                gigabitethernet0/9
                                gigabitethernet0/10
                                tengigabitethernet0/1
                                tengigabitethernet0/2
                                tengigabitethernet0/3
<output truncated>
admin@Switch#
```

7.2 Настройка Voice VLAN

7.2.1 Общие положения

Voice VLAN – это VLAN, предназначенный для передачи голосового трафика (VoIP). Как правило, Voice VLAN применяется на портах доступа (“access”), к которым подключен IP-телефон и рабочая станция (ПК). Схема подключения имеет вид, приведенный на рисунке 4.

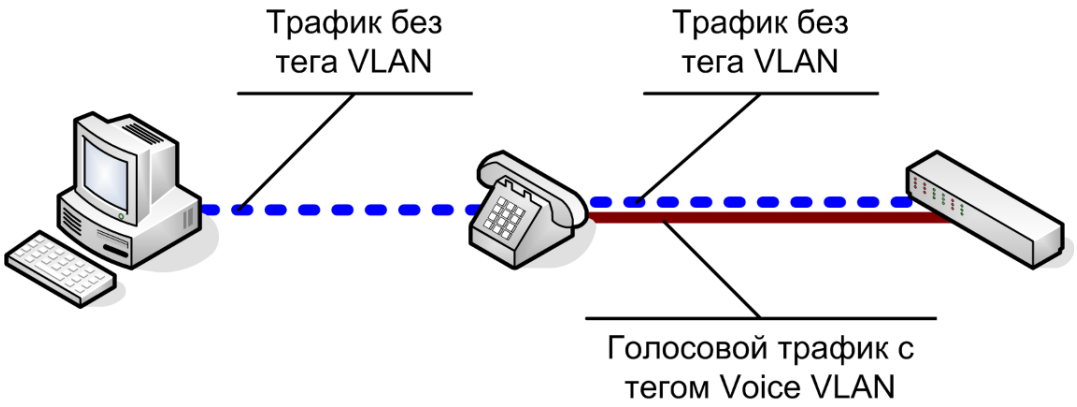

Рисунок 4 – Схема подключения IP-телефона и рабочей станции

Между рабочей станцией и IP-телефоном передается трафик без тегов VLAN. IP-телефон добавляет свой трафик с тегом Voice VLAN, который получает устройство. В обратном направлении телефон изымает трафик с тегом Voice VLAN.

Механизм Voice VLAN предназначен для упрощения настройки передачи голосового трафика при подключении IP-телефона и рабочей станции к одному порту устройства.

Для корректной работы Voice VLAN на порту устройства необходимо выполнение следующих условий:

- на устройстве должен быть включен QoS;
- Voice VLAN должен быть создан на устройстве;
- порт устройства должен быть в режиме “access”;
- на порту устройства должен быть включен LLDP и LLDP-MED;
- IP-телефон должен поддерживать протоколы LLDP и LLDP-MED.

Настройка Voice VLAN для каждого порта устройства является независимой, то есть, при необходимости, на каждом порту можно настроить свой номер Voice VLAN. Включение и отключение Voice VLAN на порту производится командой настройки интерфейса «**switchport voice vlan**».

Функция Voice VLAN работает только на портах в режиме “access”. Номер Voice VLAN не может быть равен номеру Access VLAN на порту.

Если в момент включения Voice VLAN порт не находится в режиме “access”, устройство временно отключает функцию Voice VLAN (см. “Oper status” в выводе команды «**show interfaces voice-vlan**»).

Аналогично, если функция Voice VLAN была включена на порту и порт перешел из режима “access” в другой режим, фунция Voice VLAN также временно отключается.

При включении Voice VLAN на порту коммутатор автоматически производит следующие настройки:

1. Добавляет две сетевые политики LLDP-MED для этого порта со следующими параметрами:

- Application: voice и voice-signaling;
- VLAN ID: равен номеру Voice VLAN, настроенному на порту;
- Layer 2 priority: 5;
- DSCP: 46;

2. Добавляет порт в Voice VLAN;
3. Устанавливает режим QoS “trust cos” на порту (аналогично команде настройки интерфейса «**mls qos trust cos**»).

При отключении Voice VLAN на порту устройство автоматически производит следующие настройки:

1. Удаляет сетевые политики LLDP-MED, созданные функцией Voice VLAN;
2. Удаляет порт из Voice VLAN.

Устройство поддерживает механизм обнаружения IP-телефона по протоколу LLDP. Эта функция предназначена для исключения возможности использования высокого приоритета при прямом подключении рабочей станции к устройству в обход IP-телефона. Механизм обнаружения IP-телефона включается командой «**mls qos trust device ip-phone**».

При включении проверки устройство автоматически устанавливает текущее значение параметра QoS “trust” на порту в режим “no trust”, пока на порту не будет обнаружен IP-телефон (аналогично команде настройки интерфейса «**no mls qos trust**»). После успешного обнаружения IP-телефона, устройство автоматически устанавливает параметр QoS “trust” на порту в соответствии с настройкой, заданной командой «**mls qos trust**».

Настройки пользователя

1. Настройка на интерфейсе номера Voice VLAN: целое число;
2. Включение режима доверия приоритету трафика от IP-телефона: включен, отключен.

Дополнения и ограничения

Voice VLAN поддерживается только на портах в режиме “access”. При настройке другого режима порта Voice VLAN автоматически отключается.

Сетевые политики, добавляемые устройством автоматически при включении Voice VLAN на порту, не отображаются в конфигурации устройства.

Настройка режима QoS “trust” на порту при отключении Voice VLAN не изменяется.

7.2.2 mls qos trust device ip-phone

Команда настройки интерфейса (Ethernet). Включение проверки подключения IP-телефона на порту.

Синтаксис команды:

mls qos trust device ip-phone

no mls qos trust device ip-phone

Команда с приставкой «**no**» отключает проверку.

Значение по умолчанию:

Проверка подключения IP-телефона отключена.

Использование команды:

Команда «**mls qos trust device ip-phone**» используется для включения проверки подключения IP-телефона на порту.

При включении проверки устройство автоматически устанавливает текущее значение параметра QoS “trust” на порту в режим “no trust”, пока на порту не будет обнаружен IP-телефон. Для корректной работы функции необходимо, чтобы на порту был включен протокол LLDP и LLDP-MED, так как обнаружение IP-телефона производится по протоколу LLDP.

После успешного обнаружения IP-телефона устройство автоматически устанавливает параметр QoS “trust” на порту в соответствии с настройкой, заданной командой «**mls qos trust**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# mls qos trust device ip-phone
admin@Switch(config-if)#
```

7.2.3 switchport voice vlan

Команда настройки интерфейса (Ethernet). Настройка номера VLAN, используемого для передачи голосового трафика, и включение функции Voice VLAN.

Синтаксис команды:

switchport voice vlan *vlan-id* **[cos** *cos-value***] [dscp** *dscp-value***]**

no switchport voice vlan

Команда с приставкой «**no**» используется для отключения функции.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
cos-value	приоритет CoS в диапазоне от 0 до 7. По умолчанию приоритет равен 5
dscp-value	приоритет DSCP в диапазоне от 0 до 63. По умолчанию приоритет равен 46

Значение по умолчанию:

Функция Voice VLAN отключена.

Использование команды:

Команда «**switchport voice vlan**» используется для настройки номера VLAN, используемого для передачи голосового трафика и включения функции Voice VLAN.

Функция Voice VLAN работает только на портах в режиме “access”. Номер Voice VLAN не может быть равен номеру Access VLAN на порту. Если в момент включения Voice VLAN порт не находится в режиме “access”, устройство временно отключает функцию Voice VLAN (см. “Oper status” в выводе команды «**show interfaces voice-vlan**»). Аналогично, если функция Voice VLAN была включена на порту и порт перешел из режима “access” в другой режим, фунция Voice VLAN также временно отключается.

Необязательные параметры «*cos-value*» и «*dscp-value*» используются для переопределения параметров приоритизации Voice VLAN, если значения по умолчанию не совпадают с корпоративными стандартами.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport voice vlan 10
admin@Switch(config-if)#
```

7.2.4 show interfaces voice-vlan

Команда фундаментального режима. Вывод настроек Voice VLAN.

Синтаксис команды:

show interfaces voice-vlan

Пример команды:

```
admin@Switch# show interfaces voice-vlan
tengigabitethernet0/1 Voice VLAN:
Configuration:
VLAN: 2
CoS priority: 5
DSCP priority: 46
Trust IP-phone: disabled
State:
Oper status: enabled
IP-phone detected: no
Trust state:
tengigabitethernet0/2 Voice VLAN: not configured
tengigabitethernet0/3 Voice VLAN: not configured
tengigabitethernet0/4 Voice VLAN: not configured
```

7.3 Настройка GVRP

7.3.1 Общие положения

В целях упрощения настройки VLAN в сложных сетях коммутатор поддерживает протокол GVRP.

GVRP (GARP VLAN Registration Protocol) – сетевой протокол канального уровня модели OSI, позволяющий устройству локальной сети сообщить смежным устройствам о своих активных VLAN. Использование протокола GVRP позволяет избежать перенастройки оборудования каждый раз при изменении VLAN в сети.

Протокол GVRP работает только на интерфейсах в режиме «trunk».

Коммутатор поддерживает следующие настройки GVRP:

1. Настройка режима работы GVRP: включено, отключено. Режим работы GVRP настраивается с помощью команды «**gvrp global**».
2. Установка таймеров для протокола GVRP. Установка таймеров осуществляется с помощью команды «**gvrp timer**». Коммутатор поддерживает настройку следующих таймеров:
   - таймер GVRP Join – определяет интервал отправки сообщений об активных VLAN на коммутаторе, в диапазоне от 200 до 2147483647 миллисекунд;
   - таймер GVRP Leave – определяет интервал удаления записей о динамических VLAN, для которых не получены сообщения, в диапазоне от 600 до 2147483647 миллисекунд;
   - таймер GVRP LeaveAll – предназначен для удаления избыточных записей о динамических VLAN, которые возникают при потерях и дублировании сообщений, в диапазоне от 10000 до 2147483647 миллисекунд.
3. Настройка режима создания динамических VLAN: включено, отключено. Включение режима создания динамических VLAN осуществляется с помощью команды «**gvrp vlan create**».

Вывод информации о состоянии GVRP на всех интерфейсах осуществляется с помощью команды «**show gvrp interface**».

Отображение настроек GVRP осуществляется с помощью команды «**show gvrp summary**».

7.3.2 gvrp global

Команда глобальной настройки. Включение протокола GVRP на всех интерфейсах в режиме «trunk».

Синтаксис команды:
gvrp global
no gvrp global
Команда «**no gvrp global**» отключает протокол GVRP на всех интерфейсах в режиме «trunk».
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# gvrp global
admin@Switch(config)# end
admin@Switch#
```

7.3.3 gvrp timer

Команда глобальной настройки. Установка таймеров для протокола GVRP.
Синтаксис команды:
gvrp timer {join | leave | leaveall} *timer*
no gvrp timer {join | leave | leaveall}
Команда с приставкой «**no**» устанавливает значения по умолчанию для таймеров.
Параметры команды:

join *timer* — установка значения таймера GVRP Join в диапазоне от 200 до 2147483647 миллисекунд. Таймер GVRP Join определяет интервал отправки сообщений об активных VLAN на коммутаторе

leave *timer* — установка значения таймера GVRP Leave в диапазоне от 600 до 2147483647 миллисекунд. Таймер GVRP Leave определяет интервал удаления записей о динамических VLAN, для которых не получены сообщения

leaveall *timer* — установка значения таймера GVRP LeaveAll в диапазоне от 10000 до 2147483647 миллисекунд. Таймер GVRP LeaveAll предназначен для удаления избыточных записей о динамических VLAN, которые возникают при потерях и дублировании сообщений

Значение по умолчанию:
Параметр «**join** *timer*» равен 200.
Параметр «**leave** *timer*» равен 600.
Параметр «**leaveall** *timer*» равен 10000.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# gvrp timer join 300
admin@Switch(config)# end
admin@Switch#
```

7.3.4 gvrp vlan create

Команда глобальной настройки. Включение режима создания динамических VLAN на интерфейсах в режиме «trunk».

Синтаксис команды:

gvrp vlan create

no gvrp vlan create

Команда с приставкой «**no**» отключает создание динамических VLAN на интерфейсах в режиме «trunk».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# gvrp vlan create
admin@Switch(config)# end
admin@Switch#
```

7.3.5 show gvrp interface

Команда фундаментального режима. Вывод информации о состоянии GVRP на всех интерфейсах в режиме «trunk» (включая список добавленных и анонсированных VLAN).

Синтаксис команды:

show gvrp interface

Пример команды:

```
admin@Switch# show gvrp interface
Port    Vlans declared
fa0/1   1,1200,4000,4094
gi0/2   1,1200,4000,4094
gi0/3   1,1200,4000,4094

Port    Vlans discovered
fa0/1   5,10,2000,3400
gi0/2   5,10,2000,3400
gi0/3   5,10,2000,3400

Port    Vlans registered
fa0/1   5,10,2000,3400
gi0/2   5,10,2000,3400
gi0/3   5,10,2000,3400
admin@Switch#
```

7.3.6 show gvrp summary

Команда фундаментального режима. Отображение настроек GVRP.

Синтаксис команды:

show gvrp summary

Пример команды:

```
admin@Switch# show gvrp summary
GVRP feature is currently disabled on the switch.
GVRP dynamic VLAN creation is disabled.
GVRP timers (milliseconds)
join = 200
leave = 600
leave-all = 10000
admin@Switch#
```

7.4 Настройка Selective Q-in-Q

7.4.1 Общие положения

При использовании двойного тегирования (Q-in-Q) VLAN внешнего тега называется S-VLAN (Service VLAN), а VLAN внутреннего тега называется C-VLAN (Customer VLAN).

VLAN translation подразумевает замену тега VLAN во входящем пакете и в исходящем пакете по заданным правилам. Трансляция VLAN необходима в следующих случаях:

1. При сопряжении двух сетей, использующих разные номера VLAN для передачи одного и того же трафика. В этом случае используется схема трансляции 1:1, то есть, например, VLAN 10 транслируется во VLAN 20 во входящем направлении порта, а в исходящем направлении происходит обратная трансляция.
2. Для упрощения настройки клиентского оборудования. В этом случае используется схема трансляции 1:N, то есть все клиенты используют один и тот же номер VLAN для передачи некоторого типа трафика, который преобразуется в номер VLAN, соответствующий номеру клиента. Пример: клиенты 1 и 2 используют VLAN 10 для доступа в Интернет, при этом коммутатор транслирует VLAN 10 во VLAN 100 для первого клиента и VLAN 10 во VLAN 101 для второго клиента. На исходящем направлении происходит обратное преобразование.

7.4.2 vlan mapping

Команда глобальной настройки. Настройка режима отображения VLAN.

Синтаксис команды:

vlan mapping { translate | dot1q-tunnel }

no vlan mapping

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

translate	устанавливает режим трансляции VLAN. Правила отображения замещают тег 802.1q на входящем и исходящем направлениях
dot1q-tunnel	устанавливает режим добавления и удаления тегов 802.1q (VLAN). Правила отображения добавляют новый тег 802.1q на входящем направлении и удаляют тег 802.1q на исходящем направлении

Значение по умолчанию:

По умолчанию установлен режим «translate».

Использование команды:

Команда «**vlan mapping**» используется для настройки режима отображения VLAN. Режим отображения определяет поведение всех правил на портах. При смене режима отображения VLAN, все существующие правила перезаписываются в памяти TCAM.

Режимы отображения оказывают следующее влияние на входящий трафик:

- в режиме «translate» все исходящие пакеты Q-in-Q, у которых значение VLAN во внутреннем теге 802.1q равно нулю, преобразуются в пакеты с одним тегом 802.1q (внутренний тег удаляется);
- в режиме «translate» все исходящие пакеты с одним тегом 802.1q преобразуются в пакеты Q-in-Q, у которых VLAN во внутреннем теге 802.1q равен нулю.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# vlan mapping translate
admin@Switch(config)# exit
admin@Switch#
```

7.4.3 switchport vlan mapping

Команда настройки интерфейса (Ethernet). Настройка правил отображения VLAN на интерфейсе.

Синтаксис команды:

switchport vlan mapping *vlan-id translated-id*
no switchport vlan mapping *vlan-id translated-id*
switchport vlan mapping default { *translated-id* **| drop }**
no switchport vlan mapping default { *translated-id* **| drop }**
no switchport vlan mapping all

Команда «**no switchport vlan mapping all**» используется для удаления всех правил на интерфейсе.

Параметры команды:

vlan-id	номер пользовательского VLAN
translated-id	номер VLAN провайдера (внешний или транслированный номер VLAN). Номер VLAN должен быть уникален для каждого правила
default	указывает правило для всех VLAN, которые не соответствуют остальным правилам. По умолчанию правило отсутствует
drop	включает удаление пакетов

Значение по умолчанию:

По умолчанию правила отображения VLAN на интерфейсе отсутствуют.

Использование команды:

Команда «**switchport vlan mapping**» используется для настройки правил отображения VLAN на интерфейсе.

Режим трансляции или добавления внешнего тега VLAN определяется командой глобальной настройки «**vlan mapping**».

В режиме трансляции VLAN (команда «**vlan mapping translate**») каждое правило должно иметь уникальные номера исходного и транслированного VLAN («*vlan-id*» и «*translated-id*») в пределах интерфейса.

В режиме добавления тега VLAN (команда «**vlan mapping dot1q-tunnel**») каждое правило должно иметь уникальный номер исходного VLAN («*vlan-id*») в пределах настроек интерфейса.

При вводе команды «**switchport vlan mapping**» с номером «*vlan-id*», для которого уже есть правило, происходит замена существующего правила.

При вводе команды «**switchport vlan mapping default**» всегда заменяется предыдущее правило, введенное командой «**switchport vlan mapping default**».

Будьте осторожны при создании правила «**switchport vlan mapping default**» с указанием номера VLAN в глобальном режиме «translate», т.к. обратное преобразование невозможно.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# vlan mapping translate
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport vlan mapping 2 3
admin@Switch(config-if)#
```

```
admin@Switch# configure terminal
admin@Switch(config)# vlan mapping dot1q-tunnel
admin@Switch(config)# interface gigabitethernet 0/2
admin@Switch(config-if)# switchport vlan mapping 2 3
admin@Switch(config-if)#
```

```
admin@Switch# configure terminal
admin@Switch(config)# vlan mapping dot1q-tunnel
admin@Switch(config)# interface gigabitethernet 0/2
admin@Switch(config-if)# switchport vlan mapping default 10
admin@Switch(config-if)#
```

7.4.4 switchport trunk allowed

Команда настройки интерфейса (Ethernet). Настройка списка VLAN, которые интерфейс будет передавать и принимать в режиме «Trunk».

Синтаксис команды:

switchport trunk allowed vlan { add | remove } { *vlan-list* **| all }**

Параметры команды:

add	добавление VLAN к существующему списку
remove	удаление VLAN из существующего списка

vlan-list	список VLAN (через запятую), которые необходимо добавить или удалить. Для задания диапазонов можно использовать знак «-» (минус), например: «1–5,10,12–14»
all	добавление или удаление всех VLAN, существующих на коммутаторе, кроме Native VLAN для порта

Значение по умолчанию:

По умолчанию порты в режиме «Trunk» передают и принимают только Native VLAN.

Использование команды:

Команда «**switchport trunk allowed vlan**» используется для настройки списка VLAN, которые интерфейс будет передавать и принимать в режиме «Trunk».

Native VLAN на интерфейсе не может быть удален с помощью команды «**switchport trunk allowed vlan**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport trunk allowed vlan add 10-20
admin@Switch(config-if)#
```

7.4.5 show interfaces vlan mapping

Команда, доступная из любого режима. Вывод правил отображения пользовательких VLAN и провайдерских VLAN.

Синтаксис команды:

show interfaces *interface-id* **vlan mapping**

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show interfaces vlan mapping**» используется для вывода правил отображения пользовательких VLAN и провайдерских VLAN.

Пример команды:

```
admin@Switch# show interfaces gigabitethernet 0/1 vlan mapping
VLAN translation mode: Translate

Original VLAN   Translated VLAN
-------------   ---------------
10              100
20              200
admin@Switch#
```

8 QoS

8.1 Настройка качества обслуживания QoS

8.1.1 Общие положения

Качество обслуживания (Quality of Service) определяет резервирование ресурсов сети для различных видов трафика. Качество связи определяется следующими параметрами:

- полоса пропускания (bandwidth), характеризующая пропускную способность среды передачи информации;
- задержка при передаче пакета (delay), измеряющаяся в миллисекундах;
- колебания задержки при передаче пакетов – джиттер (jitter);
- потеря пакетов (packet loss), характеризующаяся количеством пакетов, потерянных в сети во время передачи.

Коммутатор поддерживает следующие настройки QoS:

- преобразование приоритетов между CoS и внутренними приоритетами;
- преобразование приоритетов между DSCP и внутренними приоритетами;
- включение или отключение классификации приоритета пакетов по CoS и DSCP для каждого интерфейса в отдельности.

Коммутатор поддерживает восемь уровней внутренних приоритетов от 0 до 7 (0 – наименьший приоритет, 7 – наибольший приоритет). Разделение полосы пропускания между пакетами с различными приоритетом производится по схеме 8-7-6-5-4-3-2-1, то есть для трафика с приоритетом 0 выделяется одна условная единица полосы пропускания, а для трафика с приоритетом 7 – 8 условных единиц полосы пропускания.

Установка режима поддержки QoS производится с помощью команды «**mls qos**».

Установка правил преобразований между CoS (802.1p), DSCP (IP) и внутренними приоритетами очередей передачи (Prio) осуществляется с помощью команды «**mls qos map**».

Установка режима классификации приоритета пакетов по параметрам CoS (802.1p) и DSCP (IP) осуществляется с помощью команды «**mls qos trust**».

Установка количества очередей, которые обслуживаются по приоритету (SPQ), осуществляется с помощью команды «**priorityqueue out num-of-queues**».

Установка весов для 8 очередей осуществляется с помощью команды «**wrr-queue bandwidth**».

Вывод глобальных настроек QoS осуществляется с помощью команды «**show mls qos**».

Вывод настроек QoS для интерфейсов Ethernet осуществляется с помощью команды «**show mls qos interface**».

Вывод таблиц преобразований CoS – Prio, DSCP – Prio осуществляется с помощью команды «**show mls qos maps**».

8.1.2 mls qos

Команда глобальной настройки. Включение поддержки QoS на всех интерфейсах коммутатора.

Синтаксис команды:

mls qos

no mls qos

Команда «**no mls qos**» отключает поддержку QoS на всех интерфейсах коммутатора.

Значение по умолчанию:

По умолчанию поддержка QoS включена на всех интерфейсах.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mls qos
admin@Switch(config)# end
admin@Switch#
```

8.1.3 mls qos map

Команда глобальной настройки. Установка правил преобразований между CoS (802.1p), DSCP (IP) и внутренними приоритетами очередей передачи (Prio).

Синтаксис команды:

mls qos map {cos-prio *prio1...prio8* **| dscp-prio** *dscp-list* **to** *prio***}**

no mls qos map {cos-prio | dscp-prio}

Команда с приставкой «**no**» устанавливает значения по умолчанию, приведенные в Приложении А.

Параметры команды:

cos-prio	установка правила преобразования для CoS – Prio
prio1...prio8	указывается 8 значений Prio в диапазоне от 0 до 7 для всех значений CoS
dscp-prio *dscp-list*	установка правила преобразования для DSCP – Prio
to *prio*	указанным значениям DSCP ставится в соответствие значение Prio. Диапазон значений DSCP – от 0x00 до 0x3F. Диапазон значений Prio – от 0 до 7

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mls qos map cos-prio 0 1 2 3 4 5 6 7
admin@Switch(config)# end
admin@Switch#
```

8.1.4 mls qos trust

Команда настройки интерфейса. Установка режимов классификации приоритета пакетов по параметрам CoS (802.1p) и DSCP (IP).

Синтаксис команды:

mls qos trust [**cos | dscp | device** {*ip-phone*}]

no mls qos trust [cos | dscp]

Команда без параметров включает классификацию приоритета пакетов по параметрам CoS и DSCP.

Команда с приставкой «**no**» отключает классификацию приоритета пакетов по параметрам CoS и DSCP.

Параметры команды:

cos	установка режима классификации для CoS
dscp	установка режима классификации для DSCP
device	настройка QoS для оборудования
ip-phone	выставляет наибольший приоритет на интерфейсе для пакетов IP-телефонии

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# mls qos trust
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

8.1.5 priority-queue out num-of-queues

Команда глобальной настройки. Установка количества очередей, которые обслуживаются по приоритету (SPQ).

Синтаксис команды:

priority-queue out num-of-queues *number-of-queues*

no priority-queue out num-of-queues

Команда с приставкой «**no**» устанавливает значение по умолчанию «8».

Параметры команды:

number-of-queues	количество очередей, которые обслуживаются по приоритету (SPQ), в диапазоне от 0 до 8

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# priority-queue out num-of-queues 8
admin@Switch(config)# end
admin@Switch#
```

8.1.6 traffic-shape

Команда настройки интерфейса (Ethernet). Установка ограничения исходящего трафика на интерфейсе.

Синтаксис команды:

traffic-shape *committed-rate* **[***committed-burst***]**

no traffic-shape

Команда с приставкой «**no**» отключает ограничение исходящего трафика на интерфейсе.

Параметры команды:

committed-rate	средняя скорость трафика (CIR) в диапазоне от 1 Мбит/с до максимальной скорости порта (в Мбит/с)
committed-burst	превышенный размер блока (CBS) в диапазоне от 4096 до 16762902 байт. Значение настройки округляется до ближайшего целого числа, кратного 4096. По умолчанию равен 16384

Значение по умолчанию:

Ограничение исходящего трафика отключено.

Использование команды:

Команда «**traffic-shape**» используется для установки ограничения исходящего трафика на интерфейсе.

Команда «**traffic-shape**» заменяет команду «**queue bandwidth limit**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# traffic-shape 100
admin@Switch(config-if)#
```

8.1.7 traffic-shape queue

Команда настройки интерфейса (Ethernet). Установка ограничения исходящего трафика на очереди передачи интерфейса.

Синтаксис команды:

traffic-shape queue *queue-id committed-rate* **[***committed-burst***]**

no traffic-shape queue *queue-id*

Команда с приставкой «**no**» отключает ограничения исходящего трафика на очереди передачи интерфейса.

Параметры команды:

queue-id	номер очереди передачи в диапазоне от 1 до 8
committed-rate	средняя скорость трафика (CIR) в диапазоне от 1 Мбит/с до максимальной скорости порта (в Мбит/с)
committed-burst	превышенный размер блока (CBS) в диапазоне от 4096 до 16762902 байт. Значение настройки округляется до ближайшего целого числа, кратного 4096. По умолчанию равен 16384

Значение по умолчанию:

Ограничение исходящего трафика отключено.

Использование команды:

Команда «**traffic-shape queue**» используется для установки ограничения исходящего трафика на очереди передачи интерфейса.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# traffic-shape queue 1 500
admin@Switch(config-if)#
```

8.1.8 qos wrr-queue wrtd

Команда глобальной настройки. Включение механизма защиты от перегрузок очередей Random Tail Drop.

Синтаксис команды:

qos wrr-queue wrtd

no qos wrr-queue wrtd

Команда с приставкой «**no**» отключает механизм защиты от перегрузок очередей Random Tail Drop.

Значение по умолчанию:

Random Tail Drop отключен.

Использование команды:

Команда «**qos wrr-queue wrtd**» используется для включения механизма защиты от перегрузок очередей Random Tail Drop.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# qos wrr-queue wrtd
admin@Switch(config)#
```

8.1.9 wrr-queue bandwidth

Команда глобальной настройки. Установка весов для 8 очередей.

Синтаксис команды:

wrr-queue bandwidth *weight1 weight2 ... weight_n*

no wrr-queue bandwidth

Команда с приставкой «**no**» устанавливает значения весов по умолчанию: 1, 2, 4, 8, 16, 32, 64, 128.

Параметры команды:

weight1 weight2 ... weight_n значения весов в диапазоне от 0 до 255

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# wrr-queue bandwidth 1, 2, 4, 8, 16, 32, 64, 128
admin@Switch(config)# end
admin@Switch#
```

8.1.10 show mls qos

Команда фундаментального режима. Вывод глобальных настроек QoS.

Синтаксис команды:

show mls qos

Пример команды:

```
admin@Switch# show mls qos

QoS is enabled
Number of expedite queues: 8
WRR bandwidth weights: 1 2 4 8 16 32 64 128

admin@Switch#
```

8.1.11 show mls qos interface

Команда фундаментального режима. Вывод настроек QoS для интерфейсов Ethernet.

Синтаксис команды:

show mls qos interface [*interface-id*]

Команда без параметров выводит настройки QoS для всех интерфейсов.

Параметры команды:

interface-id идентификатор интерфейса

Пример команды:

```
admin@Switch# show mls qos interface gigabitethernet 1/1
gigabitethernet 1/1
Trust CoS: not trusted
Trust DSCP: not trusted
admin@Switch#
```

8.1.12 show mls qos maps

Команда фундаментального режима. Вывод таблиц преобразований CoS – Prio, DSCP – Prio.

Синтаксис команды:

show mls qos maps [cos-prio | dscp-prio]

Команда без параметров выводит все таблицы преобразований.

Параметры команды:

cos-prio вывод таблицы преобразований из CoS во внутренние приоритеты

dscp-prio вывод таблицы преобразований из DSCP во внутренние приоритеты

Пример команды:

```
admin@Switch# show mls qos maps
CoS-Prio map:
CoS: 0 1 2 3 4 5 6 7
--------------------
Prio: 1 0 2 3 4 5 6 7

DSCP-Prio map:
D1:D2 0 1 2 3 4 5 6 7 8 9
-----------------------
0: 0 0 0 0 0 0 0 0 1 1
1: 1 1 1 1 1 1 2 2 2 2
2: 2 2 2 2 3 3 3 3 3 3
3: 3 3 4 4 4 4 4 4 4 4
4: 5 5 5 5 5 5 5 5 6 6
5: 6 6 6 6 6 6 7 7 7 7
6: 7 7 7 7
admin@Switch#
```

9 ACL

9.1 Настройка списков контроля доступа (ACL)

9.1.1 Общие положения

Списки контроля доступа (ACL) предназначены для ограничения приема/передачи трафика и его перемаркировки на отдельных портах устройства. Также ACL может альтернативно называться как PCL – Policy Control List.

ACL содержит множество правил классификации и действий, выполняемых при совпадении правила.

Каждое правило классификации и его действие называются элементом контроля доступа (Access Control Element, ACE). Один ACL может содержать более одного ACE. Порядок расположения правил в ACL имеет значение, так как правила применяются по порядку.

Проверка соответствия пакета ACL выполняется по следующему алгоритму:

- если пакет соответствует правилу, то применяется действие правила и обработка ACL останавливается;
- иначе обработка ACL продолжается со следующего правила;
- если в ACL не найдено ни одного правила, соответствующего пакету, обработка продолжается со следующего ACL (при наличии);
- если ни в одном ACL не найдено подходящего правила, то применяется правило по умолчанию. Правило по умолчанию может быть настроено пользователем: передать или отбросить пакет.

Устройство поддерживает следующие типы ACL:

1. MAC ACL – классификация пакета на основе полей L2.
2. IP ACL – применяется только к пакетам IPv4. Классификация на основе полей L3/L4.
3. IPv6 ACL – применяется только к пакетам IPv6. Классификация на основе полей L3/L4.

ACL можно назначать как на входящее направление, так и на исходящее направление интерфейсов Ethernet. ACL можно назначать только на входящее направление интерфейсов VLAN.

Устройство поддерживает одновременную установку одного MAC ACL и одного IP/IPv6 ACL на интерфейс. Устройство не поддерживает одновременную установку двух правил одного типа на интерфейс, так как они используют общую аппаратную таблицу (TCAM).

Администратор может настраивать приоритеты правил ACL (ACE), для настройки порядка применения правил в ACL.

Классификация MAC ACL поддерживает следующие параметры:

- MAC-адрес источника с обратной маской (wildcard);
- MAC-адрес назначения с обратной маской (wildcard);
- номер VLAN;
- приоритет IEEE 802.1p (user priority);
- тип протокола Ethernet.

Классификация IP ACL поддерживает следующие параметры:

1. Общие параметры:

- тип протокола IP;
- IP-адрес источника с обратной маской (wildcard);
- IP-адрес назначения с обратной маской (wildcard);
- DSCP.

2. Параметры протоколов TCP и UDP:

- порт источника или диапазон портов;
- порт назначения или диапазон портов.

3. Параметры протокола ICMP:

- код ICMP;
- тип ICMP.

4. Параметры протокола IGMP:

- тип IGMP.

Классификация IPv6 ACL поддерживает следующие параметры:

1. Общие параметры:

- тип протокола IP;
- IP-адрес источника с обратной маской (wildcard);
- IP-адрес назначения с обратной маской (wildcard);
- DSCP.

2. Параметры протоколов TCP и UDP:

- порт источника или диапазон портов;
- порт назначения или диапазон портов.

3. Параметры протокола ICMPv6:

- код ICMPv6;
- тип ICMPv6.

Примечание – Классификация протокола IGMP в IPv6 ACL отсутствует, так как функционал IGMP в IPv6 является частью ICMPv6 (Multicast Listener Discovery).

Доступные типы действий правил ACL:

- передача пакета получателю (forward);
- отбрасывание пакета (drop);
- отбрасывание пакета и отключение порта.

Настройки пользователя

1. Глобальные настройки:

- создание и удаление MAC ACL;
- создание и удаление IPv4 ACL;
- создание и удаление IPv6 ACL.

2. Настройки интерфейсов:

- назначение ACL на интерфейс и удаление ACL с входящего направления интерфейса;
- назначение ACL на интерфейс и удаление ACL с исходящего направления интерфейса;
- назначение ACL на интерфейс и удаление ACL с входящего направления интерфейса VLAN.

3. Настройки MAC, IPv4 и IPv6 ACL:

- добавление и удаление разрешающих правил;
- добавление и удаление запрещающих правил.

Дополнения и ограничения

ACL используются в качестве одного из механизмов обеспечения безопасности.

Назначение ACL на интерфейс VLAN доступно только для входящего направления интерфейса.

Во всех ACL последним правилом является правило, назначенное пользователем:

- если пользователем назначен режим передачи по умолчанию при назначении ACL на интерфейс («**deny-any**», то «**permit any any any**»);

– иначе «**deny any any any**».

Перед правилом по умолчанию автоматически добавляются следующие правила:

1. Для MAC ACL: разрешение передачи ARP-пакетов.
2. Для IP ACL: нет.
3. Для IPv6 ACL: разрешение передачи пакетов ICMPv6 Neighbor Discovery (два правила).

Описание настройки

Порядок настройки ACL приведен в таблице 9.

Таблица 9 – Порядок настройки ACL

Шаг	Команда	Назначение
1	**configure terminal**	Переход в режим глобальной настройки
2	**ip access-list** *acl-name*	Добавление IPv4 ACL и переход в режим настройки правил IPv4 ACL
3	[*sequence-number*] **permit** ...	Добавление разрешающего правила в IPv4 ACL
4	[*sequence-number*] **deny** ...	Добавление запрещающего правила в IPv4 ACL
5	**exit**	Переход в предыдущий режим настройки
6	**ipv6 access-list** *acl-name*	Добавление IPv6 ACL и переход в режим настройки правил IPv6 ACL
7	[*sequence-number*] **permit** ...	Добавление разрешающего правила в IPv6 ACL
8	[*sequence-number*] **deny** ...	Добавление запрещающего правила в IPv6 ACL
9	**exit**	Переход в предыдущий режим настройки
10	**mac access-list** *acl-name*	Добавление MAC ACL и переход в режим настройки правил MAC ACL
11	[*sequence-number*] **permit** ...	Добавление разрешающего правила в MAC ACL
12	[*sequence-number*] **deny** ...	Добавление запрещающего правила в MAC ACL
13	**exit**	Переход в предыдущий режим настройки
14	**interface** *interface-id*	Переход в режим настройки интерфейса
15	**service-acl input** *acl-name1* [*acl-name2*] [**default-action** {**deny-any** | **permit-any**}]	Привязка ACL на входящее направление интерфейса

Продолжение таблицы 9

Шаг	Команда	Назначение
16	**service-acl output** *acl-name1* [*acl-name2*] [**default-action** {**deny-any** | **permit-any**}]	(Опционально) Привязка ACL на исходящее направление интерфейса. Как правило, ACL используются для фильтрации входящего трафика
17	**exit**	Переход в предыдущий режим настройки
18	**exit**	Переход в предыдущий режим настройки
19	**show access-lists** [*name*]	Проверка настроек ACL
20	**show interfaces access-lists** [*interface-id*]	Проверка настроек ACL на интерфейсах
21	**copy running-config startup-config**	Сохранение текущей конфигурации

Рассмотрим вариант настройки со следующими условиями:

- на входящее направление интерфейса gigabitethernet 0/1 необходимо добавить IPv4 ACL, который разрешает HTTP трафик (порт TCP 80) с IPv4-адреса 10.0.0.1/24;
- на входящее направление интерфейса gigabitethernet 0/1 необходимо добавить IPv6 ACL, который разрешает HTTP трафик (порт TCP 80) с IPv6-адреса 2001:000:CAFE:BABE::/64;
- на входящее направление интерфейса gigabitethernet 0/1 необходимо добавить MAC ACL, который запрещает трафик от хостов со старшими байтами MAC-адреса источника, равными “00:1B:28:00:00”, и разрешает весь остальной.

Создадим требуемые ACL:

```
admin@Switch# configure terminal
admin@Switch(config)# ip access-list server1
admin@Switch(config-ip-acl)# permit tcp 10.0.0.1 0.0.0.255 any any 80
admin@Switch(config-ip-acl)# exit
admin@Switch(config)# ipv6 access-list server2
admin@Switch(config-ipv6-acl)# permit tcp 2001:000:CAFE:BABE::/64 any any 80
admin@Switch(config-ipv6-acl)# exit
admin@Switch(config)# mac access-list server3
admin@Switch(config-mac-acl)# deny 00:1B:28:00:00:01 00:00:00:00:00:ff any
admin@Switch(config-mac-acl)# permit any any
admin@Switch(config-mac-acl)# exit
admin@Switch(config)#
```

Привяжем ACL к соответствующим им интерфейсам:

```
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# service-acl input server1
admin@Switch(config-if)# exit
admin@Switch(config)# interface gigabitethernet 0/2
admin@Switch(config-if)# service-acl input server2
admin@Switch(config-if)# exit
admin@Switch(config)# interface gigabitethernet 0/3
admin@Switch(config-if)# service-acl input server3
admin@Switch(config-if)# exit
admin@Switch(config)# exit
admin@Switch#
```

Проверим параметры и сохраним файл конфигурации:

```
admin@Switch# show access-lists

IP ACL   IPv6 ACL   MAC ACL   Total
------   --------   -------   -----
1         1          1         3

MAC access list server3
  10 deny 00:1B:28:00:00:01 00:00:00:00:00:FF any
  20 permit any any

IP access list server1
  10 permit tcp 10.0.0.1 0.0.0.255 any any 80

IPv6 access list server2
  10 permit tcp 2001:000:CAFE:BABE::/64 any any 80

admin@Switch(config)# show interfaces access-lists
Interface   Ingress ACLs   Egress ACLs
---------   ------------   -----------
gi0/1       server1, default: deny-any
gi0/2       server2, default: deny-any
gi0/3       server3, default: deny-any

admin@Switch# copy running-config startup-config
admin@Switch#
```

9.1.2 clear access-lists counters

Команда фундаментального режима. Очистка счетчиков статистики ACL.

Синтаксис команды:

clear access-lists counters [*interface-id* | **vlan** *vlan-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Использование команды:

Команда «**clear access-lists counters**» используется для очистки счетчиков статистики ACL.

Если команда введена без аргументов, то происходит очистка всех счетчиков статистики ACL.

Пример команды:

```
admin@Switch# clear access-lists counters vlan 1
admin@Switch#
```

9.1.3 access-list logging interval

Команда глобальной настройки. Установка минимального интервала между сообщениями, генерируемыми системой журналирования ACL.

Синтаксис команды:
access-list logging interval *interval*
no access-list logging interval
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

interval	минимальный интервал между сообщениями, генерируемыми системой журналирования ACL. Диапазон значений: от 100 до 2147483647 миллисекунд

Значение по умолчанию:
10000 миллисекунд (10 секунд).
Использование команды:
Команда «**access-list logging interval**» используется для установки минимального интервала между сообщениями, генерируемыми системой журналирования ACL.
Формат сообщений: %SEC-6-ACL_LOG: WHAT COUNT packets on IF via RULE, где:
“WHAT” – действие с пакетами: permitted или denied;
“COUNT” – количество пакетов;
“IF” – идентификатор интерфейса;
“RULE” – описание правила ACL, к которому относятся пакеты.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# access-list logging interval 20000
admin@Switch(config)#
```

9.1.4 ip access-list

Команда глобальной настройки. Добавление IPv4 ACL и переход в режим настройки правил IPv4 ACL.
Синтаксис команды:
ip access-list *acl-name*
no ip access-list *acl-name*
Команда с приставкой «**no**» удаляет IPv4 ACL.
Параметры команды:

acl-name	имя IPv4 ACL в виде текстовой строки. Рекомендуемая длина: до 32 символов

Значение по умолчанию:
IPv4 ACL отсутствуют.
Использование команды:
Команда «**ip access-list**» используется для добавления IPv4 ACL и перехода в режим настройки правил IPv4 ACL.
IPv4 ACL, IPv6 ACL и MAC ACL не могут иметь одинаковые имена.
Команды режима настройки правил IPv4 ACL «**permit**» и «**deny**» используются для добавления правил.

Команды «**service-acl input**» и «**service-acl output**» используются для добавления ACL на интерфейс.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip access-list server1
admin@Switch(config-ip-acl)# permit tcp 10.0.0.1 0.0.0.255 any any 80
admin@Switch(config-ip-acl)#
```

9.1.5 ipv6 access-list

Команда глобальной настройки. Добавление IPv6 ACL и переход в режим настройки правил IPv6 ACL.

Синтаксис команды:

ipv6 access-list *acl-name*

no ipv6 access-list *acl-name*

Команда с приставкой «**no**» удаляет IPv6 ACL.

Параметры команды:

acl-name	имя IPv6 ACL в виде текстовой строки. Рекомендуемая длина: до 32 символов

Значение по умолчанию:

IPv6 ACL отсутствуют.

Использование команды:

Команда «**ipv6 access-list**» используется для добавления IPv6 ACL и перехода в режим настройки правил IPv6 ACL.

IPv4 ACL, IPv6 ACL и MAC ACL не могут иметь одинаковые имена.

Команды режима настройки правил IPv6 ACL «**permit**» и «**deny**» используются для добавления правил.

Команды «**service-acl input**» и «**service-acl output**» используются для добавления ACL на интерфейс.

Каждая IPv6 ACL имеет неявные правила «**permit icmp any any nd-ns any**», «**permit icmp any any nd-na any**» и «**deny ipv6 any any**» в качестве последних правил. Первые два правила разрешают работу механизма обнаружения соседей IPv6 (ICMPv6 Neighbor Discovery). В сетях IPv4 используется протокол ARP (Address Resolution Protocol), который не может быть ограничен IPv4 ACL, а, значит, IPv4 ACL неявно разрешают прием и передачу ARP-пакетов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 access-list server2
admin@Switch(config-ipv6-acl)# permit tcp 2001:000:CAFE:BABE::/64 any any 80
admin@Switch(config-ipv6-acl)#
```

9.1.6 mac access-list

Команда глобальной настройки. Добавление MAC ACL и переход в режим настройки правил MAC ACL.

Синтаксис команды:

mac access-list *acl-name*
no mac access-list *acl-name*
Команда с приставкой «**no**» удаляет MAC ACL.
Параметры команды:

acl-name	имя MAC ACL в виде текстовой строки. Рекомендуемая длина: до 32 символов

Значение по умолчанию:
MAC ACL отсутствуют.
Использование команды:
Команда «**mac access-list**» используется для добавления MAC ACL и перехода в режим настройки правил MAC ACL.
IPv4 ACL, IPv6 ACL и MAC ACL не могут иметь одинаковые имена.
Команды режима настройки правил IPv6 ACL «**permit**» и «**deny**» используются для добавления правил.
Команды «**service-acl input**» и «**service-acl output**» используются для добавления ACL на интерфейс.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac access-list server3
admin@Switch(config)# permit 00:1B:28:00:00:01 00:00:00:00:00:ff any
admin@Switch(config)#
```

9.1.7 service-acl input

Команда настройки интерфейса (Ethernet/VLAN). Привязка ACL на входящее направление интерфейса.
Синтаксис команды:
service-acl input *acl-name* [**default-action** {**deny-any** | **permit-any**}]
no service-acl input
Команда с приставкой «**no**» удаляет привязку ACL с исходящего направления интерфейса.
Параметры команды:

acl-name	имя ACL для привязки
deny-any	пакеты, не соответствующие ни одному из правил ACL, отбрасываются. Используется по умолчанию
permit-any	пакеты, не соответствующие ни одному из правил ACL, передаются

Значение по умолчанию:
ACL не назначены ни на один интерфейс.
Использование команды:
Команда «**service-acl input**» используется для привязки ACL на исходящее направление интерфейса.

Ограничения команды:

– два ACL одного типа не могут быть одновременно назначены на интерфейс;
– IPv4 ACL и IPv6 ACL могут быть одновременно назначены на интерфейс;
– если на интерфейс уже были назначены ACL, то они замещаются на ACL, указанные в команде.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac access-list server
admin@Switch(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
admin@Switch(config-mac-acl)# exit
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# service-acl input server
admin@Switch(config-if)#
```

9.1.8 service-acl output

Команда настройки интерфейса Ethernet. Привязка ACL на исходящее направление интерфейса Ethernet.

Синтаксис команды:

service-acl output *acl-name* [**default-action** {**deny-any** | **permit-any**}]

no service-acl output

Команда с приставкой «**no**» удаляет привязку ACL на исходящее направление интерфейса.

Параметры команды:

acl-name	имя ACL для привязки
deny-any	пакеты, не соответствующие ни одному из правил ACL, отбрасываются. Используется по умолчанию
permit-any	пакеты, не соответствующие ни одному из правил ACL, передаются

Значение по умолчанию:

ACL не назначены ни на один интерфейс.

Использование команды:

Команда «**service-acl output**» используется для привязки ACL на исходящее направление интерфейса.

Ограничения команды:

– два ACL одного типа не могут быть одновременно назначены на интерфейс;
– IPv4 ACL и IPv6 ACL могут быть одновременно назначены на интерфейс;
– если на интерфейс уже были назначены ACL, то они замещаются на ACL, указанные в команде;

– параметры правил «**log-input**» и «**disable-port**» не могут присутствовать в ACL, работающей на исходящем направлении. Попытка привязки ACL с указанными параметрами приведет к выводу сообщения об ошибке.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac access-list server
admin@Switch(config-mac-acl)# permit 00:00:00:00:00:01 00:00:00:00:00:ff any
admin@Switch(config-mac-acl)# exit
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# service-acl output server
admin@Switch(config-if)#
```

9.1.9 permit (настройка IPv4 ACL)

Команда настройки IPv4 ACL. Добавление разрешающего правила в IPv4 ACL.

Синтаксис команды:

[*sequence-number*] **permit** *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **permit icmp** {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*] [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **permit igmp** {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*igmp-type*] [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **permit tcp** {**any** | *source source-wildcard*} {**any** | *source-port/port-range*} {**any** | *destination destination-wildcard*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**log-input**]

[*sequence-number*] **permit udp** {**any** | *source source-wildcard*} {**any** | *source-port/port-range*} {**any** | *destination destination-wildcard*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**log-input**]

no [**permit**] [*sequence-number*]

Команда с приставкой «**no**» удаляет разрешающее правило из IPv4 ACL.

Параметры команды:

sequence-number	номер правила в списке доступа. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
protocol	номер протокола IP в диапазоне от 0 до 255 или одно из зарезервированных имен: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. Для указания соответствия любому протоколу используется зарезервированное слово «**ip**»
any	соответствие любому значению поля в пакете
source	IP-адрес источника
source-wildcard	обратная маска (wildcard) IP-адреса источника

destination	IP-адрес назначения
destination-wildcard	обратная маска (wildcard) IP-адреса назначения
dscp *number*	значение DSCP в заголовке IP
precedence *number*	значение IP Precedence в заголовке IP
icmp-type	тип пакета ICMP в диапазоне от 0 до 255 или одно из зарезервированных имен: cho-reply, destination-unreachable, sourcequench, redirect, alternate-host-address, echo-request, router-advertisement, routersolicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris
icmp-code	код пакета ICMP в диапазоне от 0 до 255
igmp-type	тип пакета IGMP в диапазоне от 0 до 255 или одно из зарезервированных имен: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3
source-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Для TCP допускается использование предопределенных значений: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). Для UDP допускается использование предопределенных значений: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177)

destination-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Допускается использование предопределенных значений, аналогично параметру «*source-port/port-range*»
match-all *list-of-flags*	список флагов TCP. Если флаг должен быть установлен, то необходимо поставить перед его названием знак “+” (плюс). Если флаг должен быть снят, то необходимо поставить перед его названием знак “-” (минус). Доступные варианты: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin. Флаги должны быть указаны в виде единой строки без пробелов, например, “+fin-ack”
log-input	логирование входящих пакетов, попавших под правило

Значение по умолчанию:

Правила ACL отсутствуют.

Использование команды:

Команда «**permit**» используется для добавления разрешающего правила в IPv4 ACL.

Количество диапазонов портов источника и назначения (TCP/UDP) ограничено. Действуют следующие ограничения:

- если в правиле используется диапазон портов источника (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных аппаратных ресурсов;
- если в правиле используется диапазон портов назначения (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных аппаратных ресурсов;
- если в правиле используется одинаковый диапазон портов источника и назначения (TCP/UDP), то используются две аппаратные записи.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip access-list server1
admin@Switch(config-ip-acl)# permit tcp 10.0.0.1 0.0.0.255 any any 80
admin@Switch(config-ip-acl)#
```

9.1.10 deny (настройка IPv4 ACL)

Команда настройки IPv4 ACL. Добавление запрещающего правила в IPv4 ACL.

Синтаксис команды:

[*sequence-number*] **deny** *protocol* {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **deny icmp** {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [**any** | *icmp-type*] [**any** | *icmp-code*] [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **deny igmp** {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*igmp-type*] [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **deny tcp** {**any** | *source source-wildcard*} {**any** | *source-port/port-range*} {**any** | *destination destination-wildcard*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**log-input**]

[*sequence-number*] **deny udp** {**any** | *source source-wildcard*} {**any** | *source-port/port-range*} {**any** | *destination destination-wildcard*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**log-input**]

no [**deny**] [*sequence-number*]

Команда с приставкой «**no**» удаляет запрещающее правило из IPv4 ACL.

Параметры команды:

sequence-number	номер правила в списке доступа. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
protocol	номер протокола IP в диапазоне от 0 до 255 или одно из зарезервированных имен: icmp, igmp, ip, tcp, egp, igp, udp, hmp, rdp, idpr, ipv6, ipv6:rout, ipv6:frag, idrp, rsvp, gre, esp, ah, ipv6:icmp, eigrp, ospf, ipinip, pim, l2tp, isis. Для указания соответствия любому протоколу используется зарезервированное слово «**ip**»
any	соответствие любому значению поля в пакете
source	IP-адрес источника
source-wildcard	обратная маска (wildcard) IP-адреса источника
destination	IP-адрес назначения
destination-wildcard	обратная маска (wildcard) IP-адреса назначения
dscp *number*	значение DSCP в заголовке IP
precedence *number*	значение IP Precedence в заголовке IP

icmp-type	тип пакета ICMP в диапазоне от 0 до 255 или одно из зарезервированных имен: cho-reply, destination-unreachable, sourcequench, redirect, alternate-host-address, echo-request, router-advertisement, routersolicitation, time-exceeded, parameter-problem, timestamp, timestamp-reply, information-request, information-reply, address-mask-request, address-mask-reply, traceroute, datagram-conversion-error, mobile-host-redirect, mobile-registration-request, mobile-registration-reply, domain-name-request, domain-name-reply, skip, photuris
icmp-code	код пакета ICMP в диапазоне от 0 до 255
igmp-type	тип пакета IGMP в диапазоне от 0 до 255 или одно из зарезервированных имен: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3
source-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Для TCP допускается использование предопределенных значений: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). Для UDP допускается использование предопределенных значений: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177)
destination-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Допускается использование предопределенных значений, аналогично параметру «*source-port/port-range*»

match-all *list-of-flags*	список флагов TCP. Если флаг должен быть установлен, то необходимо поставить перед его названием знак “+” (плюс). Если флаг должен быть снят, то необходимо поставить перед его названием знак “-” (минус). Доступные варианты: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin. Флаги должны быть указаны в виде единой строки без пробелов, например, “+fin-ack”
log-input	логирование входящих пакетов, попавших под правило

Значение по умолчанию:

Правила ACL отсутствуют.

Использование команды:

Команда «**deny**» используется для добавления запрещающего правила в IPv4 ACL.

Количество диапазонов портов источника и назначения (TCP/UDP) ограничено. Действуют следующие ограничения:

- если в правиле используется диапазон портов источника (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных аппаратных ресурсов;
- если в правиле используется диапазон портов назначения (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных аппаратных ресурсов;
- если в правиле используется одинаковый диапазон портов источника и назначения (TCP/UDP), то используются две аппаратные записи.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip access-list server1
admin@Switch(config-ip-acl)# deny tcp 10.0.0.1 0.0.0.255 any any 80
admin@Switch(config-ip-acl)#
```

9.1.11 permit (настройка IPv6 ACL)

Команда настройки IPv6 ACL. Добавление разрешающего правила в IPv6 ACL.

Синтаксис команды:

[*sequence-number*] **permit** *protocol* {**any** | *source-prefix/length*} {**any** | *destination-prefix/length*} [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **permit icmp** {**any** | *source-prefix/length*} {**any** | *destination-prefix/length*} [**any** | *icmp-type*] [**any** | *icmp-code*] [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **permit tcp** {**any** | *source-prefix/length*} {**any** | *source-port/port-range*} {**any** | *destination-prefix/length*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**log-input**]

[*sequence-number*] **permit udp** {**any** | *source-prefix/length*} {**any** | *source-port/port-range*} {**any** | *destination-prefix/length*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**log-input**]

no [**permit**] [*sequence-number*]

Команда с приставкой «**no**» удаляет разрешающее правило из IPv6 ACL.

Параметры команды:

sequence-number	номер правила в списке доступа. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию, первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
protocol	номер протокола IP в диапазоне от 0 до 255 или одно из зарезервированных имен: icmp (58), tcp (6), udp (17). Для указания соответствия любому протоколу используется зарезервированное слово «**ipv6**»
any	соответствие любому значению поля в пакете
source-prefix/length	сеть источника IPv6 или класс сетей, для которых необходимо применить правило. Аргумент должен иметь формат, указанный в RFC 3513, где адрес указывается в шестнадцатеричном формате с разделением 16-битных данных двоеточиями
destination-port/port-range	сеть источника IPv6 или класс сетей, для которых необходимо применить правило. Аргумент должен иметь формат, указанный в RFC 3513, где адрес указывается в шестнадцатеричном формате с разделением 16-битных данных двоеточиями
dscp *number*	значение DSCP в заголовке IP
precedence *number*	значение IP Precedence в заголовке IP
icmp-type	тип пакета ICMP в диапазоне от 0 до 255 или одно из зарезервированных имен: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mldreport (131), mldv2-report (143), mld-done (132), router-solicitation (133), routeradvertisement (134), nd-ns (135), nd-na (136)
icmp-code	код пакета ICMP в диапазоне от 0 до 255
igmp-type	тип пакета IGMP в диапазоне от 0 до 255 или одно из зарезервированных имен: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3

source-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Для TCP допускается использование предопределенных значений: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). Для UDP допускается использование предопределенных значений: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177)
destination-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Допускается использование предопределенных значений, аналогично параметру «*source-port/port-range*»
match-all *list-of-flags*	список флагов TCP. Если флаг должен быть установлен, то необходимо поставить перед его названием знак “+” (плюс). Если флаг должен быть снят, то необходимо поставить перед его названием знак “-” (минус). Доступные варианты: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin. Флаги должны быть указаны в виде единой строки без пробелов, например, “+fin-ack”
log-input	логирование входящих пакетов, попавших под правило

Значение по умолчанию:

Правила ACL отсутствуют.

Использование команды:

Команда «**permit**» используется для добавления разрешающего правила в IPv6 ACL.

Количество диапазонов портов источника и назначения (TCP/UDP) ограничено. Действуют следующие ограничения:

– если в правиле используется диапазон портов источника (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных

аппаратных ресурсов;

- если в правиле используется диапазон портов назначения (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных аппаратных ресурсов;
- если в правиле используется одинаковый диапазон портов источника и назначения (TCP/UDP), то используются две аппаратные записи.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 access-list server2
admin@Switch(config-ipv6-acl)# permit tcp 2001:000:CAFE:BABE::/64 any any 80
admin@Switch(config-ipv6-acl)#
```

9.1.12 deny (настройка IPv6 ACL)

Команда настройки IPv6 ACL. Добавление запрещающего правила в IPv6 ACL.

Синтаксис команды:

[*sequence-number*] **deny** *protocol* {**any** | *source-prefix/length*} {**any** | *destination-prefix/length*} [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **deny icmp** {**any** | *source-prefix/length*} {**any** | *destination-prefix/length*} [**any** | *icmp-type*] [**any** | *icmp-code*] [**dscp** *number* | **precedence** *number*] [**log-input**]

[*sequence-number*] **deny tcp** {**any** | *source-prefix/length*} {**any** | *source-port/port-range*} {**any** | *destination-prefix/length*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**match-all** *list-of-flags*] [**log-input**]

[*sequence-number*] **deny udp** {**any** | *source-prefix/length*} {**any** | *source-port/port-range*} {**any** | *destination-prefix/length*} {**any** | *destination-port/port-range*} [**dscp** *number* | **precedence** *number*] [**log-input**]

no [**deny**] [*sequence-number*]

Команда с приставкой «**no**» удаляет запрещающее правило из IPv6 ACL.

Параметры команды:

sequence-number	номер правила в списке доступа. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию, первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
sequence-number	номер правила в списке доступа. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию, первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
protocol	номер протокола IP в диапазоне от 0 до 255 или одно из зарезервированных имен: icmp (58), tcp (6), udp (17). Для указания соответствия любому протоколу используется зарезервированное слово «**ipv6**»

any	соответствие любому значению поля в пакете
source-prefix/length	сеть источника IPv6 или класс сетей, для которых необходимо применить правило. Аргумент должен иметь формат, указанный в RFC 3513, где адрес указывается в шестнадцатеричном формате с разделением 16-битных данных двоеточиями
destination-port/port-range	сеть источника IPv6 или класс сетей, для которых необходимо применить правило. Аргумент должен иметь формат, указанный в RFC 3513, где адрес указывается в шестнадцатеричном формате с разделением 16-битных данных двоеточиями
dscp *number*	значение DSCP в заголовке IP
precedence *number*	значение IP Precedence в заголовке IP
icmp-type	тип пакета ICMP в диапазоне от 0 до 255 или одно из зарезервированных имен: destination-unreachable (1), packet-too-big (2), time-exceeded (3), parameter-problem (4), echo-request (128), echo-reply (129), mld-query (130), mldreport (131), mldv2-report (143), mld-done (132), router-solicitation (133), routeradvertisement (134), nd-ns (135), nd-na (136)
icmp-code	код пакета ICMP в диапазоне от 0 до 255
igmp-type	тип пакета IGMP в диапазоне от 0 до 255 или одно из зарезервированных имен: host-query, host-report, dvmrp, pim, cisco-trace, host-report-v2, host-leave-v2, host-report-v3
source-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Для TCP допускается использование предопределенных значений: bgp (179), chargen (19), daytime (13), discard (9), domain (53), drip (3949), echo (7), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (42), irc (194), klogin (543), kshell (544), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (1110), syslog (514), tacacs-ds (49), talk (517), telnet (23), time (37), uucp (117), whois (43), www (80). Для UDP допускается использование предопределенных значений: biff (512), bootpc (68), bootps (67), discard (9), dnsix (90), domain (53), echo (7), mobile-ip (434), nameserver (42), netbios-dgm (138), netbios-ns (137), on500-isakmp (4500), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (49), talk (517), tftp (69), time (37), who (513), xdmcp (177)

destination-port/port-range	порт назначения или диапазон портов для протоколов TCP/UDP. Для ввода диапазона портов необходимо использовать символ “-” (дефис), например: “10-20”. Диапазон значений: от 0 до 65535. Допускается использование предопределенных значений, аналогично параметру «*source-port/port-range*»
match-all *list-of-flags*	список флагов TCP. Если флаг должен быть установлен, то необходимо поставить перед его названием знак “+” (плюс). Если флаг должен быть снят, то необходимо поставить перед его названием знак “-” (минус). Доступные варианты: +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn и -fin. Флаги должны быть указаны в виде единой строки без пробелов, например, “+fin-ack”
log-input	логирование входящих пакетов, попавших под правило

Значение по умолчанию:

Правила ACL отсутствуют.

Использование команды:

Команда «**deny**» используется для добавления запрещающего правила в IPv6 ACL.

Количество диапазонов портов источника и назначения (TCP/UDP) ограничено. Действуют следующие ограничения:

- если в правиле используется диапазон портов источника (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных аппаратных ресурсов;
- если в правиле используется диапазон портов назначения (TCP/UDP), то этот же диапазон может быть использован в другом правиле без дополнительных аппаратных ресурсов;
- если в правиле используется одинаковый диапазон портов источника и назначения (TCP/UDP), то используются две аппаратные записи.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 access-list server2
admin@Switch(config-ipv6-acl)# deny tcp 2001:000:CAFE:BABE::/64 any any 80
admin@Switch(config-ipv6-acl)#
```

9.1.13 permit (настройка MAC ACL)

Команда настройки MAC ACL. Добавление разрешающего правила в MAC ACL.

Синтаксис команды:

[*sequence-number*] **permit** {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*eth-type eth-wildcard* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000**] [**vlan** *vlan-id vlan-wildcard*] [**cos** *cos cos-wildcard*] [**log-input**]

no [**permit**] [*sequence-number*]

Команда с приставкой «**no**» удаляет разрешающее правило в MAC ACL.

Параметры команды:

sequence-number	номер правила в списке доступа. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
any	соответствие любому значению поля в пакете
source	MAC-адрес источника в шестнадцатеричном формате
source-wildcard	обратная маска MAC-адрес источника. Установить в значение “1” те биты, которые необходимо игнорировать
destination	MAC-адрес назначения в шестнадцатеричном формате
destination-wildcard	обратная маска MAC-адрес назначения. Установить в значение “1” те биты, которые необходимо игнорировать
eth-type eth-wildcard	тип протокола Ethernet и обратная маска протокола Ethernet. Установить в значение “1” те биты обратной маски, которые необходимо игнорировать. Допускается использование предопределенных значений: aarp, amber, dec-spanning, decnet-iv, diagnostic, dsm, etype-6000
vlan *vlan-id vlan-wildcard*	идентификатор VLAN в диапазоне от 1 до 4094 и его обратная маска. Установить в значение “1” те биты обратной маски, которые необходимо игнорировать
cos *cos cos-wildcard*	значение класса обслуживания (IEEE 802.1p) в диапазоне от 0 до 7 и его обратная маска. Установить в значение “1” те биты обратной маски, которые необходимо игнорировать
log-input	логирование входящих пакетов, попавших под правило

Значение по умолчанию:

Правила ACL отсутствуют.

Использование команды:

Команда «**permit**» используется для добавления разрешающего правила в MAC ACL.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac access-list server3
admin@Switch(config-mac-acl)# permit 00:1B:28:00:00:01 00:00:00:00:00:ff any
admin@Switch(config-mac-acl)#
```

9.1.14 deny (настройка MAC ACL)

Команда настройки MAC ACL. Добавление запрещающего правила в MAC ACL.

Синтаксис команды:

[*sequence-number*] **deny** {**any** | *source source-wildcard*} {**any** | *destination destination-wildcard*} [*eth-type eth-wildcard* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000**] [**vlan** *vlan-id vlan-wildcard*] [**cos** *cos cos-wildcard*] [**log-input**]

no [**deny**] [*sequence-number*]

Команда с приставкой «**no**» удаляет запрещающее правило в MAC ACL.

Параметры команды:

sequence-number	номер правила в списке доступа. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
any	соответствие любому значению поля в пакете
source	MAC-адрес источника в шестнадцатеричном формате
source-wildcard	обратная маска MAC-адрес источника. Установить в значение “1” те биты, которые необходимо игнорировать
destination	MAC-адрес назначения в шестнадцатеричном формате
destination-wildcard	обратная маска MAC-адрес назначения. Установить в значение “1” те биты, которые необходимо игнорировать
eth-type eth-wildcard	тип протокола Ethernet и обратная маска протокола Ethernet. Установить в значение “1” те биты обратной маски, которые необходимо игнорировать. Допускается использование предопределенных значений: aarp, amber, dec-spanning, decnet-iv, diagnostic, dsm, etype-6000
vlan *vlan-id vlan-wildcard*	идентификатор VLAN в диапазоне от 1 до 4094 и его обратная маска. Установить в значение “1” те биты обратной маски, которые необходимо игнорировать
cos *cos cos-wildcard*	значение класса обслуживания (IEEE 802.1p) в диапазоне от 0 до 7 и его обратная маска. Установить в значение “1” те биты обратной маски, которые необходимо игнорировать
log-input	логирование входящих пакетов, попавших под правило

Значение по умолчанию:

Правила ACL отсутствуют.

Использование команды:

Команда «**deny**» используется для добавления запрещающего правила в MAC ACL.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac access-list server3
admin@Switch(config-mac-acl)# deny 00:1B:28:00:00:01 00:00:00:00:00:ff any
admin@Switch(config-mac-acl)#
```

9.1.15 show access-lists

Команда, доступная из любого режима. Вывод всех или определенного ACL, созданных на устройстве.

Синтаксис команды:

show access-lists [*name*]

Параметры команды:

name имя ACL

Использование команды:

Команда «**show access-lists**» используется для вывода всех или определенного ACL, созданных на устройстве. Если команда введена без аргументов, то выводятся все ACL.

Порядок вывода ACL определяется типом: IP ACL, IPv6 ACL, MAC ACL. Порядок сортировки (вывода) внутри одного типа ACL производится по алфавиту.

Пример команды:

```
admin@Switch# show access-lists

IP ACL   IPv6 ACL   MAC ACL   Total
------   --------   -------   -----
1         1          1         3

MAC access list server3
 10 deny 00:1B:28:00:00:01 00:00:00:00:00:FF any
 20 permit any any

IP access list server1
 10 permit tcp 10.0.0.1 0.0.0.255 any any 80

IPv6 access list server2
 10 permit tcp 2001:000:CAFE:BABE::/64 any any 80
```

9.1.16 show interfaces access-lists

Команда, доступная из любого режима. Вывод списка ACL, назначенных на все или определенный интерфейс.

Синтаксис команды:

show interfaces access-lists [*interface-id*]
Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show interfaces access-lists**» используется для вывода списка ACL, назначенных на все или определенный интерфейс. Если команда введена без аргументов, то выводится список ACL, назначенных на все интерфейсы.

Пример команды:

```
admin@Switch# show interfaces access-lists
Interface   Ingress ACLs   Egress ACLs
---------   ------------   -----------
gi0/1       server1        server2
gi0/3       server3
```

9.1.17 show interfaces access-lists counters

Команда, доступная из любого режима. Вывод счетчиков статистики ACL.

Синтаксис команды:

show interfaces access-lists counters [*interface-id* | *vlan vlan-id*] [**brief**]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)
vlan vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
brief	вывод сводной информации – только количество срабатываний для правил «**permit**» и «**deny**»

Использование команды:

Команда «**show interfaces access-lists counters**» используется для вывода счетчиков статистики ACL. Если команда введена без аргументов, то происходит вывод всех счетчиков статистики ACL.

Пример команды:

```
admin@Switch# show interfaces access-lists counters vlan 1
Interface VLAN0001
 Total PERMIT Hits: 0
 Total DENY Hits: 9
  IPv4 ACL: test
   10 deny ip any any log-input: 4 Hits
  IPv6 ACL: test2
   10 deny ipv6 2001:0000:CAFE:BABE::/64
    2001:0000:DEAD:BEEF::/64 log-input: 3 Hits
   20 deny ipv6 2001:0000:1111:2222::/64
    2001:0000:2222:1111::/64 log-input: 2 Hits
```

9.1.18 show interfaces access-lists vlan

Команда, доступная из любого режима. Вывод списков ACL, назначенных на определенный VLAN.

Синтаксис команды:

show interfaces access-lists vlan *vlan-id*

Параметры команды:

vlan-id	идентификатор интерфейса VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# show interfaces access-lists vlan 1
Interface   Ingress ACLs   Egress ACLs
---------   ------------   -----------
VLAN0001     name, default: deny-any
```

9.2 Ограничение управления устройством (Management ACL)

9.2.1 management access-list

Команда глобальной настройки. Создание списка ограничения доступа к управлению.

Синтаксис команды:

management access-list *name*

no management access-list *name*

Команда с приставкой «**no**» удаляет список ограничения доступа к управлению.

Параметры команды:

name	имя списка ограничения доступа к управлению. Рекомендуемая длина: от 1 до 32 символов

Значение по умолчанию:

Списки ограничения доступа к управлению отсутствуют.

Использование команды:

Команда «**management access-list**» используется для создания списка ограничения доступа к управлению.

В каждый момент времени может быть активен только один список ограничения доступа к управлению.

Устройство не позволяет удалить список ограничения доступа к управлению (и выводит сообщение об ошибке), если он используется в текущий момент.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# management access-list MyManACL
admin@Switch(config-macl)#
```

```
admin@Switch# configure terminal
admin@Switch(config)# no management access-list MyManACL
%Can not delete management ACL which is currenly in use. Disable it first before
trying to delete.
admin@Switch(config)#
```

9.2.2 management access-class

Команда глобальной настройки. Назначение активного списка ограничения доступа к управлению.

Синтаксис команды:

management access-class {console-only | *name***}**

no management access-class

Команда с приставкой «**no**» отменяет использование списка ограничения доступа к управлению.

Параметры команды:

console-only	запрет доступа по всем протоколам управления, кроме управления через консольный порт "F"
name	имя существующего списка ограничения доступа к управлению

Значение по умолчанию:

Доступ к управлению не ограничен.

Использование команды:

Команда «**management access-class**» используется для назначения активного списка ограничения доступа к управлению.

В каждый момент времени может быть активен только один список ограничения доступа к управлению.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# management access-class MyManACL
admin@Switch(config)#
```

9.2.3 deny

Команда настройки списка ограничения доступа к управлению. Добавление запрещающего правила.

Синтаксис команды:

[*rule-number***] deny [service** *service***]**

[*rule-number***] deny ip-source** *ipv4-address* **[mask {***mask* **|** *prefix-length***}] [service** *service***]**

no [deny] *rule-number*

Команда с приставкой «**no**» удаляет запрещающее правило.

Параметры команды:

rule-number	номер правила в списке. Если не задан, то система автоматически добавляет правило в конец списка с инкрементом в 10 (первое правило имеет номер 10, второе – 20 и т.д.). Если правило с таким номером уже существует, то оно будет заменено
ipv4-address	IP-адрес хоста или подсети
mask	маска подсети. Если параметр не задан, то маска подсети определяется в соответствии с правилами классовой адресации (поддерживаются классы A, B и C)
prefix-length	длина префикса. Если параметр не задан, то маска подсети определяется в соответствии с правилами классовой адресации (поддерживаются классы A, B и C)

service	имя запрещаемого сервиса (протокола) управления из списка: telnet, ssh, http, https, snmp. Если параметр не задан, то правило применяется ко всем сервисам управления

Значение по умолчанию:

Правила отсутствуют.

Использование команды:

Команда «**deny**» используется для добавления запрещающего правила.

В конце списка доступа управления устройство автоматически добавляет правило, запрещающее доступ ко всем протоколам управления («**deny**»), которое не отображается в конфигурации.

В случае ввода команды «**no deny**» с номером правила, который соответствует правилу «**permit**» будет выведено сообщение об ошибке.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# management access-list MyManACL
admin@Switch(config-macl)# deny ip-source 192.168.0.0 mask /20
admin@Switch(config-macl)# permit
admin@Switch(config-macl)# exit
admin@Switch(config)# management access-class MyManACL
admin@Switch(config)#
```

9.2.4 permit

Команда настройки списка ограничения доступа к управлению. Добавление разрешающего правила.

Синтаксис команды:

[*rule-number***] permit [service** *service***]**

[*rule-number***] permit ip-source** *ipv4-address* **[mask {***mask* **|** *prefix-length***}] [service** *service***]**

no [permit] *rule-number*

Команда с приставкой «**no**» удаляет разрешающее правило.

Параметры команды:

rule-number	номер правила в списке. Если не задан, то система автоматически добавляет правило в конец списка с инкрементом в 10 (первое правило имеет номер 10, второе – 20 и т.д.). Если правило с таким номером уже существует, то оно будет заменено
ipv4-address	IP-адрес хоста или подсети
mask	маска подсети. Если параметр не задан, то маска подсети определяется в соответствии с правилами классовой адресации (поддерживаются классы A, B и C)
prefix-length	длина префикса. Если параметр не задан, то маска подсети определяется в соответствии с правилами классовой адресации (поддерживаются классы A, B и C)

service имя запрещаемого сервиса (протокола) управления из списка: telnet, ssh, http, https, snmp. Если параметр не задан, то правило применяется ко всем сервисам управления

Значение по умолчанию:

Правила отсутствуют.

Использование команды:

Команда «**permit**» используется для добавления разрешающего правила. В конце списка доступа управления устройство автоматически добавляет правило, запрещающее доступ ко всем протоколам управления («**deny**»), которое не отображается в конфигурации.

В случае ввода команды «**no permit**» с номером правила, который соответствует правилу «**deny**» будет выведено сообщение об ошибке.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# management access-list MyManACL2
admin@Switch(config-macl)# permit ip-source 192.168.0.0 mask /20
admin@Switch(config-macl)# exit
admin@Switch(config)# management access-class MyManACL2
admin@Switch(config)#
```

9.2.5 show management access-list

Команда, доступная из любого режима. Вывод списков ограничения доступа к управлению.

Синтаксис команды:

show management access-list [*name***]**

Параметры команды:

name имя списка ограничения доступа к управлению

Использование команды:

Команда «**show management access-list**» используется для вывода списков ограничения доступа к управлению. Если команда введена без параметров, то устройство выводит все списки доступа.

Пример команды:

```
admin@Switch# show management access-list
MyManACL
---------------------------------------
  10 deny ip-source 192.168.0.0 mask /20
  20 permit
MyManACL2
---------------------------------------
  10 permit ip-source 192.168.0.0 mask /20
```

9.2.6 show management access-class

Команда, доступная из любого режима. Вывод настройки активного списка ограничения доступа к управлению.

Синтаксис команды:
show management access-class

Использование команды:

Команда «**show management access-class**» используется для вывода настройки активного списка ограничения доступа к управлению.

Примеры команды:

```
admin@Switch# show management access-class
Management acess-class is enabled, using access list MyManACL
```

```
admin@Switch# show management access-class
Management acess-class is disabled
```

10 Spanning tree и резервирование соединений

10.1 Настройка протоколов Spanning Tree

10.1.1 Общие положения

Протокол связующего дерева (Spanning tree, IEEE 802.1D-1998) предназначен для защиты широковещательного домена уровня L2 от пакетных “штормов” путем перевода избыточных соединений в режим готовности, при котором они не передают пользовательские пакеты, но могут быть автоматически переведены в рабочий режим при смене топологии сети.

Протокол быстрого связующего дерева (Rapid Spanning tree, IEEE 802.1D2004) является усовершенствованной версией протокола, основным преимуществом которого является существенно уменьшенное время сходимости сети.

Протокол связующего дерева является стандартным требованием к коммутаторам уровня L2 и позволяет мостам (bridge) автоматически предотвращать и разрешать закольцовывания топологии на уровне L2.

Коммутаторы обмениваются конфигурационными сообщениями в виде специальных фреймов, называемых BPDU (Bridge Protocol Data Unit), и избирательно включают режим приема и передачи пользовательского трафика на портах.

Конечным результатом является логическая топология в виде дерева с таким набором активных портов, что между любыми двумя устройствами есть возможность передачи пользовательского трафика без закольцовывания трафика в сети. Пример топологии сети приведен на рисунке 5.

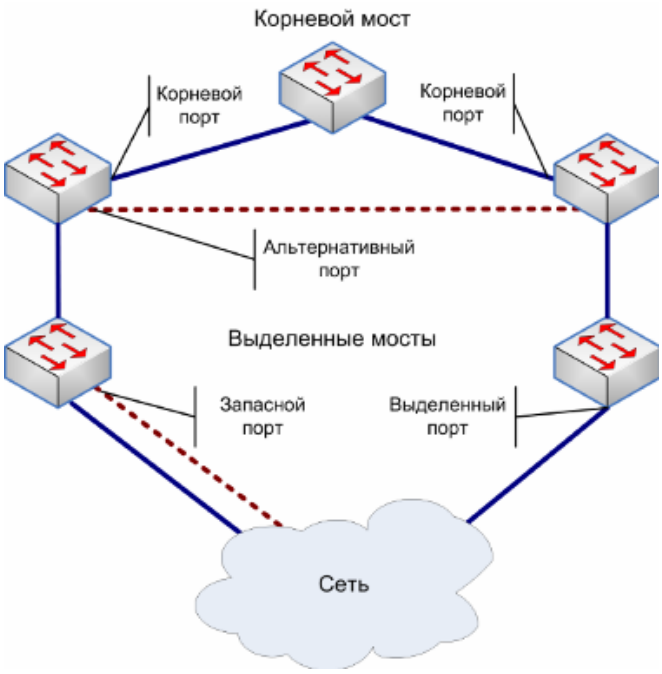

Рисунок 5 – Пример топологии сети с протоколом Spanning Tree

Устройства, поддерживающие протокол связующего дерева, производят выбор корневого моста (Root Bridge), который осуществляет управление всей логической

топологией в сети. Устройства, к которым подключены сегменты сети без других мостов и не являющиеся корневыми мостами, являются выделенными устройствами для этих сегментов сети (Designated Bridge).

Каждому порту моста назначается его роль, определяющая его функции в сети:

1. Корневой (Root) – порт, который всегда находится в состоянии передачи и предоставляет наименьшую стоимость пути до корневого моста (у корневого моста корневой порт отсутствует).
2. Выделенный (Designated) – порт на сегменте сети (без мостов), находящийся в состоянии передачи и предоставляющий наименьшую стоимость пути от этого сегмента сети до корневого моста.
3. Альтернативный (Alternate) – порт, который может предоставить резервный путь для подключения к корневому мосту в случае нарушения текущей физической топологии.
4. Запасной (Backup) – порт, который может предоставить резервный путь для подключения к сегменту сети или корневому мосту в случае нарушения текущей физической топологии. В отличие от альтернативного порта, запасной порт не может гарантировать резервный путь для подключения к корневому мосту.
5. Отключенный (Disabled) – на порту отсутствует соединение по любой причине.

Устройство поддерживает следующие режимы работы Spanning Tree:

- протокол связующего дерева (Spanning Tree Protocol);
- быстрый протокол связующего дерева (Rapid Spanning Tree Protocol);
- протокол множественного связующего дерева (Multiple Spanning Tree Protocol);
- быстрый протокол связующего дерева для каждого VLAN (Rapid PerVLAN Spanning Tree mode).

Протокол множественного связующего дерева (Multiple Spanning Tree Protocol, IEEE 802.1Q-2011) предоставляет пользователю назначать группы VLAN на поддеревья MST. Каждое поддерево MST является независимым от других поддеревьев, то есть оно имеет свою топологию и корневой мост.

Быстрый протокол связующего дерева для каждого VLAN (Rapid Per-VLAN Spanning Tree mode).

В соответствии со спецификацией (IEEE 802.1Q-2011) мост MST должен поддерживать как минимум два поддерева MST:

- Одно внутреннее связующее дерево (Internal Spanning Tree, IST);
- Одно или несколько множественных связующих деревьев (Multiple Spanning Tree Instance, MSTI).

Внутреннее связующее дерево (IST) используется для обеспечения совместимости MSTP с сетями 802.1Q, для которых используется только одна сеть связующего дерева (Common Spanning Tree, CST).

Поддерево IST по сути является поддеревом RSTP, которая расширяет CST внутрь MST-региона.

Поддерево IST отправляет и принимает BPDU из CST. С помощью поддерева IST весь MST-регион предоставляется как один виртуальный мост для дерева CST. Множественные связующие поддеревья (MSTI) также являются поддеревьями RSTP, но существуют только в пределах MST-региона. В отличие от IST, поддеревья MSTI никогда не взаимодействуют с устройствами за пределами MST-региона. Протокол MSTP поддерживает только одно связующее поддерево за пределами MST-региона, поэтому, за исключением поддерева IST, поддеревья региона не имеют своих аналогов за пределами региона. Кроме того, поддеревья MSTI не отправляют пакеты BPDU за пределы MST-региона (отправляет только IST).

MSTI не отправляют независимых пакетов BPDU. Внутри MST-региона мосты обмениваются MST BPDU, выглядящими как нормальные RSTP BPDU для поддерева IST с дополнительной информацией для каждого поддерева MSTI.

Использование нескольких поддеревьев MST позволяет балансировать передачу трафика в сети по различным путям путем назначения соответствующих групп VLAN на поддеревья MST. Пример балансировки трафика приведен на рисунке 6. В приведенном примере на поддерево 1 и поддерево 2 назначены разные VLAN.

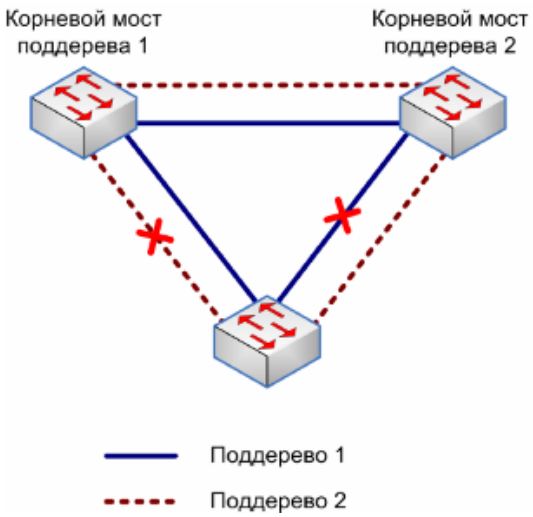

Рисунок 6 – Балансировка трафика с помощью MSTP

Настройка поддеревьев MST не применяется сразу, что позволяет пользователю проверить корректность настроек и применить (или откатить) внесенные изменения.

Для работы в составе единого MST-региона, устройства должны иметь одинаковое отображение VLAN на поддеревья, одинаковую ревизию конфигурации и одинаковое имя региона.

Устройство поддерживает следующие механизмы защиты Spanning-Tree:

– Root Guard – защита от подмены корневого коммутатора;

– Topology Change Guard – защита от нежелательного перестроения топологии;
– BPDU Guard – защита от некорректных настроек на границе сети.

Механизм Root Guard используется при вероятности подключения нелегитимного коммутатора к порту устройства, для предотвращения возможности перехода нелегитимного коммутатора в режим корневого моста сети.

Если механизм Root Guard включен на порту, то порт никогда не сможет получить роль корневого порта, а только роль из списка: Designated, Alternate, Backup или Disabled.

Протокол связующего дерева (Spanning Tree) определяет роль порта в соответствии с алгоритмом, описанном в стандарте. Включив механизм Root Guard, системный администратор предотвращает возможность перехода порта (и подключенного к нему устройства) в режим корневого.

Topology Change Guard предотвращает передачу извещения об изменении топологии сети на другие интерфейсы. Это означает, что даже если порт получит BPDU с установленным флагом изменения топологии, порт не будет очищать свои динамические MAC-адреса и не будет передавать дальше BPDU с установленным флагом изменения топологии.

BPDU Guard используется в целях безопасности для защиты сети от некорректных настроек. Как правило, BPDU Guard применяется на интерфейсах, подключенных к конечным клиентам и на стыках двух сетей, принадлежащих разным организациям.

При получении BPDU на интерфейсе со включенным BPDU Guard данный интерфейс автоматически отключается.

Настройки пользователя

Общие настройки протоколов Spanning-Tree:

1. Глобальные настройки:

– режим работы: stp, rstp, mst, pvrst;
– приоритет устройства (Bridge Priority): целое число в диапазоне от 0 до 61440 с шагом 4096;
– время задержки для перехода портов в режим передачи (Forward Delay): целое число в диапазоне от 6 до 30 секунд;
– интервал отправки Hello BPDU: целое число в диапазоне от 1 до 2 секунд;
– время старения информации от корневого моста: целое число в диапазоне от 6 до 40 секунд.

2. Настройки на интерфейсах:

– режим фильтрации BPDU: включен, выключен;
– режим контроля приема BPDU: включен, выключен;

– режим PortFast: auto, force;
– внутренняя стоимость пути: целое число в диапазоне от 1 до 200 000 000;
– тип подключения: point-to-point, shared, auto;
– приоритет интерфейса: целое число в диапазоне от 0 до 240 с шагом 16;
– запрет на переход порта в режим корневого порта: включен, выключен;
– запрет на трансляцию сообщений об изменении топологии: включен, выключен.

Настройки протокола MSTP:

1. Глобальные настройки:

– количество мостов (hops) в MST-регионе перед тем, как пакет BPDU будет удален: целое число в диапазоне от 1 до 40.

2. Настройки на интерфейсах:

– внутренняя стоимость пути для каждого поддерева MST: целое число в диапазоне от 1 до 200 000 000;
– интервал отправки Hello BPDU для каждого поддерева MST: целое число в диапазоне от 1 до 10 секунд;
– приоритет интерфейса для каждого поддерева MST: целое число в диапазоне от 0 до 240 с шагом 16;
– режим portfast: auto, force.

3. Настройки поддеревьев MST:

– список VLAN, назначенный на поддерево, диапазон значений номеров поддеревьев: от 0 до 4095;
– имя MST-региона: текстовая строка длиной до 32 символов;
– версия конфигурации MST-региона: целое число в диапазоне от 0 до 65535.

Настройки механизмов защиты Spanning-Tree:

1. Настройки на интерфейсах:

– режим Root Guard: включен, отключен;
– режим Topology Change Guard: включен, отключен;
– режим STP BPDU Guard: включен, отключен.

Дополнения и ограничения

Для быстрой сходимости логической топологии сети рекомендуется использовать протокол RSTP или MSTP.

Включение фильтрации BPDU автоматически отключает Spanning Tree на интерфейсе. Устройство поддерживает 64 поддерева MST.

Настройка Root Guard на интерфейсе может привести к разрыву взаимодействия устройства с остальной частью сети (например, при настройке функции на легитимном корневом порту).

В режиме MSTP настройки Root Guard и Topology Change Guard влияют на все поддеревья MST одновременно.

STP BPDU Guard рекомендуется использовать на граничных портах сети (как правило, на граничных портах включена фильтрация Spanning Tree).

Описание настройки

Порядок настройки протокола Spanning Tree приведен в таблице 10.

Таблица 10 – Порядок настройки Spanning Tree

Шаг	Команда	Назначение
1	configure terminal	Переход в режим глобальной настройки
2	**spanning-tree mode** {**stp** | **rstp** | **mst** | **pvrst**}	Установка режима работы протокола Spanning Tree
3	**spanning-tree priority** *priority*	Установка приоритета моста в сети. Рекомендуется задать повышенной приоритет для корневого моста (меньшее числовое значение)
4	**interface** *interface-id*	Переход в режим настройки интерфейса
5	**spanning-tree cost** *cost*	(Опционально) Установка внутренней стоимости пути на интерфейсе
6	**spanning-tree port-priority** *priority*	(Опционально) Установка приоритета интерфейса
7	**exit**	Переход в предыдущий режим настройки
8	**exit**	Переход в предыдущий режим настройки
9	show spanning-tree summary	Проверка настроек Spanning Tree
10	copy running-config startup-config	Сохранение текущей конфигурации

Рассмотрим вариант настройки со следующими условиями:

- необходимо установить режим RSTP;
- устройство должно иметь приоритет 4096;
- необходимо установить внутреннюю стоимость на интерфейсах gigabitetethernet 0/1-4 равной 50000;
- интерфейсы gigabitetethernet 0/1-4 должны иметь приоритет 160.

Выполним глобальные настройки:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree mode rstp
admin@Switch(config)# spanning-tree priority 4096
admin@Switch(config)#
```

Выполним настройки стоимости пути и приоритета на интерфейсах:

```
admin@Switch(config)# interface range gigabitetethernet 0/11-4
admin@Switch(config-if)# spanning-tree cost 50000
admin@Switch(config-if)# spanning-tree port-priority 160
admin@Switch(config-if)# exit
admin@Switch(config)# exit
admin@Switch#
```

Проверим параметры и сохраним файл конфигурации:

```
admin@Switch# show spanning-tree summary
STP configuration:
-----------------
Root ID
Priority:               4096
MAC-address:            00:1B:28:00:00:01
Cost:                   20000
Port:                   gigabitethernet 0/1
Bridge ID
Switch mode:            rstp
Priority:               4096
Forward time:           15 sec
Hello time:             2 sec
Max age:                20 sec
Transmit hold count:    6 pps
Port                    State
---------------         ----------
gigabitethernet 0/1     forwarding
gigabitethernet 0/2     disabled
gigabitethernet 0/3     disabled
gigabitethernet 0/4     disabled
admin@Switch# copy running-config startup-config
```

Порядок настройки протокола MSTP приведен в таблице 11.

Таблица 11 – Порядок настройки Spanning Tree

Шаг	Команда	Назначение
1	configure terminal	Переход в режим глобальной настройки
2	**spanning-tree mode mst**	Установка режима работы протокола MSTP

3	**spanning-tree mst max-hops** *value*	(Опционально) Установка количества мостов (hops) в MST-регионе перед тем, как пакет BPDU будет удален. Рекомендуется увеличить значение настройки для большой сети
4	**spanning-tree mst** *instance* **priority** *value*	Установка приоритета моста на указанном поддереве MST. Рекомендуется задать повышенной приоритет для корневого моста поддерева MST (меньшее числовое значение)
5	**interface** *interface-id*	Переход в режим настройки интерфейса
6	**spanning-tree mst** *instance* **cost {auto |** *value***}**	(Опционально) Установка внутренней стоимости пути на поддереве MST настраиваемого интерфейса
7	**spanning-tree mst** *instance* **port-priority** *value*	(Опционально) Установка приоритета интерфейса в поддереве MST
8	exit	Переход в предыдущий режим настройки
9	spanning-tree mst configuration	Переход в режим настройки MST-региона
10	**instance** *instance-to-add* **vlan** *vlan-range*	Добавление одного или нескольких VLAN к поддереву MST
11	**name** *string*	Установка имени конфигурации MST
12	**revision** *level*	Установка номера версии конфигурации MST
13	commit	Применение настроек MST
14	show pending	Проверка конфигурации MST-региона
15	exit	Выход из режима настройки MST-региона с применением внесенных изменений
16	exit	Переход в предыдущий режим настройки
17	**show spanning-tree mst** *instance*	Проверка настроек MSTP
18	copy running-config startupconfig	Сохранение текущей конфигурации

Рассмотрим вариант настройки со следующими условиями:

- необходимо установить максимальное количество мостов (hops) в MST-регионе равным 30;
- устройство должно иметь приоритет 4096 в поддереве MST 0 и приоритет 16384 в поддереве MST 1;
- необходимо установить внутреннюю стоимость в поддереве MST 1 на интерфейсах gigabitetethernet 0/1-4 равной 50000;
- интерфейсы gigabitetethernet 0/1-4 должны иметь приоритет 160 в поддереве MST 0;
- необходимо назначить VLAN 1–10 на поддерево MST 0, а VLAN 11–20 – на поддерево MST 1;

– MST-регион должен иметь имя “region” и номер ревизии 5.

Выполним глобальные настройки:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree mode mst
admin@Switch(config)# spanning-tree mst 0 priority 4096
admin@Switch(config)# spanning-tree mst 1 priority 16384
admin@Switch(config)#
```

Выполним настройки стоимости пути и приоритета на интерфейсах:

```
admin@Switch(config)# interface range gigabitetethernet 0/1-4
admin@Switch(config-if)# spanning-tree mst 1 cost 50000
admin@Switch(config-if)# spanning-tree mst 0 port-priority 160
admin@Switch(config-if)# exit
admin@Switch(config)#
```

Проверим и проверим настройки MST-региона:

```
admin@Switch(config)# spanning-tree mst configuration
admin@Switch(config-mst)# instance 0 vlan 1-10
admin@Switch(config-mst)# instance 1 vlan 11-20
admin@Switch(config-mst)# name region
admin@Switch(config-mst)# revision 5
admin@Switch(config-mst)# show pending
Name: [region]
Revision: 5
Instance     VLANs
--------     -----
0            1-10
1            11-20
admin@Switch(config-mst)# exit
admin@Switch(config)# exit
admin@Switch#
```

Проверим параметры и сохраним файл конфигурации:

```
admin@Switch# show spanning-tree mst 0
MST instance 0
------------
VLANs mapped: 1-11
Root
  Priority                    0
  MAC-address                 00:1B:28:00:8D:80
  Cost                        0
  Port                        gigabitethernet 0/4
Regional root
  Priority                    4096
  MAC-address                 00:1B:28:01:43:60
  Cost                        0
  Remaining hops              29
Bridge
  Priority                    32768
  MAC-address                 00:1B:28:01:43:60
Configured settings
  Forward time                15 sec
  Hello time                  2 sec
  Max age                     20 sec
Operational settings
  Forward time                15 sec
  Hello time                  2 sec
  Max age                     20 sec
  Transmit hold count 6 pps

Interface           Role         State        Cost    Prio.Nbr  Type
------------------  --------     --------     -----   --------  ----
gigabitethernet0/1  disabled     disabled     20000   160.25    auto
gigabitethernet0/2  disabled     disabled     20000   160.26    auto
gigabitethernet0/3  designated   forwarding   20000   160.27    auto
gigabitethernet0/4  root         forwarding   20000   160.28    auto

admin@Switch# show spanning-tree mst 1
MST instance 1
------------
VLANs mapped: 2

Root
  Priority                    16384
  MAC-address                 00:1B:28:01:43:60
  Cost                        0
  Remaining hops              no port
Bridge
  Priority                    8193
  MAC-address                 00:1B:28:01:43:60

Interface           Role         State        Cost    Prio.Nbr  Type
------------------  --------     --------     -----   --------  ----
gigabitethernet0/1  disabled     disabled     50000   128.25    auto
gigabitethernet0/2  disabled     disabled     50000   128.26    auto
gigabitethernet0/3  designated   forwarding   50000   128.27    auto
gigabitethernet0/4  designated   forwarding   50000   128.28    auto

admin@Switch# copy running-config startup-config
```

10.1.2 clear spanning-tree statistics

Команда фундаментального режима. Сброс статистики BPDU пакетов.
Синтаксис команды:
clear spanning-tree statistics
Пример команды:

```
admin@Switch# clear spanning-tree statistics
admin@Switch#
```

10.1.3 debug spanning-tree

Команда фундаментального режима. Включение отладки STP.
Синтаксис команды:
debug spanning-tree {all | bpdu [receive | transmit] | events | root}
no debug spanning-tree {all | bpdu [receive | transmit] | events | root}
Команда с приставкой «**no**» отключает отладку STP.
Параметры команды:

all	отображение всех сообщений отладки
bpdu	отображение информации о полученных и отправленных BPDU
bpdu receive	отображение информации только о полученных BPDU
bpdu transmit	отображение информации только об отправленных BPDU
events	отображение информации о событиях изменения топологии
root	отображение информации о событиях смены корневого моста

Пример команды:

```
admin@Switch# debug spanning-tree all
admin@Switch#
```

10.1.4 spanning-tree bpdufilter

Команда настройки интерфейса. Установка режима фильтрации BPDU на интерфейсе Ethernet. Включение фильтрации автоматически отключает STP на данном интерфейсе.
Синтаксис команды:
spanning-tree bpdufilter {disable | enable}
no spanning-tree bpdufilter
Команда с приставкой «**no**» отключает фильтрацию BPDU на данном интерфейсе.
Параметры команды:

disable	отключение фильтрации BPDU
enable	включение фильтрации BPDU

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet0/1
admin@Switch(config-if)# spanning-tree bpdufilter enable
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

10.1.5 spanning-tree bpduguard

Команда настройки интерфейса. Установка режима контроля прихода BPDU на интерфейс Ethernet. Включение контроля означает, что при приходе BPDU на данный интерфейс коммутатор автоматически отключает интерфейс и выводит сообщение об ошибке.

Синтаксис команды:

spanning-tree bpduguard {disable | enable}

no spanning-tree bpduguard

Команда с приставкой «**no**» отключает контроль прихода BPDU на данном интерфейсе.

Параметры команды:

disable отключение контроля прихода BPDU

enable включение контроля прихода BPDU

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet0/1
admin@Switch(config-if)# spanning-tree bpduguard enable
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

10.1.6 spanning-tree cost

Команда настройки интерфейса. Установка стоимости пути для интерфейса Ethernet.

Синтаксис команды:

spanning-tree cost {*cost* **| auto}**

no spanning-tree cost

Команда с приставкой «**no**» устанавливает значение 20 000 для интерфейсов gigabitethernet и значение 2 000 для интерфейсов tengigabitethernet.

Параметры команды:

cost стоимость пути в диапазоне от 1 до 200 000 000

auto автоматическая установка стоимости пути для интерфейса Ethernet

Использование команды:

Рекомендуемые значения стоимости пути для интерфейсов gigabitethernet: от 1 до 20 000. Рекомендуемые значения стоимости пути для интерфейсов tengigabitethernet: от 1 до 2000.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet0/1
admin@Switch(config-if)# spanning-tree cost 100000
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

10.1.7 spanning-tree forward-time

Команда глобальной настройки. Установка времени перехода портов в режим передачи данных («FORWARDING») при изменении топологии сети для протокола STP.

Синтаксис команды:

spanning-tree forward-time *seconds*

no spanning-tree forward-time

Команда с приставкой «**no**» устанавливает значение 15 секунд.

Параметры команды:

seconds время перехода в диапазоне от 6 до 30 секунд

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree forward-time 10
admin@Switch(config)# end
admin@Switch#
```

10.1.8 spanning-tree hello-time

Команда глобальной настройки. Установка периода отправки сообщений «hello».

Синтаксис команды:

spanning-tree hello-time *seconds*

no spanning-tree hello-time

Команда с приставкой «**no**» устанавливает значение периода отправки, равное 2 секундам.

Параметры команды:

seconds период отправки в диапазоне от 1 до 2 секунд

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree hello-time 1
admin@Switch(config)# end
admin@Switch#
```

10.1.9 spanning-tree link-type

Команда настройки интерфейса. Установка типа подключения на интерфейсе “точка-точка”, “сеть” или автоматическое определение типа подключения.

Синтаксис команды:

spanning-tree link-type {point-to-point | shared | auto}

no spanning-tree link-type

Команда с приставкой «**no**» устанавливает автоматическое определение типа подключения на интерфейсе.

Параметры команды:

point-to-point	тип подключения «точка-точка»
shared	тип подключения «сеть»
auto	автоматическое определение типа подключения в зависимости от состояния дуплекса на интерфейсе: полный дуплекс – «сеть», полудуплекс – «точка-точка»

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# spanning-tree link-type shared
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

10.1.10 spanning-tree portfast

Команда настройки интерфейса. Установка режима ускоренного перехода интерфейса в статус FORWARDING. Устанавливаается на access-портах.

Синтаксис команды:

spanning-tree portfast {auto}

no spanning-tree portfast

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

auto	добавляет трехсекундную задержку перед переходом в состояние FORWARDING

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# spanning-tree portfast
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

10.1.11 spanning-tree max-age

Команда глобальной настройки. Установка времени старения информации от корневого моста. По истечении данного времени корневой мост считается вышедшим из строя и происходит выбор нового корневого моста.

Синтаксис команды:

spanning-tree max-age *seconds*

no spanning-tree max-age

Команда с приставкой «**no**» устанавливает значение 20 секунд.

Параметры команды:

seconds	время старения в диапазоне от 6 до 40 секунд

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree max-age 10
admin@Switch(config)# end
admin@Switch#
```

10.1.12 spanning-tree mode

Команда глобальной настройки. Установка режима работы протокола Spanning Tree.

Синтаксис команды:

spanning-tree mode {stp | rstp | mst | pvrst}

no spanning-tree mode

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

stp	выбор режима STP (Spanning Tree Protocol)
rstp	выбор режима RSTP (Rapid Spanning Tree Protocol)
mst	выбор режима MSTP (Multiple Spanning Tree Protocol)
pvrst	выбор режима PVRST (Per-VLAN Rapid Spanning Tree). Протокол совместим с Rapid PVST+

Значение по умолчанию:

Режим RSTP.

Использование команды:

Команда «**spanning-tree mode**» используется для установки режима работы протокола Spanning Tree.

Протокол MSTP (mst) имеет отдельный набор настроек, частично перекрывающий настройки STP и RSTP:

1. Приоритет для каждого поддерева MST.
2. Стоимость пути для каждого интерфейса. Стоимость пути указывается для каждого поддерева MST в отдельности.

3. Приоритет для каждого интерфейса. Приоритет указывается для каждого поддерева MST в отдельности.
4. Интервал отправки Hello BPDU для каждого интерфейса.

Протокол PVRST (pvrst) имеет отдельный набор настроек, частично перекрывающий настройки STP и RSTP:

1. Приоритет для каждого VLAN.
2. Время старения информации для каждого VLAN.
3. Время перехода портов в режим передачи данных (“forwarding”) при изменении топологии сети для каждого VLAN.
4. Интервал отправки Hello BPDU для каждого VLAN.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree mode rstp
admin@Switch(config)#
```

10.1.13 spanning-tree port-priority

Команда настройки интерфейса. Установка приоритета интерфейса в коммутаторе. Приоритет интерфейса используется при расчете активной топологии. При наличии более одной связи (соединения между интерфейсами) между двумя коммутаторами активным становится интерфейс с наименьшим числовым значением приоритета.

Синтаксис команды:

spanning-tree port-priority *priority*

no spanning-tree port-priority

Команда с приставкой «**no**» устанавливает значение 128.

Параметры команды:

priority приоритет интерфейса в диапазоне от 0 до 240 с шагом 16

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# spanning-tree port-priority 160
admin@Switch(config-if)# end
admin@Switch(config)# end
admin@Switch#
```

10.1.14 spanning-tree priority

Команда глобальной настройки. Установка приоритета моста в сети. Приоритет моста необходим для определения корневого моста: корневым мостом становится устройство с наименьшим числовым значением приоритета.

Синтаксис команды:
spanning-tree priority *priority*
no spanning-tree priority
Команда с приставкой «**no**» устанавливает значение 36864.
Параметры команды:

priority приоритет моста в диапазоне от 0 до 61440 с шагом 4096

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree priority 32768
admin@Switch(config)# end
admin@Switch#
```

10.1.15 spanning-tree transmit hold-count

Команда глобальной настройки. Установка ограничения по управляющему трафику протоколов Spanning Tree, проходящему через интерфейсы.
Синтаксис команды:
spanning-tree transmit hold-count *value*
no spanning-tree transmit hold-count
Команда с приставкой «**no**» устанавливает значение «6 пакетов в секунду».
Параметры команды:

value ограничение в диапазоне от 1 до 10 пакетов в секунду

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree transmit hold-count 10
admin@Switch(config)# end
admin@Switch#
```

10.1.16 spanning-tree mst max-hops

Команда глобальной настройки. Определяет число прыжков (hops) в MST-регионе перед тем, как пакет BPDU будет удален.
Синтаксис команды:
spanning-tree mst max-hops *value*
no spanning-tree mst max-hops
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

value количество прыжков (hops) в MST-регионе перед тем, как пакет BPDU будет удален, в диапазоне от 1 до 40

Значение по умолчанию:
По умолчанию устанавливается значение 20.
Пример команды:

```
admin@Switch(config)# spanning-tree mst max-hops 10
```

10.1.17 spanning-tree mst priority

Команда глобальной настройки. Устанавливает приоритет устройства для указанного поддерева (instance) Spanning Tree.

Синтаксис команды:

spanning-tree mst *instance* **priority** *value*

no spanning-tree mst *instance* **priority**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды

instance	идентификатор поддерева Spanning Tree в диапазоне от 0 до 4095
value	приоритет устройства для указанного поддерева Spanning Tree в диапазоне от 0 до 61440 с шагом 4096. Чем меньше значение приоритета, тем выше вероятность того, что коммутатор будет выбран в качестве корневого коммутатора

Значение по умолчанию:

По умолчанию устанавливается значение 32768.

Коммутатор с наименьшим приоритетом является корневым коммутатором Spanning Tree.

Пример команды:

```
admin@Switch(config)# spanning-tree mst 1 priority 4096
```

10.1.18 spanning-tree mst configuration

Команда глобальной настройки. Вход в режим настройки MST-региона (Multiple Spanning Tree).

Синтаксис команды:

spanning-tree mst configuration

Использование команды:

Для того чтобы несколько устройств находилось в одном MST-регионе, они должны иметь одинаковое отображение VLAN на поддеревья, одинаковые ревизии конфигурации и одинаковое имя.

Пример команды:

```
admin@Switch(config)# spanning-tree mst configuration
admin@Switch(config-mst)# instance 1 vlan 10-20
admin@Switch(config-mst)# name region1
admin@Switch(config-mst)# revision 1
```

10.1.19 abort (настройка MST)

Команда режима настройки MST-региона. Выход из режима настройки MST-региона без сохранения внесенных изменений.

Синтаксис команды:
abort
Пример команды:

```
admin@Switch(config-mst)# abort
admin@Switch(config)#
```

10.1.20 commit (настройка MST)

Команда режима настройки MST-региона. Применение внесенных изменений.
Синтаксис команды:
commit
Пример команды:

```
admin@Switch(config)# spanning-tree mst configuration
admin@Switch(config-mst)# commit
```

10.1.21 exit (настройка MST)

Команда режима настройки MST-региона. Выход из режима настройки MST-региона с применением внесенных изменений.
Синтаксис команды:
exit
Пример команды:

```
admin@Switch(config)# spanning-tree mst configuration
admin@Switch(config-mst)# exit
admin@Switch(config)#
```

10.1.22 instance (настройка MST)

Команда режима настройки MST-региона. Добавление одного или нескольких VLAN к поддереву MST.

ВНИМАНИЕ

Всего можно задать не более 128 поддеревьев MST, включая нулевое!

Синтаксис команды:
instance *instance-to-add* **vlan** *vlan-range*
no instance *instance-to-remove* **[vlan** *vlan-range***]**
Команда с приставкой «**no**» удаляет указанные или все VLAN из указанного поддерева MST и добавляет их в поддерево MST по умолчанию (нулевое).

Параметры команды:

instance-to-add	номер поддерева MST в диапазоне от 0 до 4095
instance-to-remove	номер поддерева MST в диапазоне от 1 до 4095
vlan-range	набор VLAN в диапазоне от 1 до 4094. Для указания диапазона необходимо использовать дефис. Для указания последовательности необходимо использовать запятую

Значение по умолчанию:

По умолчанию все VLAN добавляются в CIST (Common and Internal Spanning Tree) – поддерево 0.

Использование команды:

Для того чтобы несколько устройств находилось в одном MST-регионе, они должны иметь одинаковое отображение VLAN на поддеревья, одинаковую ревизию конфигурации и одинаковое имя.

Команда «**no instance 1 vlan 10-20**» равносильна команде «**instance 0 vlan 10-20**».

Пример команды:

```
admin@Switch(config)# spanning-tree mst configuration
admin@Switch(config-mst)# instance 1 vlan 10-20
```

10.1.23 name (настройка MST)

Команда режима настройки MST-региона. Установка имени конфигурации MST.

Синтаксис команды:

name *string*

no name

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

string	текстовая строка длиной до 32 символов

Значение по умолчанию:

Имя по умолчанию – пустая строка.

Пример команды:

```
admin@Switch(config)# spanning-tree mst configuration
admin@Switch(config-mst)# name region1
```

10.1.24 revision (настройка MST)

Команда режима настройки MST-региона. Установка номера версии конфигурации MST.

Синтаксис команды:

revision *level*

no revision

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

level номер версии конфигурации MST в диапазоне от 0 до 65535 символов

Значение по умолчанию:

По умолчанию используется значение 0.

Пример команды:

```
admin@Switch(config)# spanning-tree mst configuration
admin@Switch(config-mst)# revision 1
```

10.1.25 spanning-tree guard

Команда режима настройки сетевых интерфейсов. Включение Root Guard или Topology Change Guard на интерфейсе. Root Guard запрещает интерфейсу становиться корневым портом устройства. Topology Change Guard предотвращает передачу извещения об изменении топологии сети на другие интерфейсы.

Синтаксис команды:

spanning-tree guard {root | topology-change}

no spanning-tree guard {root | topology-change}

Команда с приставкой «**no**» отключает Root Guard или Topology Change Guard на интерфейсе.

Значение по умолчанию:

По умолчанию Root Guard и Topology Change Guard отключены.

Пример команды:

```
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# spanning-tree guard root
```

10.1.26 spanning-tree mst hello-time

Команда режима настройки сетевых интерфейсов. Установка интервала отправки BPDU.

Синтаксис команды:

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds период отправки BPDU в диапазоне от 1 до 10 секунд

Значение по умолчанию:

По умолчанию используется значение 2 секунды.

Использование команды:

При установке периода отправки BPDU должно выполняться следующее соотношение: Max-Age >= 2 * (Hello-Time + 1)

Пример команды:

```
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# spanning-tree mst hello-time 5
```

10.1.27 spanning-tree mst cost

Команда режима настройки сетевых интерфейсов. Установка внутренней стоимости пути для порта. При возникновении петли Spanning Tree учитывает стоимость пути при выборе интерфейса для передачи.

Синтаксис команды:

spanning-tree mst *instance* **cost {auto | *value*}**

no spanning-tree mst *instance* **cost**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

instance	номер поддерева MST в диапазоне от 0 до 4095
auto	автоматическое определение стоимости пути по скорости соединения
value	стоимость пути в диапазоне от 1 до 200 000 000

Значение по умолчанию:

По умолчанию производится автоматическое определение стоимости пути по скорости соединения.

Пример команды:

```
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# spanning-tree mst 1 cost 35000
```

10.1.28 spanning-tree mst port-priority

Команда режима настройки сетевых интерфейсов. Установка приоритета порта.

Синтаксис команды:

spanning-tree mst *instance* **port-priority** *value*

no spanning-tree mst *instance* **port-priority**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

instance	номер поддерева Spanning Tree в диапазоне от 0 до 4095
value	приоритет порта в диапазоне от 0 до 240 с шагом 16

Значение по умолчанию:

По умолчанию устанавливается значение 128.

Пример команды:

```
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# spanning-tree mst 2 port-priority 144
```

10.1.29 spanning-tree vlan

Команда глобальной настройки. Установка глобальных настроек режима PVRST Spanning Tree.

ВНИМАНИЕ

Всего можно настроить не более 128 VLAN для PVRST!

Синтаксис команды:

spanning-tree vlan *vlan-id* {**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority*}

no spanning-tree vlan *vlan-id* {**forward-time** *seconds* | **hello-time** *seconds* | **maxage** *seconds* | **priority** *priority*}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
forward-time *seconds*	время перехода портов в режим передачи данных (“forwarding”) при изменении топологии сети в диапазоне от 6 до 30 секунд
hello-time *seconds*	интервал отправки Hello BPDU в диапазоне от 1 до 2 секунд
max-age *seconds*	время старения информации от корневого моста в диапазоне от 6 до 40 секунд
priority *priority*	приоритет моста в диапазоне от 0 до 61440 с шагом 4096

Значение по умолчанию:

- время перехода в режим передачи данных (“forwarding”) равно 15 секундам;
- интервал отправки Hello BPDU равен 2 секундам;
- время старения равно 20 секундам;
- приоритет моста равен 32768.

Использование команды:

Команда «**spanning-tree vlan**» используется для установки глобальных настроек режима PVRST Spanning Tree.

Настройки игнорируются устройством, если режим работы Spanning-Tree не равен PVRST.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# spanning-tree vlan 2 hello-time 1
admin@Switch(config)#
```

10.1.30 show current

Команда настройки MST-региона. Вывод текущей примененной конфигурации MST.

Синтаксис команды:

show current

Использование команды:

Команда «**show current**» используется для вывода текущей примененной конфигурации MST.

Пример команды:

```
admin@Switch(config-mst)# show current
Name: [region1]
Revision: 1
Instance   VLANs
--------   -----
0          1-9,21-4094
1          10-20
```

10.1.31 show pending

Команда настройки MST-региона. Вывод измененной, но еще не примененной конфигурации MST.

Синтаксис команды:

show pending

Использование команды:

Команда «**show pending**» используется для вывода измененной, но еще не примененной конфигурации MST.

Пример команды:

```
admin@Switch(config-mst)# show pending
There are no changes.
admin@Switch(config-mst)#
```

10.1.32 show spanning-tree

Команда, доступная из любого режима. Вывод информации о состоянии и настройках Spanning Tree.

Синтаксис команды:

show spanning-tree [interface *interface-id* **| vlan** *vlan-id* **| summary]**

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)
vlan-id	идентификатор VLAN. Параметр доступен только в режиме PVRST
summary	вывод сводной информации для всех интерфейсов

Использование команды:

Команда «**show spanning-tree**» используется для вывода информации о состоянии и настройках Spanning-Tree. Команда без параметров выводит информацию о настройках Spanning Tree и корневом мосту.

Интерфейсы Ethernet могут находиться в следующих состояниях Spanning Tree:

– «disabled» – на интерфейсе заблокированы прием и передача данных. В данном состоянии находятся все интерфейсы, на которых отсутствует физическое соединение;
– «blocking» – на интерфейсе заблокированы прием и передача данных. В данном состоянии находятся все интерфейсы, которые находятся на запасном пути, а также интерфейсы, которые не добавлены в топологию;
– «learning» – на интерфейсе заблокированы прием и передача данных, устройство заносит в таблицу MAC-адресов все MAC-адреса из приходящих пакетов. В данном состоянии находятся все интерфейсы перед переходом в режим передачи данных для улучшения стабильности сети;
– «forwarding» – интерфейс работает в режиме приема и передачи данных.

Команда предоставляет состояние и настройки для поддеревьев MST.

Примеры команды:

```
admin@Switch(config)# show spanning-tree interface gigabitethernet 0/1

BPDU filter: disable Link type: auto
BPDU guard: disable Portfast: disable

Inst.    Role State    Cost          Prio.Nbr   Vlans      mapped
-----    ----------    ----------    --------   -----      ------
0        root          forwarding    200000     128.1      1, 3-4094
1        designated    forwarding    200000     128.1      2
```

```
admin@Switch# show spanning-tree summary
Bridge is in MSTP mode

Name          Discarding   Learning     Forwarding   STP Active
----------    ----------   --------     ----------   ----------
Instance 0    0            0            2            2
Instance 1    0            0            1            1
----------    ----------   --------     ----------   ----------
2 Instance(s) 0            0            3            3
```

```
admin@Switch(config)# show spanning-tree
Bridge is in MSTP mode
MST instance 0
------------
VLANs mapped: 1, 3-4094
Root
  Priority                        0
  MAC-address                     00:1B:28:02:6C:60
  Cost                            242000
  Port                            gigabitethernet0/1
Regional root
  Priority                        32768
  MAC-address                     00:1B:28:01:97:A0
```

```
Cost 0
  Remaining hops                19
Bridge
  Priority                      32768
  MAC-address                   00:1B:28:01:97:A0
Configured settings
  Forward time                  15 sec
  Hello time                    2 sec
  Max age                       20 sec
Operational settings
  Forward time                  15 sec
  Hello time                    2 sec
  Max age                       20 sec
  Transmit hold count           6 pps
Interface           Role         State         Cost    Prio.Nbr   Type
------------------  ----------   ----------    ------  --------   ----
gigabitethernet0/1  root         forwarding    200000  128.1      auto
gigabitethernet0/2  designated   forwarding    200000  128.7      auto

MST instance 1
-----------
VLANs mapped: 2
Root
  Priority                      32769
  MAC-address                   00:1B:28:01:97:A0
  Cost                          0
  Port                          no port
Bridge
  Priority                      32769
  MAC-address                   00:1B:28:01:97:A0

Interface           Role         State         Cost    Prio.Nbr   Type
------------------  ----------   ----------    ------  --------   ----
gigabitethernet0/3  designated   forwarding    200000  128.1      auto
```

10.1.33 show spanning-tree mst

Команда, доступная из любого режима. Вывод информации о конфигурации и состоянии поддеревьев MST.

Синтаксис команды:

show spanning-tree mst *instance*

Параметры команды:

instance номер поддерева MST в диапазоне от 0 до 4095

Использование команды:

Команда «**show spanning-tree mst**» используется для вывода информации о конфигурации и состоянии поддеревьев MST.

Примеры команды:

```
admin@Switch(config)# show spanning-tree mst 0
MST instance 0
------------
VLANs mapped: 1, 11-4094

Root
  Priority                0
  MAC-address             00:1B:28:00:8D:80
  Cost                    24000
  Port                    gigabitethernet0/1
Regional root
  Priority                32768
  MAC-address             00:1B:28:01:43:60
  Cost                    0
  Remaining hops          29
Bridge
  Priority                32768
  MAC-address             00:1B:28:01:43:60
Configured settings
  Forward time            15 sec
  Hello time              2 sec
  Max age                 20 sec
Operational settings
  Forward time            15 sec
  Hello time              2 sec
  Max age                 20 sec
  Transmit hold count     6 pps

Interface                 Role         State        Cost    Prio.Nbr   Type
--------------------      --------     --------     ------  --------   ----
tengigabitethernet0/1     disabled     disabled     200000  128.1      auto
tengigabitethernet0/2     disabled     disabled     200000  128.2      auto
gigabitethernet0/1        disabled     disabled     20000   128.25     auto
gigabitethernet0/2        disabled     disabled     20000   128.26     auto
gigabitethernet0/3        designated   forwarding   20000   128.27     auto
gigabitethernet0/4        root         forwarding   20000   128.28     auto
```

```
admin@Switch(config)# show spanning-tree mst 1
MST instance 1
------------
VLANs mapped: 2

Root
Priority                        8193
MAC-address                     00:1B:28:01:43:60
Cost                            0
Port                            no port
Bridge
Priority                        8193
MAC-address                     00:1B:28:01:43:60
Interface           Role        State        Cost    Prio.Nbr   Type
-----------------   --------    --------     ------  --------   ----
gigabitethernet0/1  disabled    disabled     20000   128.25     auto
gigabitethernet0/2  disabled    disabled     20000   128.26     auto
gigabitethernet0/3  designated  forwarding   20000   128.27     auto
gigabitethernet0/4  designated  forwarding   20000   128.28     auto
```

10.1.34 show spanning-tree mst configuration

Команда, доступная из любого режима. Вывод конфигурации MST-региона.

Синтаксис команды:

show spanning-tree mst configuration

Использование команды:

Команда «**show spanning-tree mst configuration**» используется для вывода конфигурации MST-региона.

Для того чтобы несколько устройств находилось в одном MST-регионе, они должны иметь одинаковое отображение VLAN на поддеревья, одинаковую ревизию конфигурации и одинаковое имя.

Примеры команды:

```
admin@Switch(config)# show spanning-tree mst configuration
Name: [REGION1]
Revision: 0
Instance     VLANs
--------     ---------
0            1,11-4094
1            2
2            3-10
```

10.1.35 show spanning-tree statistics

Команда доступна из любого режима. Вывод статистики принятых и отправленных BPDU пакетов, принятых и отправленных BPDU topology-change пакетов для каждого порта в состоянии UP. Также показывает время с момента прихода последнего topology-change и количество переходов порта в режим FORWARDING.

Синтаксис команды:

show spanning-tree statistics

Примеры команды:

```
admin@Switch(config)# show spanning-tree statistics
BDPU Packets
------------
                                                          Last seen    Last seen                  Last fwd
                                                          recv TCN,    sent TCN,    Fwd state     transition,
Interface              Recv  Sent  Recv TCN   Sent TCN    s ago        s ago        transition    s ago
--------------------   ----  ----  --------   --------    -----        -----        ----------    ----------
tengigabitethernet0/1  0     0     0          0           -            -            0             -
tengigabitethernet0/2  0     0     0          0           -            -            0             -
Last TCN packet was received - seconds ago
Last TCN packet sent - seconds ago
```

10.2 Настройка ERPS

10.2.1 clear erps

Команда фундаментального режима. Очистка счетчиков статистики групп ERPS.

Синтаксис команды:

clear erps [*groups* **] statistics**

Описание синтаксиса:

groups	список номеров групп ERPS в диапазоне от 1 до 64

Режим команды:

Фундаментальный режим.

Уровень доступа:

15.

Указания по применению:

Если команда введена без аргументов.

Пример команды:

Следующий пример показывает, как очистить счетчики статистики всех групп ERPS:

```
admin@Switch# clear erps statistics
admin@Switch(config)#
```

10.2.2 erps command

Команда фундаментального режима. Применение команды управления ERPS.

Синтаксис команды:

erps *group* **command { force | manual | clear } { porta | portb }**

no erps *group* **command [porta] [portb]**

Используйте команду «**no erps command**» для отмены команды управления ERPS.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
force	команда форсированной настройки
manual	команда ручной настройки
clear	команда очистки
porta	переключение на порт 0
portb	переключение на порт 1

Режим команды:

Фундаментальный режим.

Уровень доступа:

15.

Примеры команды:

Следующий пример показывает, как применить команду ручного переключения на порт 1 для группы ERPS 1:

```
admin@Switch# erps 1 command manual portb
admin@Switch(config)#
```

10.2.3 erps guard

Команда глобальной настройки. Установка значения таймера Guard ERPS.

Синтаксис команды:

erps *group* **guard** *guard_time_ms*

no erps *group* **guard**

Используйте команду «**no erps guard**» для установки значения по умолчанию.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
guard_time_ms	значение таймера в диапазоне от 10 до 2000 миллисекунд

Значение по умолчанию:

500 миллисекунд.

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Примеры команды:

Следующий пример показывает, как установить значение таймера Guard 200 миллисекунд для группы ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 guard 200
admin@Switch(config)#
```

10.2.4 erps holdoff

Команда глобальной настройки. Установка значения таймера Holdoff ERPS.

Синтаксис команды:

erps *group* **holdoff** *holdoff_time_ms*

no erps *group* **holdoff**

Используйте команду «**no erps holdoff**» для установки значения по умолчанию.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
holdoff_time_ms	значение таймера в диапазоне от 0 до 10000 миллисекунд

Значение по умолчанию:

0 миллисекунд.

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Примеры команды:

Следующий пример показывает, как установить значение таймера Holdoff 300 миллисекунд для группы ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 holdoff 300
admin@Switch(config)#
```

10.2.5 erps major

Команда глобальной настройки. Добавление основного кольца группы ERPS после команд «**erps** *group* **guard** *guard_time_ms*», «**erps** *group* **raps-vlan** {*vlans*}».

Синтаксис команды:

erps *group* **major porta interface** *port_type port0* **portb interface** *port_type port1* **[interconnect]**

no erps *group* **major**

Используйте команду «**no erps major**» для удаления группы ERPS.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
major	главное кольцо
porta	порт 0 ERPS
port_type	тип порта (GigabitEthernet или TengigabitEthernet)
port0	идентификатор порта в формате «номер коммутатора/номер порта»
portb	порт 1 ERPS
port1	идентификатор порта в формате «номер коммутатора/номер порта»
interconnect	главное кольцо подключено через другие

Значение по умолчанию:

Основное кольцо ERPS отсутствует.

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Пример команды:
Следующий пример показывает, как добавить основное кольцо группы ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 major porta interface GigabitEthernet 1/1 portb interface
GigabitEthernet 1/2
admin@Switch(config)#
```

10.2.6 erps mep

Команда глобальной настройки. Установка номеров MEP, ассоциированных с группой ERPS.

Синтаксис команды:
erps *group* **mep porta sf** *p0_sf* **aps** *p0_aps* **portb sf** *p1_sf* **aps** *p1_aps*
no erps *group* **mep**
Используйте команду «**no erps mep**» для установки значения по умолчанию.
Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
porta	порт 0 ERPS
p0_sf	номер SignalFail MEP порта 0
p0_aps	номер APS MEP порта 0
portb	порт 1 ERPS
p1_sf	номер SignalFail MEP порта 1
p1_aps	номер APS MEP порта 1

Значение по умолчанию:
MEP не ассоциированы с группой ERPS.
Режим команды:
Режим глобальной настройки.
Уровень доступа:
15.
Пример команды:
Следующий пример показывает, как установить номера MEP, ассоциированных с группой ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 mep porta sf 1 aps 1 portb sf 2 aps 2
admin@Switch(config)#
```

10.2.7 erps revertive

Команда глобальной настройки. Включение режима автоматического восстановления на основном маршруте.

Синтаксис команды:
erps *group* **revertive** *wtr_time_minutes*
no erps *group* **revertive**

Используйте команду «**no erps revertive**» для отключения режима.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
wtr_time_minutes	значение интервала времени, по истечении которого происходит восстановление, в диапазоне от 1 до 12 минут

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Пример команды:

Следующий пример показывает, как включить режим автоматического восстановления на основном маршруте через 2 минуты на группе ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 revertive 2
admin@Switch(config)#
```

10.2.8 erps rpl

Команда глобальной настройки. Установка режима работы узла с каналом защиты кольца (Ring Protection Link).

Синтаксис команды:

erps *group* **rpl { owner | neighbor } { porta | portb }**

no erps *group* **rpl**

Используйте команду «**no erps rpl**» для установки значения по умолчанию.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
owner	узел является владельцем канала защиты кольца
neighbor	узел является соседом канала защиты кольца
porta	каналом защиты кольца является порт 0
portb	каналом защиты кольца является порт 1

Значение по умолчанию:

Узел не является смежным с каналом защиты кольца.

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Примеры:

Следующий пример показывает, как назначить узел владельцем канала защиты кольца на порту 1 для группы ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 rpl owner portb
admin@Switch(config)#
```

10.2.9 erps sub

Команда глобальной настройки. Добавление дополнительного кольца группы ERPS.

Синтаксис команды:

erps *group* **sub port0 interface** *port_type port0* **{port1 interface** *port_type port1* **| interconnect** *group_int***}[virtual-channel]**

no erps *group*

Используйте команду «**no erps**» для удаления группы ERPS.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
porta	порт 0 ERPS
port_type	тип порта (GigabitEthernet или TengigabitEthernet)
port0	идентификатор порта в формате «номер коммутатора/номер порта»
portb	порт 1 ERPS
port1	идентификатор порта в формате «номер коммутатора/номер порта»
interconnect	главное кольцо подключено через другие
group_int	номер основной группы главного кольца

Значение по умолчанию:

Дополнительное кольцо ERPS отсутствует.

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Пример команды:

Следующий пример показывает, как добавить дополнительное кольцо группы ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 sub porta interface tengigabitethernet 0/2 portb interface
tengigabitethernet 0/3
admin@Switch(config)#
```

10.2.10 erps topology-change propagate

Команда глобальной настройки. Включение распространения изменений топологии ERPS.

Синтаксис команды:

erps *group* **topology-change propagate**

no erps *group* **topology-change propagate**

Используйте команду «**no erps topology-change propagate**» для отключения функции.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64

Значение по умолчанию:

Распространение изменений топологии ERPS отключено.

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Примеры:

Следующий пример показывает, как включить распространение изменений топологии группы ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 topology-change propagate
admin@Switch(config)#
```

10.2.11 erps version

Команда глобальной настройки. Установка версии ERPS.

Синтаксис команды:

erps *group* **version { 1 | 2 }**

no erps *group* **version**

Используйте команду «**no erps version**» для установки значения по умолчанию.

Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
1	ERPS версии 1
2	ERPS версии 2

Значение по умолчанию:

ERPS версии 2.

Режим команды:

Режим глобальной настройки.

Уровень доступа:

15.

Примеры команды:
Следующий пример показывает, как установить версию ERPS 2 для группы 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 version 2
admin@Switch(config)#
```

10.2.12 erps vlan

Команда глобальной настройки. Установка списка VLAN, защищаемых группой ERPS.

Синтаксис команды:
erps *group* **vlan {** *vlans* **}**
no erps *group* **vlan**
Используйте команду «**no erps vlan**» для удаления VLAN из списка.
Описание синтаксиса:

group	номер группы ERPS в диапазоне от 1 до 64
vlans	список VLAN в диапазоне от 1 до 4095

Значение по умолчанию:
Ни один VLAN не входит в список защищаемых.
Режим команды:
Режим глобальной настройки.
Уровень доступа:
15.
Пример команды:
Следующий пример показывает, как установить список защищаемых VLAN «1-10» для группы ERPS 1:

```
admin@Switch# configure terminal
admin@Switch(config)# erps 1 vlan 1-10
admin@Switch(config)#
```

10.2.13 show erps

Команда фундаментального режима. Вывод информации о группах ERPS.
Синтаксис команды:
show erps [*groups* **]**
Описание синтаксиса:

groups	(опционально) список номеров групп ERPS в диапазоне от 1 до 64

Режим команды:
Фундаментальный режим.
Уровень доступа:
15.

Примеры команды:

Следующий пример показывает, как вывести информацию о группе ERPS 1:

```
admin@SW3(config)# show erps 1

ERPS Information
Global Status           : Enable
Group number            : 1
--------------------------------
R-APS VLAN              : 23
Ring Status             : Enable
West Port               : tengigabitethernet 0/17 (Blocked)
East Port               : tengigabitethernet 0/19 (Forwarding)
RPL Port                : West port
Protected VLANs         : 0
RPL Owner               : Enable
Holdoff Time            : 0 milliseconds
Guard Time              : 100 milliseconds
WTR Time                : 1 minutes
Current Ring State      : Idle
```

10.3 Настройка обнаружения петель в сети

10.3.1 set interface active

Фундаментальная команда. Включение интерфейса, который находится в состоянии «Err disable». Команда доступна только пользователю с правами администратора.

Синтаксис команды:

set interface active [*interface-id*]

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:

Команда используется для включения интерфейсов, которые сконфигурированы как активные, но были отключены системой.

Пример команды:

```
admin@Switch# set interface active gigabitethernet 1/1
```

10.3.2 loopback-detection enable (глобальная настройка)

Команда глобальной настройки. Включение Loopback Detection на устройстве.

Синтаксис команды:

loopback-detection enable

no loopback-detection enable

Команда с приставкой «**no**» выключает Loopback Detection.

Значение по умолчанию:

По умолчанию Loopback Detection отключен.

Использование команды:

Данная команда используется для включения режима обнаружения возникновения петель в сети на всем устройстве. Для включения режима обнаружения возникновения петель в сети на интерфейсе необходимо использовать команду настройки интерфейса «**loopback-detection enable**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# loopback-detection enable
```

10.3.3 loopback-detection logging

Команда глобальной настройки. Включение журналирования событий обнаружения петель.

Синтаксис команды:

loopback-detection logging

no loopback-detection logging

Команда с приставкой «**no**» отключает журналирование.

Значение по умолчанию:

Журналирование событий обнаружения петель отключено.

Использование команды:

Команда «**loopback-detection logging**» используется для включения журналирования событий обнаружения петель.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# loopback-detection logging
admin@Switch(config)#
```

10.3.4 loopback-detection mode

Команда глобальной настройки. Устанавливает режим обнаружения возникновения петель в сети.

Синтаксис команды:

loopback-detection mode {*src-mac-addr* | *base-mac-addr*}

no loopback-detection mode

Команда с приставкой «**no**» устанавливает режим по умолчанию «*src-macaddr*».

Параметры команды:

src-mac-addr	MAC-адрес назначения LBD-пакета представляет собой MAC-адрес интерфейса источника
base-mac-addr	MAC-адрес назначения LBD-пакета представляет собой базовый MAC-адрес устройства

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# loopback-detection mode src-mac-addr
```

10.3.5 loopback-detection interval

Команда глобальной настройки. Задает интервал времени между LBD-пакетами.

Синтаксис команды:

loopback-detection interval *seconds*

no loopback-detection interval

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал времени между LBD-пакетами в диапазоне от 30 до 60 секунд

Значение по умолчанию:

По умолчанию устанавливается значение 30 секунд.

Использование команды:

Данная команда не применима к обработке BPDU-пакетов Spanning Tree.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# loopback-detection interval 45
```

10.3.6 loopback-detection enable (конфигурация интерфейса)

Команда настройки интерфейса (Ethernet). Включение Loopback Detection на интерфейсе.

Синтаксис команды:

loopback-detection enable

no loopback-detection enable

Команда с приставкой «**no**» выключает Loopback Detection.

Значение по умолчанию:

По умолчанию Loopback Detection отключен.

Использование команды:

Данная команда используется для включения режима обнаружения возникновения петель в сети на интерфейсе. Для включения режима обнаружения возникновения петель в сети на всем устройстве необходимо использовать команду глобальной конфигурации «**loopback-detection enable**».

Передача LBD-пакетов осуществляется, только если состояние Spanning Tree интерфейса – «forwarding».

Если режим STP – MSTP, то функция обнаружения возникновения петель может быть включена только на интерфейсах с выключенным STP.

Интерфейс должен быть членом VLAN для его PVID, иначе LBD-пакеты не принимаются устройством.

Интерфейс должен быть настроен на прием пакетов только с тегом, иначе LBD-пакеты не принимаются устройством.

При передаче LBD-пакетов учитываются пользовательские MAC ACL. Поэтому LBD-пакет может быть удален явным правилом отклонения («deny rule») и имплицитным правилом «deny all rule».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 1/4
admin@Switch(config-if)# loopback-detection enable
```

10.3.7 show loopback-detection

Фундаментальная команда. Вывод информации о режиме обнаружения возникновения петель в сети.

Синтаксис команды:

show loopback-detection [*interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Пример команды:

```
admin@Switch# show loopback-detection
Loopback detection: Enabled
Mode: src-mac-addr
LBD packets interval: 30 Seconds
Interface   Loopback Detection
---------   ------------------
gi0/1       Enabled
gi0/2       Disabled
...
```

10.4 Настройка UDLD

10.4.1 debug udld

Команда фундаментального режима. Включение отладки UDLD.

Синтаксис команды:

debug udld {events | packets | registries}

no debug udld {events | packets | registries}

Команда с приставкой «**no**» отключает отладку UDLD.

Параметры команды:

events	отображение информации о событиях протокола UDLD
packets	отображение информации об отправленных и полученных пакетах UDLD
registries	вывод сообщений при смене состояний интерфейса. Регистрация служебных UDLD сообщений

Пример команды:

```
admin@Switch# debug udld events
admin@Switch#
```

10.4.2 udld reset

Команда фундаментального режима. Восстанавливает все интерфейсы, отключенные функцией errdisable.

Синтаксис команды:

udld reset

Пример команды:

```
admin@Switch# udld reset
admin@Switch#
```

10.4.3 udld enable

Команда глобальной настройки. Включение UDLD глобально и включение UDLD в обычном режиме на оптических портах.

Синтаксис команды:

udld {enable | aggressive}

no udld

Команда с приставкой «**no**» отключает UDLD глобально.

Параметры команды:

aggressive	включение UDLD глобально и включение UDLD в агрессивном режиме
enable	включение UDLD глобально и включение UDLD в обычном режиме на оптических портах

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# udld enable
admin@Switch(config)#
```

10.4.4 udld message

Команда глобальной настройки. Настройка интервала сообщений UDLD.

Синтаксис команды:

udld message time *value*

no udld message time

Команда с приставкой «**no**» выставляет значение по умолчанию – 15 секунд.

Параметры команды:

value выбор интервала сообщений UDLD в диапазоне от 7 до 90 секунд

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# udld message time 74
admin@Switch(config)#
```

10.4.5 udld port

Команда настройки интерфейса (Ethernet). Включение UDLD на интерфейсе в соответствии с глобальной настройкой.

Команда с приставкой «**no**» отключает UDLD на интерфейсе.

Синтаксис команды:

udld port [aggressive]

no udld port

Параметры команды:

aggressive включение UDLD в агрессивном режиме

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# udld port
admin@Switch (config-if)#
```

10.4.6 show udld

Команда доступна из любого режима. Вывод информации о состоянии и настройках UDLD.

Синтаксис команды:

show udld [*interface-id***] [global] [neighbors]**

Параметры команды:

interface-id	вывод информации о состоянии и настройках UDLD для конкретного интерфейса
global	вывод информации о глобальных настройках UDLD
neighbors	вывод информации об установленных соседях UDLD

Пример команды:

```
admin@Switch# show udld gigabitethernet 0/1

Interface gigabitethernet 0/1
---
Port enable admin state: Global
Port enable oper state: No data
Current bidirectional state: No data
Current operational state: No data
Message interval: 15
Time out interval: undefined
No multiple neighbors detected

admin@Switch#
```

11 Зеркалирование портов

11.1 Настройка зеркалирования

11.1.1 monitor session

Команда глобальной настройки. Создание настройки сессии мониторинга (зеркалирования) трафика.

Синтаксис команды:

monitor session *session-number*

no monitor session *session-number*

Команда с приставкой «**no**» удаляет сессию мониторинга.

Параметры команды:

session-number номер сессии от 1 до 8

Значение по умолчанию:

По умолчанию сессии мониторинга отсутствуют.

Использование команды:

Команда «**monitor session**» используется для создания настройки сессии мониторинга (зеркалирования) трафика. При создании сессия находится в отключенном состоянии. Команда «**no shutdown**» в режиме настройки сессии мониторинга используется для активации сессии.

Коммутатор поддерживает до двух одновременно активных сессий мониторинга, если они зеркалируют разные направления трафика: одна сессия зеркалирует входящее направление, а другая – исходящее направление. При зеркалировании входящего и исходящего направления в каждый момент времени может быть активна только одна сессия.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# monitor session 5
admin@Switch(config-monitor)#
```

Примечание – При включенной функции мониторинга (monitor session) может произойти зеркалирование первого пакета с портов, на которых не задан параметр «source interface», но которые находятся в одной подсети и в одном VLAN с портом, к которому осуществляется зеркалирование. Данное поведение является особенностью реализации и анализа пакетов.

11.1.2 source

Команда настройки сессии мониторинга. Добавление портов-источников в сессию мониторинга (зеркалирования) трафика.

Синтаксис команды:

source {**interface** *interface-list* | **vlan** *vlan-list* } [**rx** | **tx** | **both**]

no source {**interface** *interface-list* | **vlan** *vlan-list* }

Команда с приставкой «**no**» удаляет порты-источники из сессии мониторинга.

Параметры команды:

interface-list	список интерфейсов вида «gigabitethernet0/1-3»
vlan-list	список VLAN вида «1,3-5»
rx | tx | both	направление трафика, которое необходимо зеркалировать: rx – входящее, tx – исходящее, both - входящее и исходящее. Для VLAN доступно только зеркалирование входящего направления

Значение по умолчанию:

По умолчанию порты-источники не заданы.

Использование команды:

Команда «**source**» используется для добавления портов-источников в сессию мониторинга (зеркалирования) трафика.

Коммутатор поддерживает до двух одновременно активных сессий мониторинга, если они зеркалируют разные направления трафика: одна сессия зеркалирует входящее направление, а другая – исходящее направление. При зеркалировании входящего и исходящего направления в каждый момент времени может быть активна только одна сессия.

Проверка корректности настроек происходит при применении команды. Если в процессе применения возникает конфликт настроек, например, после применения команды получится, что две активные сессии зеркалируют входящее направление, то настройка не применяется.

Для VLAN доступно только зеркалирование входящего направления.

В качестве источников зеркалируемого трафика разрешается указывать физические порты и VLAN в пределах одной сессии мониторинга.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# monitor session 5
admin@Switch(config-monitor)# source vlan 10 rx
```

11.1.3 destination

Команда настройки сессии мониторинга. Настройка порта-назначения сессии мониторинга (зеркалирования) трафика.

Синтаксис команды:

destination interface *interface-id* [**remote vlan** *vlan-id*]

no destination

Команда с приставкой «**no**» удаляет порт-назначения из сессии мониторинга.

Параметры команды:

interface-id	идентификатор интерфейса. Может быть указан только один физический порт
remote vlan *vlan-id*	номер VLAN, который будет использоваться для передачи зеркалируемого трафика (RSPAN VLAN)

Значение по умолчанию:

По умолчанию порт-назначения не задан.

Использование команды:

Команда «**destination**» используется для настройки порта-назначения сессии мониторинга (зеркалирования) трафика. Может быть указан только один физический порт.

Коммутатор поддерживает как локальное зеркалирование (SPAN), так и удаленное (RSPAN). Для зеркалирования трафика с удаленного коммутатора необходимо указать номер VLAN, который будет использоваться для передачи зеркалируемого трафика.

Проверка корректности настроек происходит при применении команды. Если в процессе применения возникает конфликт настроек, например, если настраиваемая сессия включена и указанный порт назначения уже используется в другой активной сессии мониторинга, то настройка не применяется.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# monitor session 5
admin@Switch(config-monitor)# destination interface gigabithernet 0/1 remote vlan 10
```

11.1.4 shutdown

Команда настройки сессии мониторинга. Отключение сессии мониторинга (зеркалирования) трафика.

Синтаксис команды:

shutdown

no shutdown

Команда с приставкой «**no**» включает сессию мониторинга.

Значение по умолчанию:

По умолчанию сессия отключена.

Использование команды:

Команда «**shutdown**» используется для отключения сессии мониторинга (зеркалирования) трафика. Команда «**no shutdown**» используется для включения сессии мониторинга.

Вновь создаваемые сессии всегда находятся в отключенном состоянии.

Проверка корректности настроек происходит при применении команды «**no shutdown**». Если в процессе применения возникает конфликт настроек с другой активной сессией, то настройка не применяется.

Варианты конфликтов:

– одинаковые направления зеркалирования (входящее или исходящее);

– одинаковые порты назначения.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# monitor session 5
admin@Switch(config-monitor)# no shutdown
```

11.1.5 show monitor session

Фундаментальная команда. Вывод настроек одной или всех сессий мониторинга (зеркалирования) трафика.

Синтаксис команды:

show monitor session [**all** | *session-number*]

Параметры команды:

session-number номер сессии от 1 до 8

all вывод настроек для всех сессий

Использование команды:

Команда «**show monitor session**» используется для вывода настроек одной или всех сессий мониторинга (зеркалирования) трафика.

Пример команды:

```
admin@Switch# show monitor session 1
Session 1
-------
Source Ports:
  RX Only: None
  TX Only: None
  Both: te0/1
Source VLANs:
  RX Only: None
  TX Only: None
  Both: None
Destination Ports: te0/1
Dest RSPAN VLAN: None
```

Обозначения, использованные в примере приведены в таблице 12.

Таблица 12 – Обозначения, использованные в примере

Обозначение	Описание
Source ports	Порты-источники, трафик которых зеркалируется
Source VLANs	VLAN-источники, трафик которых зеркалируется
RX only	Источники, для которых зеркалируется только входящий трафик

Продолжение таблицы 12

Обозначение	Описание
TX only	Источники, для которых зеркалируется только исходящий трафик
Both	Источники, для которых зеркалируется входящий и исходящий трафик
Destination ports	Порты, на которые производится зеркалирование трафика
Dest RSPAN VLAN	Тег VLAN, который присваивается зеркалируемому трафику

11.1.6 remote-span

Команда настройки интерфейса VLAN. Назначение VLAN в качестве RSPAN VLAN, используемого для передачи отзеркаленного трафика. Команда с приставкой «**no**» отключает данную функцию.

Синтаксис команды:

remote-span

Пример команды:

```
admin@Switch(config-if)# remote-span
admin@Switch(config-if)# exit
admin@Switch(config)# monitor session 5
admin@Switch(config-monitor)# source interface gigabitethernet 0/2 tx
admin@Switch(config-monitor)# destination interface gigabithernet 0/1 remote vlan 10
admin@Switch(config-monitor)# exit
admin@Switch(config)# exit
```

12 Агрегация интерфейсов

12.1 Агрегация интерфейсов

12.1.1 channel-group

Команда настройки интерфейса. Добавление порта в группу агрегации.

Синтаксис команды:

channel-group *channel-number* **{active | passive | on}**

no channel-group

Команда с приставкой «**no**» удаляет порт из группы агрегации.

Параметры команды:

channel-number	номер группы агрегации, в которую будет добавлен порт, в диапазоне от 1 до 64
active	активный режим LACP. Протокол LACP отправляет пакеты на портах по таймерам
passive	пассивный режим LACP. Протокол LACP отправляет пакеты только в ответ на принятые пакеты
on	режим безусловной агрегации. Протокол LACP отключен

Значение по умолчанию:

Порты не являются членами групп агрегации.

Использование команды:

Команда «**channel-group**» используется для добавления порта в группу агрегации. В одной группе агрегации может быть до 8 портов. Членами группы агрегации могут быть порты только одного типа. То есть одновременное членство портов gigabitethernet и tengigabitethernet в одной группе невозможно.

Рекомендуется использовать активный режим LACP на портах, входящих в группу агрегации. Не использовать разные режимы агрегации в пределах одной группы агрегации.

Группы агрегации позволяют увеличить пропускную способность соединения путем объединения нескольких портов в общую группу. Группа агрегации является отдельным интерфейсом.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabithethernet 0/1
admin@Switch(config-if)# channel-group 1 active
admin@Switch(config-if)#
```

12.1.2 port-channel load-balance

Команда глобальной настройки. Установка режима балансировки трафика на группах агрегации.

Синтаксис команды:

port-channel load-balance {src-dst-mac | src-dst-ip | src-dst-mac-ip | src-dst-ipport | src-dst-mac-ip-port}

no port-channel load-balance

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

src-dst-mac	балансировка по MAC-адресу источника и назначения
src-dst-ip	балансировка по IP-адресу источника и назначения
src-dst-mac-ip	балансировка по MAC-адресу источника и назначения, IP-адресу источника и назначения
src-dst-ip-port	балансировка по IP-адресу источника и назначения, L4 порту источника и назначения
src-dst-mac-ip-port	балансировка по MAC-адресу источника и назначения, IP-адресу источника и назначения, L4 порту источника и назначения

Значение по умолчанию:

По умолчанию режим «**src-dst-ip-port**».

Использование команды:

Команда «**port-channel load-balance**» используется для установки режима балансировки трафика на группах агрегации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# port-channel load-balance src-dst-ip
admin@Switch(config)#
```

12.2 Агрегация с помощью LACP

12.2.1 debug lacp

Команда фундаментального режима. Включение отладки LACP.
Синтаксис команды:
debug lacp {**all | events | fsm | packets**}
no debug lacp {**all | events | fsm | packets**}
Команда с приставкой «**no**» отключает отладку LACP.
Параметры команды:

all	вывод всех отладочных событий (включает/ выключает все ключи отладки)
events	вывод событий
fsm	вывод изменений в машинах состояний LACP
packets	вывод содержимого пакетов LACP

Значение по умолчанию:
Отладка отключена.
Использование команды:
Команда «**debug lacp**» используется для включения отладки LACP.
Пример команды:

```
admin@Switch# debug lacp all
admin@Switch#
```

12.2.2 lacp system-priority

Команда глобальной настройки. Настройка приоритета системы, анонсируемого протоколом LACP.
Синтаксис команды:
lacp system-priority *priority*
no lacp system-priority
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

priority	приоритет системы в диапазоне от 1 до 65535

Значение по умолчанию:
Приоритет равен 1.
Использование команды:
Команда «**lacp system-priority**» используется для настройки приоритета системы, анонсируемого протоколом LACP.

Приоритет системы влияет на выбор ведущего устройства между двумя устройствами, связанными по группе агрегации. Меньшее значение настройки означает более высокий приоритет (1 – максимальный приоритет, 65535 – минимальный приоритет). Устройство с большим приоритетом определяет порядок (приоритет) подключения портов в группе агрегации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lacp system-priority 50
admin@Switch(config)#
```

12.2.3 lacp port-priority

Команда настройки интерфейса (Ethernet). Настройка приоритета порта, анонсируемого протоколом LACP.

Синтаксис команды:

lacp port-priority *priority*

no lacp port-priority

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

priority	приоритет порта в диапазоне от 1 до 65535

Значение по умолчанию:

Приоритет равен 1.

Использование команды:

Команда «**lacp port-priority**» используется для настройки приоритета порта, анонсируемого протоколом LACP.

Приоритет порта определяет порядок подключения портов в группе агрегации. Меньшее значение настройки означает более высокий приоритет (1 – максимальный приоритет, 65535 – минимальный приоритет). Если порты имеют одинаковый приоритет, то выбирается порт с меньшим номером.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lacp port-priority 100
admin@Switch(config-if)#
```

12.2.4 lacp timeout

Команда настройки интерфейса (Ethernet). Настройка интервала таймаута LACP на порту.

Синтаксис команды:

lacp timeout {**long** | **short**}

no lacp timeout

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

long	длинный интервал таймаута (90 секунд)
short	короткий интервал таймаута (3 секунды)

Значение по умолчанию:

Длинный интервал таймаута (90 секунд).

Использование команды:

Команда «**lacp timeout**» используется для настройки интервала таймаута LACP на порту.

Интервал таймаута влияет на частоту отправки управляющих пакетов LACP на группе агрегации. Установка длинного интервала позволяет уменьшить количество управляющего трафика LACP, передаваемого в единицу времени.

Использовать короткий интервал таймаута, если агрегирующие устройства соединены между собой не напрямую, а через другое оборудование, например, через медиаконвертеры, не поддерживающие технологию LLCF. В этом случае потеря связи между транспортным оборудованием не всегда может привести к потере связи на самих агрегируемых портах устройства, а значит, устройство не узнает о потере связи со смежным устройством. Это приводит к потере связи на группе агрегации до истечения времени таймаута LACP. Уменьшение интервала таймаута позволяет сократить время сходимости группы агрегации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lacp timeout short
admin@Switch(config-if)#
```

12.2.5 show lacp

Команда, доступная из любого режима. Вывод информации о состоянии, настройках и статистики LACP на определенном интерфейсе.

Синтаксис команды:

show lacp *interface-id* [**parameters | statistics | protocol-state**]

Параметры команды:

interface-id	идентификатор интерфейса
parameters	вывод параметров
statistics	вывод статистики
protocol-state	вывод состояния протокола

Использование команды:

Команда «**show lacp**» используется для вывода информации о состоянии, настройках и статистики LACP на определенном интерфейсе.

Пример команды:

```
admin@Switch# show lacp gigabitethernet 0/1
Port gigabitethernet 0/1
 LACP Parameters
  Actor
   System Priority: 1
   System MAC Addr: 00:1B:28:12:34:56
   Port Admin key: 30
   Port Oper key: 30
   Port Oper number: 21
   Port Admin priority: 1
   Port Oper priority: 1
   Port Admin timeout: LONG
   Port Oper timeout: LONG
   LACP Activity: ACTIVE
   Aggregation: AGGREGATABLE
   Synchronization: FALSE
   Collecting: FALSE
   Distributing: FALSE
   Expired: FALSE
  Partner
   System Priority: 0
   System MAC Addr: 00:00:00:00:00:00
   Port Admin key: 0
   Port Oper key: 0
   Port Oper number: 0
   Port Admin priority: 0
   Port Oper priority: 0
   Port Admin timeout: LONG
   Port Oper timeout: LONG
   LACP Activity: PASSIVE
   Aggregation: AGGREGATABLE
   Synchronization: FALSE
   Collecting: FALSE
   Distributing: FALSE
   Expired: FALSE

 LACP Statistics:
  LACP PDUs sent: 2
  LACP PDUs received: 2
 LACP Protocol State:
  LACP State Machines:
   Receive FSM: Port Disabled State
   Mux FSM: Detached State
  Control Variables:
   BEGIN: FALSE
   LACP_Enabled: TRUE
   Ready_N: FALSE
   Selected: UNSELECTED
   Port_moved: FALSE
```

```
    NNT: FALSE
    Port_enabled: FALSE
  Timer counters:
    Periodic TX Timer: 0
    Current While Timer: 0
    Wait While Timer: 0
```

12.2.6 show lacp port-channel

Команда, доступная из любого режима. Вывод информации о состоянии LACP на всех или определенной группе агрегации.

Синтаксис команды:

show lacp port-channel [*port-channel-number*]

Параметры команды:

port-channel-number номер агрегированного канала в диапазоне от 1 до 64

Использование команды:

Команда «**show lacp port-channel**» используется для вывода информации о состоянии LACP на всех или определенной группе агрегации.

Пример команды:

```
admin@Switch# show lacp port-channel 1
Port-Channel 1:
  Port Type: 1000 Ethernet
  Active Port Limit: 8
  Actor
    System Priority: 1
    MAC Address: 00:1B:28:12:34:56
    Admin Key: 29
    Oper Key: 29
  Partner
    System Priority: 0
    MAC Address: 00:00:00:00:00:00
    Oper Key: 14
```

13 Туннелирование

13.1 Настройка PPPoE Intermediate-Agent

13.1.1 Общая информация

PPPoE Intermediate Agent перехватывает PADI и PADR пакеты, добавляя дополнительные данные, идентифицирующие местоположение пользователя, например MAC коммутатора, порт коммутатора, VLAN пользователя. Эти идентификаторы **circuit-id** и **remote-id** помещаются внутрь тега Vendor-specific (он же Vendor-tag).

Также PPPoE IA включает в себя функцию доверенного порта, который позволяет заблокировать прием нежелательных пакетов со стороны сервера на недоверенные порты.

Формирование идентификаторов circuit-id и remote-id

Уровни приоритетов при формировании тэга circuit-id:

1. Проверяется задана ли строка идентификатора **circuit-id** на интерфейсе на нужном VLAN.
2. Проверяется задана ли строка идентификатора **circuit-id** на всем интерфейсе.
3. Проверяется задан ли формат тэга **identifirer-string**.
4. Проверяется задан ли формат тэга **access-node-id**.
5. Если не задан ни один из вариантов выше, используется формат по умолчанию.

Формат тэга **circult-id**, если задана строка идентификатора на нужном vlan интерфейса или на всем интерфейсе: <*string*> – длина 63 символа.

Формат тэга **circult-id**, если используется **identifirer-string** в зависимости от *option*:

1. <spv> – {ID} {Type}{StackNum}{Dlm1}{PortNum}{Dlm2}{VlanID};
2. <sp> – {ID} {Type}{StackNum}{Dlm1}{PortNum};
3. <sv> – {ID} {Type}{StackNum}{Dlm1}{VlanID};
4. <pv> – {ID} {Type}{PortNum}{Dlm1}{VlanID};
5. {ID} – <*string*> – 32 символа.

Формат тэга **circult-id**, если используется **access-node-id**:

1. {ID} {Type} {StackNum}:{PortNum}:{VlanID};
2. {ID} – <*string*> – 32 символа.

Формат тэга **circuit-id** по умолчанию:

1. {ID} {Type} {StackNum}:{PortNum}:{VlanID};
2. {ID} – IP-address vlan, по которому пришел пакет (если он не задан устанавливается значение 0.0.0.0).

Описание общих элементов формирования тэга circult-id:

1. {ID} {Type} – тип порта (например gigabitethernet);
2. {StackNum} – стековый номер устройства порта;
3. {PortNum} – номер порта;
4. {VlanID} – номер Vlan;
5. {Dlm1}{Dlm2} – разделителители (если не задан {Dim2}, он автоматически равняется {Dim1}).

Уровни приоритетов при формировании тэга remote-id:

1. Проверяется задана ли строка идентификатора **remote-id** на интерфейсе на нужном vlan.
2. Проверяется задана ли строка идентификатора **remote-id** на всем интерфейсе.
3. Если не задан ни один из вариантов выше, используется формат по умолчанию.

Формат тэга **remote-id**, если задана строка идентификатора на vlan или на интерфейсе: <*string*> – длина 63 символа.

Строка идентификатора **remote-id**, если используется формат по умолчанию: <*mac-address*> – формируется из MAC-адреса устройства, на котором работает PPPoE-IA.

13.1.2 Настройка PPPoE-IA

Для того, чтобы функция PPPoE-IA начала инкапуслировать идентификаторы, нужно:

1. Включить PPPoE-IA в глобальном режиме. Для этого используются следующие команды:

```
configure terminal
pppoe intermediate-agent
end
```

2. Включить PPPoE-IA на интерфейсах, с которых будут приходить запросы PPPoE от клиентов, например:

```
configure terminal
interface tengigabitethernet 0/3
pppoe intermediate-agent trust
end
end
```

3. Включить режим доверенного порта на интерфейсах, с которых будут приходить PPPoE offer от серверов, например:

```
configure terminal
interface tengigabitethernet 0/3
pppoe intermediate-agent trust
end
end
```

13.1.3 clear pppoe intermediate-agent statistics

Команда фундаментального режима. Удаление статистики обнаруженных пакетов PPPoE на всех интерфейсах.

Синтаксис команды:

clear pppoe intermediate-agent statistics

Использование команды:

Команда «**clear pppoe intermediate-agent statistics**» используется для обнуления статистики по обнаруженным пакетам PPPoE на всех интерфейсах.

Пример команды:

```
admin@Switch# clear pppoe intermediate-agent statistics
admin@Switch#
```

13.1.4 pppoe intermediate-agent

Команда глобальной настройки. Включение функции “pppoe intermediate-agent” на устройстве.

Синтаксис команды:

pppoe intermediate-agent

no pppoe intermediate-agent

Команда с приставкой «**no**» отключает функцию “pppoe intermediate-agent” на устройстве.

Значение по умолчанию:

По умолчанию функция “pppoe intermediate-agent” выключена.

Использование команды:

Команда «**pppoe intermediate-agent**» используется для включения функции “pppoe intermediate-agent” на устройстве.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# pppoe intermediate-agent
admin@Switch(config)#
```

13.1.5 pppoe intermediate-agent format-type

Команда глобальной настройки. Описание см. далее в пп. Использование команды.

Синтаксис команды :

pppoe intermediate-agent format-type {**access-node-identifier string** *string* **| generic-error-message string** *string* **| identifier-string string** *string* **[option {pv | sp | spv | sv} [delimiters { , | . | : | / | # | ; }[{ , | . | : | / | # | ; }]]] }**

no pppoe intermediate-agent format-type {access-node-identifier | generic-error-message | identifier-string}

Параметры команды:

access-node-identifier string *string*

настройка идентификатора узла доступа *string* с **circuit-id**. Команда «**no**» удаляет настройку формата **access-node-identifier**.
string – строка, размером максимум 32 символа.
Пример тега: “ADBD tengigabitethernet 00:17:0001”

identifier-string string *string* **[option {pv | sp | spv | sv} [delimiters { , | . | : | / | # | ; }]]]**

настройка добавляемых полей **circuit-id**:

- **sp** – слот и порт;
- **sv** – слот и vlan;
- **pv** – порт и vlan;
- **spv** – слот, порт и vlan.

В случае использования **spv** может быть указано 2 различных разделителя **delimiter** друг за другом, без пробелов или других знаков, например так: “**#/**”, тогда первый разделитель примет значение: “**#**”, а второй – “**/**”.
Если в составе **delimiters** есть “**;**”, то весь параметр **delimiters** нужно указывать в одинарных кавычках, например: ’**;#**’.
string – строка, размером максимум 32 символа.
Пример тега: “ADBD tengigabitethernet 17:0001”.
Команда «**no**» удаляет настройку формата **identifier-string**

generic-error-message string *string*	настройка текста ошибки, посылаемой в случае превышения размера пакета максимальной величины. Размер пакета не должен превышать 1484 байта. По умолчанию не задано. *string* – строка, размером максимум 63 символа. Команда «**no**» – удаляет текст ошибки, посылаемой в случае превышения размера пакета максимальной величины. В этом случае будет послан обратно пакет с тегом ошибки, но без текста

Использование команды:

Команда с параметром «**access-node-identifier string** *string*» используется для настройки формата строки идентификации подопции **circult-id**.

Команда с параметром «**identifier-string string** *string* **[option { pv | sp | spv | sv } [delimiters { , | . | : | / | # | ; } [{ , | . | : | / | # | ; }]]]**» используется для настройки набора параметров и разделителей между ними, которые используются для формирования подопции **circult-id**.

Команда с параметром «**generic-error-message string** *string*» используется для установки текста сообщения, об ошибке превышения размера PADI или PADR пакета, отправляемого “PPPoE intermediate-agent” в PADO или PADS пакетах.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# pppoe intermediate-agent format-type identifier-string string ADBD
option pv delimiters :/
admin@Switch(config)#
```

13.1.6 pppoe intermediate-agent

Команда настройки интерфейса. Включение функции “pppoe intermediate-agent” на интерфейсе.

Синтаксис команды:

pppoe intermediate-agent [vlan *vlan-range* **]**

no pppoe intermediate-agent [vlan *vlan-range* **]**

Команда с приставкой «**no**» отключает функцию “pppoe intermediate-agent” на интерфейсе.

Параметры команды:

vlan-range	список vlan от 1 до 4094, на которых будет включена функция

Значение по умолчанию:

По умолчанию функция “pppoe intermediate-agent” выключена.

Использование команды:

Команда «**pppoe intermediate-agent**» используется для включения функции “pppoe intermediate-agent” на интерфейсе. Если не указан параметр vlan, то распространяется на все vlan используемые на интерфейсе. Если параметр vlan указан, то распространяется на все указанные в «*vlan-range*».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/5
admin@Switch(config-if))# pppoe intermediate-agent
```

13.1.7 pppoe intermediate-agent format-type

Команда настройки интерфейса. Задает строку **circult-id** или **remote-id** на порту. Настройка **format-type** на интерфейсе, будет приоритетнее, чем настройка **format-type** глобального уровня. Если указан параметр vlan, настройки распространяются только на указанные vlan, если параметр vlan не указан, настройки распростаняются на все vlan на интерфейсе.

Синтаксис команды:

pppoe intermediate-agent format-type {**remote-id | circuit-id**} **string** *string* [**vlan** *vlan-range*]

no pppoe intermediate-agent format-type {**remote-id | circuit-id**} [**vlan** *vlan-range*]

Команда с приставкой «**no**» удаляет настройки идентификаторов **circult-id** или **remote-id** на порту.

Параметры команды:

remote-id	настройка идентификатора **remote-id**, добавляемая коммутатором
circuit-id	настройка идентификатора **circult-id**, добавляемая коммутатором
string	строка, размером максимум 63 символа
vlan-range	список vlan от 1 до 4094, на которые будет распространяться настройка идентификаторов

Значение по умолчанию:

По умолчанию идентификаторы на интерфейсе не заданы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# pppoe intermediate-agent format-type circuit-id string ADBD
admin@Switch(config-if)# pppoe intermediate-agent format-type remote-id string TEST
vlan 9
```

13.1.8 pppoe intermediate-agent trust

Команда настройки интерфейса. Включение режима доверенного порта на интерфейсе.

Синтаксис команды:

pppoe intermediate-agent trust

no pppoe intermediate-agent trust

Команда с приставкой «**no**» выключает режим доверенного порта на интерфейсе.

Значение по умолчанию:

По умолчанию на всех интерфейсах выключен режим доверенного порта.

Использование команды:

Команда добавляет интерфейс к списку доверенных. Интерфейсы, к которым подключены PPPoE-серверы, настраиваются как доверенные. Интерфейсы, к которым подключены пользователи, настраиваются как недоверенные.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# pppoe intermediate-agent trust
admin@Switch(config-if)#
```

13.1.9 pppoe intermediate-agent limit rate

Команда настройки интерфейса. Задает максимально допустимое количество пакетов, которое порт может получить в секунду.

Синтаксис команды:

pppoe intermediate-agent limit rate *number*

no pppoe intermediate-agent limit rate

Команда с приставкой «**no**» убирает ограничение на максимально допустимое количество пакетов.

Параметры команды:

number	количество пакетов от 0 до 4294967295

Значение по умолчанию:

По умолчанию ограничение не установлено.

Использование команды:

Данная команда устанавливает максимально допустимое количество пакетов, которое порт может получить в секунду, в случае превышения этого значения порт уходит в состояние **errdisable**, так же в CLI шлется сообщение:

«%PPPOE-3-PORT_LIMIT_RATE_EXCEEDED: tengigabitethernet0/17 disabled because the number of allowed received packets per second was exceeded on it».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# pppoe intermediate-agent limit rate 10000
```

13.1.10 pppoe intermediate-agent vendor-tag strip

Команда настройки интерфейса. Из пакетов, полученных от сервера, удаляет тег Vendor-Specific.

Синтаксис команды:

pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Значение по умолчанию:

По умолчанию тег Vendor-Specific не удаляется.

Использование команды:

Данная команда настраивается на портах, к которым подключены PPPoE-серверы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# pppoe intermediate-agent vendor-tag strip
```

13.1.11 show pppoe intermediate-agent info

Команда, доступная из любого режима. Отображает текущие настройки функции “PPPoE intermediate-agent”.

Синтаксис команды:

show pppoe intermediate-agent info [*interface* **]**

Использование команды:

Команда «**show pppoe intermediate-agent info**» используется для вывода настроек функции “PPPoE intermediate-agent”. В выводе отображаются глобальные настройки и основные настройки интерфейсов. Если указан параметр «*interface*», выводит подробные настройки PPPoE IA на интерфейсе.

Пример команды:

```
show pppoe intermediate-agent info tengigabitethernet 0/1
   Interface: tengigabitethernet0/1

   General settings:

   PPPOE Intermediate-Agent: disabled
   Trusted: yes
   Vendor-Tag Strip: no
   Rate Limit (pps): -
   Circuit-ID: -
   Operated Circuit-ID: IP tengigabitethernet 00:01:VID
   Remote-ID: -
   Operated Remote-ID: 00-1B-28-0E-67-98

   * {VID} - variable equal to the number of VLAN of received packet
   {IP} - variable equal to IP address of this VLAN. If no IP address then 0.0.0.0

   PPPOE Intermediate-Agent is enabled on following VLANs: none

   admin@Switch#
```

13.1.12 show pppoe intermediate-agent statistics

Команда, доступная из любого режима. Отображает статистику по всем пакетам PPPoE на всех интерфейсах. Если указан интерфейс, отображает статистику указанного интерфейса с дополнительной статистикой по vlan.

Синтаксис команды:

show pppoe intermediate-agent statistics [*interface* **]**

Использование команды:

Команда отображает статистику по всем пакетам: PADI, PADO, PADR, PADS, PADT. Так же отображает дополнительные поля:

- **Rate-limit-exceeded**: сколько раз на порту количество полученных пакетов в секунду превышало максимально допустимое;
- **Resp From untrusted**: количество полученных пакетов от сервера на недоверенные порты;
- **Req towards untrusted**: количество полученных пакетов от клиентов, направляемые на недоверенные порты;
- **Malformed packets**: количество неправильных или некорректных пакетов.

Пример команды:

```
admin@Switch# show pppoe intermediate-agent statistics tengigabitethernet0/1
                                        Rate-Limit   Resp from    Req towards  Malformed
Interface  All  PADI PADO PADR PADS PADT Exceeded     Untrusted    Untrusted    Packets
---------  ---  ---- ---- ---- ---- ---- --------     ---------    ---------    -------
Fa0/1      352  0    112  0    120  120  0            0            0            16
Vlan 4094: Packets received PADI = 0 PADO = 112 PADR = 0 PADS = 120 PADT = 120
```

14 DHCP

14.1 Настройка DHCP-сервера

14.1.1 clear ip dhcp binding

Команда фундаментального режима. Удаление всех или определенного назначенного IP-адреса из базы данных DHCP-сервера.

Синтаксис команды:

clear ip dhcp binding {*address* | **all**}

Параметры команды:

address	назначенный IP-адрес, который необходимо удалить
all	удаление всех назначенных IP-адресов

Использование команды:

Команда «**clear ip dhcp binding**» используется для удаления всех или определенного назначенного IP-адреса из базы данных DHCP-сервера.

Пример команды:

```
admin@Switch# clear ip dhcp binding 192.168.0.50
admin@Switch#
```

14.1.2 debug ip dhcp client

Команда фундаментального режима. Включение отладки DHCP-клиента.

Синтаксис команды:

debug ip dhcp client {all | events | packets}

no debug ip dhcp client {all | events | packets}

Команда с приставкой «**no**» отключает отладку DHCP-клиента.

Параметры команды:

all	вывод всей диагностической информации
events	вывод событий DHCP-клиента
packets	вывод информации о полученных и отправленных пакетах DHCP-клиентом

Пример команды:

```
admin@Switch# debug ip dhcp client all
admin@Switch#
```

14.1.3 debug ip dhcp server

Команда фундаментального режима. Включение отладки DHCP-сервера.

Синтаксис команды:

debug ip dhcp server {all | events | packets}

no debug ip dhcp server {all | events | packets}

Команда с приставкой «**no**» отключает отладку DHCP-сервера.

Параметры команды:

all	вывод всей диагностической информации
events	вывод событий DHCP-сервера
packets	вывод информации о полученных и отправленных пакетах DHCP-сервером

Пример команды:

```
admin@Switch# debug ip dhcp server all
admin@Switch#
```

14.1.4 ip dhcp excluded-address

Команда глобальной настройки. Добавление диапазона IP-адресов, которые DHCP-сервер не должен назначать DHCP-клиентам (исключаемые адреса).

Синтаксис команды:

ip dhcp excluded-address *low-address* [*high-address*]

no ip dhcp excluded-address *low-address* [*high-address*]

Команда с приставкой «**no**» удаляет диапазон IP-адресов, которые DHCP-сервер не должен назначать DHCP-клиентам.

Параметры команды:

low-address	исключенный IP-адрес или первый IP-адрес исключаемого диапазона адресов
high-address	последний IP-адрес в исключаемом диапазоне адресов

Значение по умолчанию:

По умолчанию весь пул IP-адресов может быть назначен.

Использование команды:

Команда «**ip dhcp excluded-address**» используется для добавления диапазона IP-адресов, которые DHCP-сервер не должен назначать DHCP-клиентам (исключаемые адреса).

По умолчанию DHCP-сервер выделяет DHCP-клиентам все адреса из настроенных пользователем диапазонов за исключением локальных адресов на интерфейсах устройства. Команда глобальной настройки «**ip dhcp excludedaddress**» позволяет исключить выделение IP-адреса или диапазона IP-адресов. Это может потребоваться, если некоторые адреса выделены статически или зарезервированы по каким-либо причинам.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# address 192.168.0.0 255.255.255.0
admin@Switch(config-dhcp-network)# exit
admin@Switch(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.10
admin@Switch(config)#
```

14.1.5 ip dhcp pool host

Команда глобальной настройки. Создание пула хостов DHCP (статической привязки IP-адреса клиента) на DHCP-сервере и запуск режима конфигурации пула хостов DHCP.

Синтаксис команды:

ip dhcp pool host *name*

no ip dhcp pool host *name*

Команда с приставкой «**no**» удаляет пул хостов DHCP.

Параметры команды:

name	имя пула хостов DHCP. Рекомендуемая длина: до 32 символов

Значение по умолчанию:

Пулы хостов отсутствуют.

Использование команды:

Команда «**ip dhcp pool host**» используется для создания пула хостов DHCP (статической привязки IP-адреса клиента) на DHCP-сервере и запуска режима конфигурации пула хостов DHCP.

Пул хостов DHCP настройку привязку IP-адреса только для одного клиента. Если необходимо создать статические IP-адреса для нескольких клиентов, то для каждого из них требуется создание отдельного пула хостов DHCP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool host myhostpool
admin@Switch(config-dhcp-host)# address 192.168.0.100
hardware-address 00:1B:28:00:BA:BA
```

14.1.6 ip dhcp pool network

Команда глобальной настройки. Создание пула сетей DHCP и переход в режим настройки пула сетей DHCP.

Синтаксис команды:

ip dhcp pool network *name*

no ip dhcp pool network *name*

Команда с приставкой «**no**» удаляет пул сетей DHCP.

Параметры команды:

name	имя пула адресов DHCP. Рекомендуемая длина: до 32 символов

Значение по умолчанию:

Пулы сетей отсутствуют.

Использование команды:

Команда «**ip dhcp pool network**» используется для создания пула сетей DHCP и перехода в режим настройки пула сетей DHCP.

Один пул сетей DHCP может содержать несколько подсетей, адреса из которых будет выделять DHCP-сервер. Локальные адреса на интерфейсах устройства автоматически удаляются из списка выделяемых адресов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# address 192.168.0.0 255.255.255.0
admin@Switch(config-dhcp-network)#
```

14.1.7 ip dhcp server

Команда глобальной настройки. Включение функции DHCP-сервера на устройстве.

Синтаксис команды:

ip dhcp server

no ip dhcp server

Команда с приставкой «**no**» отключает функцию DHCP-сервера на устройстве.

Значение по умолчанию:

По умолчанию DHCP-сервер выключен.

Использование команды:

Команда «**ip dhcp server**» используется для включения функции DHCP-сервера на устройстве.

DHCP-сервер позволяет динамически выделять IP-адреса хостам, подключенным к интерфейсам устройства

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp server
admin@Switch(config)#
```

14.1.8 address (настройка пулов хостов)

Команда настройки пулов хостов. Добавление привязки IP-адреса к клиенту.

Синтаксис команды:

address *ip-address* **{client-identifier** *unique-identifier* **| hardware-address** *macaddress***}**

no address *ip-address*

Команда с приставкой «**no**» удаляет привязку.

Параметры команды:

ip-address	IP-адрес клиента
unique-identifier	уникальный идентификатор клиента в виде шестнадцатеричной строки (вида “001B2800AABB05”)
hardware-address	MAC-адрес клиента. Байты MAC-адреса (задаются двумя шестнадцатеричными цифрами) должны быть разделены двоеточием

Значение по умолчанию:

Привязка IP-адреса отсутствует.

Использование команды:

Команда «**address**» используется для добавления привязки IP-адреса к клиенту. IP-адрес может быть привязан к аппаратному адресу (MAC-адресу) или идентификатору клиента.

Пул хостов DHCP добавляет привязку IP-адреса только для одного клиента. Если необходимо создать статические IP-адреса для нескольких клиентов, то для каждого из них требуется создание отдельного пула хостов DHCP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool host myhostpool
admin@Switch(config-dhcp-host)# address 192.168.0.100 255.255.255.0 hardware-address
00:1B:28:00:BA:BA
admin@Switch(config-dhcp-host)#
```

14.1.9 client-name

Команда настройки пула. Установка имени клиента.

Синтаксис команды:

client-name *name*

no client-name

Команда с приставкой «**no**» удаляет имя клиента.

Параметры команды:

name	имя клиента в виде текстовой строки из стандартных символов ASCII длиной до 32 символов. Имя клиента не должно включать имя домена. Например, имя “mail” не должно быть указано как “mail.plgn.ru”

Значение по умолчанию:

Имя клиента не определено.

Использование команды:

Команда «**client-name**» используется для установки имени клиента.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool host myhostpool
admin@Switch(config-dhcp-host)# client-name mail
admin@Switch(config-dhcp-host)#
```

14.1.10 address (настройка пулов сетей)

Команда настройки пулов сетей. Добавление сети в пул адресов DHCPсервера.

Синтаксис команды:

address {*network-number* | **low** *low-address* **high** *high-address*} {*mask* | *prefixlength*}

no address {*network-number* | **low** *low-address* **high** *high-address*} {*mask* | *prefixlength*}

Команда с приставкой «**no**» удаляет подсеть из пула адресов DHCP-сервера.

Параметры команды:

network-number	IP-адрес сети
low-address	первый IP-адрес в диапазоне адресов
high-address	последний IP-адрес в диапазоне адресов. mask маска подсети
prefix-length	длина префикса сети. Длина префикса является альтернативным методом указания маски подсети и должна предваряться символом “/” (слеш)

Значение по умолчанию:

Пустой пул адресов.

Использование команды:

Команда «**address**» используется для добавления сети в пул адресов DHCP-сервера.

Если в качестве аргумента команды указан IP-адрес сети, то первый выделяемый адрес будет равен первому адресу сети, а последний выделяемый адрес будет равен последнему адресу сети.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# address 192.168.0.0 255.255.255.0
admin@Switch(config-dhcp-network)#
```

14.1.11 lease

Команда настройки пулов сетей. Установка интервала времени, на который выделяются IP-адреса (время действия).

Синтаксис команды:

lease {*days* **[{***hours***} [***minutes***]] | infinite}**

no lease

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

days	время действия IP-адреса в днях
hours	время действия IP-адреса в часах. Параметр «days» должен быть указан перед параметром «hours»
minutes	время действия IP-адреса в минутах. Параметры «days» и «hours» должны быть указаны перед параметром «minutes»
infinite	неограниченное время действия IP-адреса

Значение по умолчанию:

IP-адреса выделяются на 1 час.

Использование команды:

Команда «**lease**» используется для установки интервала времени, на который выделяются IP-адреса (время действия).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# address 192.168.0.0 255.255.255.0
admin@Switch(config-dhcp-network)# lease infinite
admin@Switch(config-dhcp-network)#
```

14.1.12 default-router

Команда настройки пулов хостов и сетей. Установка списка IP-адресов шлюзов (маршрутизаторов) по умолчанию.

Синтаксис команды:

default-router *ip-address* [*ip-address2 ... ip-address8*]

no default-router

Команда с приставкой «**no**» удаляет список IP-адресов шлюзов (маршрутизаторов) по умолчанию.

Параметры команды:

ip-address	IP-адрес шлюза по умолчанию
ip-address2 ... ip-address8	IP-адреса дополнительных шлюзов по умолчанию. Поддерживается до 7 дополнительных IP-адресов

Значение по умолчанию:

IP-адреса шлюзов по умолчанию отсутствуют.

Использование команды:

Команда «**default-router**» используется для установки списка IP-адресов шлюзов (маршрутизаторов) по умолчанию.

IP-адреса шлюзов по умолчанию должны принадлежать той же сети, что и IP-адреса, назначаемые клиентам.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# address 192.168.0.0 255.255.255.0
admin@Switch(config-dhcp-network)# default-router 192.168.0.1
admin@Switch(config-dhcp-network)#
```

14.1.13 dns-server

Команда настройки пулов хостов и сетей. Установка списка IP-адресов DNScepверов.

Синтаксис команды:

dns-server *ip-address* [*ip-address2 ... ip-address8*]

no dns-server

Команда с приставкой «**no**» удаляет список IP-адресов DNS-серверов.

Параметры команды:

ip-address		IP-адрес DNS-сервера
ip-address2 *ipaddress8*	...	IP-адреса дополнительных DNS-серверов. Поддерживается до 7 дополнительных IP-адресов

Значение по умолчанию:

IP-адреса DNS-серверов отсутствуют.

Использование команды:

Команда «**dns-server**» используется для установки списка IP-адресов DNS-серверов.

Если IP-адреса DNS-серверов не заданы, то клиенты не смогут определить IP-адрес удаленного хоста по доменному имени и наоборот.

Если IP-адреса DNS-серверов находятся в подсети, отличной от подсети клиента, то необходимо указать IP-адрес шлюза по умолчанию с помощью команды «**default-router**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# address 192.168.0.0 255.255.255.0
admin@Switch(config-dhcp-network)# dns-server 192.168.0.2
admin@Switch(config-dhcp-network)#
```

14.1.14 domain-name

Команда настройки пулов хостов и сетей. Установка имени домена, к которому принадлежит DHCP-клиент.

Синтаксис команды:

domain-name *domain*

no domain-name

Команда с приставкой «**no**» удаляет имя домена.

Параметры команды:

domain	имя домена DHCP-клиента. Рекомендуемая длина: до 32 символов

Значение по умолчанию:

Имя домена не определено.

Использование команды:

Команда «**domain-name**» используется для установки имени домена, к которому принадлежит DHCP-клиент.

Имя клиента и имя домена позволяют сформировать полное доменное имя клиента – FQDN (Fully Qualified Domain Name).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# domain-name plgn.ru
admin@Switch(config-dhcp-network)#
```

14.1.15 next-server

Команда настройки пулов хостов и сетей. Установка IP-адреса следующего сервера (сервера с загрузочным файлом), используемого клиентом в процессе загрузки.

Синтаксис команды:

next-server *ip-address*

no next-server

Команда с приставкой «**no**» удаляет IP-адреса следующего сервера.

Параметры команды:

ip-address	IP-адрес следующего сервера, используемого клиентом в процессе загрузки, который обычно является TFTP-сервером

Значение по умолчанию:

IP-адрес сервера не определен.

Использование команды:

Команда «**next-server**» используется для установки IP-адреса следующего сервера (сервера с загрузочным файлом), используемого клиентомв процессе загрузки.

Клиент подключается к указанному серверу по протоколу SCP/TFTP для получения загрузочного файла. Команда «**bootfile**» используется для установки имени загрузочного файла, используемого клиентом в процессе загрузки.

Если IP-адрес следующего сервера находится в подсети, отличной от подсети клиента, то необходимо указать IP-адрес шлюза по умолчанию с помощью команды «**default-router**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# next-server 192.168.0.3
admin@Switch(config-dhcp-network)#
```

14.1.16 bootfile

Команда настройки пулов хостов и сетей. Установка имени загрузочного файла, используемого клиентом в процессе загрузки.

Синтаксис команды:

bootfile *filename*

no bootfile

Команда с приставкой «**no**» удаляет имя загрузочного файла.

Параметры команды:

filename	имя загрузочного файла, используемого клиентом в процессе загрузки. Рекомендуемая длина: до 128 символов

Значение по умолчанию:

Имя загрузочного файла не задано. **Использование команды:**

Команда «**bootfile**» используется для установки имени загрузочного файла, используемого клиентом в процессе загрузки. Команда «**next-server**» используется для установки IP-адреса следующего сервера (сервера с загрузочным файлом), используемого клиентом в процессе загрузки

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# next-server 192.168.0.3
admin@Switch(config-dhcp-network)# bootfile da_boot_file
admin@Switch(config-dhcp-network)#
```

14.1.17 option

Команда настройки пулов хостов и сетей. Добавление опции DHCP, отправляемой клиенту.

Синтаксис команды:

option *code* **{ascii** *ascii-string* **| hex** *hex-string* **| ip** *ip-address* **| ip-list** *ip-address...ip-address8***}**

no option *code*

Команда с приставкой «**no**» удаляет опции DHCP.

Параметры команды:

code	код опции DHCP в диапазоне от 1 до 254
ascii-string	текстовая строка (NVT ASCII) без пробельных символов
hex-string	шестнадцатеричная строка, каждый байт в которой состоит из двух шестнадцатеричных цифр
ip-address	IP-адрес
ip-address...ipaddress8	список IP-адресов. Могут быть указаны только для варианта «**option ip-list**»

Значение по умолчанию:

Опции не заданы.

Использование команды:

Команда «**option**» используется для добавления опции DHCP, отправляемой клиенту. Данная команда предназначена для настройки опций, которые не имеют выделенных команд настройки.

DHCP обеспечивает основу для передачи конфигурационной информации клиентам (хостам) в сети TCP/IP. DHCP позволяет передавать параметры конфигурации и другую управляющую информацию в полях опций DHCPсообщения. Текущий набор опций DHCP приведен в RFC2131 (DHCP).

Для опций в шестнадцатеричном формате строковый параметр должен содержать в себе все байты со значением опции, включая ведущие нули.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp pool network mynetworkpool
admin@Switch(config-dhcp-network)# option 2 hex 0005460
admin@Switch(config-dhcp-network)#
```

```
admin@Switch(config-dhcp-network)# option ip-list 69 192.168.0.4 192.168.0.5
admin@Switch(config-dhcp-network)#
```

14.1.18 show ip dhcp

Команда, доступная из любого режима. Вывод глобальных настроек DHCP-сервера.

Синтаксис команды:

show ip dhcp

Использование команды:

Команда «**show ip dhcp**» используется для вывода глобальных настроек DHCP-сервера.

Пример команды:

```
admin@Switch# show ip dhcp
DHCP server is enabled
```

14.1.19 show ip dhcp binding

Команда, доступная из любого режима. Вывод привязок IP-адресов, назначенных всем или определенному клиенту.

Синтаксис команды:

show ip dhcp binding [*ip-address*]

Параметры команды:

ip-address	IP-адрес клиента в привязке

Использование команды:

Команда «**show ip dhcp binding**» используется для вывода привязок IP-адресов, назначенных всем или определенному клиенту. Если команда введена без аргументов, то выводятся все привязки IP-адресов.

Пример команды:

```
admin@Switch# show ip dhcp binding
DHCP server enabled
The number of allocated entries is 3
The number of offered entries is 0
The number of declined entries is 0

IP address   Client ID/Hardware address   Expiration time      Type      State
------------ -------------------------   -----------------   -------   ---------
192.168.0.11 00:1B:28:C0:DE:01           01 Jun 2014 12:05   dynamic   allocated
192.168.0.12 00:1B:28:C0:DE:02           01 Jun 2014 12:10   dynamic   allocated
192.168.0.13 00:1B:28:C0:DE:03           01 Jun 2014 12:15   dynamic   allocated
```

14.1.20 show ip dhcp excluded-address

Команда, доступная из любого режима. Вывод диапазонов IP-адресов, которые DHCP-сервер не должен назначать DHCP-клиентам.

Синтаксис команды:

show ip dhcp excluded-address

Использование команды:

Команда «**show ip dhcp excluded-addresses**» используется для вывода диапазонов IP-адресов, которые DHCP-сервер не должен назначать DHCP-клиентам.

Пример команды:

```
admin@Switch# show ip dhcp excluded-address
From         To
-----------  ------------
192.168.0.1  192.168.0.10
```

14.1.21 show ip dhcp pool host

Команда, доступная из любого режима. Вывод настроек всех или определенного пула хостов DHCP.

Синтаксис команды:

show ip dhcp pool host [*address* | *name*]

Параметры команды:

address	IP-адрес клиента в пуле хостов DHCP
name	имя пула хостов DHCP

Использование команды:

Команда «**show ip dhcp pool host**» используется для вывода настроек всех или определенного пула хостов DHCP.

Примеры команды:

```
admin@Switch# show ip dhcp pool host 192.168.0.100
Name               IP address      Hardware address      Client identifier
----------         -------------   -----------------     -----------------
myhostpool         192.168.0.100   00:1B:28:00:BA:BA

Lease time         1 day
Next server        192.168.0.3
Bootfile           da_boot_file
DNS servers        192.168.0.2
Domain name        plgn.ru
Client name        mail
Default routers    192.168.0.1
Options:
Code               Value
----               -------
2                  0005460
69                 192.168.0.4 192.168.0.5
```

```
admin@Switch# show ip dhcp pool host
The number of host pools is 1
Name         IP address     Hardware address     Client identifier
----------   -------------  -----------------    -----------------
myhostpool   192.168.0.100  00:1B:28:00:BA:BA
```

14.1.22 show ip dhcp pool network

Команда, доступная из любого режима. Вывод настроек всех или определенного пула сетей DHCP.

Синтаксис команды:

show ip dhcp pool network *name*

Параметры команды:

name имя пула сетей DHCP

Использование команды:

Команда «**show ip dhcp pool network**» используется для вывода настроек всех или определенного пула сетей DHCP.

Пример команды:

```
admin@Switch# show ip dhcp pool network mynetworkpool
Name              Address range                Prefix length     Lease time
-------------     --------------------------   -------------     ----------
mynetworkpool     192.168.0.1 - 192.168.0.254  24                infinite

Next server       192.168.0.3
Bootfile          da_boot_file
DNS servers       192.168.0.2
Domain name       plgn.ru
Default routers   192.168.0.1

Options:
Code              Value
----              -------
2                 0005460
69                192.168.0.4 192.168.0.5
```

14.2 Настройка IPv6 DHCP-сервера

14.2.1 ipv6 dhcp server

Команда глобальной настройки. Включение функции dhcpv6 сервера на устройстве.

Синтаксис команды:

ipv6 dhcp server

no ipv6 dhcp server

Команда с приставкой «**no**» отключает функцию dhcpv6 сервера на устройстве.

Значение по умолчанию:

По умолчанию dhcpv6 сервер выключен.

Использование команды:

Команда «**ipv6 dhcp server**» используется для включения функции dhcpv6 сервера на устройстве.

dhcpv6 сервер позволяет динамически выделять ipv6-адреса хостам, подключенным к интерфейсам устройства.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 dhcp server
admin@Switch(config)#
```

14.2.2 address (настройка пулов сетей)

Команда настройки пулов сетей. Добавление сети в пул адресов dhcpv6 сервера.

Синтаксис команды:

address low *low ipv6-address* **high** *high ipv6-address ipv6-prefix*

Параметры команды:

low ipv6-address	первый ipv6-адрес в диапазоне адресов
high ipv6-address	последний ipv6-адрес в диапазоне адресов
ipv6-prefix	длина префикса сети. Длина префикса является альтернативным методом указания маски подсети и должна предваряться символом “/” (слеш)

Значение по умолчанию:

Пустой пул адресов.

Использование команды:

Команда «**address**» используется для добавления сети в пул адресов dhcpv6-сервера.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 dhcp pool network mynetworkpool
admin@Switch(config-dhcpv6-network)# address low 2001:0DB8:0000:ABCD::2 high
2001:0DB8:0000:ABCD::10 /64
admin@Switch(config-dhcpv6-network)#
```

14.2.3 dns-server

Настройка адреса DNS-сервера (опция 23).
Синтаксис команды:
dns-server *ip-address*
no dns-server
Команда с приставкой «**no**» удаляет ipv6-адрес DNS-сервера.
Параметры команды:

ip-address ipv6-адрес DNS-сервера

Значение по умолчанию:
ipv6-адрес DNS-сервера отсутствует.
Использование команды:
Команда «**dns-server**» используется для установки ipv6-адреса DNS-сервера.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 dhcp pool network mynetworkpool
admin@Switch((config-dhcpv6-network)# dns-server 2001:0DB8:0000:ABCD::2
```

14.2.4 clear ipv6 dhcp binding all

Команда фундаментального режима. Удаление всех ipv6-адресов из базы данных ipv6 DHCP-сервера.
Использование команды:
Команда «**clear ipv6 dhcp binding all**» используется для удаления всех из базы данных ipv6 DHCP-сервера.
Пример команды:

```
admin@Switch# clear ipv6 dhcp binding all
admin@Switch#
```

14.2.5 show ipv6 dhcp binding

Команда, доступная из любого режима. Вывод привязок ipv6-адресов, назначенных всем или определенному клиенту.
Синтаксис команды:
show ipv6 dhcp binding [*pool-name*]
Параметры команды:

pool-name имя пула dhcpv6

Использование команды:
Команда «**show ipv6 dhcp binding**» используется для вывода привязок ipv6-адресов, назначенных всем или определенному клиенту. Если команда введена без аргументов, то выводятся все привязки ipv6-адресов.

Пример команды:

```
admin@Switch# show ipv6 dhcp binding

DUID                TYPE    IAID   DDRESS
------------------  ------  ------  --------------------------
000100012A2A0A1160   na      0      2001 DB8 0 ABCD 0 0 0 2
```

14.3 Настройка IPv6 DHCP-клиента

14.3.1 ipv6 address dhcp

Команда режима интерфейса. Получение ipv6-адреса от сервера для этого интерфейса.

Синтаксис команды:

ipv6 address dhcp [{*domain-name* | *domain-name-servers* | *domain-name-servers domain-name* }]

Параметры команды:

domain-name	доменное имя
domain-name-servers	адрес домена
domain-name-servers domain-name	доменное имя и адрес домена

Режим команды:

Режим интерфейса.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ipv6 address dhcp
```

14.3.2 show ipv6 route

Фундаментальная команда. Вывод информации о текущем состоянии таблицы маршрутизации.

Синтаксис команды:

show ipv6 route [*all*]

Параметры команды:

all	выводит на экран детальную информацию обо всех маршрутах

Пример команды:

```
admin@Switch# show ipv6 route

Codes: C - connected, S - static, R - RIP, B - BGP,
       O - OSPF, IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2,
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       * - candidate default, > - selected route

> C* 2a02:1234:420a:100b::13/128 (240) directly connected

admin@Switch#
```

14.4 Настройка DHCP Relay

14.4.1 Общие положения

DHCP Relay предназначен для передачи широковещательных пакетов от DHCP-клиентов на DHCP-серверы, если они расположены в разных подсетях.

Устройство поддерживает две функции, реализующие функционал L3 DHCP Relay: DHCP Snooping и DHCP Relay, которые могут добавлять DHCP-опцию 82 (RFC3046) в проходящие пакеты. DHCP Snooping с добавлением опции 82 предоставляет прозрачную передачу DHCP-пакетов, если DHCP-клиент и DHCP-сервер находятся в одном VLAN. DHCP Relay с добавлением опции 82 предоставляет прозрачную передачу DHCP-пакетов от DHCP-клиентов на DHCP-серверы и наоборот, если они находятся в разных VLAN.

Устройство обеспечивает добавление и обработку двух подопций опции 82: Circuit ID (код 1) и Remote ID (код 2). Остальные подопции не добавляются и не обрабатываются устройством.

Алгоритм обработки опции 82 и поля адреса шлюза в DHCP-пакетах, полученных от DHCP-клиентов, приведены в таблице 13. Клиент может генерировать следующие типы пакетов: DHCPDISCOVER, DHCPREQUEST, DHCPDECLINE, DHCPRELEASE, DHCPINFORM.

Таблица 13 – Алгоритм обработки опции 82 и поля адреса шлюза в DHCP-пакетах, полученных от DHCP-клиентов

Параметры пакета	Действия DHCP Relay
Адрес шлюза равен 0.0.0.0 (поле “giaddr”) и отсутствует опция 82	В пакет добавляется опция 82 и передается соответствующему DHCP-серверу
Адрес шлюза равен 0.0.0.0 (поле “giaddr”) и присутствует опция 82	Пакет отбрасывается
Адрес шлюза не равен 0.0.0.0 (поле “giaddr”) и отсутствует опция 82	Пакет отбрасывается
Адрес шлюза не равен 0.0.0.0 (поле “giaddr”) и присутствует опция 82	Если адрес шлюза в пакете равен IP-адресу одного из локальных интерфейсов устройства, то пакет отбрасывается. В противном случае пакет передается соответствующему DHCP-серверу без опции 82

Отправка пакета от DHCP-клиента на DHCP-сервер выполняется следующим образом:

1. Определяется IP-адрес DHCP-сервера (или нескольких серверов), на который необходимо переправить пакет:

– если для VLAN, на котором получен пакет, настроен IP-адрес (или несколько IP-адресов) DHCP-сервера, то пакет будет отравлен на сервер, указанный в настройке VLAN;

– иначе, если настроен глобальный IP-адрес (или несколько IP-адресов) DHCP-сервера, то пакет будет отправлен на сервер, указанный в глобальной настройке;
– иначе, пакет будет отброшен.

2. Определяется исходящий интерфейс отправки:

– если ни на одном интерфейсе (VLAN) устройства не настроен IP-адрес, находящийся в одной подсети с DHCP-сервером, то пакет отбрасывается;
– выбирается первый по порядку интерфейс, на котором настроен IP-адрес, находящийся в одной подсети с DHCP-сервером;
– если интерфейс, на котором был принят пакет, и интерфейс, который выбран для передачи, совпадают, то пакет отбрасывается (исключение пересылки внутри одного и того же VLAN).

3. Если адрес шлюза в пакете равен 0.0.0.0 (поле “giaddr”), то его значение заменяется на IP-адрес интерфейса отправки.
4. Пакет передается через интерфейс отправки.

Алгоритм обработки DHCP-пакетов, полученных от DHCP-серверов:

1. Если пакет не содержит опции 82, то:

– если адрес шлюза (поле “giaddr”) не равен IP-адресу на интерфейсе-приемнике пакета и на одном из интерфейсов устройства (VLAN) настроен IP-адрес, находящийся в одной подсети с хостом, указанным в адресе шлюза, то пакет передается через соответствующий интерфейс;
– иначе пакет отбрасывается.

2. Иначе выполняются следующие действия:

– если MAC-адрес устройства и MAC-адрес в подопции Remote ID не совпадают, то пакет отбрасывается;
– если значению подопции Circuit ID не соответствует ни одно из значений локальных Circuit ID, настроенных на интерфейсах (VLAN), то пакет отбрасывается. Иначе для пакета устанавливается номер VLAN, который имеет настройку Circuit ID, равную значению Circuit ID в пакете;
– из пакета удаляется опция 82;
– пакет передается в установленный интерфейс и VLAN.

Администратор может изменить значения подопций Circuit ID и Remote ID (опция 82). По умолчанию в качестве значения Remote ID используется шестнадцатеричное (текстовое) представление MAC-адреса системы, а в качестве Circuit ID – текстовый идентификатор VLAN вида “vlanN”, где N – идентификатор VLAN (номер).

Настройки пользователя

1. Глобальные настройки:

- режим работы DHCP Relay: вкл, выкл.;
- добавление и удаление IP-адресов DHCP-серверов, используемых DHCP Relay;
- настройка формата подопции Remote ID опции 82: MAC-адрес устройства, имя устройства (sysName), произвольная текстовая строка (длина до 63 символов).

2. Настройки интерфейсов (VLAN):

- режим работы DHCP Relay: вкл, выкл.;
- добавление и удаление IP-адресов DHCP-серверов, используемых DHCP Relay;
- настройка формата подопций опции 82: Circuit ID и Remote ID;
- настройка формата подопции Circuit ID опции 82: текстовый идентификатор VLAN, произвольная текстовая строка (длина до 63 символов).

Дополнения и ограничения

Для работы DHCP Relay необходимо настроить IP-адрес на интерфейсе (VLAN), на который будут приниматься пакеты DHCP от клиентов.

DHCP Relay не поддерживает IPv6.

DHCP Relay получает копии DHCP-пакетов, поэтому широковещательные пакеты будут переправлены во все порты, находящиеся в том же VLAN, что и порт-источник независимо от решения DHCP Relay.

14.4.2 debug ip dhcp relay

Команда фундаментального режима. Включение отладки DHCP Relay.

Синтаксис команды:

debug ip dhcp relay {**all** | **events** | **packets**}

no debug ip dhcp relay {**all** | **events** | **packets**}

Команда с приставкой «**no**» отключает отладку DHCP Relay.

Параметры команды:

all	вывод всей диагностической информации
events	вывод событий DHCP Relay
packets	вывод информации о полученных и отправленных пакетах DHCP Relay

Пример команды:

```
admin@Switch# debug ip dhcp relay all
admin@Switch#
```

14.4.3 ip dhcp information option

Команда глобальной настройки. Включение вставки опции 82 в DHCP-пакеты механизмом DHCP Relay.

Синтаксис команды:

ip dhcp information option

Значение по умолчанию:

Вставка опции 82 отключена.

Использование команды:

Команда «**ip dhcp information option**» используется для включения вставки опции 82 в DHCP-пакеты механизмом DHCP Relay.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# no ip dhcp information option
admin@Switch(config)#
```

14.4.4 ip dhcp information option format remote-id

Команда глобальной настройки. Установка значения подопции Remote ID опции 82, вставляемой в пакеты механизмом DHCP Relay.

Синтаксис команды:

ip dhcp information option format remote-id {**string** *string* | **system-name**}

no ip dhcp information option format remote-id

Команда с приставкой «**no**» используется для установки значения по умолчанию.

Параметры команды:

string	текстовая строка длиной от 1 до 63 символов, которая будет использоваться в качестве Remote ID
system-name	в качестве Remote ID будет использоваться имя системы (параметр sysName)

Значение по умолчанию:

MAC-адрес устройства в шестнадцатеричном формате (текстовом).

Использование команды:

Команда «**ip dhcp information option format remote-id**» используется для установки значения подопции Remote ID опции 82, вставляемой в пакеты механизмом DHCP Relay.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp information option format remote-id string sometext
admin@Switch(config)#
```

14.4.5 ip dhcp relay enable

Команда глобальной настройки. Включение DHCP Relay на устройстве.

Синтаксис команды:

ip dhcp relay enable

no ip dhcp relay enable

Команда с приставкой «**no**» используется для отключения DHCP Relay на устройстве.

Значение по умолчанию:

DHCP Relay отключен.

Использование команды:

Команда «**ip dhcp relay enable**» используется для включения DHCP Relay на устройстве.

Команда настройки интерфейса (VLAN) «**ip dhcp relay enable**» используется для включения DHCP Relay на соответствующем VLAN.

Для работы DHCP Relay необходимо настроить IP-адрес на интерфейсе (VLAN), на который будут приниматься пакеты DHCP от клиентов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp relay enable
admin@Switch(config)#
```

14.4.6 ip dhcp relay address

Команда глобальной настройки. Добавление IP-адреса DHCP-сервера, используемого DHCP Relay.

Синтаксис команды:

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Команда с приставкой «**no**» используется для удаления IP-адреса DHCP-сервера, используемого DHCP Relay.

Параметры команды:

ip-address	IP-адрес DHCP-сервера. Может быть определено до 8 серверов

Значение по умолчанию:

IP-адреса DHCP-серверов отсутствуют.

Использование команды:

Команда «**ip dhcp relay address**» используется для добавления IP-адреса DHCP-сервера, используемого DHCP Relay. Команда «**no ip dhcp relay address**», введенная без аргументов, удаляет все IP-адреса DHCP-серверов, используемых DHCP Relay (глобальные адреса).

Команда настройки интерфейса (VLAN) «**ip dhcp relay address**» имеет больший приоритет и позволяет переопределить IP-адреса DHCP-серверов для конкретного VLAN.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp relay address 192.168.0.1
admin@Switch(config)#
```

14.4.7 ip dhcp information option format circuit-id

Команда настройки интерфейса (VLAN). Установка значения подопции Circuit ID опции 82, вставляемой в пакеты механизмом DHCP Relay.

Синтаксис команды:

ip dhcp information option format circuit-id string *string*

no ip dhcp information option format circuit-id

Команда с приставкой «**no**» используется для установки значения по умолчанию.

Параметры команды:

string	текстовая строка длиной от 1 до 63 символов, которая будет использоваться в качестве Circuit ID

Значение по умолчанию:

Текстовая строка вида “vlanN”, где N – идентификатор VLAN (номер).

Использование команды:

Команда «**ip dhcp information option format circuit-id**» используется для установки значения подопции Circuit ID опции 82, вставляемой в пакеты механизмом DHCP Relay.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip dhcp information option format circuit-id string servers
admin@Switch(config-if-vlan)#
```

14.4.8 ip dhcp relay enable

Команда настройки интерфейса (VLAN). Включение DHCP Relay на VLAN.

Синтаксис команды:

ip dhcp relay enable

no ip dhcp relay enable

Команда с приставкой «**no**» используется для отключения DHCP Relay на VLAN.

Значение по умолчанию:

DHCP Relay отключен.

Использование команды:

Команда «**ip dhcp relay enable**» используется для включения DHCP Relay на VLAN.

Для работы DHCP Relay на VLAN он предварительно должен быть включен с помощью команды глобальной настройки «**ip dhcp relay enable**».

Для работы DHCP Relay необходимо настроить IP-адрес на интерфейсе (VLAN), на который будут приниматься пакеты DHCP от клиентов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip dhcp relay enable
admin@Switch(config-if-vlan)#
```

14.4.9 ip dhcp relay address

Команда настройки интерфейса (VLAN). Добавление IP-адреса DHCP-сервера, используемого DHCP Relay на VLAN.

Синтаксис команды:

ip dhcp relay address *ip-address*

no ip dhcp relay address [*ip-address*]

Команда с приставкой «**no**» используется для удаления IP-адреса DHCP-сервера, используемого DHCP Relay на VLAN.

Параметры команды:

ip-address	IP-адрес DHCP-сервера. Может быть определено до 8 серверов

Значение по умолчанию:

IP-адреса DHCP-серверов отсутствуют.

Использование команды:

Команда «**ip dhcp relay address**» используется для добавления IP-адреса DHCP-сервера, используемого DHCP Relay на VLAN. Команда «**no ip dhcp relay address**», введенная без аргументов, удаляет все IP-адреса DHCP-серверов, используемых DHCP Relay на VLAN.

Если IP-адреса DHCP-серверов на VLAN не заданы, то используется глобальный список, заданный с помощью команды глобальной настройки «**ip dhcp relay address**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip dhcp relay address 192.168.0.1
admin@Switch(config-if-vlan)#
```

14.4.10 show ip dhcp relay

Команда, доступная из любого режима. Вывод настроек DHCP Relay.

Синтаксис команды:

show ip dhcp relay

Использование команды:

Команда «**show ip dhcp relay**» используется для вывода настроек DHCP Relay.

Пример команды:

```
admin@Switch# show ip dhcp relay
DHCP relay is globally enabled.
DHCP relay is enabled on VLANs: 1, 2
Global servers: 192.168.0.2, 192.168.0.3

VLAN   Servers
----   -----------
1      192.168.0.1
```

14.5 Настройки IPv6-адресации

14.5.1 ipv6 address

Команда настройки интерфейса VLAN. Установка IPv6-адреса на VLAN.

Синтаксис команды:

ipv6 address<*ip-address-v6*> <*prefix*> **[secondary]**

no ipv6 address <*ip-address-v6*> **[secondary]**

Команда с приставкой «**no**» удаляет IPv6-адрес с VLAN.

Параметры команды:

ip-address-v6	IPv6-адрес
prefix	длина префикса адреса в битах. Диапазон значений от 1 до 128
secondary	добавление или удаление дополнительного IP-адреса

Значение по умолчанию:

По умолчанию значение не задано.

Использование команды:

Команда «**ipv6 address**» используется для установки IP-адреса на VLAN.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ipv6 address 66::33 /64
admin@Switch(config-if-vlan)#
```

15 Функции безопасности

15.1 Настройка DHCP Snooping

15.1.1 debug ip dhcp snooping

Команда фундаментального режима. Включение отладки DHCP Snooping.
Синтаксис команды:
debug ip dhcp snooping {all | events | packets}
no debug ip dhcp snooping {all | events | packets}
Команда с приставкой «**no**» отключает отладку DHCP Snooping.
Параметры команды:

all	вывод всей диагностической информации
events	вывод событий DHCP Snooping
packets	вывод информации и полученных пакетах DHCP Snooping

Пример команды:

```
admin@Switch# debug ip dhcp snooping all
admin@Switch#
```

15.1.2 clear ip dhcp snooping database

Команда фундаментального режима. Удаление всех назначенных IP адресов из базы данных DHCP Snooping.
Синтаксис команды:
clear ip dhcp snooping database
Пример команды:

```
admin@Switch# clear ip dhcp snooping database
admin@Switch#
```

15.1.3 ip dhcp snooping

Команда глобальной настройки. Включение DHCP Snooping.
Синтаксис команды:
ip dhcp snooping
no ip dhcp snooping
Команда с приставкой «**no**» отключает DHCP Snooping.
Значение по умолчанию:
DHCP Snooping отключен.
Использование команды:
Команда «**ip dhcp snooping**» используется для включения DHCP Snooping.
Для работы DHCP Snooping необходимо также включить его хотя бы на одном VLAN с помощью команды «**ip dhcp snooping vlan**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp snooping
admin@Switch(config)#
```

15.1.4 ip dhcp snooping vlan

Команда глобальной настройки. Включение DHCP Snooping на VLAN.

Синтаксис команды:

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping *vlan-id*

Команда с приставкой «**no**» отключает DHCP Snooping на VLAN.

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

DHCP Snooping на VLAN отключен.

Использование команды:

Команда «**ip dhcp snooping**» используется для включения DHCP Snooping на VLAN.

Для работы DHCP Snooping на VLAN необходимо также включить его глобально с помощью команды «**ip dhcp snooping**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp snooping vlan 1
admin@Switch(config)#
```

15.1.5 ip dhcp snooping trust

Команда настройки интерфейса (Ethernet). Установка режима доверенного интерфейса.

Синтаксис команды:

ip dhcp snooping trust

no ip dhcp snooping trust

Команда с приставкой «**no**» устанавливает режим недоверенного интерфейса.

Значение по умолчанию:

Интерфейс не является доверенным.

Использование команды:

Команда «**ip dhcp snooping trust**» используется для установки режима доверенного интерфейса.

Устанавливайте доверенный режим на интерфейсах, к которым подключены DHCP-серверы, коммутаторы или маршрутизаторы. Устанавливайте недоверенный режим на интерфейсах, к которым подключены конечные пользователи (например, рабочие станции).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip dhcp snooping trust
admin@Switch(config-if)#
```

15.1.6 ip dhcp snooping limit rate

Команда настройки интерфейса (Ethernet). Устанавливает предельное значение для пакетов, которые DHCP Snooping может обрабатывать.

Синтаксис команды:

ip dhcp snooping limit rate *rate*

no ip dhcp snooping limit rate

Команда с приставкой «**no**» убирает ограничение для пакетов.

Значение по умолчанию:

Команда отключена.

Параметры команды:

rate предельное значение в пакетах/с

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# ip dhcp snooping limit rate 10
admin@Switch(config-if)#
```

15.1.7 ip dhcp snooping information option allowed-untrusted

Команда глобальной настройки. Разрешение приема пакетов DHCP с опцией 82 на недоверенных портах.

Синтаксис команды:

ip dhcp snooping information option allowed-untrusted

no ip dhcp snooping information option allowed-untrusted

Команда с приставкой «**no**» используется для запрета приема пакетов DHCP с опцией 82 на недоверенных портах.

Значение по умолчанию:

Прием пакетов DHCP с опцией 82 на недоверенных портах запрещен. Использование команды:

Команда «**ip dhcp snooping information option allowed-untrusted**» используется для разрешения приема пакетов DHCP с опцией 82 на недоверенных портах.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp snooping information option allowed-untrusted
admin@Switch(config)#
```

15.1.8 ip dhcp snooping verify

Команда глобальной настройки. Включение проверки соответствия MAC-адреса источника в DHCP-пакете, полученном на недоверенном порту, MAC-адресу клиента.

Синтаксис команды:

ip dhcp snooping verify

no ip dhcp snooping verify

Команда с приставкой «**no**» отключает проверку.

Значение по умолчанию:

Проверка соответствия MAC-адреса источника отключена.

Использование команды:

Команда «**ip dhcp snooping verify**» используется для включения проверки соответствия MAC-адреса источника в DHCP-пакете, полученном на недоверенном порту, MAC-адресу клиента.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp snooping verify
admin@Switch(config)#
```

15.1.9 ip dhcp snooping database

Команда глобальной настройки. Включение сохранения базы данных привязок DHCP Snooping локально или на удаленных серверах.

Синтаксис команды:

ip dhcp snooping database [*url* | **timeout** *seconds* | **write-delay** *seconds*]

no ip dhcp snooping database [*url* | **timeout** *seconds* | **write-delay** *seconds*]

Команда с приставкой «**no**» изменяет настройки или отключает сохранение базы данных привязок DHCP Snooping.

Параметры команды:

url	(опционально) URL назначения. Если параметр не указан, то сохранение происходит в локальную память
timeout *seconds*	(опционально) таймаут времени завершения процесса записи на удаленный сервер в диапазоне от 0 до 86400 секунд. По умолчанию равен 300 секундам. Если за указанный интервал времени процесс записи не завершен, то процесс прерывается
write-delay *seconds*	(опционально) Интервал задержки записи таблицы привязок в диапазоне от 15 до 86400 секунд. По умолчанию равен 300 секундам. При изменении таблицы привязок запись изменений откладывается на указанный интервал

В качестве префиксов URL могут выступать:

tftp://	сохранение базы данных привязок DHCP Snooping на внешний сервер TFTP. Синтаксис: **tftp://**[location/][directory/]filename
ftp://	сохранение базы данных привязок DHCP Snooping на внешний сервер FTP. Синтаксис: **ftp://**[username[:password]@]location/[directory/]filename. Если имя учетной записи “username” и пароль “password” не указаны, то устройство производит анонимное подключение. Если пароль не указан, то он равен пустой строке
scp://	сохранение базы данных привязок DHCP Snooping на внешний сервер по протоколу SCP. Синтаксис: **scp://**username[:password]@location/[directory/]filename Если пароль не указан, то он равен пустой строке

Значение по умолчанию:

База данных DHCP Snooping не сохраняется в файл.

Использование команды:

Команда «**ip dhcp snooping database**» используется для включения сохранения базы данных привязок (binding) DHCP Snooping в файл. Устройство позволяет настроить до 4-х URL.

Запись данных производится в двух случаях: при включении настройки (если до этого она была выключена) и при изменении таблицы привязок. При изменении таблицы привязок запись изменений происходит не сразу, а откладывается на интервал, определенный параметром «**write-delay**». Если за интервал времени, определенный параметром «**timeout**», процесс записи не завершен, то процесс прерывается.

Изменение параметров «**write-delay**» и «**timeout**» приводит к обнулению подсчитываемых интервалов. Если в этот момент происходил процесс записи, то он не прерывается.

Команда «**no ip dhcp snooping database**» без параметров отключает сохранение таблицы привязок DHCP Snooping. Команда «**no ip dhcp snooping database**» с параметрами устанавливает соответствующий параметр в значение по умолчанию.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp snooping database
admin@Switch(config)#
```

15.1.10 ip dhcp snooping database update-freq

Команда глобальной настройки. Установка интервала сохранения базы данных привязок (binding) DHCP Snooping в файл.

Синтаксис команды:

ip dhcp snooping database update-freq *seconds*

no ip dhcp snooping database update-freq

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал сохранения базы данных привязок в диапазоне от 600 до 86400 секунд

Значение по умолчанию:

Интервал обновления равен 1200 секундам.

Использование команды:

Команда «**ip dhcp snooping database update-freq**» используется для установки интервала сохранения базы данных привязок (binding) DHCP Snooping в файл.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp snooping database update-freq 1000
admin@Switch(config)#
```

15.1.11 ip dhcp snooping binding

Команда фундаментального режима. Добавление привязок DHCP Snooping.

Синтаксис команды:

ip dhcp snooping binding *mac-address vlan-id ip-address interface-id* **expiry** {*seconds* | **infinite**}

no ip dhcp snooping binding *mac-address vlan-id*

Команда с приставкой «**no**» удаляет привязки DHCP Snooping.

Параметры команды:

mac-address	MAC-адрес хоста
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
ip-address	IP-адрес хоста
interface-id	идентификатор интерфейса (Ethernet)
expiry *seconds*	интервал времени, по истечении которого запись становится недействительной, в диапазоне от 10 до 4294967295 секунд
expiry infinite	срок действия записи не ограничен

Значение по умолчанию:

По умолчанию статические привязки отсутствуют.

Использование команды:

Команда «**ip dhcp snooping binding**» используется для добавления привязок DHCP Snooping.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip dhcp snooping binding 00:1B:28:00:55:01 1 10.0.0.2
gigabitethernet 0/1 expiry 900
admin@Switch(config)#
```

15.1.12 show ip dhcp snooping

Команда, доступная из любого режима. Вывод конфигурации DHCP Snooping на всех или определенном интерфейсе.

Синтаксис команды:

show ip dhcp snooping [*interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Пример команды:

```
admin@Switch# show ip dhcp snooping
DHCP snooping is Enabled
DHCP snooping is configured on following VLANs: 1
DHCP snooping database is Enabled
Relay agent Information option 82 is Enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is Enabled
DHCP snooping file update frequency is configured to: 666 seconds

Interface  Trusted
---------  -------
gi0/1      Yes
gi0/2      Yes
gi0/3      No
gi0/4      No
```

15.1.13 show ip dhcp snooping binding

Команда, доступная из любого режима. Вывод всех или определенных привязок DHCP Snooping.

Синтаксис команды:

show ip dhcp snooping binding [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan-id*] [*interface-id*]

Параметры команды:

mac-address	MAC-адрес хоста
ip-address	IP-адрес хоста
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
interface-id	идентификатор интерфейса (Ethernet)

Пример команды:

```
admin@Switch# show ip dhcp snooping binding
Update frequency: 1200
Total number of binding: 2

Mac Address        IP Address   Lease   Type       VLAN    Interface
-----------------  ----------   -----   --------   ----    ---------
00:1B:28:BA:D0:01  10.0.0.2     1507    snooping   1       gi0/1
00:1B:28:DA:D0:02  172.16.1.2   8719    snooping   2       gi0/2
```

15.2 Настройка безопасности на интерфейсах (Port Security)

15.2.1 clear port-security

Команда фундаментального режима. Удаление записей из таблицы MAC-адресов, которые были изучены автоматически на безопасном порту.

Синтаксис команды:

clear port-security dynamic [interface *interface-id***]**

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**clear port-security**» используется для удаления записей из таблицы MAC-адресов, которые были изучены автоматически на защищенном порту.

Пример команды:

```
admin@Switch# clear port-security dynamic interface gigabitethernet 0/1
admin@Switch#
```

15.2.2 switchport port-security

Команда настройки интерфейса (Ethernet). Включение безопасного изучения адресов на интерфейсе.

Синтаксис команды:

switchport port-security

no switchport port-security

Команда с приставкой «**no**» отключает безопасное изучение адресов на интерфейсе.

Значение по умолчанию:

Безопасное изучение адресов отключено.

Использование команды:

Команда «**switchport port-security**» используется для включения безопасного изучения адресов на интерфейсе.

При включении и отключении безопасности на интерфейсе выполняются следующие условия:

- при включении безопасности все динамические адреса на интерфейсе удаляются;
- при отключении безопасности все безопасные адреса переводятся в динамические.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport port-security mode lock
admin@Switch(config-if)# switchport port-security violation restrict
admin@Switch(config-if)# switchport port-security
admin@Switch(config-if)#
```

15.2.3 switchport port-security mac-address

Команда настройки интерфейса (Ethernet). Добавление безопасного MAC-адреса на интерфейс.

Синтаксис команды:

switchport port-security mac-address *mac-addr* **[vlan** *vlan-id* **|** *vlan-list***]**

no switchport port-security mac-address *mac-addr* **[vlan** *vlan-id* **|** *vlan-list***]**

Команда с приставкой «**no**» удаляет безопасный MAC-адрес с интерфейса.

Параметры команды:

mac-addr	безопасный MAC-адрес
vlan-id	номер VLAN, на который нужно добавить адрес. Если номер VLAN не задан, то MAC-адрес добавляется на “Access VLAN” для порта в режиме “Access”, “Native VLAN” для порта в режиме “Trunk”, “Customer VLAN” для порта в режиме “Customer”. В случае смены режима порта устройство автоматически удаляет настройку
vlan-list	список VLAN, на которые нужно добавить адрес. Команда может быть применена только к портам в режиме “Trunk”. В случае смены режима порта из “Trunk” в любой другой, устройство автоматически удаляет настройку

Значение по умолчанию:

Безопасные MAC-адреса не заданы.

Использование команды:

Команда «**switchport port-security mac-address**» используется для добавления безопасного MAC-адреса на интерфейс.

Информация по ограничениям:

- на порт со включенным режимом безопасности можно добавлять статические адреса;
- существующий вручную добавленный безопасный адрес можно переопределить как статический на другом порту в том же VLAN (при этом безопасный адрес будет удален с порта, на котором он был определен);
- вручную добавленный безопасный адрес фактически является статическим и не может быть динамически изучен на другом порту;
- если на порту режим безопасности отключен, то безопасный адрес добавить нельзя;

– при отключении режима безопасности происходит удаление адреса из конфигурации и перевод адреса в динамический режим.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport port-security mac-address 00:1b:28:cc:cc:cc
admin@Switch(config-if)#
```

15.2.4 switchport port-security maximum

Команда настройки интерфейса (Ethernet). Установка максимального количества адресов, которое может быть изучено на интерфейсе.

Синтаксис команды:

switchport port-security maximum *value*

no switchport port-security maximum

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

value	максимальное количество адресов, которое может быть изучено на интерфейсе, в диапазоне от 0 до 254

Значение по умолчанию:

Максимальное количество адресов равно 1.

Использование команды:

Команда «**switchport port-security maximum**» используется для установки максимального количества адресов, которое может быть изучено на интерфейсе.

Команда может быть использована, только если интерфейс находится в обычном режиме (не безопасном).

Размер ограничения определяет общее количество динамических, статических и безопасных MAC-адресов, которые могут быть привязаны (изучены) к интерфейсу. Один и тот же MAC-адрес, изученный на двух разных VLAN, считается как два MAC-адреса.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport port-security max 10
admin@Switch(config-if)# switchport port-security mode max
admin@Switch(config-if)# switchport port-security
admin@Switch(config-if)#
```

15.2.5 switchport port-security mode

Команда настройки интерфейса (Ethernet). Установка режима изучения при включении безопасности на интерфейсе.

Синтаксис команды:

switchport port-security mode {max-addresses | lock | sticky} [trap *interval***]**

no switchport port-security mode

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

max-addresses	режим с ограничением максимального количества изучаемых MAC-адресов. Фактически является режимом с отключенной безопасностью (non secure mode)
lock	безопасный режим без изучения адресов. Статические и безопасные адреса могут быть добавлены вручную
sticky	режим сохранения динамически изученных MAC-адресов на интерфейсе. Динамически изученные MAC-адреса в режиме «sticky» будут добавлены в текущую конфигурацию
trap *interval*	назначение интервала между двумя сообщениями SNMP. Если будет сгенерировано еще одно сообщение в заданный интервал, то данное сообщение будет отброшено

Значение по умолчанию:

Безопасный режим без изучения адресов («**lock**»).

Использование команды:

Команда «**switchport port-security mode**» используется для установки режима изучения при включении безопасности на интерфейсе.

Команда может быть использована, только если интерфейс находится в обычном режиме (не безопасном).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport port-security mode lock
admin@Switch(config-if)# switchport port-security
admin@Switch(config-if)#
```

15.2.6 switchport port-security violation

Команда настройки интерфейса (Ethernet). Установка реакции на нарушения безопасности при безопасном изучении адресов на интерфейсе.

Синтаксис команды:

switchport port-security violation {forward | restrict | shutdown}

no switchport port-security violation

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

forward	передача пакетов с неизвестным MAC-адресом. MAC-адрес не вносится в таблицу MAC-адресов
restrict	фильтрация пакетов с неизвестным MAC-адресом
shutdown	фильтрация пакетов с неизвестным MAC-адресом и отключение интерфейса при обнаружении пакета с неизвестным MAC-адресом

Значение по умолчанию:

Фильтрация пакетов с неизвестным MAC-адресом («restrict»).

Использование команды:

Команда «**switchport port-security violation**» используется для установки реакции на нарушения безопасности при безопасном изучении адресов на интерфейсе.

Команда может быть использована, только если интерфейс находится в обычном режиме (не безопасном).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# switchport port-security mode lock
admin@Switch(config-if)# switchport port-security violation restrict
admin@Switch(config-if)# switchport port-security
admin@Switch(config-if)#
```

15.2.7 show port-security

Команда, доступная из любого режима. Вывод настроек безопасности на интерфейсе.

Синтаксис команды:

show port-security [interface *interface-id***] [address]**

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)
address	вывод безопасных адресов на интерфейсе

Использование команды:

Команда «**show port-security**» используется для вывода настроек безопасности на интерфейсе. Если команда введена без аргументов, то устройство выводит настройки всех интерфейсов, на которых включена безопасность.

Примеры команды:

```
admin@Switch# show port-security
Secure Port  Learning     MaxAddr   CurrAddr  Action    Trap Freq
-----------  --------     -------   --------  ------    ---------
gi0/1        Max-address  10        5         restrict  30
gi0/2        Lock         --        2         shutdown  30
```

```
admin@Switch# show port-security interface gigabitethernet 0/1 address
VLAN    MAC Address        Type               Ports
----    -----------------  ----------------   -----
1       00:1b:28:12:34:56  SecureConfigured   gi0/1
1       00:1b:28:56:34:12  Learned            gi0/2
```

15.3 Настройка IP Source Guard

15.3.1 Общие положения

IP Source Guard является функцией безопасности, предназначенной для ограничения IP-трафика на немаршрутизирумых интерфейсах (Layer 2) путем фильтрации трафика на основе динамичесих (из DHCP Snooping) и статических привязок IP- и MAC-адресов. Трафик от IP-адресов, не находящихся в привязках, фильтруется устройством.

IP Source Guard предназначен для предотвращения атак, основанных на использовании IP-адреса другого хоста (подмена IP-адреса). IP Source Guard должен быть включен глобально для того, чтобы включить его на интерфейсе.

Если IP Source Guard включен на интерфейсе, то:

1. IP-пакеты фильтруются по следующим критериям:

- DHCP-пакеты обрабатываются DHCP Snooping;
- если на VLAN, к которому относится пакет, DHCP Snooping отключен, то пакет пропускается;
- если на интерфейсе задана статическая привязка или есть активная динамическая привязка, MAC-адрес, IP-адрес и номер VLAN которой соответствует IP-пакету, то пакет пропускается. Проверка MAC-адреса производится, только если задан режим «verify-mac»;
- все остальные IP-пакеты фильтруются. В случае фильтрации пакета, выводится предупреждающее сообщение. Не может быть выведено более 1 сообщения в течение 5 секунд.

2. Пакеты, не являющиеся IP-пакетами, пропускаются.

IP Source Guard использует ресурсы TCAM для хранения привязок. В некоторых случаях динамические привязки могут быть неактивными из-за нехватки места в таблице TCAM. По умолчанию, ПО осуществляет поиск свободного места в таблице TCAM для неактивных динамических записей с интервалом в 60 секунд.

Если в результате работы IP Source Guard будет создана динамическая привязка, имеющая тот же MAC-адрес, IP-адрес и номер VLAN, что и существующая статическая привязка, но другой идентификатор интерфейса, то динамическая привязка помечается как неактивная и выводится предупреждающее сообщение.

Аналогично при добавлении статической привязки, имеющей тот же MAC-адрес, IP-адрес и номер VLAN, что и существующая динамическая привязка, но другой идентификатор интерфейса, то динамическая привязка помечается как неактивная и выводится предупреждающее сообщение.

Настройки пользователя

1. Глобальные настройки:

- режим работы: включен, отключен;
- интервал поиска свободного места в таблице TCAM для неактивных динамических записей: целое число в диапазоне от 10 до 600 секунд;
- добавление и удаление статических привязок.

2. Настройки интерфейсов:

- режим работы: включен, отключен. Опционально может быть задан режим фильтрации MAC-адресов.

Дополнения и ограничения

IP Source Guard имеет следующие ограничения:

- для работы IP Source Guard необходимо включить DHCP Snooping глобально, а также на тех VLAN, для которых необходимо включить IP Source Guard.
- IP Source Guard работает только на недоверенных портах DHCP Snooping (untrusted). Статические привязки IP Source Guard можно задать и на доверенных портах DHCP Snooping (trusted), однако они не будут активны, пока порт не будет переведен в недоверенный режим. При переводе порта из недоверенного в доверенный режим динамические привязки будут удалены, а статические привязки перейдут в неактивный режим.
- если суммарное количество привязок превысит доступный объем записей TCAM, то новые привязки будут неактивными. IP-пакеты, соответствующие неактивным привязкам фильтруются устройством.

Описание настройки

Порядок настройки IP Source Guard приведен в таблице 14.

Таблица 14 – Порядок настройки IP Source Guard

Шаг	Команда	Назначение
1	**configure terminal**	Переход в режим глобальной настройки
2	**ip source-guard**	Включение проверки IP- и MAC-адресов для входящих IP-пакетов на устройстве (IP Source Guard)
3	**ip source-guard binding** *mac-address vlan-id ip-address interface-id*	(Опционально) Добавление статических привязок

Продолжение таблицы 14

Шаг	Команда	Назначение
4	**interface** *interface-id*	Переход в режим настройки интерфейса
5	**ip source-guard**	Включение проверки IP-адресов для входящих IP-пакетов на интерфейсе
6	**ip source-guard verify-mac**	(Опционально) Включение проверки MAC-адресов для входящих IP-пакетов на интерфейсе
7	**exit**	Переход в предыдущий режим настройки
8	**show ip source-guard configuration**	Проверка настроек IP Source Guard
9	**show ip source-guard status** [**macaddress** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan*] [*interface-id*]	Проверка настроек IP Source Guard
10	**copy running-config startup-config**	Сохранение текущей конфигурации

Рассмотрим вариант настройки со следующими условиями:

- необходимо включить механизм IP Source Guard на интерфейсах gigabitethernet 0/1-4 с проверкой MAC-адресов;
- на порт gigabitethernet 0/1 требуется добавить статическую привязку в VLAN 10 с MAC-адресом “00:1B:28:11:11:11” и IP-адресом 10.0.0.1;
- DHCP Snooping предварительно был включен на VLAN 10 и интерфейсы gigabitethernet 0/1-4 были настроены как недоверенные.

Выполним глобальные настройки:

```
admin@Switch# configure terminal
admin@Switch(config)# ip source-guard
admin@Switch(config)# ip source-guard binding 00:1b:28:11:11:11 10 10.0.0.1
gigabitethernet 0/1
admin@Switch(config)#
```

Произведем настройки на интерфейсах:

```
admin@Switch(config)# interface range gigabitethernet 0/1-4
admin@Switch(config-if)# ip source-guard
admin@Switch(config-if)# ip source-guard verify-mac
admin@Switch(config-if)# exit
admin@Switch(config)# exit
```

Проверим параметры и сохраним файл конфигурации:

```
admin@Switch# show ip source-guard configuration

IP source guard is globally enabled.
TCAM resources search frequency: 60 seconds

Interface   State
---------   -------
gi0/1       Enabled
gi0/2       Enabled
gi0/3       Enabled
gi0/4       Enabled

admin@Switch# show ip source-guard status

Interface   Filter   Status   IP Address   MAC Address        VLAN   Type
---------   ------   ------   ----------   -----------------   ----   ------
gi0/1       IP/MAC   Active   10.0.0.1     00:1B:28:11:11:11   10     Static
gi0/2       IP/MAC   Active   Deny all
gi0/3       IP/MAC   Active   Deny all
gi0/4       IP/MAC   Active   Deny all

admin@Switch# copy running-config startup-config
admin@Switch#
```

15.3.2 ip source-guard

Команда глобальной настройки. Включение проверки IP- и MAC-адресов для входящих IP-пакетов на устройстве (IP Source Guard).

Синтаксис команды:

ip source-guard

no ip source-guard

Команда с приставкой «**no**» отключает проверку.

Значение по умолчанию:

Проверка IP- и MAC-адресов для входящих IP-пакетов отключена.

Использование команды:

Команда «**ip source-guard**» используется для включения проверки IP- и MAC-адресов для входящих IP-пакетов на устройстве (IP Source Guard).

Функция IP Source Guard должна быть включена на устройстве перед ее включением на интерфейсах.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip source-guard
admin@Switch(config)#
```

15.3.3 ip source-guard binding

Команда глобальной настройки. Добавление статической привязки IP- и MAC-адреса для входящих IP-пакетов на устройстве (IP Source Guard).

Синтаксис команды:
ip source-guard binding *mac-address vlan-id ip-address interface-id*
no ip source-guard binding *mac-address vlan-id ip-address*
Команда с приставкой «**no**» удаляет привязку.
Параметры команды:

mac-address	MAC-адрес привязки
vlan-id	номер VLAN в диапазоне от 1 до 4094
ip-address	IP-адрес привязки
interface-id	идентификатор интерфейса (Ethernet)

Значение по умолчанию:
Статические привязки отсутствуют.
Использование команды:
Команда «**ip source-guard binding**» используется для добавления статической привязки IP- и MAC-адреса для входящих IP-пакетов на устройстве (IP Source Guard).
Если в результате работы IP Source Guard будет создана динамическая привязка, имеющая тот же MAC-адрес, IP-адрес и номер VLAN, что и существующая статическая привязка, но другой идентификатор интерфейса, то динамическая привязка помечается как неактивная и выводится предупреждающее сообщение.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip source-guard binding 00:1b:28:11:22:33 100 10.0.0.1
gigabitethernet 0/1
admin@Switch(config)#
```

15.3.4 ip source-guard vlan

Команда глобальной настройки. Включение проверки IP- и MAC-адресов для входящих IP-пакетов на VLAN.
Синтаксис команды:
ip source-guard vlan *vlan-id*
no ip source-guard vlan *vlan-id*
Команда с приставкой «**no**» отключает проверку.
Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:
Проверка отключена.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip source-guard vlan 10
```

15.3.5 ip source-guard

Команда настройки интерфейса (Ethernet). Включение проверки IP-адресов для входящих IP-пакетов на интерфейсе.

Синтаксис команды:

ip source-guard [**verify-mac**]

no ip source-guard [**verify-mac**]

Команда с приставкой «**no**» отключает проверку.

Параметры команды:

verify-mac	проверка MAC-адресов для входящих IP-пакетов на интерфейсе

Значение по умолчанию:

Проверка IP-адресов для входящих IP-пакетов отключена.

Использование команды:

Команда «**ip source-guard**» используется для включения проверки IP-адресов для входящих IP-пакетов на интерфейсе.

Функция IP Source Guard должна быть включена на устройстве перед ее включением на интерфейсах.

Функция IP Source Guard активна только на недоверенных интерфейсах DHCP Snooping. DHCP Snooping должен быть включен как минимум на одном из VLAN интерфейсе.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip source-guard
admin@Switch(config-if)#
```

15.3.6 show ip source-guard configuration

Команда, доступная из любого режима. Вывод настроек IP Source Guard на всех или определенном интерфейсе.

Синтаксис команды:

show ip source-guard configuration [**interface** *interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show ip source-guard configuration**» используется для вывода настроек IP Source Guard на всех или определенном интерфейсе. Если команда введена без аргументов, то выводится информация для всех интерфейсов.

Пример команды:

```
admin@Switch# show ip source-guard configuration
IP source guard is globally enabled.
TCAM resources search frequency: 10 minutes

Interface   State
---------   -------
gi0/1       Enabled
gi0/2       Disabled
gi0/3       Enabled
gi0/4       Enabled
```

15.3.7 show ip source-guard status

Команда, доступная из любого режима. Вывод состояния привязок IP Source Guard.

Синтаксис команды:

show ip source-guard status [**mac-address** *mac-address*] [**ip-address** *ip-address*] [**vlan** *vlan*] [**interface** *interface-id*]

Параметры команды:

mac-address	MAC-адрес привязки
ip-address	IP-адрес привязки
vlan	номер VLAN в диапазоне от 1 до 4094
interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show ip source-guard status**» используется для вывода состояния привязок IP Source Guard. Если команда введена без аргументов, то выводятся все привязки.

Примеры команды:

```
admin@Switch# show ip source-guard status
IP source guard is globally disabled.
```

```
admin@Switch# show ip source-guard status

Interface   Filter   Status    IP Address   MAC Address         VLAN    Type
---------   ------   ------    ----------   -----------------   ----    ------
gi0/1       IP/MAC   Active    10.0.8.1     00:1B:28:11:22:33   10      DHCP
gi0/2       IP       Active    10.0.1.1     00:1B:28:11:22:33   20      DHCP
gi0/3       IP       Active    Deny all                         DHCP
gi0/4       IP       Active    10.0.8.2     00:1B:28:11:22:33   10      Static
gi0/5       IP       Inactive  10.0.8.3     00:1B:28:11:22:33   10      DHCP
```

15.3.8 show ip source-guard inactive

Команда, доступная из любого режима. Вывод списка неактивных привязок IP Source Guard.

Синтаксис команды:

show ip source-guard inactive

Использование команды:

Команда «**show ip source-guard inactive**» используется для вывода списка неактивных привязок IP Source Guard.

IP Source Guard использует ресурсы TCAM для хранения привязок. В некоторых случаях динамические привязки могут быть неактивными из-за нехватки места в таблице TCAM. По умолчанию ПО осуществляет поиск свободного места в таблице TCAM для неактивных динамических записей с интервалом в 60 секунд.

Для отключения автоматического поиска свободного места в таблице TCAM для динамических записей IP Source Guard используется команда «**ip source-guard tcam retries-freq never**», а затем для ручной активации поиска свободного места используется команда «**ip source-guard tcam locate**».

Пример команды:

```
admin@Switch# show ip source-guard inactive
TCAM resources search frequency: 10 minutes

Interface   Filter   IP Address   MAC Address         VLAN   Type    Reason
---------   ------   ----------   -----------------   ----   -----   ----------------
gi0/1       IP       10.0.8.3     00:1B:28:44:55:66   10     DHCP    Resource problem
gi0/2       IP                    Trusted port
gi0/3       IP                    No snooping VLAN
```

15.3.9 show ip source-guard statistics

Команда, доступная из любого режима. Вывод статистики IP Source Guard на всех или определенном VLAN.

Синтаксис команды:

show ip source-guard statistics [**vlan** *vlan-id*]

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Использование команды:

Команда «**show ip source-guard statistics**» используется для вывода статистики IP Source Guard на всех или определенном VLAN. Если команда введена без аргументов, то выводится статистика для всех VLAN.

Пример команды:

```
admin@Switch# show ip source-guard statistics vlan 10
VLAN   Static Bindings   DHCP Snooping Bindings
----   ---------------   ----------------------
10     2                 3
```

15.4 Настройка таблицы MAC-адресов

15.4.1 Общие положения

Система управления коммутатора поддерживает вывод MAC-адресов, находящихся в таблице, по следующим критериям:

- вывод списка всех MAC-адресов по команде «**show mac address-table**»;
- вывод динамических MAC-адресов, который осуществляется по команде «**show mac address-table dynamic**»;
- вывод статических MAC-адресов, который осуществляется по команде «**show mac address-table static**»;
- вывод MAC-адресов, относящихся к определенному интерфейсу, который осуществляется по команде «**show mac address-table interface**»;
- вывод MAC-адресов, относящихся к определенному VLAN, который осуществляется по команде «**show mac address-table vlan**».

Система управления коммутатора обеспечивает следующие действия с таблицей MAC-адресов:

- добавление статических MAC-адресов, осуществляемое по командам «**mac address-table static**» и «**mac address-table static drop**»;
- удаление всех динамических MAC-адресов, осуществляемое по команде «**clear mac address-table**»;
- установку времени старения MAC-адресов, осуществляемую с помощью команды «**mac address-table aging-time**».

Вывод информации об определенном MAC-адресе осуществляется с помощью команды «**show mac address-table address**».

Вывод времени старения MAC-адресов в таблице осуществляется с помощью команды «**show mac address-table aging-time**».

Вывод количества статических и динамических MAC-адресов в таблице осуществляется с помощью команды «**show mac address-table count**».

15.4.2 clear mac address-table dynamic

Команда фундаментального режима. Удаление динамических MAC-адресов из таблицы.

Синтаксис команды:

clear mac address-table dynamic [address *mac-addr* **| interface** *interface-id* **| vlan** *vlan-id***]**

Параметры команды:

address *mac-addr*	удаление MAC-адреса, определенного параметром «*mac-addr*». MAC-адрес необходимо указать в виде 6 пар шестнадцатеричных цифр, разделенных двоеточиями
interface *interface-id*	удаление всех MAC-адресов на определенном интерфейсе с идентификатором «*interface-id*»
vlan *vlan-id*	удаление всех MAC-адресов на VLAN с идентификатором «*vlan-id*»

Использование команды:

Команда «**clear mac address-table dynamic**» используется для удаления динамических MAC-адресов из таблицы. Команда без аргументов удаляет все динамические адреса из таблицы.

Пример команды:

```
admin@Switch# clear mac address-table dynamic
admin@Switch#
```

15.4.3 mac address-table aging-time

Команда глобальной настройки. Установка времени старения MAC-адресов в секундах. Значение «0» означает, что старение MAC-адресов отключено.

Синтаксис команды:

mac address-table aging-time {0 | *15-3825***}**

Параметры команды:

0	старение MAC-адресов отключено
15-3825	время старения MAC-адресов в секундах

Значение по умолчанию:

По умолчанию время старения равняется 300.

Использование команды:

По истечении времени старения динамический MAC-адрес автоматически удаляется из таблицы MAC-адресов, если за прошедшее время через коммутатор не проходил ни один пакет с данным MAC-адресом.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac address-table aging-time 200
admin@Switch(config)# end
admin@Switch#
```

15.4.4 mac address-table static

Команда глобальной настройки. Добавление статического MAC-адреса в таблицу.

Синтаксис команды:

mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

no mac address-table static *mac-addr* **vlan** *vlan-id* **[interface** *interface-id***]**

Команда с приставкой «**no**» удаляет статический MAC-адрес из таблицы.

Параметры команды:

mac-addr	статический MAC-адрес. MAC-адрес необходимо указать в виде 6 пар шестнадцатеричных цифр, разделенных двоеточиями
vlan *vlan-id*	номер VLAN, в который нужно добавить MAC-адрес, в диапазоне от 1 до 4094
interface *interface-id*	идентификатор интерфейса назначения для пакетов с указанным MAC-адресом

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac address-table static 00:1B:28:00:00:01 vlan 1 interface
tengigabitethernet0/1
admin@Switch(config)# end
admin@Switch#
```

15.4.5 mac address-table static drop

Команда глобальной настройки. Добавление статического MAC-адреса в таблицу, для которого будет производиться фильтрация и пакеты с данным MAC-адресом будут удаляться коммутатором.

Синтаксис команды:

mac address-table static *mac-addr* **vlan** *vlan-id* **drop**

no mac address-table static *mac-addr* **vlan** *vlan-id* **drop**

Команда с приставкой «**no**» удаляет статический MAC-адрес из таблицы.

Параметры команды:

mac-addr	статический MAC-адрес. MAC-адрес необходимо указать в виде 6 пар шестнадцатеричных цифр, разделенных двоеточиями
vlan *vlan-id*	номер VLAN, в который нужно добавить MAC-адрес, в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# mac address-table static 00:1B:28:00:00:01 vlan 1 drop
admin@Switch(config)# end
admin@Switch#
```

15.4.6 show mac address-table

Фундаментальная команда. Вывод списка всех MAC-адресов в таблице MAC-адресов коммутатора.

Синтаксис команды:

show mac address-table

Пример команды:

```
admin@Switch show mac address-table
VLAN    MAC address        Type    Ports
----    -----------------  ------- -----
1       68:05:CA:38:1C:4D  dynamic fa0/3
admin@Switch#
```

15.4.7 show mac address-table address

Фундаментальная команда. Вывод информации об определенном MAC-адресе.
Синтаксис команды:
show mac address-table address *mac-addr* **[interface** *interface-id***] [vlan** *vlan-id***]**
Параметры команды:

mac-addr	MAC-адрес, для которого выводится информация. MAC-адрес необходимо указать в виде 6 пар шестнадцатеричных цифр, разделенных двоеточиями
interface *interface-id*	идентификатор интерфейса
vlan *vlan-id*	номер VLAN в диапазоне от 1 до 4094

Использование команды
Команда без параметров выводит информацию обо всех VLAN, в которых есть указанный MAC-адрес, и идентификаторах интерфейсов, с которыми он связан.
Команда с параметрами «**interface**» или «**vlan**» выводит информацию только для данного интерфейса или VLAN.
Пример команды:

```
admin@Switch# show mac address-table address 00:02:4B:28:C4:82
        MAC Address Table
-------------------------
Vlan    MAC Address        Type    Ports
-----------------------------------
All     00:02:4B:28:C4:82  STATIC  CPU
Total MAC Addresses for this criterion: 1
admin@Switch#
```

15.4.8 show mac address-table aging-time

Фундаментальная команда. Вывод времени старения MAC-адресов в таблице.
Синтаксис команды:
show mac address-table aging-time
Пример команды:

```
admin@Switch# show mac address-table aging-time
Aging Time: 300
admin@Switch#
```

15.4.9 show mac address-table count

Фундаментальная команда. Вывод количества статических и динамических MAC-адресов в таблице.

Синтаксис команды:

show mac address-table count [vlan *vlan-id***]**

Параметры команды:

vlan *vlan-id* номер VLAN в диапазоне от 1 до 4094

Использование команды:

Команда без параметров выводит информацию для всех VLAN.

Пример команды:

```
admin@Switch# show mac address-table count
MAC Entries for Vlan: 1
------------------------
Dynamic Address Count: 2
Static Address Count: 0
Total MAC Addresses: 2
admin@Switch#
```

15.4.10 show mac address-table dynamic

Фундаментальная команда. Вывод списка динамических MAC-адресов в таблице.

Синтаксис команды:

show mac address-table dynamic [address *mac-addr***] [interface** *interface-id***] [vlan** *vlan-id***]**

Параметры команды:

address *mac-addr* MAC-адрес, для которого выводится информация. MAC-адрес необходимо указать в виде 6 пар шестнадцатеричных цифр, разделенных двоеточиями

interface *interface-id* идентификатор интерфейса

vlan *vlan-id* номер VLAN в диапазоне от 1 до 4094

Использование команды:

Команда без параметров выводит информацию обо всех динамических MAC-адресах в таблице.

Команда с параметрами «**address**», «**interface**» или «**vlan**» выводит информацию только для данного MAC-адреса, интерфейса или VLAN.

Пример команды:

```
admin@Switch# show mac address-table dynamic
---------------------
Vlan    MAC Address        Type    Ports
----    ----------------  ------- -----
1       00:30:B6:35:78:62  DYNAMIC gi0/2
1       00:B0:64:96:27:41  DYNAMIC gi0/2
Total MAC Addresses for this criterion: 2
admin@Switch#
```

15.4.11 show mac address-table interface

Фундаментальная команда. Вывод списка MAC-адресов в таблице для определенного интерфейса.

Синтаксис команды:

show mac address-table interface *interface-id* **[vlan** *vlan-id***]**

Параметры команды:

interface *interface-id*	идентификатор интерфейса
vlan *vlan-id*	номер VLAN в диапазоне от 1 до 4094

Использование команды:

Команда с параметром «**vlan**» выводит информацию только для определенного VLAN.

Пример команды:

```
admin@Switch# show mac address-table interface gigabitethernet1/1
        MAC Address Table
---------------------------
Vlan    MAC Address       Type    Ports
---------------------------------------
1       00:30:B6:35:78:62  DYNAMIC gi0/1
1       00:B0:64:96:27:41  DYNAMIC gi0/1
Total MAC Addresses for this criterion: 2
admin@Switch#
```

15.4.12 show mac address-table static

Фундаментальная команда. Вывод списка статических MAC-адресов в таблице.

Синтаксис команды:

show mac address-table static [address *mac-addr***] [interface** *interface-id***] [vlan** *vlan-id***]**

Параметры команды:

address *mac-addr*	MAC-адрес, для которого выводится информация. MAC-адрес необходимо указать в виде 6 пар шестнадцатеричных цифр, разделенных двоеточиями
interface *interface-id*	идентификатор интерфейса
vlan *vlan-id*	номер VLAN в диапазоне от 1 до 4094

Использование команды:

Команда без параметров выводит информацию обо всех статических MAC-адресах в таблице.

Команда с параметрами «**address**», «**interface**» или «**vlan**» ограничивает вывод информации только для данного MAC-адреса, интерфейса или VLAN.

Пример команды:

```
admin@Switch# show mac address-table static
        MAC Address Table
---------------------------------------
Vlan    MAC Address        Type    Ports
---------------------------------------
All     01:80:C2:00:00:01  STATIC  CPU
4       00:01:00:02:00:04  STATIC  Drop
6       00:01:00:02:00:07  STATIC  Drop
Total MAC Addresses for this criterion: 3
admin@Switch#
```

15.4.13 show mac address-table vlan

Фундаментальная команда. Вывод списка MAC-адресов в таблице для определенного номера VLAN.

Синтаксис команды:

show mac address-table vlan *vlan-id*

Параметры команды:

vlan *vlan-id* номер VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# show mac address-table vlan 1
        MAC Address Table
------------------------
Vlan    MAC Address        Type    Ports
----------------------------------------
1       01:80:C2:00:00:00  STATIC  CPU
1       01:80:C2:00:00:01  STATIC  CPU
1       01:80:C2:00:00:02  STATIC  CPU
1       01:80:C2:00:00:03  STATIC  CPU
1       01:80:C2:00:00:05  STATIC  CPU
1       01:80:C2:00:00:06  STATIC  CPU
1       01:80:C2:00:00:07  STATIC  CPU
Total MAC Addresses for this criterion: 7
admin@Switch#
```

15.5 Настройка Dynamic ARP Inspection

15.5.1 Общие положения

Dynamic ARP Inspection (Protection) – функция коммутатора, предназначенная для защиты от атак с использованием протокола ARP. Например, атаки ARP-spoofing, позволяющей перехватывать трафик между узлами, которые расположены в пределах одного широковещательного домена. Dynamic ARP Inspection (Protection) регулирует только сообщения протокола ARP и не может повлиять напрямую на трафик пользователей или другие протоколы. Протокол ARP обеспечивает взаимодействие по протоколу IP в рамках широковещательного домена L2 путем установки соответствия IP-адреса и MAC-адреса.

Например, хост B хочет отправить информацию хосту A, но не имеет MAC-адреса хоста A в своей ARP-таблице. Хост B генерирует широковещательный ARP-запрос для всех хостов в рамках широковещательного домена L2 с целью получения MAC-адреса, соответствующего IP-адресу хоста A. Все хосты в широковещательном домене получают этот запрос, и хост A отвечает ARP-ответом хосту B. Однако ARP позволяет отправку добровольных ARP-ответов (gratuituous ARP reply), даже если ARP-запрос не был получен, что открывает возможность так называемой ARP-spoofing атаки, приводящей к заполнению ARP-таблицы неверными данными (ARP poisoning).

После атаки весь трафик, предназначенный для хостов, которые были атакованы, будет отправляться на атакующий хост.

Злоумышленник может атаковать хосты, коммутаторы и маршрутизаторы, подключенные к L2 сети, путем заполнения ARP-таблиц устройств в сети неверными данными и последующим перехватом данных, которые предназначались для других хостов в сети. Пример атаки ARP-spoofing приведен на рисунках 7, 8 и 9.

Хосты A, B и C подключены к коммутатору по интерфейсам A, B и C, которые находятся в одной подсети. IP-адреса и MAC-адреса хостов указаны в скобках. Например, хост A имеет IP-адрес IA и MAC-адрес MA. Если хост A хочет отправить данные хосту B по протоколу IP, он отправляет широковещательный ARP-запрос MAC-адреса, который связан с IP-адресом IB. По получении пакета коммутатор и хост B вносят в свою ARP-таблицу связку IP-адреса IA и MAC-адреса MA. Когда хост B отвечает на запрос, аналогично коммутатор и хост A вносят в свою ARP-таблицу связку IP-адреса IB и MAC-адреса MB.

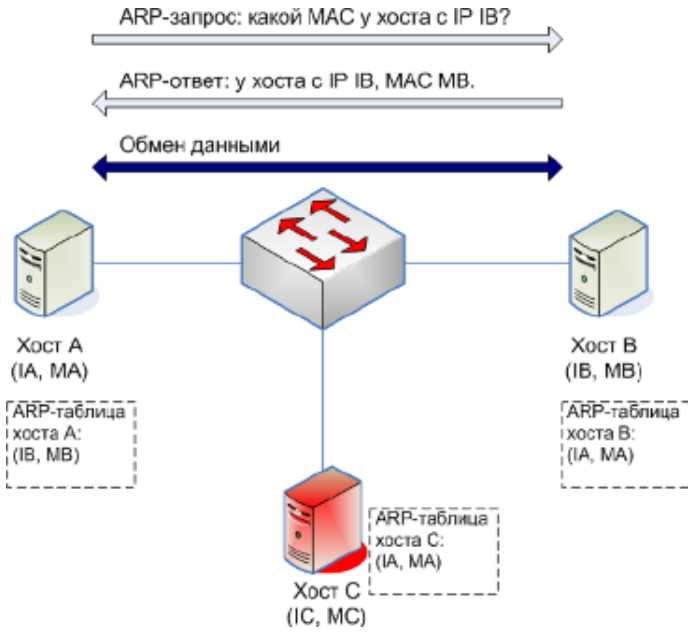

Рисунок 7 – Нормальный обмен между хостами A и B

Рисунок 8 – Хост C перехватывает трафик от хоста B

Хост C может подменить записи в ARP-таблицах коммутатора, хоста A и хоста B путем отправки поддельных ARP-ответов с IP-адресом хоста IA или IB и MAC-адресом MC. Хосты с подмененными записями будут использовать MAC-адрес MC для отправки пакетов, предназначенных для хоста A или хоста B. Таким образом, хост C будет перехватывать весь трафик. Так как хост C знает настоящие MAC-адреса, связанные с IP-адресами IA и IB, он может переправлять трафик соответствующему хосту. Хост C внедрил себя в потоки данных между хостами A и B, с помощью так называемой атаки посредника (man in the middle).

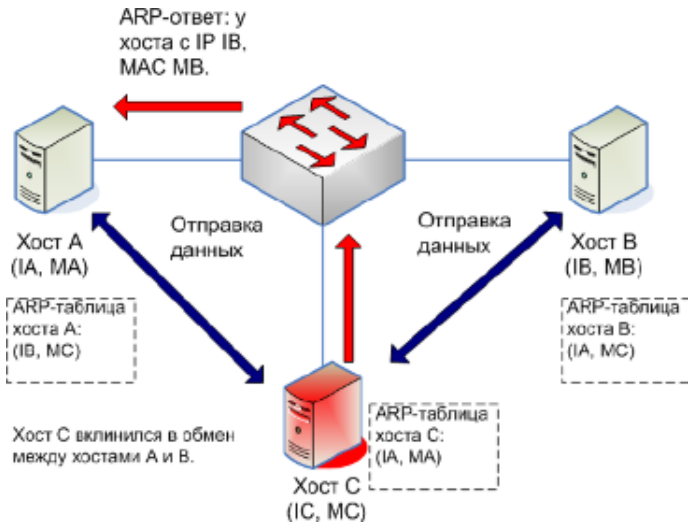

Рисунок 9 – Хост С вклинивается в обмен между хостами А и В

Dynamic ARP inspection представляет собой функцию безопасности, которая проверяет ARP-пакеты в сети. Она проверяет, журналирует и удаляет ARP-пакеты с неверными комбинациями IP-адреса и MAC-адреса, что обеспечивает защиту от атаки посредника путем подмены записей в ARP-таблицах.

ARP inspection подразделяет интерфейсы на доверенные (trusted) и недоверенные (untrusted). Проверка пакетов производится только на недоверенных интерфейсах. Пакеты, полученные на доверенных интерфейсах, передаются без каких-либо проверок.

При получении ARP-пакета на недоверенном интерфейсе, устройство проводит следующие основные проверки:

1. Если для VLAN, на котором получен пакет, задан список статических ARP-привязок (привязки IP и MAC), то производится поиск соответствия IP-адреса и MAC-адреса одной из ARP-привязок. Если привязка найдена, то пакет считается корректным.
2. Если для VLAN, на котором получен пакет, включен DHCP Snooping, то производится поиск соответствия IP-адреса и MAC-адреса одной из динамических привязок DHCP Snooping. Если привязка найдена и интерфейс, на котором получен пакет, соответствует интерфейсу в привязке DHCP Snooping, то пакет считается корректным.
3. Если IP-адрес пакета не найден ни в статических ARP-привязках, ни динамических привязках DHCP Snooping, то он отбрасывается.

При необходимости, можно активировать дополнительные проверки ARP-заголовка, которые включают в себя:

1. Проверку соответствия MAC-адреса источника в заголовке Ethernet и MAC-адреса отправителя в заголовке ARP-пакета. Проверка производится для всех ARP-пакетов.

2. Проверку соответствия MAC-адреса назначения в заголовке Ethernet и MAC-адреса назначения в заголовке ARP-пакета. Проверка производится только для ARP-ответов (включая gratuitous ARP).
3. Проверку корректности IP-адресов в заголовке ARP-пакета. Некорректными IP-адресами являются адреса 0.0.0.0, 255.255.255.255 и все мультикастовые адреса. Проверка производится для всех ARP-пакетов.

Если пакет прошел все проверки, то он переправляется в соответствующий порт или группу портов:

1. Широковещательный пакет перенаправляется во все порты, которые являются членами VLAN пакета. При этом соблюдаются ограничения Private VLAN:
   - если исходный порт пакета является изолированным, то пакет отправляется только в promiscuous порты;
   - если исходный порт пакета является членом сообщества Private VLAN (community), то пакет отправляется только в promiscuous порты и порты, относящиеся к тому же сообществу;
   - если на исходном порту пакета задан uplink-интерфейс (команда «**switchport protected**»), то пакет отправляется только в uplink-интерфейс.
2. Одноадресный пакет (unicast) отправляется в соответствии с таблицей MAC-адресов. При этом соблюдаются ограничения Private VLAN. Если в таблице MAC-адресов нет MAC-адреса, совпадающего с MAC-адресом пакета назначения, то пакет отправляется аналогично широковещательному.
3. Если пакет не может быть отправлен ни в один интерфейс из-за ограничений Private VLAN, то пакет отбрасывается.

Настройки пользователя

1. Глобальные настройки:
   - режим работы, определяющий использование статических ARP-привязок: включен, выключен;
   - интервал журналирования сообщений: целое число в диапазоне от 0 до 86400 секунд;
   - режим дополнительных проверок заголовка ARP: включен, выключен;
   - создание и удаление списков статических ARP-привязок;
   - ассоциации списков статических ARP-привязок с VLAN.

2. Настройки интерфейсов:

   – режим доверия на интерфейсе: доверенный, не доверенный.

3. Настройки списков статических ARP-привязок:

   – добавление и удаление статических ARP-привязок, состоящих из пар IP-адрес и MAC-адрес.

Дополнения и ограничения
ARP Inspection активен только на недоверенных портах DHCP Snooping.

Описание настройки
Порядок настройки ARP Inspection приведен в таблице 15.

Таблица 15 – Порядок настройки ARP Inspection

Шаг	Команда	Назначение
1	**configure terminal**	Переход в режим глобальной настройки
2	**ip arp inspection validate**	(Опционально) Включение дополнительных проверок ARP-пакетов
3	**ip arp inspection list create** *name*	(Опционально) Создание статического списка ARP-привязок
4	**ip** *ip-address* **mac** *mac-address*	(Опционально) Добавление статической ARP-привязки
5	**exit**	(Опционально) Переход в предыдущий режим настройки
6	**ip arp inspection list assign** *vlan-id name*	(Опционально) Назначение статического списка ARP-привязок на VLAN
7	**interface** *interface-id*	Переход в режим настройки интерфейса
8	**ip arp inspection trust**	Настройка режима доверия на интерфейсе
9	**exit**	Переход в предыдущий режим настройки
10	**ip arp inspection**	Включение ARP Inspection на устройстве
11	**ip arp inspection vlan** *vlan-id*	(Опционально) Включение ARP Inspection на VLAN. Для корректной работы на указанном VLAN должен быть включен DHCP Snooping
12	**exit**	Переход в предыдущий режим настройки
13	**show ip arp inspection** [*interfaceid*]	Проверка настроек ARP Inspection
14	**show ip arp inspection list** [*name*]	Проверка настроек статических списков ARP-привязок
15	**copy running-config startupconfig**	Сохранение текущей конфигурации

Рассмотрим вариант настройки со следующими условиями:

- необходимо включить ARP Inspection глобально и на VLAN 1 и 2;
- интерфейсы gigabitethernet 0/1–2 должны быть доверенными;
- на VLAN 1 и 2 необходимо добавить статические привязки с IP-адресами и MAC-адресами соответственно: 10.0.0.1 и 00:1B:28:00:00:01, 10.0.0.2 и 00:1B:28:00:00:02.

Создадим и назначим статическую привязку:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection list create servers
admin@Switch(config-ARP-list)# ip 10.0.0.1 mac 00:1B:28:00:00:01
admin@Switch(config-ARP-list)# ip 10.0.0.2 mac 00:1B:28:00:00:02
admin@Switch(config-ARP-list)# exit
admin@Switch(config)# ip arp inspection list assign 1 servers
admin@Switch(config)# ip arp inspection list assign 2 servers
admin@Switch(config)#
```

Назначим режимы доверия на интерфейсах:

```
admin@Switch(config)# interface range gigabitethernet 0/1-2
admin@Switch(config-if-range)# ip arp inspection trust
admin@Switch(config-if-range)# exit
admin@Switch(config)#
```

Включим ARP Inspection:

```
admin@Switch(config)# ip arp inspection
admin@Switch(config)# ip arp inspection vlan 1
admin@Switch(config)# ip arp inspection vlan 2
admin@Switch(config)# exit
admin@Switch#
```

Проверим параметры и сохраним файл конфигурации:

```
admin@Switch# show ip arp inspection
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1,2
Verification of packet header is Disabled
IP ARP inspection logging interval is: 5 seconds

Interface    Trusted
---------    -------
gi0/1        Yes
gi0/2        Yes
gi0/3        No
gi0/4        No

admin@Switch# show ip arp inspection list

List name: servers
Assigned to VLANs: 1,2
IP-address   MAC-address
----------   -----------------
10.0.0.1     00:1B:28:00:00:01
10.0.0.2     00:1B:28:00:00:02

admin@Switch# copy running-config startup-config
admin@Switch#
```

15.5.2 clear ip arp inspection statistics

Команда фундаментального режима. Очистка статистики ARP Inspection на всех или определенном VLAN.

Синтаксис команды:

clear ip arp inspection statistics [vlan *vlan-id***]**

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Использование команды:

Команда «**clear ip arp inspection statistics**» используется для очистки статистики ARP Inspection на всех или определенном VLAN. Если команда введена без аргументов, то очищается статистика для всех VLAN.

Пример команды:

```
admin@Switch# clear ip arp inspection statistics vlan 10
admin@Switch#
```

15.5.3 debug ip arp inspection

Команда фундаментального режима. Включение отладки ARP Inspection.

Синтаксис команды:

debug ip arp inspection all

no debug ip arp inspection all

Пример команды:

```
admin@Switch# debug ip arp inspection all
admin@Switch#
```

15.5.4 ip arp inspection

Команда глобальной настройки. Включение ARP Inspection на устройстве.

Синтаксис команды:

ip arp inspection

no ip arp inspection

Команда с приставкой «**no**» отключает ARP Inspection.

Значение по умолчанию:

ARP Inspection отключен.

Использование команды:

Команда «**ip arp inspection**» используется для включения ARP Inspection на устройстве. Указанная команда включает ARP Inspection глобально, при этом для проверки пакетов ARP используются только статические записи. Для включения проверки на основе данных DHCP Snooping используется команда «**ip arp inspection vlan**».

Если порт настроен как недоверенный (untrusted), то его также необходимо настроить как недоверенный для DHCP Snooping, либо настроить статические при-

вязки IP-адреса источника и MAC-адреса источника. В противном случае устройства, подключенные к этому порту, не смогут отвечать на ARP-запросы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection
admin@Switch(config)#
```

15.5.5 ip arp inspection debug interval

Команда глобальной настройки. Настройка минимального интервала между последовательными сообщениями, выводимыми диагностикой ARP Inspection.

Синтаксис команды:

ip arp inspection debug interval *seconds*

no ip arp inspection debug interval

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	минимальный интервал времени между последовательными сообщениями, выводимыми диагностикой ARP Inspection, в диапазоне от 0 до 86400 секунд

Значение по умолчанию:

0 секунд.

Пример команды:

```
admin@Switch(config)# ip arp inspection debug interval 120
admin@Switch(config)#
```

15.5.6 ip arp inspection list assign

Команда глобальной настройки. Назначение статического списка ARP-привязок на VLAN.

Синтаксис команды:

ip arp inspection list assign *vlan-id name*

no ip arp inspection list assign *vlan-id*

Команда с приставкой «**no**» прекращает использование статического списка ARP-привязок на VLAN.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
name	имя статического списка ARP-привязок

Значение по умолчанию:

Статические списки ARP-привязок не назначены ни на один VLAN.

Использование команды:

Команда «**ip arp inspection list assign**» используется для назначения статического списка ARP-привязок на VLAN.

На один и тот же VLAN можно назначить несколько статических списков ARPпривязок, а также использовать один и тот же список в нескольких VLAN.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection list assign 10 servers
admin@Switch(config)#
```

15.5.7 ip arp inspection list create

Команда глобальной настройки. Создание статического списка ARP-привязок и переход в режим настройки списка (ARP list configuration mode).

Синтаксис команды:

ip arp inspection list create *name*

no ip arp inspection list create *name*

Команда с приставкой «**no**» удаляет статический список ARP-привязок.

Параметры команды:

name	имя статического списка ARP-привязок

Значение по умолчанию:

Статические списки ARP-привязок отсутствуют.

Использование команды:

Команда «**ip arp inspection list create**» используется для создания статического списка ARP-привязок и перехода в режим настройки списка (ARP list configuration mode). Каждая ARP-привязка представляет собой связанную пару из MAC-адреса источника и IP-адреса источника.

После настройки статического списка ARP-привязок его можно назначить на VLAN с помощью команды «**ip arp inspection list assign**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection list create servers
admin@Switch(config-ARP-list)# ip 10.0.0.1 mac 00:1B:BA:BE:FA:CE
admin@Switch(config-ARP-list)#
```

15.5.8 ip arp inspection logging interval

Команда глобальной настройки. Настройка минимального интервала между последовательными сообщениями, выводимыми ARP Inspection.

Синтаксис команды:

ip arp inspection logging interval {*seconds* **| infinite}**

no ip arp inspection logging interval

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	минимальный интервал времени между последовательными сообщениями, выводимыми ARP Inspection, в диапазоне от 0 до 86400 секунд
infinite	отключение генерации сообщений ARP Inspection

Значение по умолчанию:

Минимальный интервал между последовательными сообщениями ARP Inspection равен 5 секундам.

Использование команды:

Команда «**ip arp inspection logging interval**» используется для настройки минимального интервала между последовательными сообщениями, выводимыми ARP Inspection.

Устройство может обрабатывать сотни ARP-запросов в секунду. Генерация сообщения для каждого из них может существенно повысить нагрузку на процессор устройства, поэтому не рекомендуется устанавливать минимальный интервал, равный нулю.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection logging interval 2
admin@Switch(config)#
```

15.5.9 ip arp inspection validate

Команда глобальной настройки. Включение дополнительных проверок ARP-пакетов.

Синтаксис команды:

ip arp inspection validate

no ip arp inspection validate

Команда с приставкой «**no**» отключает дополнительные проверки ARP-пакетов.

Значение по умолчанию:

Дополнительные проверки ARP-пакетов отключены.

Использование команды:

Команда «**ip arp inspection validate**» используется для включения дополнительных проверок ARP-пакетов.

Дополнительные проверки включают в себя:

1. Проверку соответствия MAC-адреса источника в заголовке Ethernet и MAC-адреса отправителя в заголовке ARP-пакета. Проверка производится для всех ARP-пакетов.
2. Проверку соответствия MAC-адреса назначения в заголовке Ethernet и MAC-адреса назначения в заголовке ARP-пакета. Проверка производится только для ARP-ответов (включая gratuitous ARP).
3. Проверку корректности IP-адресов в заголовке ARP-пакета. Некорректными IP-адресами являются адреса 0.0.0.0, 255.255.255.255 и все мультикастовые адреса. Проверка производится для всех ARP-пакетов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection validate
admin@Switch(config)#
```

15.5.10 ip arp inspection vlan

Команда глобальной настройки. Включение ARP Inspection на VLAN с использованием информации DHCP Snooping.

Синтаксис команды:

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan *vlan-id*

Команда с приставкой «**no**» отключает ARP Inspection на VLAN.

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

ARP Inspection отключен на всех VLAN.

Использование команды:

Команда «**ip arp inspection vlan**» применяется для включения ARP Inspection на VLAN с использованием информации DHCP Snooping.

Если порт настроен как недоверенный (untrusted), то его также необходимо настроить как недоверенный для DHCP Snooping. В противном случае устройства, подключенные к этому порту, не смогут отвечать на ARP-запросы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection vlan 10
admin@Switch(config)#
```

15.5.11 ip arp inspection trust

Команда настройки интерфейса (Ethernet). Установка доверенного режима ARP Inspection на интерфейсе.

Синтаксис команды:

ip arp inspection trust

no ip arp inspection trust

Команда с приставкой «**no**» устанавливает недоверенный режим ARP Inspection на интерфейсе.

Значение по умолчанию:

Интерфейс является недоверенным.

Использование команды:

Команда «**ip arp inspection trust**» используется для установки доверенного режима ARP Inspection на интерфейсе.

Устройство не проверяет ARP-пакеты, полученные на доверенных интерфейсах, а только перенаправляет их дальше.

На недоверенных интерфейсах устройство перехватывает ARP-пакеты и проверяет соответствие MAC-адреса источника и IP-адреса назначения. Дополнительно устройство может проверять корректность остальных параметров в ARP-пакете, если проверка включена командой глобальной настройки «**ip arp inspection validate**». Пакеты, не отвечающие требованиям, отбрасываются и устройство генерирует соответствующее сообщение.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip arp inspection trust
admin@Switch(config-if)#
```

15.5.12 ip mac

Команда настройки списков ARP-привязок. Добавление статической ARP-привязки.

Синтаксис команды:

ip *ip-address* **mac** *mac-address*

no ip *ip-address* **mac** *mac-address*

Команда с приставкой «**no**» удаляет статическую ARP-привязку.

Параметры команды:

ip-address	IP-адрес хоста
mac-address	MAC-адрес хоста

Значение по умолчанию:

Статические ARP-привязки отсутствуют.

Использование команды:

Команда «**ip mac**» используется для добавления статической ARP-привязки.

Ключом в списке ARP-привязок является IP-адрес, поэтому несколько IP-адресов могут ассоциироваться с одним MAC-адресом. Если IP-адрес создаваемой привязки совпадает с какой-либо существующей привязкой в списке, то существующая привязка замещается.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip arp inspection list create servers
admin@Switch(config-ARP-list)# ip 10.0.0.1 mac 00:1B:BA:BE:FA:CE
admin@Switch(config-ARP-list)#
```

15.5.13 show ip arp inspection interface

Команда, доступная из любого режима. Вывод настроек ARP Inspection.

Синтаксис команды:

show ip arp inspection interface [*interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show ip arp inspection interface**» используется для вывода настроек ARP Inspection. Если команда введена без аргументов, то выводятся настройки всех интерфейсов.

Пример команды:

```
admin@Switch# show ip arp inspection interface
IP ARP inspection is Enabled
IP ARP inspection is configured on following VLANs: 1
Verification of packet header is Enabled
IP ARP inspection logging interval is: 5 seconds
Interface    Trusted
---------    -------
gi0/1        Yes
gi0/2        Yes
gi0/3        No
gi0/4        Yes
```

15.5.14 show ip arp inspection list

Команда, доступная из любого режима. Вывод статических списков ARP-привязок.

Синтаксис команды:

show ip arp inspection list [*name*]

Параметры команды:

name имя статического списка ARP-привязок

Использование команды:

Команда «**show ip arp inspection list**» используется для вывода настроек статических списков ARP-привязок. Если команда введена без аргументов, то выводится информация обо всех списках.

Пример команды:

```
admin@Switch# show ip arp inspection list
List name: servers
  Assigned to VLANs: 1,2
IP-address   MAC-address
----------   -----------------
10.0.0.1     00:1B:28:00:00:01
10.0.0.2     00:1B:28:00:00:02
```

15.5.15 show ip arp inspection statistics

Команда, доступная из любого режима. Вывод статистики ARP Inspection на VLAN.

Синтаксис команды:

show ip arp inspection statistics [vlan *vlan-id***]**

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Использование команды:

Команда «**show ip arp inspection statistics**» используется для вывода статистики ARP Inspection на VLAN.

Если команда введена без аргументов, то выводится информация для всех VLAN. Описание параметров вывода приведено в таблице 16.

Пример команды:

```
admin@Switch# show ip arp inspection statistics
Vlan    Forwarded Packets  Dropped Packets    IP/MAC Failures
----    -----------------  ---------------    ---------------
2       1500               100                80
```

Таблица 16 – Описание параметров вывода

Название	Описание
Forwarded Packets	Количество пакетов, успешно прошедших проверки ARP Inspection
Dropped Packets	Количество пакетов, которые были отброшены по любой причине (несоответствие IP – MAC, некорректный заголовок ARP и т.п.)
IP/MAC Failures	Количество пакетов, которые были отброшены из-за несоответствия IP – MAC

15.6 Настройка защиты от DoS-атак (автоматизированная защита от SYN/SYN-ACK Flooding)

15.6.1 Общее положение:

SYN flood – одна из уязвимостей, которая использует преимущества TCP/IP для подавления систем. Атаки SYN/SYN-ACK Flooding используют процесс, известный как «трехстороннее рукопожатие» по протоколу TCP. В рамках подтверждения клиент и сервер обмениваются сообщениями для установления канала связи.

Данная команда предназначена для фильтрации и дальнейшей блокировки TCP-пакетов, с указанными параметрами:

- **SYN** (Synchronized) – используется при установлении TCP-соединения;
- **PSH** (Push) – флаг форсированной отправки сегмента;
- **FIN** (Finish) – используется при нормальном закрытии TCP-соединения;
- **URG** (Urgent) – флаг срочности;
- **RST** (Reset) – используется при аварийном закрытии TCP-соединения;
- **ACK** (Acknowledge) – сегмент был получен принимающей стороной.

15.6.2 ip tcp

Команда глобальной настройки. Включение фильтрации TCP-пакетов поступающих на коммутатор.

Синтаксис команды:

ip tcp {all | flag {fin-urg-psh | syn-fin | syn-rst | zero} | port {zero}}

no ip tcp {all | flag {fin-urg-psh | syn-fin | syn-rst | zero} | port {zero}}

Команда с приставкой «**no**» отключает фильтрацию по флагам TCP-пакетов поступающих на коммутатор.

Параметры команды:

all	блокировка любых TCP-пакетов, поступающих на интерфейс
flag fin-urg-psh	блокировка TCP-пакетов с флагами FIN, URG, PSH, поступающих на коммутатор
flag syn-fin	блокировка TCP-пакетов с флагами SYN, FIN, поступающих на коммутатор
flag syn-rst	блокировка TCP-пакетов с флагами SYN, RST, поступающих на коммутатор. При отправке с флагом RST, пакет будет блокироваться, так как сам флаг подразумевает разрыв соединения
flag zero	блокировка TCP-пакетов со всеми нулевыми флагами, поступающими на коммутатор
port zero	блокировка TCP-пакетов, поступающих на коммутатор, имеющих нулевые порты источника или назначения

Значение по умолчанию:

Блокировка TCP-пакетов отключена.

Использование команды:

Команда используется для фильтрации TCP-пакетов, поступающих на коммутатор.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip tcp flag fin-urg-psh
admin@Switch(config-if)# end
```

16 Маршрутизация

16.1 Команды, независимые от протокола маршрутизации IP

16.1.1 key chain

Команда глобальной настройки. Создание именованного набора ключей.

Синтаксис команды:

key chain *name-of-chain*

no key chain *name-of-chain*

Команда с приставкой «**no**» удаляет именованный набор ключей.

Параметры команды:

name-of-chain имя набора ключей в виде текстовой строки

Значение по умолчанию:

Именованные наборы ключей отсутствуют.

Использование команды:

Команда «**key chain**» используется для создания именованного набора ключей. Именованные набор ключей позволяют протоколам, использующим наборы ключей, переключаться со старых ключей на новые в автоматическом режиме.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# key chain keychain1
admin@Switch(config-keychain)# key 1
admin@Switch(config-keychain-key)# key-string string1
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 January 1 2015 11:00:00
                                        February 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 January 1 2015 10:00:00
                                        February 1 2015
admin@Switch(config-keychain-key)# exit
admin@Switch(config-keychain)# key 2
admin@Switch(config-keychain-key)# key-string string2
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 February 1 2015 11:00:00
                                        March 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 February 1 2015 10:00:00
                                        March 1 2
admin@Switch(config-keychain-key)#
```

16.1.2 key

Команда настройки набора ключей. Создание ключа в наборе ключей.

Синтаксис команды:

key *key-id*

no key *key-id*

Команда с приставкой «**no**» удаляет ключ из набора ключей.

Параметры команды:

key-id номер ключа в диапазоне от 1 до 2147483647

Значение по умолчанию:

Ключи аутентификации отсутствуют.

Использование команды:

Команда «**key**» используется для создания ключа в наборе ключей.

Каждый ключ имеет свой номер, сохраненный локально. В каждый момент времени используется только один ключ для отправки пакетов независимо от того, сколько ключей разрешено к использованию.

Для этого устройство находит первый разрешенный в настоящее время ключ, начиная с наименьшего по номеру ключа.

Рекомендуется настроить синхронизацию времени с помощью протокола NTP при использовании времени действия ключа аутентификации.

Если истек срок действия последнего ключа, то процесс аутентификации будет завершаться с ошибкой.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# key chain keychain1
admin@Switch(config-keychain)# key 1
admin@Switch(config-keychain-key)# key-string string1
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 January 1 2015 11:00:00
                                    February 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 January 1 2015 10:00:00
                                    February 1 2015
admin@Switch(config-keychain-key)# exit
admin@Switch(config-keychain)# key 2
admin@Switch(config-keychain-key)# key-string string2
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 February 1 2015 11:00:00
                                    March 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 February 1 2015 10:00:00
                                    March 1 2
admin@Switch(config-keychain-key)#
```

16.1.3 accept-lifetime

Команда настройки набора ключей. Установка времени действия ключа аутентификации, используемого при аутентификации входящих пакетов.

Синтаксис команды:

accept-lifetime *start-time* **{infinite |** *end-time* **| duration** *seconds***}**

no accept-lifetime

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

infinite	ключ действует без ограничения срока действия
duration *seconds*	период времени, в течение которого действует ключ, в диапазоне от 1 до 2147483646 секунд

end-time — время окончания действия ключа. Синтаксис данного параметра совпадает с синтаксисом параметра «*start-time*». Дата, указываемая параметром «*end-time*», должна быть хронологически позже даты, указанной в параметре «*start-time*»

start-time — время начала действия ключа, установленного командой «**key**». Синтаксис параметра: “hh:mm:ss Month day year”, где:

- *hh* – часы (от 0 до 23);
- *mm* – минуты (от 0 до 59);
- *ss* – секунды (от 0 до 59);
- *Month* – месяц из списка: January, February, March, April, May, June, July, August, September, October, November, December;
- *day* – день месяца (от 1 до 31);
- *year* – год в формате “ГГГГ”

Значение по умолчанию:

Ключ действует без ограничения срока действия.

Использование команды:

Команда «**accept-lifetime**» используется для установки времени действия ключа аутентификации, используемого при аутентификации входящих пакетов.

Рекомендуется настроить синхронизацию времени с помощью протокола NTP при использовании времени действия ключа аутентификации.

Если истек срок действия последнего ключа, то процесс аутентификации будет завершаться с ошибкой.

Настройка времени в «**accept-lifetime**» производится в UTC+0, так как не считывается смещение по часовому поясу (UTC). По умолчанию на устройстве стоит часовой пояс Екатеринбурга (UTC+5).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# key chain keychain1
admin@Switch(config-keychain)# key 1
admin@Switch(config-keychain-key)# key-string string1
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 January 1 2015 11:00:00
                                    February 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 January 1 2015 10:00:00
                                    February 1 2015
admin@Switch(config-keychain-key)# exit
admin@Switch(config-keychain)# key 2
admin@Switch(config-keychain-key)# key-string string2
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 February 1 2015 11:00:00
                                    March 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 February 1 2015 10:00:00
                                    March 1 2
admin@Switch(config-keychain-key)#
```

16.1.4 key-string

Команда настройки набора ключей. Установка значения ключа аутентификации.

Синтаксис команды:

key-string *text*

no key-string

Команда с приставкой «**no**» удаляет значение ключа аутентификации.

Параметры команды:

text	значение ключа аутентификации в виде текстовой строки длиной от 1 до 80 символов

Значение по умолчанию:

Значение ключа аутентификации не задано.

Использование команды:

Команда «**key-string**» используется для установки значения ключа аутентификации.

Значение ключа аутентификации записывается в файл конфигурации в зашифрованном виде.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# key chain keychain1
admin@Switch(config-keychain)# key 1
admin@Switch(config-keychain-key)# key-string string1
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 January 1 2015 11:00:00
                                        February 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 January 1 2015 10:00:00
                                        February 1 2015
admin@Switch(config-keychain-key)# exit
admin@Switch(config-keychain)# key 2
admin@Switch(config-keychain-key)# key-string string2
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 February 1 2015 11:00:00
                                        March 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 February 1 2015 10:00:00
                                        March 1 2
admin@Switch(config-keychain-key)#
```

16.1.5 send-lifetime

Команда настройки набора ключей. Установка времени действия ключа аутентификации, используемого при аутентификации исходящих пакетов.

Синтаксис команды:

send-lifetime *start-time* **{infinite |** *end-time* **| duration** *seconds***}**

no send-lifetime

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

infinite ключ действует без ограничения срока действия

end-time время окончания действия ключа. Синтаксис данного параметра совпадает с синтаксисом параметра «*start-time*». Дата, указываемая параметром «*end-time*», должна быть хронологически позже даты, указанной в параметре «*start-time*»

start-time время начала действия ключа, установленного командой «**key**». Синтаксис параметра: “hh:mm:ss Month day year”, где:

- *hh* – часы (от 0 до 23);
- *mm* – минуты (от 0 до 59);
- *ss* – секунды (от 0 до 59);
- *Month* – месяц из списка: January, February, March, April, May, June, July, August, September, October, November, December;
- *day* – день месяца (от 1 до 31);
- *year* – год в формате “ГГГГ”

duration *seconds* период времени, в течение которого действует ключ, в диапазоне от 1 до 2147483646 секунд

Значение по умолчанию:

Ключ действует без ограничения срока действия.

Использование команды:

Команда «**send-lifetime**» используется для установки времени действия ключа аутентификации, используемого при аутентификации исходящих пакетов.

Рекомендуется настроить синхронизацию времени с помощью протокола NTP при использовании времени действия ключа аутентификации.

Если истек срок действия последнего ключа, то процесс аутентификации будет завершаться с ошибкой.

Настройка времени в «**send-lifetime**» производится в UTC+0, так как не считывается смещение по часовому поясу (UTC). По умолчанию на устройстве стоит часовой пояс Екатеринбурга (UTC+5).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# key chain keychain1
admin@Switch(config-keychain)# key 1
admin@Switch(config-keychain-key)# key-string string1
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 January 1 2015 11:00:00
                                    February 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 January 1 2015 10:00:00
                                    February 1 2015
admin@Switch(config-keychain-key)# exit
admin@Switch(config-keychain)# key 2
admin@Switch(config-keychain-key)# key-string string2
admin@Switch(config-keychain-key)# accept-lifetime 9:00:00 February 1 2015 11:00:00
                                    March 1 2015
admin@Switch(config-keychain-key)# send-lifetime 10:00:00 February 1 2015 10:00:00
                                    March 1 2015
admin@Switch(config-keychain-key)#
```

16.1.6 show key chain

Команда, доступная из любого режима. Вывод именованных наборов ключей.

Синтаксис команды:

show key chain [*name-of-chain*]

Параметры команды:

name-of-chain имя набора ключей

Использование команды:

Команда «**show key chain**» используется для вывода именованных наборов ключей. Если команда введена без аргументов, то выводятся все именованные наборы ключей.

Пример команды:

```
admin@Switch# show key chain

keychain1:
—-
key 1
   key-string is not shown
   send-lifetime 00:00:00 January 1 2020 01:00:00 February 1 2021
   accept-lifetime 00:00:00 January 1 2020 11:00:00 February 1 2021
```

16.2 Статическая маршрутизация

16.2.1 ip route

Команда глобальной настройки. Определение статических маршрутов.

Синтаксис команды:

ip route *prefix* {*mask* | */prefix-length*} *ip-address*

no ip route *prefix* {*mask* | */prefix-length*} [*ip-address*]

Команда с приставкой «**no**» удаляет статические маршруты.

Параметры команды:

prefix	IP-префикс маршрута для IP назначения
mask	сетевая маска подсети префикса IP-адреса
/prefix-length	длина префикса IP-адреса в диапазоне от 0 до 32 бит. Значению длины префикса должна предшествовать «косая черта» (/)
ip-address	IP-адрес следующего узла назначения на пути достижения сети

Значение по умолчанию:

По умолчанию статические маршруты не определены.

Использование команды:

Используйте команду «**ip route**», чтобы прописать маршруты для маршрутизации по разным VLAN.

Команда «**no ip route**» без параметра «*ip-address*» удаляет все статические маршруты до заданной подсети.

Команда «**no ip route**» с параметром «*ip-address*» удаляет только один статический маршрут до заданной подсети через заданный следующий узел.

Примеры команды:

```
admin@Switch(config)# ip route 10.0.0.0 /24 192.168.1.1
```

```
admin@Switch(config)# ip route 123.5.0.0 255.255.0.0 192.168.5.21
```

16.2.2 show ip route

Команда фундаментального режима. Вывод информации о текущем состоянии таблицы маршрутизации.

Синтаксис команды:

show ip route [connected | static | all | bgp | address {*ip-address* **[***mask* **|** *prefixlength***] [***longer-prefixes***]}]**

Параметры команды:

connected	выводит на экран информацию только о подключенных маршрутах
static	выводит на экран информацию только о статических маршрутах
all	выводит на экран детальную информацию обо всех маршрутах
bgp	выводит на экран информацию только о BGP маршрутах
address	выводит на экран информацию об указанном маршруте
ip-address	адрес, для которого выводится информация о маршрутизации
mask	сетевая маска подсети IP-адреса
prefix-length	длина префикса IP-адреса длиной от 1 до 32. Значению длины префикса должна предшествовать «косая черта» (/)
longer-prefixes	обозначение того, что пара параметров «**address**» и «**mask**» является префиксом, и выводится информация для любого маршрута, соответствующего данному префиксу

Пример команды:

```
admin@Switch(config)# show ip route
Codes: C - connected, S - static, B - BGP derived
B ! 1.1.0.0/1 (100) via 192.168.5.22 vlan 1
S ! 1.2.0.0/1 (100) via 192.168.1.1 vlan 1
C ! 192.168.0.0/94 (0) directly connected vlan 1
```

16.3 Настройка RIP

16.3.1 Общие положения

Протокол маршрутной информации (Routing Information Protocol, RIP) – внутренний протокол маршрутизации дистанционно-векторного типа.

Самым главным преимуществом RIP является простота его развертывания и настройки. Основной недостаток RIP заключается в неспособности обеспечить масштабируемость в больших и очень больших объединенных сетях. RIP-маршрутизаторы поддерживают максимум 15 прыжков. Сети, расположенные на расстоянии 16 или более прыжков, считаются недостижимыми. По мере расширения объединенной сети периодические объявления каждого из RIP-маршрутизаторов могут существенно увеличить трафик. Еще один недостаток RIP – значительное время переконфигурирования. Если топология сети изменилась, для перенастройки RIP-маршрутизаторов с учетом новой топологии может потребоваться несколько минут.

При изменении конфигурации объединенной сети могут возникнуть циклические маршруты, следствием чего является невозможность доставки или потеря данных.

Настройки пользователя

1. Глобальные настройки:
   - включение и отключение протокола RIP.
2. Настройки интерфейсов (VLAN):
   - значение метрики, добавляемой к полученным маршрутам RIP: целое число в диапазоне от 1 до 15;
   - приостановка (временное отключение) протокола RIP на интерфейсе.
3. Настройки процесса маршрутизации:
   - добавление и удаление интерфейса в протокол RIP;
   - настройка распределения маршрутов из одного домена маршрутизации в другой;
   - приостановка (временное отключение) протокола RIP на устройстве;
   - набор ключей, который будет использован протоколом RIP при аутентификации: имя набора в виде строки;
   - режим аутентификации в протоколе RIP: none, text, md5.

Дополнения и ограничения

Поддерживается только протокол RIPv2, пакеты протокола RIPv1 игнорируются устройством.

Описание настройки

Порядок настройки маршрутизации RIP приведен в таблице 17.

Таблица 17 – Порядок настройки маршрутизации RIP

Команда	Назначение
configure terminal	Переход в режим глобальной настройки
router rip	Переход в режим настройки маршрутизации RIP
network *ip-address*	Включение RIP на интерфейсе с указанным IP-адресом
redistribute *protocol* [*process-id*] [**metric** *metric-value* | **transparent**] [**match** {**internal** | **external 1** | **external 2**}]	(Опционально) Включение распределения маршрутов из одного домена маршрутизации в другой
exit	Переход в предыдущий режим настройки
interface vlan *vlan-id*	Переход в режим настройки интерфейса VLAN
ip rip offset *offset*	Установка значения метрики, добавляемой к полученным маршрутам RIP
exit	Переход в предыдущий режим настройки
exit	Переход в предыдущий режим настройки
show ip rip	Проверка глобальных настроек RIP
copy running-config startup-config	Сохранение текущей конфигурации

16.3.2 debug ip rip

Команда фундаментального режима. Включение отладки RIP.
Синтаксис команды:
debug ip rip {all | events | filters | interfaces | packets | routes | states}
no debug ip rip {all | events | filters | interfaces | packets | routes | states}
Команда с приставкой «**no**» отключает отладку RIP.
Параметры команды:

all вывод всех сообщений

events вывод сообщений о событиях, внутренних для протокола

filters вывод подробной информации о фильтрации маршрутов

interfaces вывод событий изменения интерфейса, отправленные в протокол

packets вывод информации о пакетах, отправленных и полученных протоколом

routes вывод информации о маршрутах, которые были обменены с таблицей маршрутизации

states вывод информации об изменениях состояния протокола

Пример команды:

```
admin@Switch# debug ip rip all
admin@Switch#
```

16.3.3 router rip

Команда глобальной настройки. Включение протокола RIP и переход в режим настройки маршрутизации RIP.

Синтаксис команды:

router rip

no router rip

Команда с приставкой «**no**» отключает протокол RIP и удаляет его настройки.

Значение по умолчанию:

Протокол RIP отключен.

Использование команды:

Команда «**router rip**» используется для включения протокола RIP и перехода в режим настройки маршрутизации RIP.

Маршрутизация RIP может находиться в следующих состояниях:

1. Отключен. В этом состоянии RIP не работает и не может быть настроен. При переходе в это состояние вся конфигурация RIP удаляется. Для отключения RIP используется команда «**no router rip**».
2. Приостановлен. В этом состоянии RIP не работает, но может быть настроен. При переходе в это состояние вся конфигурация RIP сохраняется. В это состояние можно перейти только из состояния “Включен” при помощи команды «**shutdown**».
3. Включен. В этом состоянии RIP работает и может быть настроен. Для включения RIP из состояния “Отключен” используется команда «**router rip**», а для включения RIP из состояния “Приостановлен” используется команда «**no shutdown**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router rip
admin@Switch(config-rip)#
```

16.3.4 authentication key-chain

Команда настройки маршрутизации RIP. Установка набора ключей, который будет использован протоколом RIP при аутентификации.

Синтаксис команды:

authentication key-chain *name-of-chain*

no authentication key-chain

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

name-of-chain	имя набора ключей

Значение по умолчанию:

Набор ключей не определен.

Использование команды:

Команда «**authentication key-chain**» используется для установки набора ключей, который будет использован протоколом RIP при аутентификации.

Для каждого интерфейса можно указать только один набор ключей. Каждая последующая команда «**authentication key-chain**» переопределяет старое значение настройки.

В целях беспрерывного перехода на новый ключ в наборе ключей, время жизни нового ключа должно начинаться на несколько минут раньше времени окончания жизни текущего ключа.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router rip
admin@Switch(config-rip)# authentication key-chain alpha
admin@Switch(config-rip)#
```

16.3.5 authentication mode

Команда настройки маршрутизации RIP. Включение аутентификации в протоколе RIP на интерфейсе.

Синтаксис команды:

authentication mode {text | md5}

authentication mode

Команда с приставкой «**no**» отключает аутентификацию в протоколе RIP на интерфейсе.

Параметры команды:

text	аутентификации по простому текстовому паролю
md5	аутентификации с использованием алгоритма хеширования MD5

Значение по умолчанию:

Аутентификация отключена.

Использование команды:

Команда «**authentication mode**» используется для включения аутентификации в протоколе RIP на интерфейсе.

Если включена аутентификация с использованием алгоритма хеширования MD5, то необходимо задать имя набора ключей с помощью команды «**authentication key-chain**». Если набор ключей не задан или набор ключей не содержит ни одного корректного ключа, то протокол RIP на интерфейсе будет отключен.

Если включена аутентификация с простого текстового пароля, то необходимо задать пароль с помощью команды «**authentication-key**». Если пароль не задан, то протокол RIP на интерфейсе будет отключен.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router rip
admin@Switch(config-rip)# ip rip authentication mode md5
admin@Switch(config-rip)#
```

16.3.6 ip rip offset

Команда настройки интерфейса (VLAN). Установка значения метрики, добавляемой к полученным маршрутам RIP.

Синтаксис команды:

ip rip offset *offset*

no ip rip offset

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

offset	значение метрики, добавляемой к полученным маршрутам RIP, в диапазоне от 1 до 15

Значение по умолчанию:

К полученным маршрутам RIP добавляется метрика, равная 1.

Использование команды:

Команда «**ip rip offset**» используется для установки значения метрики, добавляемой к полученным маршрутам RIP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip rip offset 2
admin@Switch(config-if)#
```

16.3.7 ip rip shutdown

Команда настройки интерфейса (VLAN). Приостановка протокола RIP на интерфейсе.

Синтаксис команды:

ip rip shutdown

no ip rip shutdown

Команда с приставкой «**no**» включает протокол RIP на интерфейсе.

Значение по умолчанию:

Протокол RIP включен на интерфейсе.

Использование команды:

Команда «**ip rip shutdown**» используется для приостановки протокола RIP на интерфейсе. Эта команда может быть полезна для временного отключения протокола RIP на интерфейсе без удаления его конфигурации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip rip shutdown
admin@Switch(config-if)#
```

16.3.8 ip rip ttl-security

Команда настройки интерфейса (VLAN). Включение проверки времени жизни пакетов RIP (Time-to-Live) на интерфейсе.

Синтаксис команды:

ip rip ttl-security

no ip rip ttl-security

Команда с приставкой «**no**» отключает проверку.

Значение по умолчанию:

Протокол RIP включен на интерфейсе.

Использование команды:

Команда «**ip rip ttl-security**» используется для включения проверки времени жизни пакетов RIP (Time-to-Live) на интерфейсе.

При включении проверки времени жизни RIP отправляет пакеты с TTL, равным 255 вместо TTL 1, используемого по умолчанию. Это усложняет процесс подмены пакетов от удаленных устройств.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip rip ttl-security
admin@Switch(config-if)#
```

16.3.9 network

Команда настройки маршрутизации RIP. Включение RIP на интерфейсе с указанным IP-адресом.

Синтаксис команды:

network *ip-address* **[shutdown]**

no network *ip-address*

Команда с приставкой «**no**» отключает RIP на интерфейсе с указанным IP-адресом и удаляет конфигурацию RIP на этом интерфейсе.

Параметры команды:

p-address	IP-адрес на интерфейсе устройства
shutdown	включение RIP на интерфейсе в приостановленном состоянии

Значение по умолчанию:

RIP отключен на интерфейсе.

Использование команды:

Команда «**network**» используется для включения RIP на интерфейсе с указанным IP-адресом.

RIP может быть включен только на интерфейсах со статическими IP-адресами, то есть RIP не может быть включен на интерфейсе, который получил адрес по протоколу DHCP.

Использовать ключевое слово «**shutdown**» для включения RIP на интерфейсе в приостановленном состоянии, если необходимо изменить какие-либо настройки RIP перед его активацией.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router rip
admin@Switch(config-rip)# network 1.2.3.4
admin@Switch(config-rip)#
```

```
admin@Switch# configure terminal
admin@Switch(config)# router rip
admin@Switch(config-rip)# network 4.3.2.1 shutdown
admin@Switch(config-rip)#
```

16.3.10 redistribute (RIP)

Команда настройки маршрутизации RIP. Включение распределения маршрутов из одного домена маршрутизации в другой.

Синтаксис команды:

redistribute *protocol* **[***process-id***] [metric {***metric-value* **| transparent}] [match {internal | external 1 | external 2}]**

no redistribute *protocol* **[***process-id***] [metric {***metric-value* **| transparent}] [match {internal | external 1 | external 2}]**

Команда с приставкой «**no**» отключает распределение маршрутов.

Параметры команды:

protocol — источник маршрутов, которые будут распределены. Варианты протокола:

- bgp – источником является протокол BGP;
- connected – источником являются сети, подключенные напрямую (для которых задан IP-адрес на одном из интерфейсов устройства);
- ospf – источником является процесс OSPF;
- static – источником являются статические маршруты;
- rip – источником является протокол RIP

process-id	идентификатор процесса OSPF, из которого будут распределяться маршруты. По умолчанию используется номер 1. Не используется, если источником указан не протокол OSPF
metric *metric-value*	значение метрики маршрута, назначаемой для распределяемых маршрутов. Значение метрики указано в отображении маршрутов (заданной командой «**set metric**») имеет приоритет перед настройкой «*metric-value*» (замещает ее)
metric transparent	метрики маршрутов равны метрикам, которые им назначил протокол-источника этих маршрутов. Таким образом могут распределяться только маршруты с метрикой меньше 16
match {internal | external 1 | external 2}	критерии, по которым маршруты OSFP распределяются в процесс RIP: – **internal** – внутренние маршруты автономной системы; – **external 1** – внешние маршруты для автономной системы, которые импортированы в OSPF как внешний маршрут Тип 1; – **external 2** – внешние маршруты для автономной системы, которые импортированы в OSPF как внешний маршрут Тип 2. По умолчанию распределяются маршруты **internal** и **external 1**

Значение по умолчанию:

Распределение маршрутов отключено.

Использование команды:

Команда «**redistribute**» используется для включения распределения маршрутов из одного домена маршрутизации в другой.

Смена настройки, ассоциированной с ключевым словом, не затрагивает остальные настройки.

Устройство, получающее маршруты по протоколу на основе состояний соединения (например, OSPF) с внутренней метрикой, будет считать, что стоимость маршрута равна стоимости от самого себя до устройства, распределяющего маршруты плюс анонсированную стоимость до точки назначения. Для внешней метрики стоимость равна только анонсированной стоимости до точки назначения.

Распределение маршрутов с помощью ключевого слова «**connected**» охватывает только те сети, подключенные напрямую, которые не указаны явно с помощью команды «**network**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router rip
admin@Switch(config-ospf)# redistribute static
admin@Switch(config-ospf)#
```

16.3.11 shutdown

Команда настройки маршрутизации RIP. Перевод RIP в приостановленное состояние.

Синтаксис команды:

shutdown

no shutdown

Команда с приставкой «**no**» переводит RIP во включенное (активное) состояние.

Значение по умолчанию:

RIP включен.

Использование команды:

Команда «**shutdown**» используется для перевода RIP в приостановленное состояние. Эта команда может быть полезна для временного отключения RIP без удаления его конфигурации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router rip
admin@Switch(config-rip)# shutdown
admin@Switch(config-rip)#
admin@Switch#
```

16.3.12 show ip rip

Команда, доступная из любого режима. Вывод настроек RIP.

Синтаксис команды:

show ip rip [*ip-address*]

Параметры команды:

ip-address	вывод настроек RIP для указанного IP-интерфейса

Использование команды:

Команда «**show ip rip**» используется для вывода настроек RIP. Если команда введена без аргументов, то выводятся все настройки RIP.

Примеры команды:

```
admin@Switch# show ip rip
  RIP is enabled
  RIP Administrative state is UP
  Default metric value is 5

IP Interface Admin state  Authentication   Keychain     Metric offset
------------ -----------  --------------   -----------  -------------
1.1.1.1      Up           MD5              mykeychain   1
2.2.2.2      Up           text             mykeychain2  2
```

```
admin@Switch# show ip rip
  RIP is disabled
```

16.3.13 show ip rip statistics

Команда, доступная из любого режима. Вывод счетчиков статистики RIP.

Синтаксис команды:

show ip rip statistics

Использование команды:

Команда «**show ip rip statistics**» используется для вывода счетчиков статистики RIP.

Пример команды:

```
admin@Switch# show ip rip statistics
Routes: 0 imported, 3 exported, 0 preferred
Route change stats: received rejected filtered ignored accepted
Import updates:         0    0    0    0    0
Import withdraws:       0    0    --   0    0
Export updates:         3    0    0    --   3
Export withdraws:       0    --   --   --   0
```

16.3.14 loadbalance

Команда балансировки нагрузки ECMP (Equal-cost multi-path routing) позволяет создавать множественные параллельные пути для назначения маршрутов с одинаковой стоимостью. Данный функционал предназначен для распределения нагрузки и оптимизации пропускной способности сети. ECMP может работать как со статическими маршрутами, так и с протоколами динамической маршрутизации RIP, OSPF. Максимально можно настроить 8 путей.

Синтаксис команды:

loadbalance

no loadbalance

Команда с приставкой «**no**» выключает ECMP.

Значение по умолчанию:

По умолчанию ECMP для протоколов динамической маршрутизации выключен.

Использование команды:

Команда «**loadbalance**» используется для включения функции ECMP на устройстве.

Пример команды:

```
admin@SW# configure terminal
admin@SW(config)# router rip
admin@SW(config-ospf)# address-family-ospf ipv4
admin@SW(config-af-ospf)# loadbalance
```

16.4 Настройка RIPng

16.4.1 router rip

Команда глобальной настройки. Включение протокола RIPng и переход в режим настройки маршрутизации RIPng.

Синтаксис команды:

router ripng

no router ripng

Команда с приставкой «**no**» отключает протокол RIPng и удаляет его настройки.

Значение по умолчанию:

Протокол RIPng отключен.

Использование команды:

Команда «**router ripng**» используется для включения протокола RIPng и перехода в режим настройки маршрутизации RIPng.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)#
```

16.4.2 network

Команда настройки маршрутизации RIPng. Включение RIPng на интерфейсе с указанным Ipv6-адресом.

Синтаксис команды:

network *ipv6-address ipv6-prifix*

no network *ipv6-address ipv6-prifix*

Команда с приставкой «**no**» отключает RIPng на интерфейсе с указанным IPv6-адресом и удаляет конфигурацию RIPng на этом интерфейсе.

Параметры команды:

ipv6-address	IPv6-адрес на интерфейсе устройства
ipv6-prifix	длина префикса сети. Длина префикса является альтернативным методом указания маски подсети и должна предваряться символом “/” (слеш)

Значение по умолчанию:

RIPng отключен на интерфейсе.

Использование команды:

Команда «**network**» используется для включения RIPng на интерфейсе с указанным IPv6-адресом.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# network 2001:1234:5678:abcd:: /64
```

16.4.3 redistribute (RIPng)

Команда настройки маршрутизации RIPng. Включение распределения маршрутов из одного домена маршрутизации в другой.

Синтаксис команды:

redistribute *protocol* **[metric** *metric-value* **] [route-map** *text* **]**

no redistribute *protocol*

Команда с приставкой «**no**» отключает распределение маршрутов.

Параметры команды:

protocol — источник маршрутов, которые будут распределены. Варианты протокола:

- **bgp** – источником является протокол BGP;
- **connected** – источником являются сети, подключенные напрямую (для которых задан IPм6-адрес на одном из интерфейсов устройства);
- **ospf6** – источником является процесс OSPFv3;
- **static** – источником являются статические маршруты;
- **kernel** – источником являются маршруты, которые выводятся из ядра.

metric *metric-value* — значение метрики маршрута, назначаемой для распределяемых маршрутов

route-map *text* — указатель на записи карты маршрутов

Значение по умолчанию:

Распределение маршрутов отключено.

Использование команды:

Команда «**redistribute**» используется для включения распределения маршрутов из одного домена маршрутизации в другой.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# redistribute static
admin@Switch(config-ripng)#
```

16.4.4 aggregate-address

Команда настройки маршрутизации RIPng. Используется для создания агрегированных маршрутов.

Синтаксис команды:

aggregate-address *ipv6-address /ipv6-prefix*

no aggregate-address *ipv6-address /ipv6-prefix*

Команда с приставкой «**no**» отключает указанный агрегированный маршрут RIPng.

Параметры команды:

ipv6-address	IPv6-адрес на интерфейсе устройства
ipv6-prefix	длина префикса сети. Длина префикса является альтернативным методом указания маски подсети и должна предваряться символом “/” (слеш)

Значение по умолчанию:

Агрегированные маршруты в ripng отсутствуют.

Использование команды:

Команда «**aggregate-address**» используется для создания агрегированных маршрутов в RIPng. Агрегирование маршрутов позволяет объединять несколько более специфичных маршрутов в один более обобщённый маршрут, что сокращает количество записей в маршрутной таблице и снижает нагрузку на сеть.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# aggregate-address 2001:1234:5678:abcd:: /64
```

16.4.5 default-information originate

Команда настройки маршрутизации RIPng. Используется для объявления маршрута по умолчанию в других сетях.

Синтаксис команды:

default-information originate

no default-information originate

Команда с приставкой «**no**» отключает объявление маршрута по умолчанию.

Значение по умолчанию:

Маршрут по умолчанию не объявляется соседним маршрутизаторам.

Использование команды:

Команда «**default-information originate**» используется для объявления маршрута по умолчанию в других сетях. При ее использовании маршрутизатор начинает информировать соседние устройства о маршруте по умолчанию в обмене маршрутами RIPng.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# default-information originate
```

16.4.6 default-metric

Команда настройки маршрутизации RIPng. Используется для задания значения метрики по умолчанию, которая будет присваиваться маршруту при его объявлении.

Синтаксис команды:
default-metric metric
no default-metric
Команда с приставкой «**no**» отключает метрику по умолчанию.
Параметры команды:

metric	метрика в диапазоне от 1 до 16

Значение по умолчанию:
Метрика равна 1.
Использование команды:
Команда «**default-metric**» используется для задания значения метрики по умолчанию, которая будет присваиваться маршруту при его объявлении. Метрика может варьироваться от 1 до 16, где 16 считается недоступным маршрутом.
Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# default-metric 2
```

16.4.7 offset-list

Команда настройки маршрутизации RIPng. Используется для добавления смещения к метрикам маршрутов, которые соответствуют определенному списку доступа.
Синтаксис команды:
offset-list *acl-name* **{in | out}** *metric [vlan-id]*
no offset-list *acl-name* **{in | out}** *metric [vlan-id]*
Команда с приставкой «**no**» удаляет смещения метрик для маршрутов.
Параметры команды:

acl-name	имя IPv6 ACL в виде текстовой строки. Рекомендуемая длина: до 32 символов
in	смещение применяется к маршрутам, которые поступают через интерфейс
out	смещение применяется к маршрутам, которые отправляются через интерфейс
metric	метрика в диапазоне от 0 до 16
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:
Маршруты обрабатываются с обычными метриками.
Использование команды:
Команда «**offset-list**» используется для добавления смещения к метрикам маршрутов, которые соответствуют определенному списку доступа. Это позволяет изменять метрику маршрутов, увеличивая или уменьшая их стоимость на основе заданных критериев.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# offset-list test1 in 2 3
```

16.4.8 passive-interface

Команда настройки маршрутизации RIPng. Используется для задания интерфейсов VLAN, которые не будут участвовать в обмене маршрутизированными обновлениями.

Синтаксис команды:

passive-interface *vlan-id*

no passive-interface *vlan-id*

Команда с приставкой «**no**» включает обмен маршрутами через указанный VLAN

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Все VLAN являются активными.

Использование команды:

Команда «**passive-interface**» используется для указания интерфейсов, на которые протокол не должен отправлять обновления маршрутов.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# passive-interface 10
```

16.4.9 route

Команда настройки маршрутизации RIPng. Используется для объявления статической маршрутизации RIPng для network.

Синтаксис команды:

route *ipv6-address*

no route *ipv6-address*

Команда с приставкой «**no**» удаляет ранее заданный статический маршрут.

Параметры команды:

ipv6-address IPv6-адрес на интерфейсе устройства

Значение по умолчанию:

Статические маршруты не заданы.

Использование команды:

Команда «**route**» используется для добавления статических маршрутов в таблицу маршрутизации.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# route 2001:1234:5678:abcd::4
```

16.4.10 timers basic

Команда настройки маршрутизации RIPng. Используется для настройки таймеров, которые управляют различными аспектами работы протокола.

Синтаксис команды:

timers basic *update-timer information-timeout-timer garbage-collection-timer*

no timers basic

Команда с приставкой «**no**» устанавливает настройки таймеров по умолчанию

Параметры команды:

update-timer	значение таймера обновления таблицы маршрутизации в секундах. От 0 до 65535 секунд
information-timeout-timer	таймер тайм-аута информации о маршрутизации в секундах. От 0 до 65535 секунд
garbage-collection-timer	таймер сбора мусора в секундах. От 0 до 65535 секунд

Значение по умолчанию:

Интервал «**update-timer**» 30 секунд.

Интервал «**information-timeout-timer**» 180 секунд.

Интервал «**garbage-collection-timer**» 120 секунд.

Использование команды:

Команда «**timers basic**» используется для настройки таймеров, которые управляют различными аспектами работы протокола. Правильная настройка таймеров может помочь улучшить производительность и надежность маршрутизации.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ripng
admin@Switch(config-ripng)# timers basic 100 150 200
```

16.4.11 ipv6 ripng split-horizon

Команда настройки интерфейса (VLAN). Используется для предотвращения петель маршрутизации.

Синтаксис команды:

ipv6 ripng split-horizon [poisoned-reverse]

no ipv6 ripng split-horizon

Команда с приставкой «**no**» используется для отключения механизма «split horizon».

Параметры команды:

poisoned-reverse	параметр, который регулирует: если маршрут, полученный от соседа, становится недоступным, маршрутизатор будет сообщать об этом соседу с метрикой, равной бесконечности

Значение по умолчанию:

Механизм «**split horizon**» включен.

Использование команды:

Команда «**ipv6 ripng split-horizon**» используется для предотвращения петель маршрутизации.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ipv6 ripng split-horizon poisoned-reverse
```

16.4.12 show ipv6 ripng

Команда, доступная из любого режима. Вывод настроек RIPng.

Синтаксис команды:

show ipv6 ripng

Использование команды:

Команда «**show ipv6 ripng**» используется для вывода настроек RIPng.

Примеры команды:

```
admin@Switch# show ipv6 ripng
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
      (n) - normal, (s) - static, (d) - default, (r) - redistribute,
      (i) - interface, (a/S) - aggregated/Suppressed

      Network                    Next Hop                  Via        Metric  Tag    Time
C(i)  12:1234:5678:abcd::/64     ::                        self       1       0
R(n)  1001:1234:5678:abcd::/64   fe80::21b:28ff:fe0f:6f80   vlan-2     2       0      02:45
R(n)  3003:1234:5678:abcd::/64   fe80::21b:28ff:fe0f:7600   vlan-4     2       0      02:45
C(i)  4004:1234:5678:abcd::/64   ::                        self       1       0
R(n)  9009:1234:5678:abcd::/64   fe80::21b:28ff:fe0f:7600   vlan-4     2       0      02:45
```

16.4.13 show ipv6 ripng status

Команда, доступная из любого режима. Вывод параметров и статистики RIPng.

Синтаксис команды:

show ipv6 ripng

Использование команды:

Команда «**show ipv6 ripng**» используется для вывода параметров и статистики RIPng.

Примеры команды:

```
admin@Switch# show ipv6 ripng status

Routing Protocol is 'RIPng'
Sending updates every 30 seconds with +/-50%, next due in 23 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 1, receive version 1
   Interface               Send            Recv
   vlan-2                  1               1
   vlan-4                  1               1
Routing for Networks:
    12:1234:5678:abcd::/64
    4004:1234:5678:abcd::/64
Routing Information Sources:
Gateway                    BadPackets      BadRoutes       Distance        Last Update
fe80::21b:28ff:fe0f:7600   0               0               120             00:00:21
```

16.5 Настройка OSPFv2

16.5.1 Общие положения

OSPF (Open Shortest Path First) – протокол динамической маршрутизации для IP-сетей. Протокол OSPF является внутренним протоколом маршрутизации (Interior Gateway Protocol), то есть применяется для анонсирования маршрутов между маршрутизаторами, принадлежащих одной автономной системе.

Протокол OSPF основан на технологии отслеживания состояния линка (link-state protocol) или технологии поиска кратчайшего пути (Shortest Path First). Он включает в себя поддержку безклассовой маршрутизации (Classless Inter-Domain Routing) и добавление тегов к маршрутам, полученным от других протоколов маршрутизации (например, BGP).

Протокол OSPF поддерживает аутентификацию сообщений анонсирования состояния соединения (Link State Advertisement). OSPF использует многоадресную рассылку для обмена информацией.

Устройство поддерживает протокол OSPFv2 в соответствии с документами:

- RFC 2328: OSPF Version 2;
- RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option.

Устройство поддерживает именованные наборы ключей в протоколе маршрутизации OSFP. Именованные наборы ключей позволяют протоколу OSFP переключаться со старых ключей на новые в автоматическом режиме.

Настройки пользователя

1. Глобальные настройки:

- номер процесса OSPF в диапазоне от 1 до 2^{32}-1;
- идентификатор маршрутизатора (router-id). Если идентификатор не задан пользователем, то используется наименьший IP-адрес из настроенных на интерфейсах VLAN.

2. Настройки областей (area):

- идентификатор области (area id): IP-адрес или целое число;
- режим работы области (area nssa, area stub): normal, nssa, stub;
- режим работы области (area shutdown): включена, выключена.

3. Настройки IP-интерфейсов (в текущей реализации поддерживаются только VLAN):

- стоимость пути при передаче через интерфейс (ip ospf cost): целое число;

- интервал, через который маршрутизатор будет считаться отключенным, если от него не получено ни одного пакета “Hello” (ip ospf dead-interval): целое число;
- интервал отправки сообщений “Hello” (ip ospf hello-interval): целое число;
- приоритет интерфейса (ip ospf priority): целое число;
- интервал повторной отправки LSA (ip ospf retransmit-interval): целое число;
- режим работы области (ip ospf shutdown): true, false;
- набор ключей, который будет использован протоколом OSPF при аутентификации.

Дополнения и ограничения

В целях беспрерывного перехода на новый ключ в наборе ключей, время жизни нового ключа должно начинаться на несколько минут раньше времени окончания жизни текущего ключа.

Порядок настройки

Порядок настройки OSPF приведен в таблице 18.

Таблица 18 – Порядок настройки OSPF

Команда	Назначение
configure terminal	Переход в режим глобальной настройки
router ospf *process-id*	Создание и переход в режим настройки процесса маршрутизации OSPF
router-id *ip-address*	(опционально) Установка фиксированного значения идентификатора маршрутизатора
network *ip-address mask* **area** *area-id* **[shutdown]**	Добавление сетей (IP-интерфейсов) в область OSPF
area *area-id* **stub [no-summary]**	(опционально) Перевод области в нетранзитный (stub) режим. Типы области NSSA и stub взаимоисключающие
area *area-id* **nssa [no-summary] [translator-role {always | candidate}]**	(опционально) Перевод области в режим NSSA. Типы области NSSA и stub взаимоисключающие
redistribute *protocol* [*process-id*] **[metric** *metric-value*] **[metric-type** *type-value*] **[match {internal | external 1 | external 2}] [route-map** *map-tag*] **[subnets] [nssa-only]**	(опционально) Включение распределения маршрутов из одного домена маршрутизации в другой
exit	Переход в предыдущий режим настройки
interface vlan *vlan-id*	Переход в режим настройки интерфейса VLAN
ip ospf priority *priority*	Установка приоритета устройства на интерфейсе

Продолжение таблицы 18

Команда	Назначение
ip ospf dead-interval *seconds*	(опционально) Установка интервала времени, по истечении которого сосед считается вышедшим из строя (down), если от него не получено ни одного пакета “hello”
ip ospf hello-interval *seconds*	(опционально) Установка интервала отправки пакетов “hello”
exit	Переход в предыдущий режим настройки
exit	Переход в предыдущий режим настройки
show ip ospf [*process-id*]	Проверка глобальных настроек OSPF
show ip ospf interface [*interface-id*]	Проверка настроек OSPF на интерфейсе
copy running-config startup-config	Сохранение текущей конфигурации

16.5.2 clear ip ospf process

Команда фундаментального режима. Перезапуск процесса OSPF.
Синтаксис команды:
clear ip ospf [*process-id*] **process**
Параметры команды:

process-id — идентификатор процесса OSPF, назначенный пользователем. Идентификатор процесса имеет только локальное значение в пределах устройства. Диапазон значений: от 1 до $2^{32} - 1$

Использование команды:
Команда «**clear ip ospf process**» используется для перезапуска процесса OSPF. Команда без указания идентификатора процесса перезапускает все процессы OSPF.
Пример команды:

```
admin@Switch# clear ip ospf 50000 process
admin@Switch#
```

16.5.3 debug ip ospf

Команда фундаментального режима. Включение отладки OSPF.
Синтаксис команды:
debug ip ospf {all | events | filters | interfaces | packets | routes | states}
no debug ip ospf {all | events | filters | interfaces | packets | routes | states}
Команда с приставкой «**no**» отключает отладку OSPF.

Параметры команды:

all	вывод всех сообщений
events	вывод сообщений о событиях, внутренних для протокола
filters	вывод подробной информации о фильтрации маршрутов
interfaces	вывод событий изменения интерфейса, отправленные в протокол
packets	вывод информации о пакетах, отправленных и полученных протоколом
routes	вывод информации о маршрутах, которые были обменены с таблицей маршрутизации
states	вывод информации об изменениях состояния протокола

Пример команды:

```
admin@Switch# debug ip ospf all
admin@Switch#
```

16.5.4 router ospf

Команда глобальной настройки. Создание и переход в режим настройки процесса маршрутизации OSPF.

Синтаксис команды:

router ospf *process-id*

no router ospf *process-id*

Команда с приставкой «**no**» удаляет процесс.

Параметры команды:

process-id	идентификатор процесса OSPF, назначенный пользователем. Идентификатор процесса имеет только локальное значение в пределах устройства. Диапазон значений: от 1 до $2^{32} - 1$

Значение по умолчанию:

Процессы OSPF отсутствуют.

Использование команды:

Команда «**router ospf**» используется для создания и перехода в режим настройки процесса маршрутизации OSPF.

При удалении процесса маршрутизации OSPF с помощью команды «**no router ospf**» конфигурация процесса также удаляется.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)#
```

16.5.5 area authentication

Команда настройки маршрутизации (OSPF). Включение аутентификации в пределах области OSPF.

Синтаксис команды:

area *area-id* **authentication [message-digest]**

no area *area-id* **authentication**

Команда с приставкой «**no**» отключает аутентификацию.

Параметры команды:

area-id	идентификатор области, для которой необходимо включить аутентификацию. Идентификатор может быть указан в виде целого числа или IP-адреса
message-digest	включает аутентификацию с использованием MD5 (Message Digest 5)

Значение по умолчанию:

Аутентификация отключена.

Использование команды:

Команда «**area authentication**» используется для включения аутентификации в пределах области OSPF.

Включение аутентификации на области устанавливает режим аутентификации с помощью простого пароля (тип 1 в RFC 1247). Тип аутентификации должен быть одинаковым на всех устройствах в области для обеспечения совместной работы по протоколу OSPF.

Команда настройки интерфейса «**ip ospf authentication-key**» используется для настройки пароля на интерфейсе.

Если установлен режим аутентификации с использованием MD5, то необходимо настроить пароль на интерфейсе с помощью команды настройки интерфейса «**ip ospf message-digest-key**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip address 10.0.0.1 255.255.255.0
admin@Switch(config-if)# ip ospf authentication-key mykey
admin@Switch(config-if)# exit
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# network 10.0.0.0 255.255.255.0 area 0
admin@Switch(config-ospf)# area 0 authentication
admin@Switch(config-ospf)#
```

16.5.6 area default-cost

Команда настройки маршрутизации (OSPF). Установка стоимости пути суммарного маршрута по умолчанию, отправляемого в область stub или NSSA (Not So Stubby Area).

Синтаксис команды:

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

area-id	идентификатор области с типом stub или NSSA. Идентификатор может быть указан в виде целого числа или IP-адреса
cost	стоимость пути суммарного маршрута по умолчанию, используемого для области с типом stub или NSSA, в диапазоне от 1 до 16777215

Значение по умолчанию:

Стоимость пути равна 1.

Использование команды:

Команда «**area default-cost**» используется для установки стоимости пути суммарного маршрута по умолчанию, отправляемого в область stub или NSSA (Not So Stubby Area).

Команда используется только на пограничном маршрутизаторе области (Area Border Router), подключенном к области с типом stub или NSSA.

Режим области stub должен быть настроен на всех устройствах, подключенной к этой области с помощью команды «**area stub**». Команда «**area default-cost**» предоставляет метрику суммарного маршрута по умолчанию, который генерируется пограничным маршрутизатором области в область с типом stub.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip address 10.10.0.1 255.255.255.0
admin@Switch(config-if)# exit
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# network 10.0.0.0 255.255.255.0 area 10.0.0.0
admin@Switch(config-ospf)# area 10.0.0.0 stub
admin@Switch(config-ospf)# area 10.0.0.0 default-cost 100
admin@Switch(config-ospf)#
```

16.5.7 area nssa

Команда настройки маршрутизации (OSPF). Установка типа области NSSA (Not So Stubby Area).

Синтаксис команды:

area *area-id* **nssa [no-summary] [translator-role {always | candidate}] [translator-stability-interval** *seconds***]**

no area *area-id* **nssa**

Команда с приставкой «**no**» удаляет тип области NSSA.

Параметры команды:

area-id	идентификатор области NSSA. Идентификатор может быть указан в виде целого числа или IP-адреса
no-summary	суммарный маршрут не будет анонсироваться в область NSSA
translator-role	включение режима безусловной трансляции LSA тип 7 в LSA тип 5: – **always** – трансляция включена всегда; – **candidate** – устройство является кандидатом на роль транслятора По умолчанию используется режим **candidate**
seconds	интервал времени, прошедший с момента прекращения трансляции, после которого выбранный транслятор возобновляет трансляцию, в диапазоне от 1 до 65535 секунд. По умолчанию используется интервал 40 секунд

Значение по умолчанию:

Область не является NSSA.

Использование команды:

Команда «**area nssa**» используется для установки типа области NSSA (Not So Stubby Area).

Команда «**no area nssa**» не удаляет область, а только переводит ее в транзитный (обычный) режим.

Для удаления области используется команда «**no area**».

Типы области NSSA и stub взаимоисключающие, поэтому можно установить либо тип NSSA с помощью команды «**area nssa**», либо тип stub с помощью команды «**area stub**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# network 10.0.0.0 255.255.255.0 area 10.0.0.0
admin@Switch(config-ospf)# area 10.0.0.0 nssa
admin@Switch(config-ospf)#
```

16.5.8 area range

Команда настройки маршрутизации (OSPF). Консолидация и суммаризация маршрутов на границе области.

Синтаксис команды:

area *area-id* **range** *ip-address mask* **[advertise | not-advertise]**

no area *area-id* **range** *ip-address mask*

Команда с приставкой «**no**» отключает функцию.

Параметры команды:

area-id	идентификатор области. Идентификатор может быть указан в виде целого числа или IP-адреса
ip-address	IP-адрес сети (подсети)
mask	маска IP-адреса
advertise	генерация суммарных анонсов для указанных сетей (LSA тип 3). Значение используется по умолчанию
not-advertise	запрет генерации суммарных анонсов для указанных сетей (LSA тип 3)

Значение по умолчанию:

Суммаризация маршрутов на границе области отключена.

Использование команды:

Команда «**area range**» используется для консолидации и суммаризации маршрутов на границе области.

Команда используется только на пограничном маршрутизаторе области (Area Border Router) для консолидации и суммаризации маршрутов. Маршрутизатор анонсирует один суммарный маршрут в другие области для указанных сетей, то есть маршрутная информация консолидируется на границе областей.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip address 192.168.0.1 255.255.255.0
admin@Switch(config-if)# exit
aadmin@Switch(config)# interface vlan 2
admin@Switch(config-if)# ip address 192.168.1.1 255.255.255.0
admin@Switch(config-if)# exit
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# network 192.168.0.0 255.0.0.0 area 0
admin@Switch(config-ospf)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
admin@Switch(config-ospf)# area 0 range 192.168.1.0 255.255.0.0
admin@Switch(config-ospf)#
```

16.5.9 area shutdown

Команда настройки маршрутизации (OSPF). Запуск процесса отключения области (graceful shutdown).

Синтаксис команды:

area *area-id* **shutdown**

no area *area-id* **shutdown**

Команда с приставкой «**no**» перезапускает процесс маршрутизации OSPF.

Параметры команды:

area-id	идентификатор области. Идентификатор может быть указан в виде целого числа или IP-адреса

Значение по умолчанию:

OSPF активен в текущей области.

Использование команды:

Команда «**area shutdown**» используется для запуска процесса отключения области (graceful shutdown).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# area 10.0.0.0 shutdown
admin@Switch(config-ospf)#
```

16.5.10 area stub

Команда настройки маршрутизации (OSPF). Установка типа области stub (область без транзитного трафика).

Синтаксис команды:

area *area-id* **stub [no-summary]**

no area *area-id* **stub**

Команда с приставкой «**no**» удаляет тип области stub.

Параметры команды:

area-id	идентификатор области stub. Идентификатор может быть указан в виде целого числа или IP-адреса
no-summary	суммарный маршрут не будет анонсироваться в область stub

Значение по умолчанию:

Область не является stub.

Использование команды:

Команда «**area stub**» используется для установки типа области stub (область без транзитного трафика).

Команда «**no area stub**» не удаляет область, а только переводит ее в транзитный (обычный) режим.

Для удаления области используется команда «**no area**».

Типы области NSSA и stub взаимоисключающие, поэтому можно установить либо тип NSSA с помощью команды «**area nssa**», либо тип stub с помощью команды «**area stub**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# network 10.0.0.0 255.255.255.0 area 10.0.0.0
admin@Switch(config-ospf)# area 10.0.0.0 stub
admin@Switch(config-ospf)#
```

16.5.11 compatible rfc1583

Команда настройки маршрутизации (OSPF). Установка режима подсчета суммарных маршрутов в соответствии с RFC 1583.

Синтаксис команды:
compatible rfc1583
no compatible rfc1583
Команда с приставкой «**no**» отключает совместимость с RFC 1583.
Значение по умолчанию:
К области не относится ни одна сеть (IP-интерфейс).
Использование команды:
Команда «**compatible rfc1583**» используется для установки режима подсчета суммарных маршрутов в соответствии с RFC 1583.

Для минимизации вероятности появления закольцовывания маршрутов использовать одинаковые настройки совместимости на всех маршрутизаторах OSPF.

С появлением RFC 2328 метод подсчета суммарных маршрутов изменился. Команда «**no compatible rfc1583**» используется для отключения совместимости с RFC 1583 и перехода на режим подсчета суммарных маршрутов в соответствии с RFC 2328.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# compatible rfc1583
admin@Switch(config-ospf)#
```

16.5.12 max-metric router-lsa

Команда настройки маршрутизации (OSPF). Включение анонсирования максимальной метрики, таким образом, остальные маршрутизаторы будут предпочитать использование других маршрутизаторов при вычислении маршрутов.
Синтаксис команды:
max-metric router-lsa
no max-metric router-lsa
Команда с приставкой «**no**» отключает анонсирование максимальной метрики.
Значение по умолчанию:
Анонсируются нормальные метрики.
Использование команды:
Команда «**max-metric router-lsa**» используется для включения анонсирования максимальной метрики, таким образом, остальные маршрутизаторы будут предпочитать использование других маршрутизаторов при вычислении маршрутов.

При включении настройки устройство анонсирует максимальные метрики постоянно или до истечения интервала времени, заданного пользователем.

Метрики маршрутов (интерфейсов) в нетранзитной области (stub), подключенных напрямую, не зависят от настройки «**max-metric router-lsa**», т.к. стоимость маршрута всегда устанавливается равной стоимости на интерфейсе.

Настройка «**max-metric router-lsa**» полезна в следующих случаях:

1. Перезагрузка устройства. После перезагрузки протоколы внутренней маршрутизации (Interior Gateway Protocols) сходятся очень быстро и другие маршру-

тизаторы могут начать передачу трафика через устройство. Если устройство все еще находится в процессе загрузки маршрутов BGP, пакеты для других сетей могут быть отброшены.

2. Добавление устройства в сеть без разрешения передачи транзитного трафика через него. Если альтернативные маршруты недоступны, то устройство все равно будет пропускать транзитный трафик.
3. Удаление устройства из сети (отключение). В этом случае остальные маршрутизаторы будут использовать альтернативные маршруты для передачи трафика.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# max-metric router-lsa
admin@Switch(config-ospf)#
```

16.5.13 network area

Команда настройки маршрутизации (OSPF). Добавление сетей (IP-интерфейсов) в область OSPF.

Синтаксис команды:

network *ip-address mask* **area** *area-id* **[shutdown]**

no network *ip-address mask* **area** *area-id*

Команда с приставкой «**no**» удаляет сети (IP-интерфейсы) из области OSPF.

Параметры команды:

ip-address	IP-адрес сети (подсети)
mask	маска сети (подсети)
area-id	идентификатор области, к которой будут относиться указанные сети (подсети). Идентификатор может быть указан в виде целого числа или IP-адреса
shutdown	интерфейс добавляется в отключенном состоянии (не передает и не принимает пакеты OSPF)

Значение по умолчанию:

К области не относится ни одна сеть (IP-интерфейс).

Использование команды:

Команда «**network area**» используется для добавления сетей (IP-интерфейсов) в область OSPF.

Параметры команды «*ip-address*» и «*mask*» позволяют указать несколько интерфейсов (сетей) для добавления в область OSPF. Устройство добавляет интерфейсы по следующему алгоритму:

1. Производится логическая операция “И” между IP-адресом интерфейса и параметром «mask»;

2. Производится логическая операция “И” между параметром «ip-address» и параметром «mask»;
3. Если полученные результаты совпадают, то интерфейс добавляется в указанную пользователем область OSPF.

Интерфейс может быть добавлен только в одну область. Если диапазоны адресов для разных областей пересекаются, то устройство настраивает первую по очереди область и игнорирует все остальные. Не рекомендуется настройка пересекающихся адресов для разных областей в целях исключения неожиданных конфликтов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# network 10.0.0.0 255.255.255.0 area 1
admin@Switch(config-ospf)# network 192.168.0.0 255.255.255.0 area 2
admin@Switch(config-ospf)# network 0.0.0.0 0.0.0.0 area 0
admin@Switch(config-ospf)#
```

16.5.14 no area

Команда настройки маршрутизации (OSPF). Удаление области OSPF.

Синтаксис команды:

no area *area-id*

Параметры команды:

area-id	идентификатор области, которую необходимо удалить. Идентификатор может быть указан в виде целого числа или IP-адреса

Использование команды:

Команда «**no area**» используется для удаления области OSPF.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# no area 1
admin@Switch(config-ospf)#
```

16.5.15 passive-interface

Команда настройки маршрутизации (OSPF). Отключение отправки обновления маршрутов на всех интерфейсах OSPF.

Синтаксис команды:

passive-interface

no passive-interface

Команда с приставкой «**no**» включает отправку обновления маршрутов.

Значение по умолчанию:

Отправка обновления маршрутов включена.

Использование команды:

Команда «**passive-interface**» используется для отключения отправки обновления маршрутов на всех интерфейсах OSPF.

Маршрутная информация OSPF не будет отправляться и приниматься на всех интерфейсах OSPF.

Пассивный интерфейс ведет себя как нетранзитная сеть (stub network) в домене OSPF. Настройка полезна в сети провайдера при использовании большого количества интерфейсов.

После использования команды «**passive-interface**» пользователь может включить отправку обновления маршрутов на отдельных интерфейсах, для которых необходимо обновление, с помощью команды «**no ip ospf passive-interface**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# passive-interface
admin@Switch(config-ospf)#
```

16.5.16 redistribute

Команда настройки маршрутизации (OSPF, BGP). Включение распределения маршрутов из одного домена маршрутизации в другой.

Синтаксис команды:

redistribute *protocol* **[***process-id***] [metric** *metric-value***] [metric-type** *type-value***] [match {internal | external 1 | external 2}] route-map** *map-tag* **subnets nssa-only**

no redistribute *protocol* **[***process-id***] [metric** *metric-value***] [metric-type** *typevalue***] [match {internal | external 1 | external 2}] route-map** *map-tag* **subnets nssaonly**

Команда с приставкой «**no**» отключает распределение маршрутов.

Параметры команды:

protocol — источник маршрутов, которые будут распределены. Варианты протокола:

- **bgp** – источником является протокол BGP;
- **connected** – источником являются сети, подключенные напрямую (для которых задан IP-адрес на одном из интерфейсов устройства);
- **ospf** – источником является другой процесс OSPF;
- **static** – источником являются статические маршруты;
- **rip** – источником является протокол RIP

process-id — идентификатор процесса OSPF, из которого будут распределяться маршруты. По умолчанию используется номер 1. Не имеет значения, если источником указан не протокол OSPF

metric-value	значение метрики маршрута, назначаемой для распределяемых маршрутов. Значение метрики указано в отображении маршрутов (заданной командой «**set metric**») имеет приоритет перед настройкой «*metric-value*» (замещает ее)
type-value	тип внешнего соединения, ассоциируемого с маршрутом по умолчанию, анонсируемого в домен OSPF: – **1** – внешний маршрут Тип 1; – **2** – внешний маршрут Тип 2. По умолчанию используется внешний маршрут Тип 2.
match {internal | external 1 | external 2}	критерии, по которым маршруты OSFP распределяются в процесс OSPF: – **internal** – внутренние маршруты автономной системы; – **external 1** – внешние маршруты для автономной системы, которые импортированы в OSPF как внешний маршрут Тип 1; – **external 2** – внешние маршруты для автономной системы, которые импортированы в OSPF как внешний маршрут Тип 2. По умолчанию распределяются маршруты **internal** и **external 1**

Значение по умолчанию:

Разпределение маршрутов отключено.

Использование команды:

Команда «**redistribute**» используется для включения распределения маршрутов из одного домена маршрутизации в другой.

Смена настройки, ассоциированной с ключевым словом, не затрагивает остальные настройки.

Устройство, получающее маршруты по протоколу на основе состояний соединения (например, OSPF) с внутренней метрикой, будет считать, что стоимость маршрута равна стоимости от самого себя до устройства, распределяющего маршруты плюс анонсированную стоимость до точки назначения. Для внешней метрики стоимость равна только анонсированной стоимости до точки назначения.

При использовании команды «**redistribute**» для распределения маршрутов в домен OSPF устройство автоматически становится пограничным маршрутизатором автономной системы (Autonomous System Boundary Router).

Распределение маршрутов с помощью ключевого слова «**connected**» охватывает только те сети, подключенные напрямую, которые не указаны явно с помощью команды «**network**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# redistribute static
admin@Switch(config-ospf)#
```

16.5.17 router-id

Команда настройки маршрутизации (OSPF). Установка фиксированного значения идентификатора маршрутизатора.

Синтаксис команды:

router-id *ip-address*

no router-id *ip-address*

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

ip-address	идентификатор маршрутизатора в формате IP-адреса

Значение по умолчанию:

Наименьший IP-адрес, настроенный на устройстве.

Использование команды:

Команда «**router-id**» используется для установки фиксированного значения идентификатора маршрутизатора.

Допускается установка любого идентификатора маршрутизатора в формате IP-адреса, однако каждый идентификатор должен быть уникальным.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-ospf)# router-id 10.0.0.1
admin@Switch(config-ospf)#
```

16.5.18 ip ospf authentication

Команда настройки интерфейса (VLAN). Переопределение настроенного режима аутентификации области на интерфейсе.

Синтаксис команды:

ip ospf authentication [message-digest | null]

no ip ospf authentication

Команда с приставкой «**no**» использует режим аутентификации, настроенный для области.

Параметры команды:

message-digest	использование аутентификации MD5 (Message Digest 5)
null	отключение аутентификации. Применяется для переопределения типа аутентификации, настроенной для области

Значение по умолчанию:

Используется режим аутентификации, настроенный на области.

Использование команды:

Команда «**ip ospf authentication**» используется для переопределения настроенного режима аутентификации области на интерфейсе. Команда без параметров устанавливает режим аутентификации с помощью простого пароля (Тип 1 в RFC 1247).

Перед использованием команды «**ip ospf authentication**» необходимо настроить пароль на интерфейсе с помощью команды «**ip ospf authentication-key**» или «**ip ospf message-digest-key**» в случае использования аутентификации MD5.

Если тип аутентификации не задан, то используется режим аутентификации, настроенный для области.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf authentication message-digest
admin@Switch(config-if-vlan)#
```

16.5.19 ip ospf authentication-key

Команда настройки интерфейса (VLAN). Установка пароля, используемого при режиме аутентификации с помощью простого пароля (Тип 1 в RFC 1247).

Синтаксис команды:

ip ospf authentication-key *password* **[***ip address***]**

no ip ospf authentication-key *password* **[***ip address***]**

Команда с приставкой «**no**» удаляет пароль.

Параметры команды:

password	пароль в виде текстовой строки длиной до 32 символов
ip address	аутентификация OSPF для конкретного IP-адреса

Значение по умолчанию:

Пароль отсутствует.

Использование команды:

Команда «**ip ospf authentication-key**» используется для установки пароля, используемого при режиме аутентификации с помощью простого пароля (Тип 1 в RFC 1247).

Пароль, заданный командой, внедряется в заголовок пакетов OSPF, отправляемых устройством. Для каждой сети (интерфейса) можно назначить свой пароль. Все маршрутизаторы должны иметь одинаковые пароли, настроенные на сеть.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf authentication-key simple
admin@Switch(config-if-vlan)#
```

16.5.20 ip ospf authentication key-chain

Команда настройки интерфейса (VLAN). Установка набора ключей, который будет использован протоколом OSPF при аутентификации.

Синтаксис команды:

ip ospf authentication key-chain *name-of-chain*

no ip ospf authentication key-chain

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

name-of-chain	имя набора ключей

Значение по умолчанию:

Набор ключей не определен.

Использование команды:

Команда «**ip ospf authentication key-chain**» используется для установки набора ключей, который будет использован протоколом OSPF при аутентификации.

Для каждого интерфейса можно указать только один набор ключей. Каждая последующая команда «**ip ospf authentication key-chain**» переопределяет старое значение настройки.

В целях беспрерывного перехода на новый ключ в наборе ключей, время жизни нового ключа должно начинаться на несколько минут раньше времени окончания жизни текущего ключа.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if)# ip ospf authentication key-chain alpha
admin@Switch(config-if)#
```

16.5.21 ip ospf cost

Команда настройки интерфейса (VLAN). Установка стоимости пути на интерфейсе.

Синтаксис команды:

ip ospf cost *interface-cost*

no ip ospf cost

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

interface-cost	стоимость пути (метрика) в диапазоне от 1 до 65535

Значение по умолчанию:

Стоимость пути равна 10.

Использование команды:

Команда «**ip ospf cost**» используется для установки стоимости пути на интерфейсе.

В общем случае стоимость пути вычисляется по формуле 2:

$$\frac{10^{10}}{ifSpeed} \quad (1)$$

где ifSpeed – скорость интерфейса в бит/с.

Таким образом, значения стоимости пути для различных скоростей работы интерфейсов:

- 10 Гбит/с: 1;
- 1 Гбит/с: 10;
- 100 Мбит/с: 100;
- 10 Мбит/с: 1000.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf cost 20
admin@Switch(config-if-vlan)#
```

16.5.22 ip ospf dead-interval

Команда настройки интерфейса (VLAN). Установка интервала времени, по истечении которого сосед считается вышедшим из строя (down), если от него не получено ни одного пакета “hello”.

Синтаксис команды:

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал времени, по истечении которого сосед считается вышедшим из строя (down), если от него не получено ни одного пакета “hello”. Интервал времени: в диапазоне от 1 до 65535. По умолчанию используется значение 40. Значение должно быть одинаковым на всех устройствах в сети

Значение по умолчанию:

Значение интервала, заданного командой «**ip ospf hello-interval**», умноженное на 4.

Использование команды:

Команда «**ip ospf dead-interval**» используется для интервала времени, по истечении которого сосед считается вышедшим из строя (down), если от него не получено ни одного пакета “hello”. Значение должно быть одинаковым на всех устройствах в сети.

Настройка меньшего значения интервала позволяет устройству быстрее определить выход из строя другого устройства OSPF и скорость сходимость сети, но может привести к большей нестабильности маршрутизации.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf dead-interval 40
admin@Switch(config-if-vlan)#
```

16.5.23 ip ospf hello-interval

Команда настройки интерфейса (VLAN). Установка интервала отправки пакетов “hello” на интерфейсе.

Синтаксис команды:

ip ospf hello-interval *seconds*

no ip ospf hello-interval

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал отправки пакетов “hello” на интерфейсе в диапазоне от 1 до 65535. По умолчанию используется значение 10. Значение должно быть одинаковым на всех устройствах в сети

Значение по умолчанию:

Интервал отправки равен 10 секундам.

Использование команды:

Команда «**ip ospf hello-interval**» используется для установки интервала отправки пакетов “hello” на интерфейсе.

Чем меньше интервал отправки пакетов “hello”, тем быстрее обнаруживаются изменения топологии, однако при этом увеличивается нагрузка на сеть. Интервал повторной отправки анонсов состояний соединения (LSA) должен быть консервативным, в противном случае возникнут излишние повторные отправки анонсов состояний.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf hello-interval 10
admin@Switch(config-if-vlan)#
```

16.5.24 ip ospf mtu-ignore

Команда настройки интерфейса (VLAN). Отключает обнаружение несоответствия MTU в принятых пакетах дескриптора базы данных.

Синтаксис команды:

ip ospf mtu-ignore

no ip ospf mtu-ignore

Команда с приставкой «**no**» отключает данную функцию.

Значение по умолчанию:
Функция отключена.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf mtu-ignore
```

16.5.25 ip ospf passive-interface

Команда настройки интерфейса (VLAN). Отключение отправки обновления маршрутов на интерфейсе.

Синтаксис команды:
ip ospf passive-interface
no ip ospf passive-interface
Команда с приставкой «**no**» включает отправку обновления маршрутов.
Значение по умолчанию:
Отправка обновления маршрутов включена.
Использование команды:
Команда «**ip ospf passive-interface**» используется для отключения отправки обновления маршрутов на интерфейсе.

Маршрутная информация OSPF не будет отправляться и приниматься на интерфейсе OSPF. Пассивный интерфейс ведет себя как нетранзитная сеть (stub network) в домене OSPF. Настройка полезна в сети провайдера при использовании большого количества интерфейсов.

Команда «**no ip ospf passive-interface**» позволяет включить отправку обновления маршрутов на отдельных интерфейсах, для которых необходимо обновление, если отправка обновлений была отключена для всей области командой «**passive-interface**»
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf 50000
admin@Switch(config-router)# passive-interface
admin@Switch(config-router)# exit
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# no ip ospf passive-interface
admin@Switch(config-if-vlan)#
```

16.5.26 ip ospf priority

Команда настройки интерфейса (VLAN). Установка приоритета устройства на интерфейсе.

Синтаксис команды:
ip ospf priority *priority*
no ip ospf priority
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

priority	устройства в диапазоне от 0 до 255

Значение по умолчанию:

Приоритет устройства равен 1.

Использование команды:

Команда «**ip ospf priority**» используется для установки приоритета устройства на интерфейсе.

Приоритет устройства используется при определении выделенного маршрутизатора сети (designated router), который ответственен за рассылку обновлений другим маршрутизаторам области. Устройство с большим приоритетом становится выделенным маршрутизатором. Если у двух или более маршрутизаторов одинаковый приоритет, то выделенным маршрутизатором становится устройство с наибольшим значением идентификатора маршрутизатора.

Нулевое значение приоритета исключает устройство из процесса выбора выделенного маршрутизатора и запасного выделенного маршрутизатора.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf priority 10
admin@Switch(config-if-vlan)#
```

16.5.27 ip ospf retransmit-interval

Команда настройки интерфейса (VLAN). Установка интервала повторной отправки анонсов состояний соединения (LSA).

Синтаксис команды:

ip ospf retransmit-interval *seconds*

no ip ospf retransmit-interval

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал повторной отправки анонсов состояний соединения (LSA) на интерфейсе в диапазоне от 1 до 65535. Значение должно быть больше, чем суммарная задержка пакета между двумя маршрутизаторами (roundtrip delay)

Значение по умолчанию:

Интервал повторной отправки равен 5 секундам.

Использование команды:

Команда «**ip ospf retransmit-interval**» используется для установки интервала повторной отправки анонсов состояния соединения (LSA).

При отправке LSA соседнему маршрутизатору устройство сохраняет LSA до момента получения подтверждения о получении от соседнего маршрутизатора. Если устройство не получило подтверждения, то оно повторно отправляет LSA.

Значение интервала повторной отправки должно быть больше, чем суммарная задержка пакета между двумя маршрутизаторами (round-trip delay). Интервал повторной отправки анонсов состояний соединения (LSA) должен быть консервативным, в противном случае возникнут излишние повторные отправки анонсов состояний.

Рекомендуется использовать одинаковое значение на всех маршрутизаторах области OSFP, в противном случае могут возникнуть излишние повторные отправки анонсов состояний.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf retransmit-interval 10
admin@Switch(config-if-vlan)#
```

16.5.28 ip ospf shutdown

Команда настройки интерфейса (VLAN). Запуск процесса отключения интерфейса (graceful shutdown).

Синтаксис команды:

ip ospf shutdown

no ip ospf shutdown

Команда с приставкой «**no**» перезапускает процесс маршрутизации на интерфейсе.

Значение по умолчанию:

OSPF активен на интерфейсе.

Использование команды:

Команда «**ip ospf shutdown**» используется для запуска процесса отключения интерфейса (graceful shutdown).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf shutdown
admin@Switch(config-if-vlan)#
```

16.5.29 ip ospf ttl-security

Команда настройки интерфейса (VLAN). Включение проверки времени жизни пакетов OSPF (Time-to-Live) на интерфейсе.

Синтаксис команды:

ip ospf ttl-security

no ip ospf ttl-security

Команда с приставкой «**no**» отключает проверку времени жизни пакетов OSPF.

Значение по умолчанию:

Проверка времени жизни пакетов OSPF отключена.

Использование команды:

Команда «**ip ospf ttl-security**» используется для включения проверки времени жизни пакетов OSPF (Time-to-Live) на интерфейсе.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf ttl-security
admin@Switch(config-if-vlan)#
```

16.5.30 show ip ospf

Команда, доступная из любого режима. Вывод общей информации о процессе OSPF.

Синтаксис команды:

show ip ospf [*process-id*]

Параметры команды:

process-id	идентификатор процесса OSPF

Использование команды:

Команда «**show ip ospf**» используется для вывода общей информации о процессе OSPF. Команда без параметров выводит информацию для всех процессов OSPF.

Пример команды:

```
admin@Switch# show ip ospf 50000
OSPF process 50000

  RFC1583 compatibility: enable
  RT scheduler tick: 2
  Number of areas: 1
  Number of LSAs in DB: 32
    Area: 0.0.0.0 (0) [BACKBONE]
      Stub: No
      NSSA: No
      Transit: No
      Number of interfaces: 1
      Number of neighbors: 1
      Number of adjacent neighbors: 1
```

16.5.31 show ip ospf database

Команда, доступная из любого режима. Вывод базы анонсов (LSA) устройства.

Синтаксис команды:

show ip ospf [*process-id* [*area-id*]] **database**

Параметры команды:

process-id	идентификатор процесса OSPF
area-id	идентификатор области. Идентификатор может быть указан в виде целого числа или IP-адреса

Использование команды:

Команда «**show ip ospf**» используется для вывода базы анонсов (LSA) устройства. Команда без параметров выводит информацию для всех процессов OSPF.

Пример команды:

```
admin@Switch# show ip ospf
OSPF process 50000

Area 0.0.0.0
Type    LS ID          Router         Age     Sequence      Checksum
0001    192.168.0.126  192.168.0.126  1364    8000002c      116c
0002    192.168.0.126  192.168.0.126  1368    80000003      8420
0001    10.0.0.1       10.0.0.1       1374    80000030      37e2
```

16.5.32 show ip ospf interface

Команда, доступная из любого режима. Вывод настроек и состояний интерфейсов OSPF.

Синтаксис команды:

show ip ospf interface [*interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (VLAN)

Использование команды:

Команда «**show ip ospf interface**» используется для вывода настроек и состояний интерфейсов OSPF.

Команда без параметров выводит настройки и состояния всех интерфейсов.

Пример команды:

```
admin@Switch# show ip ospf interface
OSPF process 50000

  Interface VLAN 1 (192.168.0.0/20)
    Type: broadcast
    Area: 0.0.0.0 (0)
    State: dr
    Priority: 1
    Cost: 10
    Hello timer: 9
    Wait timer: 50
    Dead timer: 45
    Retransmit timer: 6
    Designed router (ID): 192.168.0.126
    Designed router (IP): 192.168.0.126
    Backup designed router (ID): 10.0.0.1
    Backup designed router (IP): 192.168.0.115
```

16.5.33 show ip ospf neighbor

Команда, доступная из любого режима. Вывод информации о соседних маршрутизаторах OSPF.

Синтаксис команды:

show ip ospf neighbor [*interface-id*] [*neighbor-id*]

Параметры команды:

interface-id	идентификатор интерфейса (VLAN)
neighbor-id	идентификатор соседнего маршрутизатора (IP-адрес)

Использование команды:

Команда «**show ip ospf neighbor**» используется для вывода информации о соседних маршрутизаторах OSPF. Команда без параметров выводит информацию о всех соседних маршрутизаторах OSPF.

Пример команды:

```
admin@Switch# show ip ospf neighbor
OSPF process 50000
Router ID     Pri  State     DTime   Interface     Router IP
10.0.0.1      1    full/bdr  00:41   VLAN 1        192.168.0.115
```

16.5.34 loadbalance

Команда балансировки нагрузки ECMP (Equal-cost multi-path routing) позволяет создавать множественные параллельные пути для назначения маршрутов с одинаковой стоимостью. Данный функционал предназначен для распределения нагрузки и оптимизации пропускной способности сети. ECMP может работать как со статическими маршрутами, так и с протоколами динамической маршрутизации RIP, OSPF. Максимально можно настроить 8 путей.

Синтаксис команды:

loadbalance

no loadbalance

Команда с приставкой «**no**» выключает ECMP.

Значение по умолчанию:

По умолчанию ECMP для протоколов динамической маршрутизации выключен.

Использование команды:

Команда «**loadbalance**» используется для включения функции ECMP на устройстве.

Пример команды:

```
admin@SW# configure terminal
admin@SW(config)# router ospf 1000
admin@SW(config-ospf)# address-family-ospf ipv4
 admin@SW(config-af-ospf)# loadbalance
```

16.6 Настройка OSPFv3

16.6.1 Общие положения

OSPFv3 (Open Shortest Path First) – протокол динамической маршрутизации для IPv6-сетей. Протокол OSPFv3 является внутренним протоколом маршрутизации (Interior Gateway Protocol), то есть применяется для анонсирования маршрутов между маршрутизаторами, принадлежащих одной автономной системе.

Протокол OSPFv3 основан на технологии отслеживания состояния линка (link-state protocol) или технологии поиска кратчайшего пути (Shortest Path First). Он включает в себя поддержку безклассовой маршрутизации (Classless Inter-Domain Routing) и добавление тегов к маршрутам, полученным от других протоколов маршрутизации (например, BGP).

Протокол OSPFv3 поддерживает аутентификацию сообщений анонсирования состояния соединения (Link State Advertisement). OSPFv3 использует многоадресную рассылку для обмена информацией.

Устройство поддерживает именованные наборы ключей в протоколе маршрутизации OSFPv3. Именованные наборы ключей позволяют протоколу OSFPv3 переключаться со старых ключей на новые в автоматическом режиме.

Настройки пользователя

1. Глобальные настройки:

- номер процесса OSPFv3 в диапазоне от 1 до $2^{32} – 1$;
- идентификатор маршрутизатора (router-id). Если идентификатор не задан пользователем, то используется наименьший IP-адрес из настроенных на интерфейсах VLAN.

2. Настройки областей (area):

- идентификатор области (area id): IP-адрес или целое число;
- режим работы области (area nssa, area stub): normal, nssa, stub;
- режим работы области (area shutdown): включена, выключена.

3. Настройки IP-интерфейсов (в текущей реализации поддерживаются только VLAN):

- стоимость пути при передаче через интерфейс (ip ospf cost): целое число;
- интервал, через который маршрутизатор будет считаться отключенным, если от него не получено ни одного пакета “Hello” (ip ospf dead-interval): целое число;
- интервал отправки сообщений “Hello” (ip ospf hello-interval): целое число;
- приоритет интерфейса (ip ospf priority): целое число;
- интервал повторной отправки LSA (ip ospf retransmit-interval): целое число;

– режим работы области (ip ospf shutdown): true, false;
– набор ключей, который будет использован протоколом OSPF при аутентификации.

Дополнения и ограничения

В целях беспрерывного перехода на новый ключ в наборе ключей, время жизни нового ключа должно начинаться на несколько минут раньше времени окончания жизни текущего ключа.

Порядок настройки

Порядок настройки OSPFv3 приведен в таблице 19.

Таблица 19 – Порядок настройки OSPFv3

Команда	Назначение
configure terminal	Переход в режим глобальной настройки
router ospf6 *process-id*	Создание и переход в режим настройки процесса маршрутизации OSPFv3
router-id *ip-address*	(Опционально) Установка фиксированного значения идентификатора маршрутизатора
network *ip-address prefix* **area** *area-id* **[shutdown]**	Добавление сетей (IP-интерфейсов) в область OSPFv3
area *area-id* **stub [no-summary]**	(Опционально) Перевод области в нетранзитный (stub) режим. Типы области NSSA и stub взаимоисключающие
area *area-id* **nssa [no-summary] [translator-role {always | candidate}]**	(Опционально) Перевод области в режим NSSA. Типы области NSSA и stub взаимоисключающие
redistribute *protocol* [*process-id*] **[metric** *metric-value*] **[metric-type** *type-value*] **[match {internal | external 1 | external 2}] [route-map** *map-tag*] **[subnets] [nssaonly]**	(Опционально) Включение распределения маршрутов из одного домена маршрутизации в другой
exit	Переход в предыдущий режим настройки
interface vlan *vlan-id*	Переход в режим настройки интерфейса VLAN
ip ospf priority *priority*	Установка приоритета устройства на интерфейсе
ip ospf dead-interval *seconds*	(Опционально) Установка интервала времени, по истечении которого сосед считается вышедшим из строя (down), если от него не получено ни одного пакета “hello”
ip ospf hello-interval *seconds*	(Опционально) Установка интервала отправки пакетов “hello”
exit	Переход в предыдущий режим настройки
exit	Переход в предыдущий режим настройки

Продолжение таблицы 19

Команда	Назначение
show ip ospf [*process-id***]**	Проверка глобальных настроек OSPFv3
show ip ospf interface [*interface-id***]**	Проверка настроек OSPFv3 на интерфейсе
copy running-config startup-config	Сохранение текущей конфигурации

16.6.2 clear ip ospf6 process

Команда фундаментального режима. Перезапуск процесса OSPFv3.

Синтаксис команды:

clear ip ospf6 [*process-id***] process**

Параметры команды:

process-id — идентификатор процесса OSPF, назначенный пользователем. Идентификатор процесса имеет только локальное значение в пределах устройства. Диапазон значений: от 1 до $2^{32} - 1$

Использование команды:

Команда «**clear ip ospf6 process**» используется для перезапуска процесса OSPFv3. Команда без указания идентификатора процесса перезапускает все процессы OSPFv3.

Пример команды:

```
admin@Switch# clear ip ospf6 50000 process
admin@Switch#
```

16.6.3 router ospf6

Команда глобальной настройки. Создание и переход в режим настройки процесса маршрутизации OSPFv3.

Синтаксис команды:

router ospf6 *process-id*

no router ospf6 *process-id*

Команда с приставкой «**no**» удаляет процесс.

Параметры команды:

process-id — идентификатор процесса OSPFv3, назначенный пользователем. Идентификатор процесса имеет только локальное значение в пределах устройства. Диапазон значений: от 1 до $2^{32} - 1$

Значение по умолчанию:

Процессы OSPFv3 отсутствуют.

Использование команды:

Команда «**router ospf6**» используется для создания и перехода в режим настройки процесса маршрутизации OSPFv3.

При удалении процесса маршрутизации OSPFv3 с помощью команды «**no router ospf6**» конфигурация процесса также удаляется.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)#
```

16.6.4 area authentication

Команда настройки маршрутизации (OSPFv3). Включение аутентификации в пределах области OSPFv3.

Синтаксис команды:

area *area-id* **authentication [message-digest]**

no area *area-id* **authentication**

Команда с приставкой «**no**» отключает аутентификацию.

Параметры команды:

area-id	идентификатор области, для которой необходимо включить аутентификацию. Идентификатор может быть указан в виде целого числа или IP-адреса
message-digest	включает аутентификацию с использованием MD5 (Message Digest 5)

Значение по умолчанию:

Аутентификация отключена.

Использование команды:

Команда «**area authentication**» используется для включения аутентификации в пределах области OSPFv3.

Включение аутентификации на области устанавливает режим аутентификации с помощью простого пароля. Тип аутентификации должен быть одинаковым на всех устройствах в области для обеспечения совместной работы по протоколу OSPFv3.

Команда настройки интерфейса «**ip ospf authentication-key**» используется для настройки пароля на интерфейсе.

Если установлен режим аутентификации с использованием MD5, то необходимо настроить пароль на интерфейсе с помощью команды настройки интерфейса «**ip ospf message-digest-key**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ipv6 address 2001:1234:abcd::1 /64
admin@Switch(config-if-vlan)# ip ospf authentication-key MyKey
admin@Switch(config-if-vlan)# exit
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# network 2001:1234:abcd:: /64 area 0
admin@Switch(config-ospf6)# area 0 authentication
admin@Switch(config-ospf6)#
```

16.6.5 area default-cost

Команда настройки маршрутизации (OSPFv3). Установка стоимости пути суммарного маршрута по умолчанию, отправляемого в область stub или NSSA (Not So Stubby Area).

Синтаксис команды:

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

area-id	идентификатор области с типом stub или NSSA. Идентификатор может быть указан в виде целого числа или IP-адреса
cost	стоимость пути суммарного маршрута по умолчанию, используемого для области с типом stub или NSSA, в диапазоне от 1 до 16777215

Значение по умолчанию:

Стоимость пути равна 1.

Использование команды:

Команда «**area default-cost**» используется для установки стоимости пути суммарного маршрута по умолчанию, отправляемого в область stub или NSSA (Not So Stubby Area).

Команда используется только на пограничном маршрутизаторе области (Area Border Router), подключенном к области с типом stub или NSSA.

Режим области stub должен быть настроен на всех устройствах, подключенной к этой области с помощью команды «**area stub**». Команда «**area default-cost**» предоставляет метрику суммарного маршрута по умолчанию, который генерируется пограничным маршрутизатором области в область с типом stub.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ipv6 address 2001:1234:abcd::1 /64
admin@Switch(config-if-vlan)# exit
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# network 2001:1234:abcd:: /64 area 0
admin@Switch(config-ospf6)# area 0 stub
admin@Switch(config-ospf6)# area 0 default-cost 100
admin@Switch(config-ospf6)#
```

16.6.6 area nssa

Команда настройки маршрутизации (OSPFv3). Установка типа области NSSA (Not So Stubby Area).

Синтаксис команды:

area *area-id* **nssa [no-summary] [translator-role {always | candidate}] [translator-stability-interval** *seconds***]**

no area *area-id* **nssa**

Команда с приставкой «**no**» удаляет тип области NSSA.

Параметры команды:

area-id	идентификатор области NSSA. Идентификатор может быть указан в виде целого числа или IP-адреса
no-summary	суммарный маршрут не будет анонсироваться в область NSSA
translator-role	включение режима безусловной трансляции LSA тип 2007 в LSA тип 4005: – **always** – трансляция включена всегда; – **candidate** – устройство является кандидатом на роль транслятора. По умолчанию используется режим **candidate**
seconds	интервал времени, прошедший с момента прекращения трансляции, после которого выбранный транслятор возобновляет трансляцию, в диапазоне от 1 до 65535 секунд. По умолчанию используется интервал 40 секунд

Значение по умолчанию:

Область не является NSSA.

Использование команды:

Команда «**area nssa**» используется для установки типа области NSSA (Not So Stubby Area)

Команда «**no area nssa**» не удаляет область, а только переводит ее в транзитный (обычный) режим.

Для удаления области используется команда «**no area**».

Типы области NSSA и stub взаимоисключающие, поэтому можно установить либо тип NSSA с помощью команды «**area nssa**», либо тип stub с помощью команды «**area stub**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# network 2001:1234:abcd:: /64 area 0
admin@Switch(config-ospf6)# area 0 nssa
admin@Switch(config-ospf6)#
```

16.6.7 area range

Команда настройки маршрутизации (OSPFv3). Консолидация и суммаризация маршрутов на границе области.

Синтаксис команды:

area *area-id* **range** *ip-address mask* **[advertise | not-advertise]**

no area *area-id* **range** *ip-address mask*

Команда с приставкой «**no**» отключает функцию.

Параметры команды:

area-id	идентификатор области. Идентификатор может быть указан в виде целого числа или IP-адреса
ip-address	IP-адрес сети (подсети)
mask	маска IP-адреса
advertise	генерация суммарных анонсов для указанных сетей. Значение используется по умолчанию
not-advertise	запрет генерации суммарных анонсов для указанных сетей

Значение по умолчанию:

Суммаризация маршрутов на границе области отключена.

Использование команды:

Команда «**area range**» используется для консолидации и суммаризации маршрутов на границе области.

Команда используется только на пограничном маршрутизаторе области (Area Border Router) для консолидации и суммаризации маршрутов. Маршрутизатор анонсирует один суммарный маршрут в другие области для указанных сетей, то есть маршрутная информация консолидируется на границе областей.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ipv6 address 2001:1234:abcd::1 /64
admin@Switch(config-if-vlan)# exit
admin@Switch(config)# interface vlan 2
admin@Switch(config-if-vlan)# ipv6 address 2002:1234:abcd::1 /64
admin@Switch(config-if-vlan)# exit
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# network 2001:1234:abcd:: /64 area 0
admin@Switch(config-ospf6)# area 10 range 1000:1234:abcd:: /24
admin@Switch(config-ospf6)# area 0 range 2002:1234:abcd::1 /48
admin@Switch(config-ospf6)#
```

16.6.8 area shutdown

Команда настройки маршрутизации (OSPFv3). Запуск процесса отключения области (graceful shutdown).

Синтаксис команды:

area *area-id* **shutdown**

no area *area-id* **shutdown**

Команда с приставкой «**no**» перезапускает процесс маршрутизации OSPFv3.

Параметры команды:

area-id	идентификатор области. Идентификатор может быть указан в виде целого числа или IP-адреса

Значение по умолчанию:

OSPFv3 активен в текущей области.

Использование команды:

Команда «**area shutdown**» используется для запуска процесса отключения области (graceful shutdown).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# area 0 shutdown
admin@Switch(config-ospf6)#
```

16.6.9 area stub

Команда настройки маршрутизации (OSPFv3). Установка типа области stub (область без транзитного трафика).

Синтаксис команды:

area *area-id* **stub [no-summary]**

no area *area-id* **stub**

Команда с приставкой «**no**» удаляет тип области stub.

Параметры команды:

area-id	идентификатор области stub. Идентификатор может быть указан в виде целого числа или IP-адреса
no-summary	суммарный маршрут не будет анонсироваться в область stub

Значение по умолчанию:

Область не является stub.

Использование команды:

Команда «**area stub**» используется для установки типа области stub (область без транзитного трафика).

Команда «**no area stub**» не удаляет область, а только переводит ее в транзитный (обычный) режим.

Для удаления области используется команда «**no area**».

Типы области NSSA и stub взаимоисключающие, поэтому можно установить либо тип NSSA с помощью команды «**area nssa**», либо тип stub с помощью команды «**area stub**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# network 2001:1234:abcd:: /64 area 0
admin@Switch(config-ospf6)# area 0 stub
admin@Switch(config-ospf6)#
```

16.6.10 max-metric router-lsa

Команда настройки маршрутизации (OSPFv3). Включение анонсирования максимальной метрики, таким образом, остальные маршрутизаторы будут предпочитать использование других маршрутизаторов при вычислении маршрутов.

Синтаксис команды:
max-metric router-lsa
no max-metric router-lsa
Команда с приставкой «**no**» отключает анонсирование максимальной метрики.
Значение по умолчанию:
Анонсируются нормальные метрики.
Использование команды:
Команда «**max-metric router-lsa**» используется для включения анонсирования максимальной метрики, таким образом, остальные маршрутизаторы будут предпочитать использование других маршрутизаторов при вычислении маршрутов.

При включении настройки устройство анонсирует максимальные метрики постоянно или до истечения интервала времени, заданного пользователем.

Метрики маршрутов (интерфейсов) в нетранзитной области (stub), подключенных напрямую, не зависят от настройки «**max-metric router-lsa**», т.к. стоимость маршрута всегда устанавливается равной стоимости на интерфейсе.

Настройка «**max-metric router-lsa**» полезна в следующих случаях:

1. Перезагрузка устройства. После перезагрузки протоколы внутренней маршрутизации (Interior Gateway Protocols) сходятся очень быстро и другие маршрутизаторы могут начать передачу трафика через устройство. Если устройство все еще находится в процессе загрузки маршрутов BGP, пакеты для других сетей могут быть отброшены.
2. Добавление устройства в сеть без разрешения передачи транзитного трафика через него. Если альтернативные маршруты недоступны, то устройство все равно будет пропускать транзитный трафик.
3. Удаление устройства из сети (отключение). В этом случае остальные маршрутизаторы будут использовать альтернативные маршруты для передачи трафика.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# max-metric router-lsa
admin@Switch(config-ospf6)#
```

16.6.11 network area

Команда настройки маршрутизации (OSPFv3). Добавление сетей (IP-интерфейсов) в область OSPFv3.
Синтаксис команды:
network *ip-address prefix* **area** *area-id* **[shutdown]**
no network *ip-address prefix* **area** *area-id*
Команда с приставкой «**no**» удаляет сети (IP-интерфейсы) из области OSPFv3.

Параметры команды:

ip-address	IP-адрес сети (подсети)
prefix	префикс сети (подсети)
area-id	идентификатор области, к которой будут относиться указанные сети (подсети). Идентификатор может быть указан в виде целого числа или IP-адреса
shutdown	интерфейс добавляется в отключенном состоянии (не передает и не принимает пакеты OSPFv3)

Значение по умолчанию:

К области не относится ни одна сеть (IP-интерфейс).

Использование команды:

Команда «**network area**» используется для добавления сетей (IP-интерфейсов) в область OSPFv3.

Параметры команды «*ip-address*» и «*prefix*» позволяют указать несколько интерфейсов (сетей) для добавления в область OSPFv3. Устройство добавляет интерфейсы по следующему алгоритму:

1. Производится логическая операция “И” между IP-адресом интерфейса и параметром «*prefix*».
2. Производится логическая операция “И” между параметром «*ip-address*» и параметром «*prefix*».
3. Если полученные результаты совпадают, то интерфейс добавляется в указанную пользователем область OSPFv3.

Интерфейс может быть добавлен только в одну область. Если диапазоны адресов для разных областей пересекаются, то устройство настраивает первую по очереди область и игнорирует все остальные. Не рекомендуется настройка пересекающихся адресов для разных областей в целях исключения неожиданных конфликтов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# network 2001:1234:abcd:: /64 area 0
admin@Switch(config-ospf6)# network 10:10:10:: /48 area 10
admin@Switch(config-ospf6)# network :: /24 area 1
admin@Switch(config-ospf6)#
```

16.6.12 no area

Команда настройки маршрутизации (OSPFv3). Удаление области OSPFv3.

Синтаксис команды:

no area *area-id*

Параметры команды:

area-id	идентификатор области, которую необходимо удалить. Идентификатор может быть указан в виде целого числа или IP-адреса

Использование команды:

Команда «**no area**» используется для удаления области OSPFv3.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# no area 1
admin@Switch(config-ospf6)#
```

16.6.13 passive-interface

Команда настройки маршрутизации (OSPFv3). Отключение отправки обновления маршрутов на всех интерфейсах OSPFv3.

Синтаксис команды:

passive-interface

no passive-interface

Команда с приставкой «**no**» включает отправку обновления маршрутов.

Значение по умолчанию:

Отправка обновления маршрутов включена.

Использование команды:

Команда «**passive-interface**» используется для отключения отправки обновления маршрутов на всех интерфейсах OSPFv3.

Маршрутная информация OSPFv3 не будет отправляться и приниматься на всех интерфейсах OSPFv3.

Пассивный интерфейс ведет себя как нетранзитная сеть (stub network) в домене OSPFv3. Настройка полезна в сети провайдера при использовании большого количества интерфейсов.

После использования команды «**passive-interface**» пользователь может включить отправку обновления маршрутов на отдельных интерфейсах, для которых необходимо обновление, с помощью команды «**no ip ospf passive-interface**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# passive-interface
admin@Switch(config-ospf6)#
```

16.6.14 redistribute

Команда настройки маршрутизации (OSPFv3, BGP). Включение распределения маршрутов из одного домена маршрутизации в другой.

Синтаксис команды:

redistribute *protocol* [*process-id*] **[metric** *metric-value*] **[metric-type** *type-value*] **[match {internal | external 1 | external 2}] route-map** *map-tag* **subnets nssa-only**

no redistribute *protocol* [*process-id*] **[metric** *metric-value*] **[metric-type** *typevalue*] **[match {internal | external 1 | external 2}] route-map** *map-tag* **subnets nssaonly**

Команда с приставкой «**no**» отключает распределение маршрутов.

Параметры команды:

protocol — источник маршрутов, которые будут распределены. Варианты протокола:

- bgp – источником является протокол BGP;
- connected – источником являются сети, подключенные напрямую (для которых задан IP-адрес на одном из интерфейсов устройства);
- ospf – источником является другой процесс OSPF;
- static – источником являются статические маршруты;
- rip – источником является протокол RIP

process-id — идентификатор процесса OSPFv3, из которого будут распределяться маршруты. По умолчанию используется номер 1. Не имеет значения, если источником указан не протокол OSPF

metric-value — значение метрики маршрута, назначаемой для распределяемых маршрутов. Значение метрики указано в отображении маршрутов (заданной командой «**set metric**») имеет приоритет перед настройкой «*metric-value*» (замещает ее)

type-value — тип внешнего соединения, ассоциируемого с маршрутом по умолчанию, анонсируемого в домен OSPF:

1 – внешний маршрут Тип 1;

2 – внешний маршрут Тип 2.

По умолчанию используется внешний маршрут Тип 2

match{internal| external1| external2} — критерии, по которым маршруты OSFP распределяются в процесс OSPF:

- **internal** – внутренние маршруты автономной системы;
- **external 1** – внешние маршруты для автономной системы, которые импортированы в OSPF как внешний маршрут Тип 1;
- **external 2** – внешние маршруты для автономной системы, которые импортированы в OSPF как внешний маршрут Тип 2

Значение по умолчанию:

Распределение маршрутов отключено.

Использование команды:

Команда «**redistribute**» используется для включения распределения маршрутов из одного домена маршрутизации в другой.

Смена настройки, ассоциированной с ключевым словом, не затрагивает остальные настройки.

Устройство, получающее маршруты по протоколу на основе состояний соединения (например, OSPF) с внутренней метрикой, будет считать, что стоимость маршрута равна стоимости от самого себя до устройства, распределяющего маршруты плюс анонсированную стоимость до точки назначения. Для внешней метрики стоимость равна только анонсированной стоимости до точки назначения.

При использовании команды «**redistribute**» для распределения маршрутов в домен OSPFv3 устройство автоматически становится пограничным маршрутизатором автономной системы (Autonomous System Boundary Router).

Распределение маршрутов с помощью ключевого слова «**connected**» охватывает только те сети, подключенные напрямую, которые не указаны явно с помощью команды «**network**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# redistribute static
admin@Switch(config-ospf6)#
```

16.6.15 router-id

Команда настройки маршрутизации (OSPFv3). Установка фиксированного значения идентификатора маршрутизатора.

Синтаксис команды:

router-id *ip-address*

no router-id *ip-address*

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

p-address	идентификатор маршрутизатора в формате IP-адреса

Значение по умолчанию:

Наименьший IPv4-адрес, настроенный на устройстве.

Использование команды:

Команда «**router-id**» используется для установки фиксированного значения идентификатора маршрутизатора.

Допускается установка любого идентификатора маршрутизатора в формате. IP-адреса, однако каждый идентификатор должен быть уникальным.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router ospf6 1000
admin@Switch(config-ospf6)# router-id 1.1.1.1
admin@Switch(config-ospf6)#
```

16.7 Настройка IS-IS

16.7.1 Общие положения

IS-IS (Intermediate System to Intermediate System) является протоколом маршрутизации, основанном на алгоритме SPF (Shortest Path First). Данный протокол используется для определения оптимальных путей в сети. Используется для обмена информацией о топологии сети между маршрутизаторами или другими устройствами, называемыми «Intermediate Systems — IS». Этот протокол примечателен своей эффективностью и масштабируемостью, что позволяет ему использоваться в очень крупных сетях с большим количеством маршрутизаторов.

Основные компоненты протокола IS-IS:

1. LSP (Link State Protocol): IS-IS использует LSP для обмена информацией о соседних устройствах (маршрутизаторах) и представления топологии сети. Это позволяет устройствам в сети создавать и поддерживать базу данных маршрутов.
2. SPF (Shortest Path First): IS-IS использует алгоритм SPF для определения оптимальных маршрутов в сети. Этот алгоритм вычисляет кратчайшие пути к различным узлам сети, учитывая стоимость связей и другие параметры.
3. Hello-пакеты: IS-IS использует Hello-пакеты для обнаружения и поддержания связи с соседними устройствами. Они служат для определения соседних маршрутизаторов и поддержания активных связей в сети.
4. Алгоритм выбора маршрута: IS-IS принимает решения о маршрутизации на основе различных метрик, таких как пропускная способность, задержка и стабильность связей между устройствами.
5. При настройке is-type, уровни L1 и L2 (level-1 и level-2) не взаимоисключают друг друга, а дополняют.

Преимущества IS-IS:

1. Масштабируемость: IS-IS хорошо масштабируется и эффективно работает в крупных сетях, обеспечивая стабильность и быстрое перестроение маршрутов при изменениях топологии.
2. Быстрая сходимость: протокол IS-IS имеет быструю скорость сходимости, что позволяет быстро перестраивать маршруты при изменениях в сети.
3. Поддержка разных типов сетей: IS-IS может работать как в IP-, так и в OSI-сетях, что делает его универсальным протоколом для различных типов сетей.

Протокол IS-IS предоставляет механизм для создания и поддержания базы данных маршрутов в сети, обеспечивая оптимальную маршрутизацию данных и управление трафиком.

Настройки пользователя:

1. Глобальные настройки:

- название процесса IS-IS;
- идентификатор маршрутизатора (router-id).

2. Настройка областей (NET):

- идентификатор AFI (Autority and Format Identifier);
- область принадлежности маршрутизатора (Area ID);
- идентификатор маршрутизатора (System ID);
- значение Selector.

3. Настройки IP-интерфейсов (в текущей реализации поддерживаются только VLAN):

- настройка типа соединения для интерфейса (isis circuit-type): [level-1 | level-1-2 | level-2-only];
- установка интервала CSNP (Complete Sequence Number Protocol Data Units) в секундах (isis csnp-interval): целое число;
- добавление заполнения в hello-пакеты IS-IS в hello-пакетах IS-IS (isis hello padding);
- установка интервала hello-пакетов (isis hello-interval): целое число;
- установка множителя для времени удержания hello-пакетов (isis hello-interval): целое число;
- установка метрики по умолчанию для соединения: целое число;
- установка соседства в режиме точка-точка (isis network point-to-point);
- установка пассивного режима для интерфейса (isis passive);
- установка списка ключей для аутентификации уровня (isis password): [clear | md5];
- установка приоритета маршрутизатора (isis priority): целое число;
- установка интервала генерации и отправки Partial Serquence Number Data Units (PSNP PDUs) (isis psnp-interval): целое число: [level-1| level-2].

Дополнения и ограничения:

Рекомендуется сначала задать параметры для router isis <name>, и лишь затем применять его на настраиваемый vlan.

Порядок настройки:

Порядок настройки IS-IS приведен в таблице 20.

Таблица 20 – Порядок настройки IS-IS

Команда	Назначение
configure terminal	Переход в режим глобальной настройки
router isis *procecc-name*	Создание и переход в режим настройки процесса маршрутизации IS-IS
net *net-address*	Установка идентификатора маршрутизатора net
is-type *level-id*	Установка уровня работы протокола IS-IS
log-adjacency-changes	(Опционально) Запись изменения в состоянии смежности
exit	Переход в предыдущий режим настройки
interface vlan *vlan-id*	Переход в режим настройки интерфейса VLAN
ip router isis *proccess-name*	Назначение процесса IS-IS к интерфейсу
ip address add *ip-adress*	Установка IP-адреса на vlan
exit	Переход в предыдущий режим настройки
exit	Переход в предыдущий режим настройки
show isis summary	Проверка настроек IS-IS
show isis database	Проверка состояний каналов IS-IS
copy running-config startup-config	Сохранение текущей конфигурации

Активация протокола IS-IS:

- войти в режим конфигурации configure terminal;
- ввести команду для активации IS-IS на интерфейсе: router isis <name>;
- указать идентификатор маршрутизатора: net <идентификатор>;
- назначить процесс IS-IS к интерфейсу vlan: interface vlan <номер vlan>, ip router isis <name>.

16.7.2 clear isis neighbor

Команда фундаментального режима. Перезапуск соседства IS-IS.
Синтаксис команды:
clear isis neighbor

Использование команды:

Команда «**clear isis neighbor**» используется для перезапуска процесса соседства IS-IS.

Примеры команды:

```
admin@Switch# clear isis neighbor
```

16.7.3 router isis

Команда глобальной настройки. Создание и переход в режим настройки процесса маршрутизации IS-IS.

Синтаксис команды:

router isis *isis-name*

no router isis *isis-name*

Команда с приставкой «**no**» удаляет процесс.

Параметры команды:

isis-name	идентификатор (имя) IS-IS

Использование команды:

Команда «**router isis**» используется для создания и перехода в режим настройки процесса маршрутизации IS-IS. При удалении процесса маршрутизации IS-IS с помощью команды «**no router isis**» конфигурация процесса также удаляется.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router isis example
admin@Switch(config-isis)#
```

16.7.4 area password

Команда настройки маршрутизации (IS-IS). Настраивает пароль аутентификации области IS-IS, предотвращая внесение не авторизованными маршрутизаторами ложной информации о маршрутизации в базу данных состояния каналов.

Синтаксис команды:

area-password {md5 *area-password* **| clear** *area_password***}**

no area-password

Команда с приставкой «**no**» удаляет пароль аутентификации.

Параметры команды:

area-password	пароль пользователя в виде зашифрованной строки
md5	тип шифрования md5
clear	пароль без шифрования

Значение по умолчанию:

Пароль аутентификации отсутствует.

Использование команды:

Если пароль не задан, то поле будет пустым.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router isis example
admin@Switch(config-isis)# area-password md5 pass
admin@Switch(config-isis)#
```

16.7.5 default-information originate

Команда настройки маршрутизации (IS-IS). Объявление маршрута по умолчанию по всей сети. В стандартной настройке перераспределение маршрутов по умолчанию не происходит. Если необходимо объявить маршрут по умолчанию необходимо использовать команду «**default-information originate**». Данная команда заставляет маршрутизатор объявить маршруты по умолчанию.

Синтаксис команды:

default-information originate {ipv4 | ipv6} {level-1 | level-2} [always [metric *number***] | metric** *number* **| route-map** *word***]**

no default-information originate [ipv4 | ipv6] [level-1 | level-2]

Команда с приставкой «**no**» отключает функцию.

Параметры команды:

ipv4	распределяет маршрут по умолчанию по ipv4
ipv6	распределяет маршрут по умолчанию по ipv6
level-1	распределяет маршрут по умолчанию на первом уровне
level-2	распределяет маршрут по умолчанию на первом уровне
always	постоянная раздача маршрута по умолчанию
metric	установка метрики по умолчанию
number	значение метрики в диапазоне <0-16777215>
word	указатель на записи маршрутов

Значение по умолчанию:

Объявление маршрута по умолчанию по всей сети отключено.

Пример команды:

```
admin@Switch(config-isis)# default-information originate ipv4 level-1 always metric 10
admin@Switch(config-isis)#
```

16.7.6 domain password

Команда настройки маршрутизации (IS-IS). Настройка пароля аутентификации домена маршрутизации IS-IS, предотвращает внесение не авторизованными маршрутизаторами ложной информации о маршрутизации в базу данных состояния каналов.

Синтаксис команды:
domain-password {md5 *area-password* **| clear** *area-password***}**
no domain-password
Команда с приставкой «**no**» удаляет пароль аутентификации домена маршрутизации.
Параметры команды:

area-password	пароль пользователя в виде зашифрованной строки.
md5	тип аутентификации
clear	тип аутентификации

Значение по умолчанию:
Пароль отсутствует.
Использование команды:
Если пароль не задан, то поле будет пустым.
Пример команды:

```
admin@Switch(config-isis)# domain-password md5 pass
admin@Switch(config-isis)#
```

16.7.7 hostname dynamic

Команда настройки маршрутизации (IS-IS). Данная команда позволяет передавать hostname маршрутизатора в LSP.
Синтаксис команды:
hostname dynamic
no hostname dynamic
Команда с приставкой «**no**» отключает динамическую передачу.
Значение по умолчанию:
Функция включена по умолчанию.
Использование команды:
Если пароль не задан, то поле будет пустым.
Пример команды:

```
admin@Switch(config-isis)# hostname dynamic
admin@Switch(config-isis)#
%CFG-6-CHANGED: Configuration changed by admin
admin@Switch(config-isis)#
```

16.7.8 is-type

Команда настройки маршрутизации (IS-IS). Данная команда определяет на каком уровне маршрутизации будет работать текущий процесс IS-IS.
Синтаксис команды:
is-type {level-1 | level-1-2 | level-2-only}
no is-type {level-1 | level-1-2 | level-2-only}
Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

level-1	работа производится только на 1 уровне
level-1-2	работа производится и на 1, и на 2 уровне
level-2-only	работа производится только на 2 уровне

Значение по умолчанию:
По умолчанию работает на уровне level-1-2.
Пример команды:

```
admin@Switch(config-isis)# is-type level-1-2
admin@Switch(config-isis)#
```

16.7.9 log-adjacency-changes

Команда настройки маршрутизации (IS-IS). Включение протоколирования изменений смежности.

Синтаксис команды:
log-adjacency-changes
no log-adjacency-changes
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Значение по умолчанию:
По умолчанию функция отключена.
Использование команды:
Данная команда включает журналирование изменений.
Пример команды:

```
admin@Switch(config-isis)# log-adjacency-changes
admin@Switch(config-isis)#
%CFG-6-CHANGED: Configuration changed by admin
admin@Switch(config-isis)#
```

16.7.10 lsp-gen-interval

Команда настройки маршрутизации (IS-IS). Интервал между генерацией LSP.
Синтаксис команды:
lsp-gen-interval {level-1 *interval* **| level-2** *interval***}**
no lsp-gen-interval {level-1 | level-2}
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

interval	минимальный интервал в секундах (диапазон <1-120>)
level-1	установка интервала только на 1 уровне
level-2	установка интервала только на 2 уровне

Значение по умолчанию:
По умолчанию значение lsp-gen-interval равно 30.

Использование команды:

Данная команда используется для настройки количества секунд между генерацией LSP, когда происходит изменение состояния.

Пример команды:

```
admin@Switch(config-isis)# lsp-gen-interval level-1 10
admin@Switch(config-isis)#
```

16.7.11 lsp-mtu

Команда настройки маршрутизации (IS-IS). Настройка максимального размера генерируемых LSP.

Синтаксис команды:

lsp-mtu *maximum-size*

no lsp-mtu

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

maximum-size	максимальный размер генерируемых LSP, диапазон от 128 до 4352

Значение по умолчанию:

По умолчанию значение lsp-mtu равно 1497.

Использование команды:

Размер LSP MTU описывает количество информации, которое может быть записано в одном пакете состояния канала.

Пример команды:

```
admin@Switch(config-isis)# lsp-mtu 2000
admin@Switch(config-isis)#
```

16.7.12 lsp-refresh-interval

Команда настройки маршрутизации (IS-IS). Настройка интервала обновления LSP.

Синтаксис команды:

lsp-refresh-interval {level-1 *interval* **| level-2** *interval***}**

no lsp-refresh-interval{level-1 | level-2}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

interval	интервал обновления LSP в секундах в диапазоне 1-65235
level-1	установка интервала только на 1 уровне
level-2	установка интервала только на 2 уровне

Значение по умолчанию:

По умолчанию значение lsp-refresh-interval равно 900.

Использование команды:

Устанавливает интервал, через который IS-IS регулярно генерирует LSP, независимо от того, произошли ли какие-то изменения в LSP.

Пример команды:

```
admin@Switch(config-isis)# lsp-refresh-interval level-1 500
admin@Switch(config-isis)#
```

16.7.13 max-lsp-lifetime

Команда настройки маршрутизации (IS-IS). Команда задает время жизни собственных LSP.

Синтаксис команды:

max-lsp-lifetime {level-1 *lifetime* **| level-2** *lifetime***}**

no max-lsp-lifetime {level-1 | level-2}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

lifetime	время жизни LSP в секундах в диапазоне <350-65235>
level-1	установка времени жизни только на 1 уровне
level-2	установка времени жизни только на 2 уровне

Значение по умолчанию:

По умолчанию значение max-lsp-lifetime равно 1200.

Использование команды:

Устанавливает максимальное количество секунд, в течение которых необновленное состояние канала LSP остается в базе данных устройства.

Пример команды:

```
admin@Switch(config-isis)# max-lsp-lifetime level-1 60000
admin@Switch(config-isis)#
%CFG-6-CHANGED: Configuration changed by admin
admin@Switch(config-isis)#
```

16.7.14 metric-style

Команда настройки маршрутизации (IS-IS). Данная команда устанавливает тип метрики, который будет использоваться в работе IS-IS процесса.

Синтаксис команды:

metric-style {narrow | transition | wide}

no metric-style

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

narrow	использование стиля TLV с узкой метрикой
wide	использование нового стиля TLV для более широкой метрики
transition	отправка и прием TLV обоих стилей во время перехода

Значение по умолчанию:

Параметр **narrow**.

Использование команды:

Команда настройки маршрутизации (IS-IS). С помощью данной команды можно установить тип метрики, который будет использоваться в работе IS-IS процесса.

Пример команды:

```
admin@Switch(config-isis)# metric-style wide
admin@Switch(config-isis)#
%CFG-6-CHANGED: Configuration changed by admin
admin@Switch(config-isis)#
```

16.7.15 net

Данная команда устанавливает NET (Network Entity Title) адрес.

Синтаксис команды:

net *net-address*

no net *net-address*

Команда с приставкой «**no**» удаляет область NET.

Параметры команды:

net-address	адрес NET (Network Entity Title). Формат: XX.XXXX.XXXX.XXXX.XXXX.XX

Значение по умолчанию:

Нет значения по умолчанию.

Использование команды:

Данная команда устанавливает NET (Network Entity Title) адрес. Он репрезентует AFI (Authority and Format Identifier), Area ID (зону к которой принадлежит маршрутизатор), System ID (идентификатор маршрутизатора) и значение Selector.

NET-адреса имеют несколько форм, в зависимости от требований сети. Адреса NET имеют шестнадцатеричную систему с длиной от 8 до 20 октетов. Как правило, формат состоит из идентификатора власти и формата (AFI), идентификатора домена, идентификатора области, системного идентификатора и селектора. В самом простом формате идентификатор домена отсутствует, а его длина составляет 10 октетов. Например, NET-адрес 49.0001.1921.6800.1001.00 состоит из следующих частей:

- 49 — AFI;
- 0001 — идентификатор области;
- 1921.6800.1001 — идентификатор системы;
- 00 — селектор.

Идентификатор системы должен быть уникальным в сети. Для сети, работающей только по IP, рекомендуется использовать IP-адрес интерфейса на маршрутизаторе. Настройка петлевого NET-адреса вместе с IP-адресом будет полезна при необходимости поиска неисправностей в сети.

Первая часть адреса – это номер области, который представляет собой переменное число от 1 до 13 байт. Первый байт номера области (49) – это индикатор полномочий и формата (AFI). Следующие байты – это назначенный идентификатор домена (области), который может иметь размер от 0 до 12 байт. В приведенном выше примере идентификатор области равен 0001.

Следующие шесть байтов образуют системный идентификатор. Системный идентификатор может состоять из любых шести байтов, которые уникальны для всего домена. Обычно системный идентификатор представляет собой адрес управления доступом к среде (MAC) или IP-адрес, выраженный в двоично-десятичном коде (BCD). Последний байт (00) – это n-селектор.

Пример команды:

```
admin@Switch(config-isis)# net 49.0001.0000.0000.0001.00
admin@Switch(config-isis)#
```

16.7.16 redistribute

Команда настройки маршрутизации (IS-IS). Включение распределения маршрутов из одного домена маршрутизации в другой.

Синтаксис команды:

redistribute {ipv4 | ipv6} *protocol* **{level-1 | level-2} [metric** *metric-value*] **[route-map** *map-tag*]

no redistribute {ipv4 | ipv6} *protocol* **{level-1 | level-2}**

Команда с приставкой «**no**» отключает распределение маршрутов.

Параметры команды:

ipv4 перераспределение маршрутов по IPv4

ipv6 перераспределение маршрутов по IPv6

protocol источники маршрутов, которые будут распределены. Варианты протокола:

- **bgp** – источником является протокол BGP
- **connected** – источником являются сети, подключенные напрямую (для которых задан IP-адрес на одном из интерфейсов устройства)
- **ospf** – источником является процесс OSPF
- **ospfv6** — источником является процес OSPFv6
- **static** – источником являются статические маршруты
- **rip** – источником является протокол RIP
- **ripng** – источником является ripng

level-1	перераспределение по уровню L1 (level-1)
level-2	перераспределение по уровню L2 (level-2)
metric-value	значение метрики маршрута, назначаемое для распределяемых маршрутов. Значение метрики указано в отображении маршрутов (заданной командой «**set metric**»), имеет приоритет перед настройкой «*metric-value*» (замещает ее). Изменяется в диапазоне 0-16777215
map-tag	указатель на записи карты маршрутов

Значение по умолчанию:

Перераспределение маршрутов отключено.

Использование команды:

Команда «**redistribute**» используется для включения распределения маршрутов из одного домена маршрутизации в другой. Смена настройки, ассоциированной с ключевым словом, не затрагивает остальные настройки.

Устройство, получающее маршруты по протоколу на основе состояний соединения (например, IS-IS) с внутренней метрикой, будет считать, что стоимость маршрута равна стоимости от самого себя до устройства, распределяющего маршруты плюс анонсированную стоимость до точки назначения. Для внешней метрики стоимость равна только анонсированной стоимости до точки назначения.

При использовании команды «**redistribute**» для распределения маршрутов в домен IS-IS устройство автоматически становится пограничным маршрутизатором автономной системы (Autonomous System Boundary Router).

Распределение маршрутов с помощью ключевого слова «connected» охватывает только те сети, подключенные напрямую, которые не указаны явно с помощью команды «net».

Пример команды:

```
admin@Switch(config-isis)# redistribute ipv4 bgp level-1 metric 10
admin@Switch(config-isis)#
```

16.7.17 set-overload-bit

Команда настройки маршрутизации (IS-IS). Настройка бита-перегрузки IS-IS.

Синтаксис команды:

set-overload-bit

no set-overload-bit

Команда с приставкой «**no**» отключает настройку бита-перегрузки.

Значение по умолчанию:

По умолчанию данная функция отключена.

Использование команды:

Данная команда используется во избежании, так называемых «черных дыр» в трафике до полной конвергенции протоколов маршрутизации.

Пример команды:

```
admin@Switch(config-isis)# set-overload-bit
admin@Switch(config-isis)#
```

16.7.18 mpls-te

Команда настройки маршрутизации (IS-IS). Данный функционал реализует интеграцию возможностей TE (возможность управления направлением прохождения трафика с целью выполнения определенных условий, например, резервирования каналов, распределения нагрузки сети, балансировки, предотвращения перегрузок) в протоколы третьего уровня.

Синтаксис команды:

mpls-te {on | route-address *router_address***}**

no mpls-te

Команда с приставкой «**no**» отключает mpls-te.

Параметры команды:

on	включение функциональности MPLS-TE
route-address	маршрут mpls
router_address	адрес в формате IPv4 (<A.B.C.D>)

Значение по умолчанию:

По умолчанию данная функция отключена.

Использование команды:

Данный функционал позволяет использовать однонаправленные туннели для задания пути прохождения определенного трафика. Например, для одного вида трафика — высокоприоритетного голосового, можно проложить один путь через сеть, а для низкоприоритетного — другой. Так как туннели — однонаправленные, то обратный путь может быть совершенно другим.

Пример команды:

```
admin@Switch(config-isis)# mpls-te on
admin@Switch(config-isis)#
admin@Switch(config-isis)# mpls-te router-address 1.1.1.1
admin@Switch(config-isis)#
```

16.7.19 spf-delay-ietf

Команда настройки маршрутизации (IS-IS). Данная команда в протоколе IS-IS используется для управления задержкой между двумя последовательными SPF (Shortest Path First) вычислениями.

Синтаксис команды:

spf-delay-ietf *init-delay short-delay long-delay holddown time-to-learn*

no spf-delay-ietf

Команда с приставкой «**no**» отключает управление задержкой между двумя SPF.

Параметры команды:

init-delay	задержка, используемая в состоянии quiet, в миллисекундах от 0 до 60000
short-delay	задержка, используемая в состоянии short_wait, в миллисекундах от 0 до 60000
long-delay	задержка, используемая в состоянии long_wait, в миллисекундах от 0 до 60000
holddown	время отсутствия полученных событий IGP (в миллисекундах) от 0 до 60000
time-to-learn	максимальное время для изучения всех событий, связанных с одним сбоем (в миллисекундах) от 0 до 60000

Значение по умолчанию:

Стандартные значения всех параметров: init-delay — 50 миллисекунд, short-delay — 200 миллисекунд, long-delay — 5000 миллисекунд, holddown — 10000 миллисекунд, time-to-learn — 500 миллисекунд.

Использование команды:

Это команда позволяет установить временной интервал между пересчетами SPF, что может быть полезно для снижения нагрузки на сеть во избежании чрезмерных вычислений маршрутов в короткие промежутки времени.

Пример использования:

```
admin@Switch(config-isis)# spf-delay-ietf 1 2 3 2 2
admin@Switch(config-isis)#
```

16.7.20 spf-interval

Команда настройки маршрутизации (IS-IS). Определяет интервал времени, через который выполняется алгоритм PSF (Shortest Path First), рассчитывающий кратчайший путь маршрутизации сети.

Синтаксис команды:

spf-interval {level-1 | level-2} *interval*

no spf-interval {level-1 | level-2}

Команда с приставкой «**no**» возвращает значение по умолчанию.

Параметры команды:

level-1	установка интервала только для уровня 1
level-2	установка интервала только для уровня 2
interval	минимальный интервал между последовательными SPF в секундах от 1 до 120

Значение по умолчанию:

По умолчанию 1 секунда.

Пример использования:

```
admin@Switch(config-isis)# spf-interval level-1 100
admin@Switch(config-isis)#
```

16.7.21 isis circuit-type

Команда настройки интерфейса (VLAN). Данная команда определяет на каком уровне маршрутизации будет работать текущий процесс IS-IS на конкретном интерфейсе.

Синтаксис команды:

isis circuit-type {level-1 | level-1-2 | level-2-only}

no isis circuit-type {level-1 | level-1-2 | level-2-only}

Команда с приставкой «**no**» задает значение по умолчанию.

Параметры команды:

level-1	формирование соединений только на уровне L1
level-1-2	формирование соединений на уровнях L1 и L2
level-2-only	формирование соединений только на уровне L2

Значение по умолчанию:

По умолчанию формирование соединений происходит на уровнях L1 и L2.

Использование команды:

Команда «**isis circuit-type**» используется для определения уровня маршрутизации процесса IS-IS.

Если определение уровня маршрутизации не задано, то по умолчанию, соединения происходят на уровнях L1 и L2.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis circuit-type level-1
admin@Switch(config-if-vlan)#
```

16.7.22 isis csnp-interval

Команда настройки интерфейса (VLAN). Данная команда устанавливает интервал генерации и отправки Complete Sequence Number Protocol Data Units (CSNP PDUs).

Синтаксис команды:

isis csnp-interval *csnp-interval* **{level-1 | level-2}**

no isis csnp-interval {level-1 | level-2}

Команда с приставкой «**no**» задает значение по умолчанию.

Параметры команды:

csnp-interval	значение интервала CSNP от 1 до 600
level-1	интервал для уровня L1
level-2	интервал для уровня L2

Значение по умолчанию:

По умолчанию значение интервала CSNP — 10 для обоих уровней.

Использование команды:

Команда «**isis csnp-interval**» используется для установки интервала генерации пакетов CSNP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis csnp-interval 600 level-1
admin@Switch(config-if-vlan)#
```

16.7.23 isis hello

Команда настройки интерфейса (VLAN). Влючает режим использования TLV8 в hello-пакетах

Синтаксис команды:

isis hello padding

no isis hello padding

Команда с приставкой «**no**» отключает режим использования TLV8 в hello-пакетах.

Параметры команды:

padding	hello-пакеты

Значение по умолчанию:

По умолчанию данная команда активна.

Использование команды:

Данная команда позволяет настроить и включить использование дополнительной информации («**padding**») в hello-пакетах протокола IS-IS.

Использование «**padding**» позволяет выравнивать длину пакетов и упрощает обработку пакетов на приемной стороне, обеспечивая более эффективное использование ресурсов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis hello padding
admin@Switch(config-if-vlan)#
```

16.7.24 isis hello-interval

Команда настройки интерфейса (VLAN). Данная команда устанавливает интервал отправки hello-пакетов (IIH) с интерфейса маршрутизатора.

Синтаксис команды:

isis hello-interval *hello-interval* **{level-1 | level-2}**

isis hello-interval {level-1 | level-2}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

hello-interval	значение hello-интервала от 1 до 600
level-1	интервал для уровня L1
level-2	интервал для уровня L2

Значение по умолчанию:

По умолчанию значение hello-интервала равно 3 для уровней L1 и L2.

Использование команды:

Данная команда используется для интервала времени между отправкой hello-пакетов в протоколе маршрутизации IS-IS. Данный интервал определяет частоту отправки сообщений для обновления информации о соседях и поддержания связи в сети.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis hello-interval 10 level-1
admin@Switch(config-if-vlan)#
```

16.7.25 isis hello-multiplier

Команда настройки интерфейса (VLAN). Данная команда устанавливает множитель для вычисления и отправки Hold Time (Hold Time = hello-timer * hello-multiplier) в hello-пакетах.

Синтаксис команды:

isis hello-multiplier *multiplier-value* **{level-1 | level-2}**

no isis hello-multiplier {level-1 | level-2}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

multiplier-value	число, принимающее значение от 2 до 100
level-1	интервал для уровня L1
level-2	интервал для уровня L2

Значение по умолчанию:

Значение по умолчанию 10 для уровней L1 и L2.

Использование команды:

Команда используется для определения количества пропущенных hello-сообщений, прежде чем соседнее устройство будет считаться недоступным. Этот параметр позволяет более точно определять когда устройство ушло из сети, если не было получено несколько последовательных hello-сообщений от этого устройства.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis hello-multiplier 5 level-2
admin@Switch(config-if-vlan)#
```

16.7.26 isis metric

Команда настройки интерфейса (VLAN). Данная команда устанавливает определенное значение метрики для интерфейса.

Синтаксис команды:

isis metric *metric-value* **{level-1 | level-2}**

no isis metric {level-1 | level-2}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

metric-value	значение метрики в диапазоне <0-16777215>
level-1	интервал для уровня L1
level-2	интервал для уровня L2

Значение по умолчанию:

Значение по умолчанию 10 для уровней L1 и L2.

Использование команды:

Метрика используется для определения наилучшего пути до конечного пункта в сети. Метрики в IS-IS представляют собой стоимость прохождения определенного соединения или пути. Эти метрики могут основываться на различных факторах, таких как пропускная способность, задержка или ручная настройка.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis metric 15000 level-1
admin@Switch(config-if-vlan)#
```

16.7.27 isis network point-to-point

Команда настройки интерфейса (VLAN). Данная команда переводит текущий интерфейс в режим работы point-to-point протокола IS-IS.

Синтаксис команды:

isis network point-to-point

no isis network point-to-point

Команда с приставкой «**no**» отключает режим работы point-to-point

Значение по умолчанию:

По умолчанию функция отключена.

Использование команды:

Команда «**isis network point-to-point**» используется для настройки интерфейса как точка-точка «point-to-point». Эта команда указывает протоколу IS-IS на тип сети данного интерфейса.

Когда интерфейс настроен как точка-точка, IS-IS использует определенные параметры настройки для работы в таком режиме, что включает уменьшение количества hello-пакетов, в следствии, улучшает оптимизацию работы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis network point-to-point
admin@Switch(config-if-vlan)#
```

16.7.28 isis passive

Команда настройки интерфейса (VLAN). Подавление отправки обновлений маршрутизации через данный интерфейс

Синтаксис команды:

isis passive

no isis passive

Команда с приставкой «**no**» переводит интерфейс в активный режим.

Значение по умолчанию:

По умолчанию интерфейс находится в активном режиме.

Использование команды:

Данная команда используется для подавления отправки пакетов маршрутизации через конкретный интерфейс.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis passive
admin@Switch(config-if-vlan)#
```

16.7.29 isis password

Команда настройки интерфейса (VLAN). Настройка пароля аутентификации.

Синтаксис команды:

isis password {md5 *password* **| clear** *password***}**

no isis password

Команда с приставкой «**no**» удаляет пароль аутентификации.

Параметры команды:

*passwor*d	пароль аутентификации
md5	пароль в шифровании md5
clear	пароль без шифрования

Значение по умолчанию:

Пароль аутентификации отсутствует.

Использование команды:

Команда «**isis password**» используется для установки пароля, который служит для аутентификации соседних устройств при обмене информацией о маршрутах через протокол IS-IS.

Это обеспечивает безопасность и защиту от несанкционированного доступа к маршрутной информации между устройствами, требуя указание одинакового пароля

на соседних устройствах для установления соседства и обмена данными по протоколу IS-IS.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis password md5 secret
admin@Switch(config-if-vlan)#
```

16.7.30 isis priority

Команда настройки интерфейса (VLAN). Данная команда устанавливает приоритет.

Синтаксис команды:

isis priority *priority-value* **{level-1 | level-2}**

no isis priority {level-1 | level-2}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

priority-value	значение приоритета в диапазоне от 0 до 127
level-1	установка приоритета для L1 уровня
level-2	установка приоритета для L2 уровня

Значение по умолчанию:

Для уровней L1 и L2 значение приоритета по умолчанию равно 64.

Использование команды:

Параметр «**isis priority**» используется для определения приоритета устройства при выборе DIS (Designated Intermediate System) в IS-IS протоколе. DIS играет важную роль в процессе обмена маршрутной информацией между устройствами в сети. Устройство с более высоким приоритетом имеет больше шансов быть выбранными в качестве DIS, что в свою очередь может повлиять на формирование топологических баз данных и распространение маршрутной информации в сети.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis priority 5 level-1
admin@Switch(config-if-vlan)#
```

16.7.31 isis psnp-interval

Команда настройки интерфейса (VLAN). Данная команда устанавливает интервал генерации и отправки Partial Sequence Number Protocol Data Units (PSNP PDUs).

Синтаксис команды:

isis psnp-interval *psnp-interval* **{level-1 | level-2}**

no isis psnp-interval {level-1 | level-2}

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

psnp-interval	значение интервала в диапазоне от 0 до 120
level-1	интервал для уровня L1
level-2	интервал для уровня L2

Значение по умолчанию:

Значение по умолчанию 2 для уровней L1 и L2.

Использование команды:

Команда «**isis psnp-interval**» определяет интервал времени между отправкой последовательности пакетов состояний маршрутов (PSNP – Partial Sequence Number Packet) в протоколе IS-IS. PSNP используются для обмена информацией о состоянии базы данных маршрутов между соседними устройствами.

Этот интервал определяет частоту отправки пакетов PSNP, позволяя устройствам поддерживать синхронизацию и обновлять информацию о маршрутах в сети. Установка данного интервала позволяет эффективно управлять частотой обмена пакетами PSNP и поддерживать соответствующий уровень согласованности данных между устройствами.

Пример использования:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# isis psnp-interval 100 level-1
admin@Switch(config-if-vlan)#
```

16.7.32 ip router isis

Команда настройки интерфейса (VLAN). Назначает процесс IS-IS к интерфейсу.

Синтаксис команды:

ip router isis *proccess tag*

no ip router isis *proccess tag*

Команда с приставкой «**no**» удаляет процесс.

Параметры команды:

proccess tag	метка (имя) процесса

Использование команды:

Команда «**ip router isis**» используется для назначения процесса IS-IS к интерфейсу.

Пример команды:

```
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip router isis TEST
admin@Switch(config-if-vlan)#
```

16.7.33 show isis

Команда, доступная из любого режима. Вывод информации о конфигурации и состоянии протокола ISIS (между промежуточными системами) на маршрутизаторе.

Синтаксис команды:

show isis [database | hostname | interface | mpls-te | neighbor | spf-delay-ietf | summary | topology]

Параметры команды:

database	используется для отображения содержимого базы данных состояния каналов ISIS (между промежуточными системами) на маршрутизаторе. Эта команда предоставляет подробную информацию о топологии сети, видимой протоколом маршрутизации ISIS
hostname	используется для отображения информации о имени хоста (hostname) в рамках протокола маршрутизации ISIS
interface	используется для отображения информации о параметрах интерфейсов, связанных с протоколом маршрутизации ISIS
mpls-te	используется для отображения информации о MPLS Traffic Engineering (MPLS-TE) в рамках протокола маршрутизации ISIS
neighbor	используется для отображения списка соседей протокола маршрутизации ISIS
spf-delay-ietf	используется для отображения времени задержки (delay) в расчете SPF (Shortest Path First) в соответствии с предложением IETF (Internet Engineering Task Force) при работе с протоколом маршрутизации ISIS
summary	используется для проверки настроек IS-IS
topology	используется для отображения текущей топологии маршрутов, обучаемых протоколом маршрутизации ISIS

Пример команды:

```
admin@SW3# show isis summary
Process Id : 1
Up time : 03:29:10 ago
Number of areas : 0

admin@SW3#
```

16.8 Настройка BFD

16.8.1 Общие положения

Протокол BFD (Bidirectional Forwarding Detection) проставляет быстрый и эффективный способ обнаружения проблем связности между двумя устройствами. BFD необходимо включать на отдельных интерфейсах для протоколов маршрутизации. Для создания сессии BFD протокол должен быть включен на двух устройствах, подключенных друг к другу.

Протокол OSPF позволяет уменьшить время обнаружения выхода соседа из строя до двух секунд, если установить минимально возможные значения интервала отправки пакетов “Hello” и интервала времени, по истечении которого сосед считается вышедшим из строя (1 и 2 секунды соответственно).

Использование протокола BFD имеет следующие преимущества над применением уменьшенных интервалов на самих протоколах маршрутизации:

1. Уменьшение интервалов протокола OSPF позволяет добиться времени обнаружения выхода соседа из строя равным двум секундам, а протокол BFD позволяет добиться значений менее 1 секунды.
2. Протокол BFD не привязан ни к какому протоколу маршрутизации, поэтому BFD можно использовать в качестве механизма обнаружения проблем с любым протоколом маршрутизации.

16.8.2 bfd

Команда глобальной настройки. Открывает узел конфигурации демона BFD.

Синтаксис команды:

bfd

no bfd

Команда с приставкой «**no**» удаляет процесс.

Использование команды:

Команда «**bfd**» используется для перехода в режим настройки BFD.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
```

16.8.3 peer

Команда настройки BFD. Используется для создания и настройки BFD-сессии с конкретным пиром (соседним устройством).

Синтаксис команды:

peer *ip-address* **[local-address** *ip address* **| interface vlan** *vlan* **[local-address** *ip address*]]

no peer *ip-address* **[local-address** *ip address* **| interface vlan** *vlan* **[local-address** *ip address*]]

Команда с приставкой «**no**» удаляет конкретный пир.

Параметры команды:

ip-address	IP-адрес соседа
local-address *ip address*	локальный адрес, к которому необходимо привязать peer, и адрес, который необходимо использовать для отправки пакетов
interface vlan *vlan*	интерфейс, на котором будет работать BFD

Использование команды:

Команда «**peer**» используется для создания и настройки новых пиров BFD.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# peer 1.1.1.1
admin@Switch(config_bfd-peer)#
```

16.8.4 profile

Команда настройки BFD. Позволяет создать профиль BFD с набором параметров, которые могут быть применены к различным соседям или интерфейсам.

Синтаксис команды:

profile *name*

no profile *name*

Команда с приставкой «**no**» удаляет профиль.

Параметры команды:

name	имя профиля

Использование команды:

Команда «**profile**» используется для создания профиля BFD.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
```

16.8.5 detect-multiplier

Команда настройки BFD. Настраивает множитель обнаружения для определения потери пакетов.

Пример: если локальная система имеет множитель detect-multiplier 3, а удаленная система имеет интервал передачи 300, локальная система обнаружит сбой только через 900 миллисекунд без получения пакетов.

Синтаксис команды:

detect-multiplier *detect-multiplier*

Параметры команды:

detect-multiplier можно задать значения от 2 до 255

Значение по умолчанию:

Значение по умолчанию равно 3.

Использование команды:

Команда «**detect-multiplier**» настраивает множитель обнаружения для определения потери пакетов.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
admin@Switch(config-bfd-profile)# detect-multiplier 10
```

16.8.6 receive-interval

Команда настройки BFD. Настраивает интервал, в течение которого устройство ожидает получение контрольных пакетов от соседнего устройства.

Синтаксис команды:

receive-interval *receive-interval*

no receive-interval

Параметры команды:

receive-interval можно задать значения от 10-60000

Значение по умолчанию:

300 миллисекунд.

Использование команды:

Команда «**receive-interval**» настраивает минимальный интервал, через который эта система может получать управляющие пакеты.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
admin@Switch(config-bfd-profile)# receive-interval 100
```

16.8.7 transmit-interval

Команда настройки BFD. Используется для определения частоты передачи контрольных пакетов (hello-пакетов) между устройствами.

Синтаксис команды:

transmit-interval *transmit-interval*

no transmit-interval

Параметры команды:

receive-interval можно задать значения от 10-60000

Значение по умолчанию:

300 миллисекунд.

Использование команды:

Команда «**transmit-interval**» используется для определения частоты передачи контрольных пакетов (hello-пакетов) между устройствами.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
admin@Switch(config-bfd-profile)#transmit-interval 100
```

16.8.8 echo receive-interval

Устанавливает интервал времени (в миллисекундах), в течение которого устройство ожидает получение эхо-пакетов от коммутатора для проверки работоспособности канала связи.

Синтаксис команды:

echo receive-interval {disabled | *receive-interval***}**

no echo receive-interval

Параметры команды:

disabled	запрет на принятие эхо-пакетов
receive-interval	интервал времени в значении от 10 до 60000 миллисекунд

Значение по умолчанию:

50 миллисекунд.

Использование команды:

Команда «**echo receive-interval**» настраивает интервал, через который коммутатор сможет принимать эхо-пакеты.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
admin@Switch(config-bfd-profile)#echo receive-interval 100
```

16.8.9 echo transmit-interval

Устанавливает интервал времени (в миллисекундах), через который устройство начнет отправлять эхо-пакеты на коммутатор для проверки работоспособности канала связи.

Синтаксис команды:

echo transmit-interval *transmit-interval*

no echo transmit-interval

Параметры команды:

transmit-interval	интервал времени в значении от 10 до 60000 миллисекунд

Значение по умолчанию:

50 миллисекунд.

Использование команды:

Команда «**echo transmit-interval**» настраивает интервал, через который коммутатор сможет отправлять эхо-пакеты.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# peer 1.1.1.1
admin@Switch(config_bfd-peer)# echo transmit-interval 100
admin@Switch(config_bfd-peer)#
```

16.8.10 echo-mode

Команда настройки BFD. Включает режим передачи эха. Отправление эхо-пакетов позволяет BFD выявлять, работает ли соединение.

Синтаксис команды:

echo-mode

no echo-mode

Команда с приставкой «**no**» выключает режим передачи эха.

Значение по умолчанию:

По умолчанию этот режим отключен.

Использование команды:

Команда «**echo-mode**» включает режим передачи эха.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
admin@Switch(config-bfd-profile)#echo-mode
```

16.8.11 shutdown

Команда настройки BFD. Используется для деактивации BFD на интерфейсе или в профиле.

Синтаксис команды:

shutdown

no shutdown

Команда с приставкой «**no**» включает интерфейс.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
admin@Switch(config-bfd-profile)#shutdown
```

16.8.12 passive-mode

Команда настройки BFD. Помечает сессию как пассивную: пассивная сессия не будет пытаться начать соединение и будет ждать управляющих пакетов от аналога, прежде чем начать отвечать.

Синтаксис команды:
passive-mode
no passive-mode
Команда с приставкой «**no**» включает сессию как активную.
Значение по умолчанию:
По умолчанию используется активный режим.
Использование команды:
Команда «**passive-mode**» помечает сессию как пассивную.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config-bfd)# profile POV
admin@Switch(config-bfd-profile)#passive-mode
```

16.8.13 profile

Команда настройки BFD. Настройка peer на использование конфигураций профиля.
Синтаксис команды:
profile *name*
no profile
Команда с приставкой «**no**» удаляет профиль на этом peer.
Параметры команды:

name	название профиля

Использование команды:
Команда «**profile**» используется для настройки конфигураций профиля.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# bfd
admin@Switch(config)#peer 1.1.1.1
admin@Switch(config)#profile POV
```

16.8.14 ip ospf bfd

Команда настройки интерфейса (VLAN). Включение поддержки BFD на интерфейсе.
Синтаксис команды:
ip ospf bfd [profile *name***]**
no ip ospf bfd
Команда с приставкой «**no**» отключает поддержку BFD.
Параметры команды:

name	название профиля

Значение по умолчанию:
BFD на интерфейсе отключен.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip ospf bfd
```

16.8.15 neighbor bfd

Команда настройки маршрутизации BGP. Включает BFD, который используется для быстрого обнаружения проблем в соединении.

Синтаксис команды:

neighbor *ip address* **bfd [profile** *name***]**

no neighbor *ip address* **bfd**

Команда с приставкой «**no**» отключает поддержку BFD.

Параметры команды:

ip address	IP-адрес соседнего маршрутизатора BGP
name	название профиля

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 1000
admin@Switch(config-bgp)# neighbor 1.1.1.1 bfd
```

16.8.16 show bfd peer

Команда, доступная из любого режима. Отображает информацию о текущих пирах BFD.

Синтаксис команды:

show bfd peer {*ipv4* | *ipv6*} **[counters | interface vlan** *vlan* **[counters | local-address** *local-address* **[counters]]]**

Параметры команды:

ipv4	отображение информации о BFD пирах для IPv4
ipv6	отображение информации о BFD пирах для IPv6
counters	отображение счетчиков для BFD-соседей, включая информацию о количестве посланных и полученных BFD-сообщений
vlan	фильтрация по интерфейсу VLAN
local-address	фильтрация по локальному IP-адресу

Использование команды:

Команда «**show bfd peer**» отображает информацию о текущих пирах BFD.

Пример команды:

```
Switch# show bfd peer 1.1.1.1
BFD Peer:
peer 1.1.1.1 vrf default
ID: 192582246
Remote ID: 0
Passive mode
Status: down
Downtime: 1 hour(s), 9 minute(s), 37 second(s)
Diagnostics: ok
Remote diagnostics: ok
Peer Type: configured
RTT min/avg/max: 0/0/0 usec
Local timers:
Detect-multiplier: 3
Receive interval: 300ms
Transmission interval: 300ms
Echo receive interval: 50ms
Echo transmission interval: disabled
Remote timers:
Detect-multiplier: 3
Receive interval: 1000ms
Transmission interval: 1000ms
Echo receive interval: disabled
```

16.8.17 show bfd peers

Команда, доступная из любого режима. Показывает общее состояние BFD-пиров и их статусы.

Синтаксис команды:

show bfd peers [brief | counters]

Параметры команды:

brief	показывает информацию о BFD-соседях в табличной форме, позволяя быстро увидеть основные параметры, такие как состояние соединения и IP-адреса
counters	отображает счетчики для BFD-соседей, включая информацию о количестве посланных и полученных BFD-сообщений

Использование команды:

Используйте команду «**show bfd peers**» для отображения состояний BFD-пиров и их статусов.

Пример команды:

```
admin@Switch(config_bfd-peer)# show bfd peers brief

Session count: 1
SessionId          LocalAddress       PeerAddress        Status
=========          ============       ============       ======
2963640421         0.0.0.0            1.1.1.1            down

admin@Switch(config_bfd-peer)#
```

16.9 Настройка BGP

16.9.1 debug ip bgp

Команда фундаментального режима. Включение отладки BGP.
Синтаксис команды:
debug ip bgp {**all** | **events** | **filters** | **interfaces** | **packets** | **routes** | **states**}
no debug ip bgp {**all** | **events** | **filters** | **interfaces** | **packets** | **routes** | **states**}
Команда с приставкой «**no**» отключает отладку BGP.
Параметры команды:

all	вывод всех сообщений
events	вывод сообщений о событиях, внутренних для протокола
filters	вывод подробной информации о фильтрации маршрутов
interfaces	вывод событий изменения интерфейса, отправленные в протокол
packets	вывод информации о пакетах, отправленных и полученных протоколом
routes	вывод информации о маршрутах, которые были обменены с таблицей маршрутизации
states	вывод информации об изменениях состояния протокола

Пример команды:

```
admin@Switch# debug ip bgp all
admin@Switch#
```

16.9.2 router bgp

Команда глобальной настройки. Включение протокола маршрутизации BGP, установка номера автономной системы и переход в режим настройки протокола BGP.
Синтаксис команды:
router bgp *as-number*
no router bgp *as-number*
Команда с приставкой «**no**» отключает протокол маршрутизации BGP.
Параметры команды:

as-number	номер автономной системы, которая идентифицирует маршрутизатор перед другими BGP-маршрутизаторами и применяется для добавления в транслируемую маршрутную информацию. Диапазон значений: от 1 до 65535. Поддерживаются 4-байтные идентификаторы автономной системы в диапазоне от 65536 до 4294967295

Значение по умолчанию:
Маршрутизация BGP отключена.

Использование команды:

Команда «**router bgp**» используется для включения протокола маршрутизации BGP, установки номера автономной системы и перехода в режим настройки протокола BGP.

Ввод команды «**router bgp**» номером автономной системы, отличным от установленного ранее, перезапускает протокол BGP.

Устройство поддерживает только один экземпляр протокола маршрутизации BGP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)#
```

16.9.3 bgp always-compare-med

Команда настройки маршрутизации (BGP). Включение учёта атрибутов MED (Multi Exist Discriminator), получаемых от путей, ведущих к соседям из других автономных систем (AS).

Синтаксис команды:

bgp always-compare-med

no bgp always-compare-med

Команда с приставкой «**no**» отключает учёт атрибутов MED.

Значение по умолчанию:

Учёт атрибутов MED от путей из других AS отключён.

Использование команды:

Команда «**bgp always-compare-med**» используется для включения учёта атрибутов MED (Multi Exist Discriminator), получаемых от путей, ведущих к соседям из других автономных систем (AS).

Атрибут MED (RFC 1771) является опциональным нетранзитным атрибутом, представляющим собой 32-битное неотрицательное число. Значение этого атрибута может быть использовано алгоритмом выбора наилучшего пути протокола BGP при наличии множества точек выхода в соседнюю автономную систему. Меньшее значение MED означает больший приоритет при выборе пути. В процессе выбора наилучшего пути сравнение атрибута MED производится только для путей от одной и той же автономной системы. Команда «**bgp always-compare-med**» включает сравнение атрибута MED для всех путей, независимо от автономной системы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# bgp always-compare-med
admin@Switch(config-bgp)#
```

16.9.4 bgp bestpath as-path ignore

Команда настройки маршрутизации (BGP). Отключение сравнения длины путей внутри автономной системы при выборе наилучшего пути.

Синтаксис команды:

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Команда с приставкой «**no**» включает сравнение длины путей внутри автономной системы при выборе наилучшего пути.

Значение по умолчанию:

При построении оптимального маршрута протокол BGP учитывает длину пути внутри AS.

Использование команды:

Команда «**bgp bestpath as-path ignore**» используется для отключения сравнения длины путей внутри автономной системы при выборе наилучшего пути.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# bgp bestpath as-path ignore
admin@Switch(config-bgp)#
```

16.9.5 bgp cluster-id

Команда настройки маршрутизации (BGP). Установка идентификатора кластера на рефлекторе маршрутов (Route Reflector).

Синтаксис команды:

bgp cluster-id *cluster-id*

no bgp cluster-id

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

cluster-id	идентификатор кластера на рефлекторе маршрутов (Route Reflector). Идентификатор должен быть указан в виде IP-адреса

Значение по умолчанию:

В качестве идентификатора кластера используется локальный идентификатор маршрутизатора.

Использование команды:

Команда «**bgp cluster-id**» используется для установки идентификатора кластера на рефлекторе маршрутов (Route Reflector).

Рефлектор маршрутов и его клиенты формируют кластер маршрутизаторов. Если в кластере используется только один рефлектор маршрутов, то идентификатор кластера равен идентификатору маршрутизатора. Для обеспечения резервирования и повышения надежности в кластер добавляют два или более рефлекторов маршрутов. В этом случае всем рефлекторам маршрутов необходимо задать один и тот же

идентификатор кластера с помощью команды «**bgp cluster-id**».

При использовании нескольких рефлекторов маршрутов в пределах кластера обязательно наличие стабильных соединений между всеми участниками кластера. Если выполнение этого требования невозможно, необходимо использовать рефлекторы маршрутов с разными идентификаторами кластера.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# bgp cluster-id 10.0.0.1
admin@Switch(config-bgp)#
```

16.9.6 bgp default local-preference

Команда настройки маршрутизации (BGP). Установка атрибута локальной приоритетности путей.

Синтаксис команды:

bgp default local-preference *number*

no bgp default local-preference

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

number	значение атрибута локальной приоритетности путей в диапазоне от 0 до 4294967295

Значение по умолчанию:

Атрибут локальной приоритетности путей равен 100.

Использование команды:

Команда «**bgp default local-preference**» используется для установки атрибута локальной приоритетности путей.

Атрибут локальной приоритетности путей используется только внутри автономной системы между соседями iBGP для определения локальной политики. Маршрут с большим значением атрибута является более приоритетным при выборе наилучшего пути BGP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# bgp default local-preference 2000
admin@Switch(config-bgp)#
```

16.9.7 bgp deterministic-med

Команда настройки маршрутизации (BGP). Принудительное включение детерминистского сравнения атрибута MED между путями, полученными от одной и той же автономной системы.

Синтаксис команды:
bgp deterministic-med
no bgp deterministic-med
Команда с приставкой «**no**» отключает функцию.
Значение по умолчанию:
Детерминистское сравнение атрибута MED отключено.
Использование команды:
Команда «**bgp deterministic-med**» используется для принудительного включения детерминистского сравнения атрибута MED между путями, полученными от одной и той же автономной системы.

Если на устройстве не включено детерминистское сравнение атрибута MED, то на выбор наилучшего пути протоколом BGP может повлиять порядок получения маршрутов.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# bgp deterministic-med
admin@Switch(config-bgp)#
```

16.9.8 bgp ebgp-requires-policy

Команда настройки маршрутизации (BGP). Команда применения фильтров входящих/исходящих маршрутов для сессий eBGP в соответствии с RFC-8212.
Синтаксис команды:
bgp ebgp-requires-policy
no bgp ebgp-requires-policy
Команда с приставкой «**no**» отключает учёт атрибутов MED.
Значение по умолчанию:
Команда по умолчанию включена.
Использование команды:
Команда используется для применения фильтров входящих/исходящих маршрутов для сессий eBGP в соответствии с RFC-8212. Без входящего фильтра никакие маршруты не будут приниматься. Без исходящего маршрута никакие маршруты не будут объявлены. Для корректной работы объявления/принятия маршрутов необходимо отключить данную команду.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# no bgp ebgp-requires-policy
admin@Switch(config-bgp)#
```

16.9.9 neighbor local-as

Команда настройки маршрутизации (BGP). Включение изменения номера автономной системы, которая передается внешним маршрутизаторам (eBGP).

Синтаксис команды:
neighbor *ip-address* **local-as** *as-number* [**no-prepend**[**replace-as**]]
no neighbor *ip-address* **local-as**
Команда с приставкой «**no**» отключает функцию.
Параметры команды:

ip-address	IP-адрес соседнего маршрутизатора BGP
as-number	корректный номер автономной системы в диапазоне от 1 до 65535. Поддерживаются 4-байтные идентификаторы автономной системы в диапазоне от 65536 до 4294967295. Не указывать номер автономной системы, к которой относится соседний маршрутизатор
no-prepend	отключение вставки номера локальной автономной системы (заданной командой «**router bgp**») в атрибут AS_PATH для маршрутов, которые получены от внешних маршрутизаторов
replace-as	к атрибутам маршрута AS_PATH добавляется только номер автономной системы, заданный в команде

Значение по умолчанию:
По умолчанию протокол BGP добавляет номер автономной системы ко всем внешним маршрутам.

При включении этой функции соседний маршрутизатор BGP будет получать информацию от устройства, как если бы оно находилось в автономной системе asnumber. Остальные соседние маршрутизаторы, для которых функция не включена, будут получать информацию от устройства в соответствии с номером автономной системы, заданной командой «**router bgp**».

Протокол BGP добавляет номер автономной системы всех сетей, через которые проходит маршрут. Это необходимо для получения информации о доступности сети и предотвращения закольцовывания маршрутов. Некорректная настройка может привести к образованию закольцовывания маршрутов.

Использование команды:
Команда «**neighbor local-as**» используется для включения изменения номера автономной системы, которая передается внешним маршрутизаторам (eBGP).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.1 local-as 10000
admin@Switch(config-bgp)#
```

16.9.10 neighbor maximum-prefix

Команда настройки маршрутизации (BGP). Установка ограничения максимального количества префиксов, которое может быть получено от соседа BGP.

Синтаксис команды:
neighbor *ip-address* **maximum-prefix** *maximum* [**warning-only**]
no neighbor *ip-address* **maximum-prefix** [**warning-only**]
Команда с приставкой «**no**» отключает ограничение.
Параметры команды:

ip-address	IP-адрес соседа BGP
maximum	максимальное количество префиксов, допустимое к получению от выбранного соседа. Диапазон значений: от 1 до 4294967295
warning-only	при превышении максимального количества префиксов устройство генерирует предупреждение, но не завершает сессию BGP

Значение по умолчанию:
Количество получаемых префиксов не ограничено.
Использование команды:
Команда «**neighbor maximum-prefix**» используется для установки ограничения максимального количества префиксов, которое может быть получено от соседа BGP.
В случае превышения максимального количества префиксов, по умолчанию устройство завершает сессию с соседом BGP. Параметр «**warning-only**» позволяет включить генерацию предупреждения без завершения сессии BGP.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.10 maximum-prefix 500
admin@Switch(config-bgp)#
```

16.9.11 neighbor next-hop-self

Команда настройки маршрутизации (BGP). Установка устройства как следующего узла указанному соседу BGP.
Синтаксис команды:
neighbor *ip-address* **next-hop-self**
no neighbor *ip-address* **next-hop-self**
Команда с приставкой «**no**» отключает функцию.
Параметры команды:

ip-address	IP-адрес соседа BGP

Значение по умолчанию:
Функция отключена.
Использование команды:
Команда «**neighbor next-hop-self**» используется для установки устройства как следующего узла указанному соседу BGP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.10 next-hop-self
admin@Switch(config-bgp)#
```

16.9.12 neighbor password

Команда настройки маршрутизации (BGP). Включение аутентификации MD5 на TCP-соединениях протокола BGP.

Синтаксис команды:

neighbor *ip-address* **password** *string*

no neighbor *ip-address* **password**

Команда с приставкой «**no**» отключает аутентификацию MD5.

Параметры команды:

ip-address	IP-адрес соседнего маршрутизатора BGP
string	пароль в виде текстовой строки длиной до 25 символов. Первый символ не может быть цифрой. Не рекомендуется использовать пробел между цифрами и другими символами, т.к. это может привести к ошибкам при аутентификации

Значение по умолчанию:

Аутентификация BGP отключена.

Использование команды:

Команда «**neighbor password**» используется для включения аутентификации MD5 на TCP-соединениях протокола BGP.

Аутентификация должна быть включена на обоих устройствах, взаимодействующих друг с другом.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.1 password mypassword
admin@Switch(config-bgp)#
```

16.9.13 neighbor remote-as

Команда настройки маршрутизации (BGP). Добавление соседнего маршрутизатора и настройка номера его автономной системы.

Синтаксис команды:

neighbor *ip-address* **remote-as** *as-number*

no neighbor *ip-address* **remote-as**

Команда с приставкой «**no**» удаляет соседний маршрутизатор.

Параметры команды:

ip-address	IP-адрес соседнего маршрутизатора BGP
as-number	номер автономной системы, которой принадлежит сосед-ний маршрутизатор в диапазоне от 1 до 65535. Поддержи-ваются 4-байтные идентификаторы автономной системы в диапазоне от 65536 до 4294967295

Значение по умолчанию:

Соседние маршрутизаторы BGP отсутствуют.

Использование команды:

Команда «**neighbor remote-as**» используется для добавления соседнего маршру-тизатора и настройки номера его автономной системы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.1 remote-as 50000
admin@Switch(config-bgp)#
```

16.9.14 neighbor route-map

Команда настройки маршрутизации (BGP). Применение указанной route-map к обновлениям маршрутов BGPr.

Синтаксис команды:

neighbor *ip-address* **route-map** [*name*] [*in* | *out*]

no neighbor *ip-address* **route-map** [*name*] [*in* | *out*]

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

ip-address	IP-адрес соседа BGP
name	имя route-map (максимальный размер 32 символа)
in	применение route-map к входящим маршрутам
out	применение route-map к исходящим маршрутам

Значение по умолчанию:

По умолчанию функция отключена.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 1.0.0.1 route-map ABC out
admin@Switch(config-bgp)#
```

16.9.15 neighbor route-reflector-client

Команда настройки маршрутизации (BGP). Настройка устройства в качестве рефлектора маршрутов и установка соседа в качестве клиента.

Синтаксис команды:

neighbor *ip-address* **route-reflector-client**

no neighbor *ip-address* **route-reflector-client**

Команда с приставкой «**no**» используется для удаления соседа из списка клиентов.

Параметры команды:

ip-address IP-адрес соседа BGP

Значение по умолчанию:

Рефлектор маршрутов отсутствует.

Использование команды:

Команда «**neighbor route-reflector-client**» используется для настройки устройства в качестве рефлектора маршрутов и установки соседа в качестве клиента.

По умолчанию маршрутизаторы BGP в пределах автономной системы (iBGP) должны иметь активные сессии BGP по схеме “каждый к каждому” и маршрутизаторы не анонсируют соседям изученные маршруты для исключения закольцовывания маршрутов (routing information loop). В схеме с рефлекторами маршрутов один из маршрутизаторов (или несколько) назначается рефлектором маршрутов, ответственным за распределение изученных маршрутов между соседями BGP. В этом случае отпадает необходимость организации сессий BGP по схеме “каждый к каждому”.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.10 route-reflector-client
admin@Switch(config-bgp)#
```

16.9.16 neighbor route-server-client

Команда настройки маршрутизации (BGP). Настройка устройства в качестве сервера маршрутов и установка соседа в качестве клиента.

Синтаксис команды:

neighbor *ip-address* **route-server-client**

no neighbor *ip-address* **route-server-client**

Команда с приставкой «**no**» используется для удаления соседа из списка клиентов.

Параметры команды:

ip-address IP-адрес соседа BGP

Значение по умолчанию:

Сервер маршрутов отсутствует.

Использование команды:

Команда «**neighbor route-server-client**» используется для настройки устройства в качестве сервера маршрутов и установки соседа в качестве клиента.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.10 route-server-client
admin@Switch(config-bgp)#
```

16.9.17 neighbor timers

Команда настройки маршрутизации (BGP). Установка значений таймеров BGP, применяемых при взаимодействии с соседним маршрутизатором.

Синтаксис команды:

neighbor *ip-address* **timers** *keepalive holdtime*

no neighbor *ip-address* **timers**

Команда с приставкой «**no**» устанавливает значения по умолчанию.

Параметры команды:

ip-address	IP-адрес соседнего маршрутизатора BGP
keepalive	интервал отправки сообщений поддержания соединения (“keepalive”) в диапазоне от 0 до 65535 секунд
holdtime	интервал, по истечении которого соседний маршрутизатор считается вышедшим из строя, если от него не было получено ни одного сообщения поддержания соединения (“keepalive”). Диапазон значений: от 0 до 65535 секунд

Значение по умолчанию:

Интервал “keepalive”: 60 секунд.

Интервал “holdtime”: 180 секунд.

Использование команды:

Рекомендуется устанавливать значение “holdtime”, как минимум, в три раза большим, чем значение “keepalive”.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.1 timers 30 90
admin@Switch(config-bgp)#
```

16.9.18 neighbor transport

Команда настройки маршрутизации (BGP). Настройка параметров организации сессии BGP по протоколу TCP.

Синтаксис команды:

neighbor *ip-address* **transport connection-mode** {**active | passive**}

no neighbor *ip-address* **transport connection-mode** {**active | passive**}

Команда с приставкой «**no**» используется для установки параметров в значения по умолчанию.

Параметры команды:

ip-address	IP-адрес соседа BGP
active	активное соединение – устройство инициирует сессию к соседу

passive	пассивное соединение – устройство ожидает подключения от соседа для начала сессии

Значение по умолчанию:

По умолчанию маршрутизатор BGP выполняет активное соединение.

Использование команды:

Команда «**neighbor transport**» используется для настройки параметров организации сессии BGP по протоколу TCP.

Режим организации подключения сессии, определяемый параметрами «**active**» и ««**passive**», позволяет определить инициатора сессии и подчиненного. Это может понадобиться, если один из маршрутизаторов находится за межсетевым экраном, который запрещает входящие подключения извне. В этом случае маршрутизатор за межсетевым экраном должен работать в режиме «**active**», а его соседи – в режиме ««**passive**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.10 transport connection-mode active
admin@Switch(config-bgp)#
```

16.9.19 neighbor ttl-security

Команда настройки маршрутизации (BGP). Установка максимального количества узлов (маршрутизаторов), расположенных на пути между двумя соседями внешнего протокола BGP (eBGP).

Синтаксис команды:

neighbor *ip-address* **ttl-security hops** *hop-count*

no neighbor *ip-address* **ttl-security hops** *hop-count*

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

ip-address	IP-адрес соседа BGP
hop-count	количество узлов (маршрутизаторов), расположенных на пути между двумя соседями внешнего протокола BGP (eBGP). Значение TTL вычисляется маршрутизатором из значения параметра «*hop-count*» с диапазоном значений от 1 до 254

Значение по умолчанию:

По умолчанию ограничение отключено.

Использование команды:

Команда «**neighbor ttl-security**» используется для установки максимального количества узлов (маршрутизаторов), расположенных на пути между двумя соседями внешнего протокола BGP (eBGP).

Команда «**neighbor ttl-security**» предоставляет легковесный механизм защиты сессий BGP от атак, вызывающих повышенную нагрузку на маршрутный процессор устройства. Как правило, это атаки типа “отказ в обслуживаниии” (DoS), вызывающие перегрузку сети с помощью отправки пакетов, содержащих специально сгенерированные IP-адреса источника и назначения.

Ограничение максимального количества узлов указывает устройству принимать только те IP-пакеты, значение TTL которых равно или больше локально настроенного значения. Генерация IP-пакета с соответствующим значением TTL, в общем случае, считается невозможным. Генерация IP-пакета от доверенного соседа с соответствующим значением TTL невозможно без доступа во внутреннюю сеть получателя или отправителя.

Функция должна быть настроена на всех соседях BGP. Ограничение действует только на входящем направлении и не имеет никакого эффекта на исходящем направлении. Если ограничение включено, то устройство инициирует и поддерживает сессию BGP, только если значение TTL в IP-пакете равно или больше значения, настроенного для сессии. Устройство отбрасывает IP-пакеты со значением TTL, не соответствующим ограничению.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# neighbor 10.0.0.10 ttl-security hops 2
admin@Switch(config-bgp)#
```

16.9.20 network

Команда настройки маршрутизации (BGP). Добавление локальной сети (подсети) к таблице маршрутов, анонсируемых протоколом BGP.

Синтаксис команды:

network *ip-address* {**mask** *network-mask* | *prefix-length*}

no network *ip-address* {**mask** *network-mask* | *prefix-length*}

Команда с приставкой «**no**» удаляет локальную сеть из таблицы маршрутов, анонсируемых протоколом BGP.

Параметры команды:

ip-address	IP-адрес сети или подсети
mask *network-mask*	маска сети или подсети
prefix-length	длина префикса IP-адреса сети

Значение по умолчанию:

Анонсируемые сети отсутствуют.

Использование команды:

Команда «**network**» используется для добавления локальной сети (подсети) к таблице маршрутов, анонсируемых протоколом BGP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# network 175.10.0.0 255.255.255.0
admin@Switch(config-bgp)#
```

16.9.21 redistribute

Команда настройки маршрутизации (BGP). Включение распределения маршрутов из одного домена маршрутизации в другой.

Синтаксис команды:

redistribute *protocol* [*process-id*] [**subnets**]

no redistribute *protocol* [*process-id*] [**subnets**]

Команда с приставкой «**no**» отключает распределение маршрутов.

Параметры команды:

protocol — источник маршрутов, которые будут распределены.

Варианты протокола:

- **connected** – источником являются сети на локальных интерфейсах (для которых задан IP-адрес на одном из интерфейсов устройства);
- **ospf** – источником является процесс OSPF;
- **rip** – источником является процесс RIP;
- **static** – источником являются статические маршруты

process-id — идентификатор процесса OSPF, из которого будут распределяться маршруты. По умолчанию используется номер 1. Параметр отсутствует, если источником указан не протокол OSPF

subnets — распределение маршрутов до подсетей. По умолчанию распределяются маршруты, которые указывают на полные сети (классовые сети)

Значение по умолчанию:

Распределение маршрутов отключено.

Использование команды:

Команда «**redistribute**» используется для для включения распределения маршрутов из одного домена маршрутизации в другой. Для отключения распределения маршрутов используется команда «**no redistribute**» с одним аргументом «*protocol*» или с двумя аргументами «*protocol*» и «*process-id*».

Смена настройки, ассоциированной с ключевым словом, не затрагивает остальные настройки.

Устройство, получающее маршруты по протоколу на основе состояний соединения (например, OSPF) с внутренней метрикой, будет считать, что стоимость маршрута

равна стоимости от самого себя до устройства, распределяющего маршруты, плюс анонсированную стоимость до точки назначения. Для внешней метрики стоимость равна только анонсированной стоимости до точки назначения.

Распределение маршрутов с помощью ключевого слова «**connected**» охватывает только те сети на локальных интерфейсах (подключенные напрямую), которые не указаны явно с помощью команды «**network**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# router bgp 40000
admin@Switch(config-bgp)# redistribute static
admin@Switch(config-bgp)#
```

16.9.22 show ip bgp

Команда, доступная из любого режима. Вывод настроек и маршрутной таблицы BGP.

Синтаксис команды:

show ip bgp

Использование команды:

Команда «**show ip bgp**» используется для вывода настроек и маршрутной таблицы BGP.

Пример команды:

```
admin@Switch# show ip bgp
BGP summary
------

Autonomous system 1
 Networks: 1.1.2.0/24 1.1.1.0/24
Autonomous system 10
 Networks: 192.168.0.0/20
 Neighbor 192.168.2.163: remote AS 11

BGP routes
-----

AS 10, neighbor 192.168.2.163. State: Established

B ! 1.1.4.0/24 (100) via 192.168.0.2 vlan 1
B ! 1.1.0.1/16 (100) via 192.168.5.22 vlan 1
B ! 1.1.3.0/24 (100) via 192.168.0.1 vlan 1
```

16.9.23 show ip bgp route

Команда, доступная из любого режима. Вывод маршрутной таблицы BGP.

Синтаксис команды:

show ip bgp route [*ip-address* {*network-mask* | *prefix-length*} {**longer-prefixes**}]

Параметры команды:

ip-address	IP-адрес сети или подсети
network-mask	маска сети или подсети
prefix-length	длина префикса IP-адреса сети
longer-prefixes	вывод указанного маршрута и более частных (специфичных) маршрутов

Использование команды:

Команда «**show ip bgp route**» используется для вывода маршрутной таблицы BGP.

Пример команды:

```
admin@Switch# show ip bgp route
BGP routes
------

AS 10, neighbor 192.168.2.163. State: Established
B ! 1.1.4.0/24 (100) via 192.168.0.2 vlan 1
B ! 1.1.0.1/16 (100) via 192.168.5.22 vlan 1
B ! 1.1.3.0/24 (100) via 192.168.0.1 vlan 1
```

16.9.24 show ip bgp summary

Команда, доступная из любого режима. Вывод сводной информации о настройках и состоянии соединений протокола BGP.

Синтаксис команды:

show ip bgp summary

Использование команды:

Команда «**show ip bgp summary**» используется для вывода сводной информации о состоянии соединений протокола BGP.

Пример команды:

```
admin@Switch# show ip bgp summary
BGP summary
------

Autonomous system 1
 Networks: 1.1.2.0/24 1.1.1.0/24
Autonomous system 10
 Networks: 192.168.0.0/20
 Neighbor 192.168.2.163: remote AS 11
```

16.9.25 show ip bgp detail

Команда, доступная из любого режима. Выводит детальную информацию о состоянии таблицы маршрутизации BGP.

Синтаксис команды:

show ip bgp detail

Использование команды:

Команда «**show ip bgp detail**» используется для вывода детальной информации о состоянии таблица маршрутизации BGP.

Пример команды:

```
admin@Switch# show ip bgp detail

BGP table version is 17, local router ID is 192.168.0.1, vrf id 0
Default local pref 100, local AS 65000
BGP routing table entry for 1.1.1.0/24, version 1
Paths: (1 available, best #1, table default)
 Advertised to non peer-group peers:
 192.168.0.2
 Local
  0.0.0.0 from 0.0.0.0 (192.168.0.1)
   Origin IGP, metric 0, weight 32768, valid, sourced, local, best (First path received)
   Last update: Thu Jan  1 00:08:21 1970
```

16.10 Настройка VRRP

16.10.1 Общие положения

Протокол VRRP (The Virtual Router Redundancy Protocol) является динамическим протоколом резервирования маршрутизаторов. Маршрутизаторы, поддерживающие VRRP, автоматически выбирают главный маршрутизатор и резервный маршрутизатор.

Определение IP-адреса шлюза для клиентов сети (сетевых устройств) может быть выполнено следующими способами:

1. Статическая настройка. В случае выхода из строя шлюза требуется ручная перенастройка сетевых устройств;
2. Динамические протоколы:

(a) Proxy ARP. Клиент использует протокол ARP (Address Resolution Protocol) для доступа к требуемому узлу (по IP-адресу). Маршрутизатор отвечает на ARP-запрос своим MAC-адресом;

(b) Протоколы маршрутизации. Клиент прослушивает пакеты, содержащие обновления динамических протоколов маршрутизации (например, обновления протоколов RIP, OSFP), и формирует свою маршрутную таблицу;

(c) ICMP Router Discovery Protocol (IRDP). Клиент использует протокол IRDP для обнаружения маршрутизаторов (шлюзов) в сети;

(d) Недостатками использования динамических протоколов является необходимость поддержки динамических протоколов клиентами и дополнительные усилия по их настройке. Кроме того, в случае выхода из строя маршрутизатора (шлюза) время переключения может быть относительно долгим (десятки секунд);

(e) Использование статической настройки шлюза упрощает настройки на клиенте, но создает единую точку отказа. В случае выхода из строя шлюза клиент сможет взаимодействовать только с узлами в пределах локальной сети.

Протокол VRRP позволяет совместить простоту статической настройки и достоинства динамических протоколов обнаружения маршрутизаторов. Клиенты используют IP-адрес виртуального маршрутизатора в качестве IP-адреса шлюза. Виртуальный маршрутизатор представляет собой группу однотипно настроенных маршрутизаторов. Виртуальный маршрутизатор также называют группой резервирования VRRP.

Обобщенная топология использования VRRP представлена на рисунке 10.

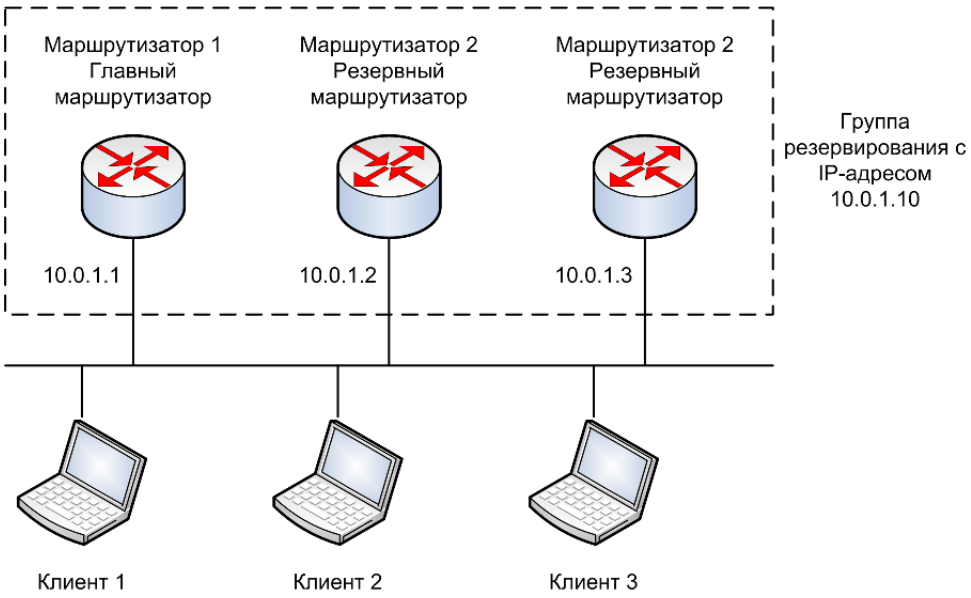

Рисунок 10 – Обобщенная топология использования VRRP

Топология, приведенная на рисунке 10, состоит из трех маршрутизаторов, которые состоят в группе резервирования VRRP с IP-адресом 10.0.1.10. Маршрутизацией пакетов в приведенной топологии занимается только главный маршрутизатор. В случае отказа главного маршрутизатора (№1), его функции на себя возьмет один из резервных маршрутизаторов.

Топология VRRP с балансировкой нагрузки представлена на рисунке 11.

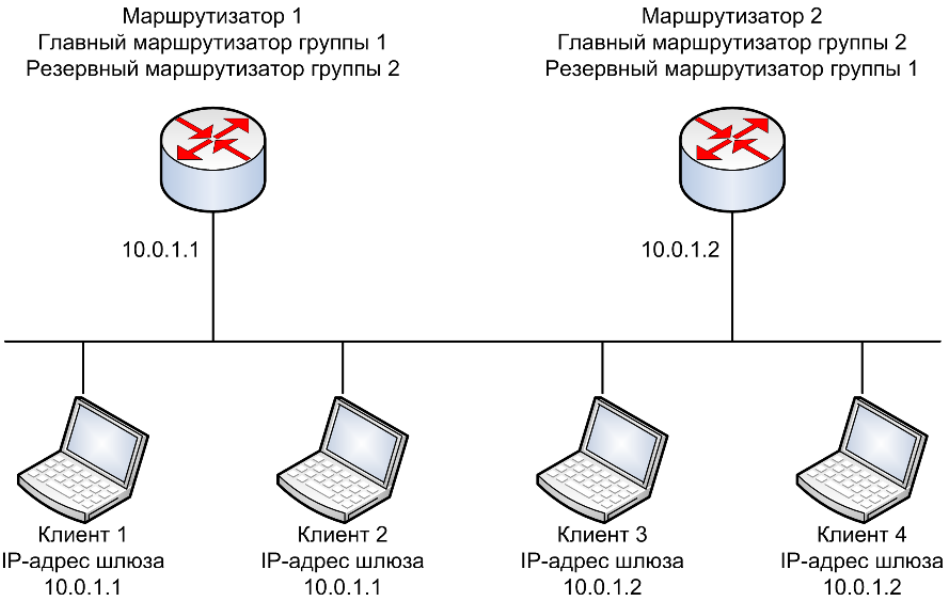

Рисунок 11 – Топология VRRP с балансировкой нагрузки

Топология, приведенная на рисунке 11, позволяет распределить клиентов сети между двумя маршрутизаторами. При нормальной работе сети трафик первой половины клиентов проходит через маршрутизатор №1, а трафик второй половины – через маршрутизатор №2. При этом каждый маршрутизатор является главным маршрутизатором своей группы резервирования VRRP и резервным маршрутизатором для другой

группы. Например, в случае отказа первого маршрутизатора, второй маршрутизатор станет главным маршрутизатором обеих групп резервирования, и через него будет проходить трафик всех клиентов.

Достоинства VRRP:

1. Резервирование. VRRP позволяет использовать несколько маршрутизаторов в качестве шлюза, что уменьшает вероятность отказа.
2. Распределение нагрузки. Администратор может настроить VRRP таким образом, что трафик от клиентов будет распределяться между несколькими маршрутизаторами.
3. VRRP поддерживает до 255 виртуальных маршрутизаторов (групп резервирования VRRP) на каждом интерфейсе устройства (VLAN). Поддержка множества виртуальных маршрутизаторов на интерфейсе позволяет реализовать резервировании распределение нагрузки в сети.
4. Множество IP-адресов. Виртуальный маршрутизатор может поддерживать несколько IP-адресов, включая дополнительные IP-адреса. Например, можно настроить VRRP на несколько подсетей в пределах одного интерфейса устройства.
5. Автоматический переход в режим главного маршрутизатора по приоритету. Например, при появлении в сети маршрутизатора с более высоким приоритетом, он автоматически перехватывает режим главного маршрутизатора.
6. Аутентификация. VRRP использует алгоритм аутентификации MD5, который защищает от VRRP-спуфинга.
7. Протокол анонсирования. VRRP использует отдельный IP-адрес для отправки и приема пакетов (224.0.0.18). Подобная схема адресации снижает количество маршрутизаторов, которые должны обрабатывать многоадресный трафик и позволяет тестовому оборудования точно определять пакеты VRRP в сегменте сети. VRRP использует номер протокола IP равный 122.

Важным аспектом резервирования VRRP является приоритет маршрутизатора, который определяет роль каждого маршрутизатора в группе резервирования VRRP и порядок назначения главного маршрутизатора в случае отказа действующего главного маршрутизатора группы. Приоритет маршрутизатора также может использоваться для переопределения главного маршрутизатора в случае появления в группе маршрутизатора с большим приоритетом.

Настройки пользователя

Настройки интерфейса:

- режим аутентификации на группе резервирования VRRP: простой пароль, MD5;
- задержка перед инициализацией групп резервирования VRRP на интерфейсе: два таймера с диапазоном от 1 до 10000 секунд;

– описание группы резервирования VRRP: текстовая строка;
– IP-адрес группы резервирования VRRP: основной и дополнительные адреса;
– режим автоматического перехода в режим главного маршрутизатора: вкл, выкл;
– приоритет устройства в группе резервирования VRRP: целое число в диапазоне от 1 до 254;
– включение и отключения группы резервирования VRRP;
– интервал отправки анонсов главным маршрутизатором: целое число в диапазоне от 50 до 25500 миллисекунд или от 1 до 255 секунд;
– поддерживаемая версия VRRP: 2, 3, 2&3.

Дополнения и ограничения
В настоящий момент поддерживается только VRRPv2 и VRRPv3 для IPv4.

Описание настройки
Порядок настройки VRRP приведен в таблице 21.

Таблица 21 – Порядок настройки OSPF

Шаг	Команда	Назначение
1	**configure terminal**	Переход в режим глобальной настройки
2	**interface vlan** *vlan-id*	Переход в режим настройки интерфейса (VLAN)
3	**vrrp** *group* **ip** *ip-address* **[secondary]**	Установка IP-адреса группы резервирования VRRP и включения VRRP на интерфейсе. Группа резервирования VRRP создается в выключенном состоянии
4	**vrrp** *group* **authentication {***text-string* **| text** *text-string* **| md5 key-string** *key-string* **[timeout** *seconds***]}**	(Опционально) Включение аутентификации на группе резервирования VRRP
5	**vrrp delay {minimum** *seconds* **[reload** *seconds***] | reload** *seconds***}**	(Опционально) Установка задержки перед инициализацией групп резервирования VRRP на интерфейсе
6	**vrrp** *group* **priority** *level*	Установка приоритета устройства в группе резервирования VRRP
7	**vrrp** *group* **version {2 | 3 | 2&3}**	(Опционально) Установка поддерживаемой версии VRRP
8	**no vrrp** *group* **shutdown**	Включение группы резервирования VRRP
9	**exit**	Переход в предыдущий режим настройки

Продолжение таблицы 21

Шаг	Команда	Назначение
10	**exit**	Переход в предыдущий режим настройки
11	**show vrrp**	Проверка настроек VRRP
12	**copy running-config startup-config**	Сохранение текущей конфигурации

Рассмотрим вариант настройки со следующими условиями:

1. Необходимо создать на интерфейсе VLAN 1 группу резервирования VRRP 1 со следующими параметрами:
   - IP-адрес – 10.0.1.10;
   - аутентификация – MD5 с паролем “secret”;
   - приоритет – 200;
   - версия VRRP – VRRPv3.
2. Необходимо создать на интерфейсе VLAN 1 группу резервирования VRRP 2 со следующими параметрами:
   - IP-адрес – 10.0.1.20;
   - аутентификация – MD5 с паролем “topsecret”;
   - приоритет – 50;
   - версия VRRP – VRRPv3.
3. В сети уже есть маршрутизатор VRRP с двумя группами VRRP и приоритетом 100.

Создадим группу резервирования VRRP 1:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 ip 10.0.1.10
admin@Switch(config-if-vlan)# vrrp 1 authentication md5 key-string secret
admin@Switch(config-if-vlan)# vrrp 1 priority 200
admin@Switch(config-if-vlan)# vrrp 1 version 3
admin@Switch(config-if-vlan)# no vrrp 1 shutdown
admin@Switch(config-if-vlan)#
```

Создадим группу резервирования VRRP 2:

```
admin@Switch(config-if-vlan)# vrrp 2 ip 10.0.1.20
admin@Switch(config-if-vlan)# vrrp 2 authentication md5 key-string topsecret
admin@Switch(config-if-vlan)# vrrp 2 priority 50
admin@Switch(config-if-vlan)# vrrp 2 version 3
admin@Switch(config-if-vlan)# no vrrp 2 shutdown
admin@Switch(config-if-vlan)# exit
admin@Switch(config)# exit
admin@Switch# exit
```

Проверим параметры и сохраним файл конфигурации:

```
admin@Switch# show vrrp
Interface: VLAN 10
  Minimum delay is 0 seconds, reload delay is 0 seconds

Interface: VLAN 10 - Group 1
  Supported version is VRRPv3
  State is Backup
  Virtual IP address is 10.0.1.10
  Virtual MAC address is 00:00:5e:00:01:01
  Advertisement interval is 3.000 sec
  Preemption enabled
    min delay is 0.000 sec
  Priority is 200
  Master Router is 10.0.1.2, priority is 100
  Master Advertisement interval is 3.000 sec
  Master Down Interval is 10.000 sec

  Interface: VLAN 10 - Group 2
  Supported version is VRRPv3
  State is Master
  Virtual IP address is 10.0.1.20
  Virtual MAC address is 00:00:5e:00:01:02
  Advertisement interval is 3.000 sec
  Preemption enabled
    min delay is 0.000 sec
  Priority is 50
  Master Router is 10.0.1.1 (local), priority is 50
  Master Advertisement interval is 3.000 sec
  Master Down Interval is 10.000 sec

admin@Switch# copy running-config startup-config
admin@Switch#
```

16.10.2 clear vrrp statistics

Команда фундаментального режима. Очистка счетчиков статистики VRRP.

Синтаксис команды:

clear vrrp statistics [vlan *vlan-id* **[group** *group*]]

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
group	номер группы резервирования VRRP в диапазоне от 1 до 255

Использование команды:

Команда «**clear vrrp statistics**» используется для очистки счетчиков статистики VRRP. Если команда введена без аргументов, то команда применяется ко всем интерфейсам.

Пример команды:

```
admin@Switch# clear vrrp statistics vlan 10
admin@Switch#
```

16.10.3 vrrp authentication

Команда настройки интерфейса (VLAN). Включение аутентификации на группе резервирования VRRP.

Синтаксис команды:

vrrp *group* **authentication {text** *text-string* **| md5 {key-string** *key-string* **| key-string encrypted** *hash-string***} [timeout** *seconds***]}**

no vrrp group authentication

Команда с приставкой «**no**» отключает аутентификацию.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255
text-string	аутентификация с помощью простого пароля (текстовая строка). Параметр «*text-string*» представляет собой строку из латинских букв и цифр длиной до 8 символов
md5	аутентификация с помощью MD5
key-string	определяет строку аутентификации MD5. Доступны следующие подпараметры: – *key-string* – текстовая строка из латинских букв и цифр длиной до 64 символов; – **timeout** *seconds* – (опционально) интервал времени, в течение которого устройство будет принимать старые и новые пароли. Диапазон значений: от 1 до 255 секунд. Параметр не сохраняется в файле конфигурации
key-string encrypted	определяет зашифрованную строку аутентификации MD5. Доступны следующие подпараметры: – *hash-string* – вычисленная хэш-функция в виде строки длиной до 64 символов; – **timeout** *seconds* – (опционально) интервал времени, в течение которого устройство будет принимать старые и новые пароли. Диапазон значений: от 1 до 255 секунд. Параметр не сохраняется в файле конфигурации

Значение по умолчанию:

Аутентификация отключена.

Использование команды:

Команда «**vrrp authentication**» используется для включения аутентификации на группе резервирования VRRP.

Группа резервирования должна быть создана с помощью команды «**vrrp ip**», в противном случае ввод команды «**vrrp authentication**» приведет к выводу сообщения об ошибке вида “

Все маршрутизаторы в группе резервирования VRRP должны иметь одинаковые настройки аутентификации группы резервирования. Если на маршрутизаторах настроены разные настройки аутентификации, то маршрутизаторы в группе резервирования VRRP не будут взаимодействовать друг с другом и считать себя главными маршрутизаторами.

В случае использования аутентификации с помощью простого пароля устройство отправляет пароль в теле пакета без какого-либо шифрования. Аутентификация с помощью простого пароля не предназначена для обеспечения безопасности, а только для исключения маршрутизаторов из группы резервирования VRRP, если они не настроены для работы в этой группе.

Интервал времени, задаваемый параметром «**timeout** *seconds*», предназначен для того, чтобы у администратора было время для настройки всех маршрутизаторов в группе резервирования. Для минимизации вероятности перестройки маршрутов VRRP необходимо настроить новый ключ сначала на всех подчиненных маршрутизаторах, затем на резервном (backup) маршрутизаторе и, в последнюю очередь, на главном маршрутизаторе группы резервирования VRRP. Настройку нового значения ключа на главном маршрутизаторе группы резервирования VRRP необходимо произвести после настройки на резервном маршрутизаторе и не позднее чем через интервал времени, заданный командой «**vrrp timers advertise**». Эта процедура позволяет исключить потерю связи между главным и резервным маршрутизаторами группы резервирования VRRP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 authentication 12345
admin@Switch(config-if-vlan)#
```

16.10.4 vrrp debug

Команда фундаментального режима. Включение отладки VRRP.

Синтаксис команды:

vrrp debug {cli {disable | enable} | shell {disable | enable}}

Параметры команды:

cli	включить/выключить (**enable/disable**) вывод сообщений отладки в CLI
shell	включить/выключить (**enable/disable**) вывод сообщений отладки в консоль Erlang

Значение по умолчанию:

Отладка VRRP отключена.

Пример команды:

```
admin@Switch# vrrp debug cli enable
admin@Switch#
```

16.10.5 vrrp debug interval

Команда фундаментального режима. Настройка минимального интервала между сообщениями отладки VRRP.

Синтаксис команды:

vrrp debug interval *number*

Параметры команды:

number	минимальный интервал между сообщениями отладки VRRP в миллисекундах

16.10.6 vrrp delay

Команда настройки интерфейса (VLAN). Установка задержки перед инициализацией групп резервирования VRRP на интерфейсе.

Синтаксис команды:

vrrp delay {minimum *seconds* **[reload** *seconds***] | reload** *seconds***}**

no vrrp delay

Команда с приставкой «**no**» удаляет задержку перед инициализацией групп резервирования VRRP на интерфейсе.

Параметры команды:

minimum *seconds*	минимальный интервал задержки перед инициализацией групп резервирования VRRP после появления соединения на интерфейсе в диапазоне от 1 до 10000 секунд
reload *seconds*	интервал задержки перед инициализацией групп резервирования VRRP после загрузки устройства в диапазоне от 1 до 10000 секунд

Значение по умолчанию:

Задержки перед инициализацией групп резервирования VRRP отсутствуют.

Использование команды:

Команда «**vrrp delay**» используется для установки задержки перед инициализацией групп резервирования VRRP на интерфейсе. Команда устанавливает задержку для всех групп резервирования VRRP на интерфейсе.

Параметр «**minimum** *seconds*» представляет собой интервал задержки перед инициализацией групп резервирования VRRP, который применяется при появлении соединения на интерфейсе после загрузки устройства.

Параметр «**reload** *seconds*» представляет собой интервал задержки перед инициализацией групп резервирования VRRP, который применяется при первом появлении соединения на интерфейсе после загрузки устройства. То есть указанный интервал задержки применяется однократно после загрузки устройства.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp delay minimum 30 reload 60
admin@Switch(config-if-vlan)#
```

16.10.7 vrrp description

Команда настройки интерфейса (VLAN). Установка описания группы резервирования VRRP.

Синтаксис команды:

vrrp *group* **description** *text*

no vrrp *group* **description**

Команда с приставкой «**no**» удаляет описание группы резервирования VRRP.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255
text	текстовое описание назначения группы резервирования VRRP длиной до 160 символов

Значение по умолчанию:

Описание отсутствует.

Использование команды:

Команда «**vrrp description**» используется для установки описания группы резервирования VRRP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 description Evil Programmers
admin@Switch(config-if-vlan)#
```

16.10.8 vrrp ip

Команда настройки интерфейса (VLAN). Установка IP-адреса группы резервирования VRRP и создание группы резервирования VRRP на интерфейсе.

Синтаксис команды:

vrrp *group* **ip** *ip-address* **[secondary]**

no vrrp *group* **ip [***ip-address* **[secondary]]**

Команда с приставкой «**no**» удаляет IP-адрес группы резервирования VRRP и отключает VRRP на интерфейсе.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255
ip-address	IP-адрес группы резервирования VRRP
secondary	IP-адрес будет дополнительным адресом группы

Значение по умолчанию:

IP-адреса группы резервирования VRRP отсутствуют.

Использование команды:

Команда «**vrrp ip**» используется для установки IP-адреса группы резервирования VRRP и создания группы резервирования VRRP на интерфейсе. Команда создает группу резервирования.

Команда «**no vrrp ip**» используется для удаления IP-адреса группы резервирования VRRP и удаления группы резервирования VRRP на интерфейсе. Если команда введена без аргументов, то группа резервирования VRRP удаляется из настроек.

Первый настроенный IP-адрес используется как основной адрес для виртуального маршрутизатора. Для работы виртуального маршрутизатора VRRP необходимо чтобы IP-адрес виртуального маршрутизаторы был настроен хотя бы на одном из устройств.

Смена основного адреса виртуального маршрутизатора на главном маршрутизаторе группы резервирования VRRP приводит к немедленной смене основного адреса.

Все маршрутизаторы в группе резервирования VRRP должны иметь одинаковый основной адрес группы резервирования. Если на маршрутизаторах настроены разные основные адреса, то маршрутизаторы в группе резервирования VRRP не будут взаимодействовать друг с другом и считать себя главными маршрутизаторами. Команда «**vrrp ip**» без ключевого слова «**secondary**» используется для установки основного адреса группы резервирования. При необходимости установки дополнительных адресов используется команда «**vrrp ip**» с ключевым словом «**secondary**».

Группа резервирования VRRP создается в выключенном состоянии. Команда «**no vrrp shutdown**» используется для включения группы резервирования VRRP.

Примеры команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 ip 10.0.1.1
admin@Switch(config-if-vlan)#
```

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 ip 10.0.2.1 secondary
admin@Switch(config-if-vlan)#
```

16.10.9 vrrp preempt

Команда настройки интерфейса (VLAN). Включение автоматического перехода в режим главного маршрутизатора, если устройство имеет больший приоритет, чем текущий главный маршрутизатор.

Синтаксис команды:

vrrp *group* **preempt [delay minimum** *seconds***]**

no vrrp *group* **preempt**

Команда с приставкой «**no**» отключает функцию.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255
seconds	задержка перед отправкой анонса о переходе в режим главного маршрутизатора в диапазоне от 0 до 2147483647 секунд. По умолчанию задержка отсутствует

Значение по умолчанию:

Автоматический переход включен.

Использование команды:

Команда «**vrrp preempt**» используется для включения перехода в режим главного маршрутизатора, если устройство имеет больший приоритет, чем текущий главный маршрутизатор.

Устройство позволяет настроить задержку перед отправкой анонса о переходе в режим главного маршрутизатора.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 preempt delay minimum 10
admin@Switch(config-if-vlan)#
```

16.10.10 vrrp priority

Команда настройки интерфейса (VLAN). Установка приоритета устройства в группе резервирования VRRP.

Синтаксис команды:

vrrp *group* **priority** *level*

no vrrp *group* **priority**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255
level	приоритет устройства в группе резервирования VRRP с диапазоном значений от 1 до 254

Значение по умолчанию:

Приоритет устройства в группе резервирования VRRP равен 100.

Использование команды:

Команда «**vrrp priority**» используется для установки приоритета устройства в группе резервирования VRRP.

Приоритет позволяет указать, какое устройство будет выбрано главным в группе резервирования VRRP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 priority 200
admin@Switch(config-if-vlan)#
```

16.10.11 vrrp shutdown

Команда настройки интерфейса (VLAN). Отключение группы резервирования VRRP.

Синтаксис команды:

vrrp *group* **shutdown**

no vrrp *group* **shutdown**

Команда с приставкой «**no**» включает группу резервирования VRRP.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255

Значение по умолчанию:

Группа резервирования VRRP отключена.

Использование команды:

Команда «**vrrp shutdown**» используется для отключения группы резервирования VRRP.

Группа резервирования VRRP создается в выключенном состоянии. Команда «**no vrrp shutdown**» используется для включения группы резервирования VRRP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 ip 10.0.1.1
admin@Switch(config-if-vlan)# no vrrp 1 shutdown
admin@Switch(config-if-vlan)#
```

16.10.12 vrrp timers advertise

Команда настройки интерфейса (VLAN). Установка интервала отправки анонсов главным маршрутизатором группы резервирования VRRP.

Синтаксис команды:

vrrp *group* **timers advertise [msec]** *interval*

no vrrp *group* **timers advertise**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255
msec	значение интервала отправки анонсов будет указано в миллисекундах. Если параметр не указан, то значение интервала отправки анонсов будет указано в секундах

interval	интервал отправки анонсов главным маршрутизатором группы резервирования VRRP. Если значение указано в секундах, то значения параметра должны быть в диапазоне от 1 до 255. Если значение указано в миллисекундах, то значения параметра должны быть в диапазоне от 50 до 25500

Значение по умолчанию:

Интервал отправки анонсов равен 1 секунде.

Использование команды:

Команда «**vrrp timers advertise**» используется для установки интервала отправки анонсов главным маршрутизатором группы резервирования VRRP. Настройки таймеров на главном маршрутизаторе группы резервирования VRRP всегда переопределяют настройки на остальных членах группы.

Значение настройки всегда округляется в меньшую сторону до ближайшей секунды для протокола VRRPv2 и до ближайшего значения сотой части секунды для протокола VRRPv3. Если значение интервала отправки анонсов задано в миллисекундах и администратор устанавливает версию протокола VRRPv2, то устройство автоматически округляет значение настройки до ближайшей секунды.

Все маршрутизаторы в группе резервирования VRRP должны иметь одинаковые значения настроек таймеров. Если на маршрутизаторах настроены разные значения настроек таймеров, то маршрутизаторы в группе резервирования VRRP не будут взаимодействовать друг с другом и считать себя главными маршрутизаторами.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 timers advertise 5
admin@Switch(config-if-vlan)#
```

16.10.13 vrrp version

Команда настройки интерфейса (VLAN). Установка поддерживаемой версии VRRP.

Синтаксис команды:

vrrp *group* **version 2 | 3 | 2&3**

no vrrp *group* **version**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

group	номер группы резервирования VRRP в диапазоне от 1 до 255
2	поддержка VRRPv2 в соответствии с RFC3768. Полученные пакеты VRRPv3 отбрасываются устройством. Устройство отправляет только анонсы VRRPv2

3	поддержка VRRPv3 в соответствии с RFC5798. Полученные пакеты VRRPv2 отбрасываются устройством. Устройство отправляет только анонсы VRRPv3
2&3	поддержка VRRPv3 в соответствии с RFC5798, а также совместимость с VRRPv2 в соответствии с пунктом 8.4 RFC5798. Полученные пакеты VRRPv2 обрабатываются устройством. Устройство отправляет анонсы VRRPv2 и VRRPv3

Значение по умолчанию:

Версия 2.

Использование команды:

Команда «**vrrp version**» используется для установки поддерживаемой версии VRRP.

Режим «**2&3**» использовать только в случае обновления оборудования или ПО и перехода с VRRPv2 на VRRPv3. Режим «**2&3**» не предназначен для постоянной работы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# vrrp 1 version 3
admin@Switch(config-if-vlan)#
```

16.10.14 show vrrp

Команда, доступная из любого режима. Вывод состояния и настроек протокола VRRP.

Синтаксис команды:

show vrrp [interface *interface-id***] [all | brief | detail | statistics]**

Параметры команды:

interface-id	идентификатор интерфейса
all	вывод информации о всех группах, включая отключенные группы (в состоянии «**vrrp shutdown**»)
brief	вывод краткой информации о группах
detail	вывод детальной информации о группах, включая статистику
statistics	вывод счетчиков статистики

Использование команды:

Команда «**show vrrp**» используется для вывода состояния и настроек протокола VRRP. Описание параметров статистики приведено в таблице 22.

Примеры команды:

```
admin@Switch# show vrrp
Interface: VLAN 10
  Minimum delay is 30 seconds, reload delay is 60 seconds
Interface: VLAN 10 - Group 1
  Supported version is VRRPv3
  State is Master
  Virtual IP address is 10.0.1.1
  Virtual MAC address is 00:00:5e:00:01:01
  Advertisement interval is 3.000 sec
  Preemption enabled
    min delay is 0.000 sec
  Priority is 100
  Master Router is 10.0.1.1 (local), priority is 100
  Master Advertisement interval is 3.000 sec
  Master Down Interval is 10.500 sec
Interface: VLAN 10 - Group 2
  Supported version is VRRPv3
  State is Master
  Virtual IP address is 10.0.2.10
  Virtual MAC address is 00:00:5e:00:01:02
  Advertisement interval is 3.000 sec
  Preemption enabled
    min delay is 0.000 sec
  Priority is 100
  Master Router is 10.0.2.1 (local), priority is 100
  Master Advertisement interval is 3.000 sec
  Master Down Interval is 10.500 sec
```

```
admin@Switch# show vrrp
Interface  Group   Prio Timer  Own  Preempt State  Master addr/Group addr
---------  -----   ---- -----  ---  ------- -----  ----------------------
VLAN       10      1    100    10   Y       Yes    Master 10.0.1.1/10.0.1.1
VLAN       10      2    100    20   N       Yes    Master 10.0.2.1/10.0.2.10
```

```
admin@Switch# show vrrp 1 statistics
Interface: VLAN 10 - Group 1
  CheckSum Errors: 0
Version Errors: 0
  VRID Errors: 0
Advertisement Interval Err: 0
  IP TTL Errors: 0
Auth Failures: 0
  Invalid Auth Type: 0
Auth Type Mismatch: 0
  Packet Length Err: 0
Address List Errors: 0
  Become Master: 0
Priority Zero Pkts Rcvd: 0
  Advertise Rcvd: 1
Priority Zero Pkts Sent: 0
  Advertise Sent: 35
Invalid Type Pkts Rcvd: 0
```

```
admin@Switch# show vrrp 1 detail
Interface: VLAN 10 - Group 1
  Supported version is VRRPv3
  State is Master
  Virtual IP address is 10.0.1.10
  Virtual MAC address is 00:00:5e:00:01:01
  Advertisement interval is 3.000 sec
  Preemption enabled
    min delay is 0.000 sec    Priority is 100
  Master Router is 10.0.1.1 (local), priority is 100
  Master Advertisement interval is 3.000 sec
  Master Down Interval is 10.500 sec
  CheckSum Errors: 0 Version Errors: 0
  VRID Errors: 0 Advertisement Interval Err: 0
  IP TTL Errors: 0
Auth Failures: 0
  Invalid Auth Type: 0
Auth Type Mismatch: 0
  Packet Length Err: 0
Address List Errors: 0
  Become Master: 0
Priority Zero Pkts Rcvd: 0
  Advertise Rcvd: 1
Priority Zero Pkts Sent: 0
  Advertise Sent: 35
Invalid Type Pkts Rcvd: 0
```

```
Auth Type Mismatch: 0
  Packet Length Err: 0
Address List Errors: 0
  Become Master: 1
Priority Zero Pkts Rcvd: 0
  Advertise Rcvd: 1
Priority Zero Pkts Sent: 0
  Advertise Sent: 35
Invalid Type Pkts Rcvd: 0

Interface: VLAN 10 - Group 2
  CheckSum Errors: 0
Version Errors: 1
  VRID Errors: 0
Advertisement Interval Err: 0
  IP TTL Errors: 0
Auth Failures: 0
  Invalid Auth Type: 0
Auth Type Mismatch: 0
  Packet Length Err: 0
Address List Errors: 0
  Become Master: 1
Priority Zero Pkts Rcvd: 0
  Advertise Rcvd: 1
Priority Zero Pkts Sent: 0
  Advertise Sent: 29
Invalid Type Pkts Rcvd: 0
```

```
admin@Switch# show vrrp interface vlan 10 statistics
Interface: VLAN 10 - Group 1
  Checksum Errors: 0
Version Errors: 0
  VRID Errors: 0
Advertisement Interval Err: 0
  IP TTL Errors: 0
Auth Failures: 0
  Invalid Auth Type: 0
```

Таблица 22 – Описание параметров статистики

Поле	Описание
Checksum Errors	Количество принятых пакетов с ошибкой контрольной суммы
VRID Errors	Количество принятых пакетов с некорректным номером группы резервирования
IP TTL Errors	Количество принятых пакетов с некорректным значением времени жизни (TTL)
Invalid Auth Type	Количество принятых пакетов с некорректным типом аутентификации (несуществующим)
Packet Length Err	Количество принятых пакетов с некорректной длиной
Become Master	Количество переходов в режим главного маршрутизатора группы резервирования
Advertise Rcvd	Количество принятых анонсов
Advertise Sent	Количество отправленных анонсов
Version Errors	Количество принятых пакетов с некорректной версией протокола
Advertisement Interval Err	Количество принятых пакетов с некорректным значением интервала анонса
Auth Failures	Количество принятых пакетов, не прошедших аутентификацию
Auth Type Mismatch	Количество принятых пакетов с несоответствующим типом аутентификации
Address List Errors	Количество принятых пакетов с ошибками в списке адресов
Priority Zero Pkts Rcvd	Количество принятых пакетов со значением приоритета, равным нулю
Priority Zero Pkts Sent	Количество отправленных пакетов со значением приоритета, равным нулю
Invalid Type Pkts Rcvd	Количество принятых пакетов с некорректным значением типа пакета

16.11 Настройка Route-Map

16.11.1 Общие положения

Route-map – это объект в конфигурационном файле, с помощью которого можно настраивать такой функционал, как PBR.

Route map позволяет фильтровать маршруты при перераспределении и изменять различные атрибуты маршрутов.

Использование Route-Map для Policy-based routing

Route-map для PBR состоит из правил, у каждого правила route-map есть порядковый номер:

- когда пакеты проходят сквозь интерфейс, к которому применена PBR, пакеты проверяются по порядку по правилам;
- если пакет совпал с описанием в «**match**», то он маршрутизируется по правилу «**set**»;
- если пакет не совпал с описанием в «**match**», правила проверяются дальше;
- если ни в одном правиле совпадения не найдено, то пакет будет маршрутизироваться по стандартной таблице маршрутизации.

16.11.2 route-map

Команда режима настройки. Вход в режим “route-map” и разрешение или запрет действий «**match**»/«**set**».

Эта команда управляет и изменяет информацию о маршруте, чтобы разрешить перераспределение маршрутов. Она имеет список команд «**match**» и «**set**», связанных с ним. Команды «**match**» задают условия, при которых допускается перераспределение, а команды «**set**» задают конкретные действия перераспределения, которые должны выполняться, если выполняются критерии, применяемые командами «**match**». Карты маршрутов используются для детального контроля распределения маршрутов между процессами маршрутизации. Карты маршрутов также допускают маршрутизацию политики и могут направлять пакеты по другому маршруту, чем очевидный кратчайший путь.

Синтаксис команды:

route-map *name* {**permit** *sequence* | **deny** *sequence* | **optimization**}

no route-map *name* {**permit | deny | optimization**}

Команда с приставкой «**no**» отключает объявление.

Параметры команды:

name	имя route-map (максимальный размер 32 символа)
permit	установка разрешения операций с route-map
deny	установка запрета операций с route-map
optimization	настройка оптимизации route-map
sequence	последовательнось для вставки/удаления в существующей route-map

Значение по умолчанию:

Значение по умолчанию не задано.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# route-map PBR permit 10
admin@Switch(config-rmap)#
```

16.11.3 match access-group

Команда режима “route-map”. Определение критерия соответствия интерфейса. Эта команда задает имя интерфейса “next-hop” для сопоставляемого маршрута.

Синтаксис команды:

match access-group [*name***]**

no match access-group

Команда с приставкой «**no**» удаляет указанный критерий соответствия.

Параметры команды:

name	имя access-group

Значение по умолчанию:

По умолчанию функция отключена.

Использование команды:

Перед настройкой «**match access-group**» нужно создать имя IPv4 ACL, например: ip access-list route-pbr (пункт 9.1.4).

Пример команды:

```
admin@Switch(config)# route-map PBR
admin@Switch(config-rmap)# match access-group route-pbr
admin@Switch(config-rmap)#
```

16.11.4 set metric

Команда режима “route-map”. Команда установки метрики для маршрута.

Синтаксис команды:

set metric *metric*

no set metric

Команда с приставкой «**no**» удаляет указанный критерий соответствия.

Параметры команды:

metric	значение метрики

Значение по умолчанию:
По умолчанию функция отключена.
Пример команды:

```
admin@Switch(config)# route-map PBR permit 10
admin@Switch(config-rmap)# set metric 100
admin@Switch(config-rmap)#
```

16.11.5 set next-hop

Команда режима “route-map”. Установка значения next-hop. Описывает куда перенаправлять трафик, который описан в **match**.
Синтаксис команды:
set next-hop *ip address*
no set next-hop
Команда с приставкой «**no**» отключает данную функцию.
Параметры команды:
ip address указывает адрес следующего хопа
Значение по умолчанию:
Значения по умолчанию не заданы.
Пример команды:

```
admin@Switch(config)# route-map PBR
admin@Switch(config-rmap)# match access-group route-pbr
admin@Switch(config-rmap)# set next-hop 11.11.11.22
```

16.11.6 service-route-policy

Команда настройки интерфейса (Ethernet, Port-channel, Vlan). Установка карты маршрутов на интерфейсе.
Синтаксис команды:
service-route-policy *policy-map-name*
no service-route-policy
Команда с приставкой «**no**» отключает данную функцию.
Параметры команды:
policy-map-name имя service-route-policy
Использование команды:
Команда используется для применения PBR к интерфейсу.
Значение по умолчанию:
Значения по умолчанию не заданы.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# service-route-policy PBR
admin@Switch(config-if)#
```

16.11.7 show route-map

Команда, доступная из любого режима. Вывод информации о карте маршрута.

Синтаксис команды:

show route-map

Значение по умолчанию:

Значение по умолчанию не задано.

Пример команды:

```
admin@Switch(config)# show route-map

Route Map PBR
  match access-group route-pbr
  set next-hop 11.11.11.22
```

17 Многоадресная рассылка

17.1 Настройка IGMP Snooping

17.1.1 Общие положения

IGMP Snooping – процесс отслеживания сетевого трафика IGMP, который позволяет сетевым устройствам канального уровня (свитчам) отслеживать IGMP-обмен между потребителями и поставщиками (маршрутизаторами) многоадресного (multicast) IP-трафика, формально происходящий на более высоком (сетевом) уровне.

Коммутатор обеспечивает:

- включение IGMP Snooping глобально или на определенном VLAN с помощью команды «**ip igmp snooping**»;
- установку максимальной версии используемого протокола IGMP с помощью команды «**ip igmp snooping version**»;
- установку количества IGMP-запросов, отправляемых в порт при получении из него сообщения «Leave», с помощью команды «**ip igmp snooping last-member-query-count**»;
- установку интервала IGMP-запросов, отправляемых в интерфейс при получении из него сообщения «Leave», с помощью команды «**ip igmp snooping last-member-query-interval**»;
- включение механизма периодического опроса хостов (IGMP Querier) с помощью команды «**ip igmp snooping querier**»;
- установку интервала опроса хостов механизмом IGMP Querier с помощью команды «**ip igmp snooping query-interval**»;
- установку интервала времени, в течение которого хосты обязаны ответить на запрос, с помощью команды «**ip igmp snooping querymax-response-time**»;
- установку чувствительности устройства к потерям пакетов IGMP с помощью команды «**ip igmp snooping robustness-variable**»;
- установку количества опросов хостов механизмом IGMP Querier при его включении с помощью команды «**ip igmp snooping startup-query-count**»;
- установку интервала опроса хостов механизмом IGMP Querier при его включении с помощью команды «**ip igmp snooping startup-query-interval**»;
- добавление интерфейсов, к которым подключены маршрутизаторы многоадресного трафика, с помощью команды «**ip igmp snooping vlan mrouter**»;
- добавление статической многоадресной группы на интерфейс (установка статического членства интерфейса) с помощью команды «**ip igmp snooping vlan static**».

Вывод общих настроек IGMP Snooping осуществляется с помощью команды «**show ip igmp snooping**».

Вывод информации о многоадресных группах IGMP Snooping осуществляется с помощью команды «**show ip igmp snooping groups**».

Вывод информации об интерфейсах, к которым подключены многоадресные маршрутизаторы, осуществляется с помощью команды «**show ip igmp snooping mrouter**».

Вывод настроек и информации об IGMP querier, включенных на устройстве или обнаруженных на интерфейсах, осуществляется с помощью команды «**show ip igmp snooping querier**».

17.1.2 clear ip igmp group

Команда фундаментального режима. Сброс информации об изученных группах мультикастового трафика.

Синтаксис команды:

clear ip igmp group [interface *interface-id* **{vlan** *vlan-id***}] [***ip-address* **{vlan** *vlan-id***}]**

Параметры команды:

interface-id	идентификатор интерфейса Ethernet
ip-address	IP-адрес мультикастовой группы
vlan-id	идентификатор интерфейса VLAN в диапазоне от 1 до 4094

Примеры команды:

```
admin@Switch# clear ip igmp group
admin@Switch#
```

```
admin@Switch# clear ip igmp group 225.0.0.5 vlan 10
admin@Switch#
```

17.1.3 ip igmp profile

Команда глобальной настройки. Создание профиля IGMP и переход в режим настройки профиля.

Синтаксис команды:

ip igmp profile {*number* | *name***}**

no ip igmp profile {*number* | *name***}**

Команда с приставкой «**no**» удаляет профиль IGMP.

Параметры команды:

number	номер профиля в диапазоне от 1 до 1024
name	имя профиля в виде текстовой строки. Рекомендуемая длина: до 32 символов

Значение по умолчанию:

Профили IGMP отсутствуют.

Использование команды:

Команда «**ip igmp profile**» используется для создания профиля IGMP и перехода в режим настройки профиля.

Профили IGMP предназначены для ограничения списка многоадресных групп, к которым может присоединиться интерфейс. Все многоадресные группы, которым не соответствуют ограничения (правила), заданные пользователем, будут запрещены по умолчанию.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp profile 1
admin@Switch(config-igmp-profile)# permit 226.0.0.1 226.0.0.255
admin@Switch(config-igmp-profile)# exit
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip igmp filter 1
admin@Switch(config-if)#
```

17.1.4 ip igmp snooping

Команда глобальной настройки. Включение IGMP Snooping глобально или на определенном VLAN.

Синтаксис команды:

ip igmp snooping [vlan *vlan-id***]**

no ip igmp snooping [vlan *vlan-id***]**

Команда с приставкой «**no**» отключает IGMP Snooping.

Параметры команды:

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

IGMP Snooping отключен глобально и для всех VLAN по отдельности. При создании VLAN по умолчанию IGMP Snooping отключен.

Использование команды:

Команда «**ip igmp snooping**» используется для включения IGMP Snooping глобально или на определенном VLAN. IGMP Snooping будет активен только на тех VLAN, на которых он был включен командой «**ip igmp snooping vlan**».

При отключении IGMP Snooping с помощью команды «**no ip igmp snooping**», IGMP Snooping будет отключен на всех VLAN независимо от значения настроек на VLAN.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping
admin@Switch(config)# ip igmp snooping vlan 10
```

17.1.5 ip igmp snooping last-member-query-count

Команда глобальной настройки. Установка количества IGMP-запросов, отправляемых в порт при получении из него сообщения «Leave».

Синтаксис команды:

ip igmp snooping last-member-query-count *count* **[vlan** *vlan-id***]**

no ip igmp snooping last-member-query-count [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

count	количество IGMP-запросов, отправляемых при получении сообщения «Leave» в диапазоне от 1 до 7
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Количество IGMP-запросов, отправляемых при получении сообщения «Leave», равно 2.

Использование команды:

Команда «**ip igmp snooping last-member-query-count**» устанавливает количество IGMP-запросов, отправляемых в порт при получении из него сообщения «Leave». Если команда введена без аргумента «*vlan-id*», то значение параметра «*count*» применяется для VLAN, на которых не установлена собственная настройка с помощью команды «**ip igmp snooping last-member-query-count**».

При получении сообщения «Leave» на каком-либо интерфейсе, которое индицирует о желании подписчика выйти из группы, устройство отправляет IGMP-запрос, чтобы удостовериться в отсутствии подписчиков на этом интерфейсе. Количество запросов определяется параметром «**last-member-query-count**» (LMQC), а интервал отправки определяется параметром «**last-member-query-interval**» (LMQI).

Если по истечении времени, равного LMQC * LMQI, устройство не получит ответа от хостов, то передача многоадресного трафика для многоадресной группы на интерфейсе (или нескольких групп) будет отключена.

Нежелательно устанавливать параметр «**last-member-query-count**» равным 1, так как при потере IGMP-запроса, устройство отключит передачу многоадресного трафика на интерфейсе, даже если на нем есть активные подписчики (актуально только при подключении нескольких подписчиков на один интерфейс).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping last-member-query-count 3
admin@Switch(config)#
```

17.1.6 ip igmp snooping last-member-query-interval

Команда глобальной настройки. Установка интервала IGMP-запросов, отправляемых в интерфейс при получении из него сообщения «Leave».

Синтаксис команды:

ip igmp snooping last-member-query-interval *time* **[vlan** *vlan-id***]**

no ip igmp snooping last-member-query-interval [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

time	интервал отправки IGMP-запросов в диапазоне от 1 до 25 секунд
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Интервал отправки IGMP-запросов равен 1 секунде.

Использование команды:

Команда «**ip igmp snooping last-member-query-interval**» используется для установки интервала IGMP-запросов, отправляемых в интерфейс при получении из него сообщения «Leave». Если команда введена без аргумента «*vlan-id*», то значение параметра «*time*» применяется для VLAN, на которых не установлена собственная настройка с помощью команды «**ip igmp snooping last-member-query-interval**».

При получении сообщения «Leave» на каком-либо интерфейсе, которое индицирует о желании подписчика выйти из группы, устройство отправляет IGMP-запрос, чтобы удостовериться в отсутствии подписчиков на этом интерфейсе. Количество запросов определяется параметром «**last-member-query-count**» (LMQC), а интервал отправки определяется параметром «**last-member-query-interval**» (LMQI).

Если по истечении времени, равного LMQC * LMQI, устройство не получит ответа от хостов, то передача многоадресного трафика для многоадресной группы на интерфейсе (или нескольких групп) будет отключена.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping last-member-query-interval 3
admin@Switch(config)#
```

17.1.7 ip igmp snooping vlan mrouter

Команда глобальной настройки. Добавление интерфейсов, к которым подключены маршрутизаторы многоадресного трафика.

Синтаксис команды:

ip igmp snooping vlan *vlan-id* **mrouter {interface** *interface-id* **| learn}**

no ip igmp snooping vlan *vlan-id* **mrouter {interface** *interface-id* **| learn}**

Команда с приставкой «**no**» удаляет интерфейсы, к которым подключены маршрутизаторы многоадресного трафика.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
interface-id	идентификатор интерфейса (Ethernet, Port-channel)
learn	включение автоматического определения интерфейсов, к которым подключены маршрутизаторы многоадресного трафика

Значение по умолчанию:

Автоматическое определение интерфейсов, к которым подключены маршрутизаторы многоадресного трафика.

Использование команды:

Команда «**ip igmp snooping vlan mrouter**» используется для добавления интерфейсов, к которым подключены маршрутизаторы многоадресного трафика.

Команда «**ip igmp snooping vlan mrouter learn**» позволяет включить автоматическое обнаружение маршрутизаторов многоадресного трафика (интерфейсов, к которым они подключены) по следующим признакам:

– IGMP Query;

– IGMP-пакеты Multicast Router Discovery (RFC4286).

При включении IGMP Snooping устройство перехватывает пакеты IGMP для их обработки. После обработки устройство перенаправляет пакеты маршрутизаторам многоадресного трафика. Если интерфейсы, к которым подключены маршрутизаторы многоадресного трафика, не заданы статически и не обнаружены динамически, то входящие пакеты IGMP будут отбрасываться после обработки.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping vlan 10 mrouter learn
admin@Switch(config)#
```

17.1.8 ip igmp snooping querier

Команда глобальной настройки. Включение механизма периодического опроса хостов (IGMP Querier).

Синтаксис команды:

ip igmp snooping querier [*ip-address*] **[vlan** *vlan-id* **]**

no ip igmp snooping querier [*ip-address*] **[vlan** *vlan-id*]

Команда с приставкой «**no**» отключает механизм периодического опроса хостов.

Параметры команды:

ip-address	IP-адрес коммутатора, который использует механизм опроса IGMP Querier
vlan *vlan-id*	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Механизмы опроса отключены на всех VLAN.

Использование команды:

Команда «**ip igmp snooping querier**» используется для включения механизма периодического опроса хостов (IGMP Querier). Если команда введена без аргумента «*vlan-id*», то значение настройки применяется для VLAN, на которых не установлена собственная настройка с помощью команды «**ip igmp snooping querier**».

Механизм опроса периодически отправляет запросы IGMP General Query с интервалом, заданным командой глобальной настройки «**ip igmp snooping query-interval**». Интервал времени, в течение которого хосты отвечают на запрос, задается командой «**ip igmp snooping query-max-response-time**».

Если устройство обнаруживает другое устройство, отправляющее запросы IGMP Query с IP-адресом, меньшим, чем используемый текущим устройством, то механизм

опроса автоматически отключается на соответствующем VLAN. Устройство автоматически включает механизм опроса IGMP Querier на VLAN, если в течение времени, равного 2,5 интервала опроса, устройство не получает на VLAN запросы IGMP Query с IP-адресом, меньшим, чем используемый устройством.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping querier 192.168.0.10 vlan 2
admin@Switch(config)#
```

17.1.9 ip igmp snooping query-interval

Команда глобальной настройки. Установка интервала опроса хостов механизмом IGMP Querier.

Синтаксис команды:

ip igmp snooping query-interval *interval-count* **[vlan** *vlan-id***]**

no ip igmp snooping query-interval [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

interval-count	интервал между опросами IGMP в диапазоне от 1 до 18000 секунд
vlan *vlan-id*	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Интервал между опросами IGMP равен 125 секундам.

Использование команды:

Команда «**ip igmp snooping query-interval**» используется для установки интервала опроса хостов механизмом IGMP Querier. Если команда введена без аргумента «*vlan-id*», то значение параметра «*interval-count*» применяется для VLAN, на которых не установлена собственная настройка с помощью команды «**ip igmp snooping query-interval**».

Механизм опроса включается командой «**ip igmp snooping querier**». Интервал времени, в течение которого хосты обязаны ответить на запрос, задается командой «**ip igmp snooping query-max-responsetime**».

Необходимо настроить одинаковое значение интервала опроса на всех устройствах, если в сети есть IGMP Querier с версиями протокола IGMP v1 или IGMP v2, т.к. механизм обнаружения и старения других IGMP Querier зависит от этой настройки. В версии IGMP v3 интервал опроса инкапсулирован в сообщение, поэтому настройка «**ip igmp snooping query-interval**» не оказывает негативного влияния на механизм обнаружения и старения других IGMP Querier.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping query-interval 100 vlan 10
admin@Switch(config)#
```

17.1.10 ip igmp snooping query-max-response-time

Команда глобальной настройки. Установка интервала времени, в течение которого хосты обязаны ответить на запрос.

Синтаксис команды:

ip igmp snooping query-max-response-time *response-time* **[vlan** *vlan-id***]**

no ip igmp snooping query-max-response-time [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

response-time	максимальное время ожидания ответа на запрос IGMP в диапазоне от 1 до 25 секунд
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Максимальное время ожидания ответа на запрос IGMP равно 10 секундам.

Использование команды:

Команда «**ip igmp snooping query-max-response-time**» используется для установки интервала времени, в течение которого хосты обязаны ответить на запрос. Если команда введена без аргумента «*vlan-id*», то значение настройки «*response-time*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ip igmp snooping query-max-response-time**» (QMRT).

Механизм опроса периодически отправляет запросы IGMP General Query с интервалом, заданным командой «**ip igmp snooping query-interval**». Для включения механизма опроса используется команда глобальной настройки «**ip igmp snooping querier**».

Если в течение интервала QMRT, заданного командой «**ip igmp snooping query-max-response-time**», ни один из хостов на порту не ответил на запрос IGMP Querier, то устройство автоматически удаляет порт из всех динамических многоадресных групп.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping query-max-response-time 20 vlan 10
admin@Switch(config)#
```

17.1.11 ip igmp snooping robustness-variable

Команда глобальной настройки. Установка чувствительности устройства к потерям пакетов IGMP.

Синтаксис команды:

ip igmp snooping robustness-variable *integer-value* **[vlan** *vlan-id***]**

no ip igmp snooping robustness-variable [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

integer-value	порог чувствительности к потерям пакетов IGMP в диапазоне от 1 до 7 пакетов
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Порог чувствительности к потерям пакетов IGMP равен 2.

Использование команды:

Команда «**ip igmp snooping robustness-variable**» используется для установки чувствительности устройства к потерям пакетов IGMP. Если команда введена без аргумента «*vlan-id*», то значение настройки «*integer-value*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ip igmp snooping robustness-variable**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping robustness-variable 3 vlan 10
admin@Switch(config)#
```

17.1.12 ip igmp snooping startup-query-count

Команда глобальной настройки. Установка количества опросов хостов механизмом IGMP Querier при его включении.

Синтаксис команды:

ip igmp snooping startup-query-count *integer-value* **[vlan** *vlan-id***]**

no ip igmp snooping startup-query-count [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

integer-value	количество IGMP-запросов, отправляемых механизмом IGMP Querier при его включении в диапазоне от 1 до 10
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Количество IGMP-запросов, отправляемых механизмом IGMP Querier при его включении, равно 2.

Использование команды:

Команда «**ip igmp snooping startup-query-count**» используется для установки количества опросов хостов механизмом IGMP Querier при его включении. Если команда введена без аргумента «*vlan-id*», то значение настройки «*integer-value*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ip igmp snooping startup-query-count**».

При включении механизма опроса (командой пользователя или при включении коммутатора), коммутатор отправляет запросы IGMP Query с уменьшенным интервалом для быстрого получения информации о членстве портов в многоадресных группах. Для установки интервала опроса при старте используется команда «**ip igmp snooping startup-query-interval**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping startup-query-count 2 vlan 10
admin@Switch(config)#
```

17.1.13 ip igmp snooping startup-query-interval

Команда глобальной настройки. Установка интервала опроса хостов механизмом IGMP Querier при его включении.

Синтаксис команды:

ip igmp snooping startup-query-interval *integer-value* **[vlan** *vlan-id***]**

no ip igmp snooping startup-query-interval [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

interval-count	интервал между запросами IGMP в диапазоне от 1 до 18000 секунд
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Интервал между запросами IGMP равен 31 секунде.

Использование команды:

Команда «**ip igmp snooping startup-query-interval**» используется для установки интервала опроса хостов механизмом IGMP Querier при его старте. Если команда введена без аргумента «*vlan-id*», то значение настройки «*interval-count*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ip igmp snooping startup-query-interval**».

При включении механизма опроса (командой пользователя или при включении устройства), устройство отправляет запросы IGMP Query с уменьшенным интервалом для быстрого получения информации о членстве интерфейсов в многоадресных группах. Для установки количества опросов при старте используется команда «**ip igmp snooping startup-query-count**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping startup-query-interval 25 vlan 10
admin@Switch(config)#
```

17.1.14 ip igmp snooping vlan static

Команда глобальной настройки. Добавление статической многоадресной группы на интерфейс (установка статического членства интерфейса).

Синтаксис команды:

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id* **[source** *ip-address***]**

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id* **[source** *ip-address***]**

Команда с приставкой «**no**» удаляет статическую многоадресную группу.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
static *ip-address*	IP-адрес многоадресной группы IGMP
interface-id	идентификатор интерфейса (Ethernet, Portchannel)

source *ip-address* IP-адрес адреса источника. Используется только для IGMPv3

Значение по умолчанию:

Статические многоадресные группы отсутствуют.

Использование команды:

Команда «**ip igmp snooping vlan**» используется для добавления статической многоадресной группы на интерфейс (установки статического членство интерфейса).

Команда позволяет настроить IP-адрес источника многоадресной группы для реализации Source Specific Multicast. Указывать IP-адрес источника, только если на указанном VLAN все устройства работают в режиме IGMP v3. В противном случае возможна некорректная передача трафика.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping vlan 2 static 225.1.1.1 interface
gigabitethernet 0/1
admin@Switch(config)#
```

17.1.15 ip igmp snooping version

Команда глобальной настройки. Установка максимальной версии используемого протокола IGMP.

Синтаксис команды:

ip igmp snooping version *version* **[vlan** *vlan-id***]**

no ip igmp snooping version *version* **[vlan** *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

version максимальная версия IGMP: 1, 2 или 3

vlan-id идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Версия IGMP v3.

Использование команды:

Команда «**ip igmp snooping version**» используется для установки максимальной версии используемого протокола IGMP. Устройство будет корректно работать с хостами указанной версии и более ранних. Если команда введена без аргумента «*vlan-id*», то значение настройки «*version*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ip igmp snooping startup-query-interval**».

При обнаружении хостов (устройств) на VLAN с более ранними версиями протокола по сравнению с настроенной на устройстве, устройство автоматически переходит в режим совместимости с более ранней версией протокола. Если хосты (устройства) с более ранними версиями протокола становятся неактивны, то устройство переключается на версию протокола, указанную командой «**ip igmp snooping version**» (или «**ip igmp snooping version vlan**»).

Версия протокола влияет на следующий функционал:

1. Source Specific Multicast недоступен в IGMP v1 и IGMP v2. SSM автоматически отключается на всем VLAN.
2. Пакет IGMP Leave недоступен в IGMP v1. Таким образом, реальное время выхода интерфейса из многоадресной группы определяется интервалом опроса IGMP Querier.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp snooping version 2 vlan 10
admin@Switch(config)#
```

17.1.16 ip igmp filter

Команда настройки интерфейса (Ethernet, Port-channel). Установка профиля IGMP на интерфейс.

Синтаксис команды:

ip igmp filter {*number* | *name*}

no ip igmp filter

Команда с приставкой «**no**» удаляет профиль IGMP с интерфейса.

Параметры команды:

number	номер профиля в диапазоне от 1 до 1024
name	имя профиля в виде текстовой строки

Значение по умолчанию:

На интерфейсах не установлены профили.

Использование команды:

Команда «**ip igmp filter**» используется для установки профиля IGMP на интерфейс.

Профили IGMP предназначены для ограничения списка многоадресных групп, к которым может присоединиться интерфейс. Все многоадресные группы, которым не соответствуют ограничения (правила), заданные пользователем, будут запрещены по умолчанию.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp profile 1
admin@Switch(config-igmp-profile)# permit 226.0.0.1 226.0.0.255
admin@Switch(config-igmp-profile)# exit
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip igmp filter 1
admin@Switch(config-if)#
```

17.1.17 ip igmp immediate-leave

Команда настройки интерфейса (Ethernet, Port-channel). Включение немедленного удаления интерфейса из многоадресной группы при получении сообщения «Leave».

Синтаксис команды:

ip igmp immediate-leave

no ip igmp immediate-leave

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Значение по умолчанию:

Немедленное удаление интерфейса из многоадресной группы при получении сообщения «Leave» отключено.

Использование команды:

Команда «**ip igmp immediate-leave**» используется для включения немедленного удаления интерфейса из многоадресной группы при получении сообщения «Leave».

Настройка позволяет ускорить процесс удаления многоадресной группы на интерфейсе, если используется IGMP v2 и к интерфейсу подключен только один хост. Не рекомендуется использовать данную настройку на интерфейсах, к которым подключено более одного хоста.

При получении пакета IGMP Leave на интерфейсе, устройство отправляет запрос группы всем хостам на этом интерфейсе (Group Specific Query). Количество запросов определяется параметром «**last-member-query-count**» (LMQC), а интервал отправки определяется параметром «**last-member-query-interval**» (LMQI). Таким образом, если устройство не получает ответ, многоадресная группа будет находиться на интерфейсе в течение времени, равном LMQC * LMQI. Настройка «**immediate-leave**» отключает отправку запросов хостам на интерфейсе и позволяет немедленно удалить интерфейс из многоадресной группы.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip igmp immediate-leave
admin@Switch(config-if)#
```

17.1.18 ip igmp max-groups

Команда настройки интерфейса (Ethernet, Port-channel). Установка ограничения на максимальное количество многоадресных групп, которые могут быть на интерфейсе.

Синтаксис команды:

ip igmp max-groups *group-count*

no ip igmp max-groups

Команда с приставкой «**no**» удаляет ограничение на максимальное количество многоадресных групп.

Параметры команды:

group-count	максимальное количество многоадресных групп, которые могут быть на интерфейсе, в диапазоне от 1 до 2^{32} - 2

Значение по умолчанию:

Количество многоадресных групп не ограничено.

Использование команды:

Команда «**ip igmp max-groups**» используется для установки ограничения на максимальное количество многоадресных групп, которые могут быть на интерфейсе. При достижении максимального количества многоадресных групп на интерфейсе, устройство обрабатывает последующие запросы на подключение многоадресных групп в соответствии с настройкой, заданной командой «**ip igmp max-groups action**».

В случае настройки ограничения на интерфейсе, который уже является членом многоадресных групп, действие с текущими многоадресных группами определяется настройкой «**ip igmp max-groups action**»:

- если настроен режим «**deny**», то текущие записи не удаляются. Добавление новых записей запрещается, если текущее количество записей больше ограничения;
- если настроен режим «**replace**», то текущие записи удаляются. При появлении запросов на добавление новых групп, устройство замещает случайно выбранные старые группы на новые.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip igmp max-groups 10
admin@Switch(config-if)#
```

17.1.19 ip igmp max-groups action

Команда настройки интерфейса (Ethernet, Port-channel). Установка действия, которое производится с новыми многоадресными группами, если превышено ограничение на максимальное количество многоадресных групп, которые могут быть на интерфейсе.

Синтаксис команды:

ip igmp max-groups action {deny | replace}

no ip igmp max-groups action

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

deny	при превышении ограничения, устройство блокирует добавление новых многоадресных групп на интерфейс
replace	при превышении ограничения, устройство замещает случайно выбранные старые группы на новые

Значение по умолчанию:

При превышении ограничения, устройство блокирует добавление новых многоадресных групп на интерфейс.

Использование команды:

Команда «**ip igmp max-groups action**» используется для установки действия, которое производится с новыми многоадресными группами, если превышено ограничение на максимальное количество многоадресных групп, которые могут быть

на интерфейсе. Настройка ограничения максимального количества многоадресных групп на интерфейсе задается командой «**ip igmp max-groups**».

В случае настройки ограничения на интерфейсе, который уже является членом многоадресных групп, действие с текущими многоадресными группами определяется настройкой «**ip igmp max-groups action**»:

- если настроен режим «**deny**», то текущие записи не удаляются. Добавление новых записей запрещается, если текущее количество записей больше ограничения;
- если настроен режим «**replace**», то текущие записи удаляются. При появлении запросов на добавление новых групп, устройство замещает случайно выбранные старые группы на новые.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip igmp max-groups action deny
admin@Switch(config-if)#
```

17.1.20 ip igmp snooping report-suppression

Команда настройки интерфейса (VLAN). Включение режима подавления повторных IGMP-запросов (режим прокси).

Синтаксис команды:

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Значение по умолчанию:

Устройство работает в режиме прокси.

Использование команды:

Команда «**ip igmp snooping report-suppression**» используется для включения режима подавления повторных IGMP-запросов (режим прокси).

При получении IGMP-запроса (IGMP Report) на членство в многоадресной группе от хоста устройство вносит интерфейс в многоадресную группу и переправляет IGMP-запрос многоадресным маршрутизаторам. В IGMPv3 при большом количестве хостов, запрашивающих одну и ту же группу, это приведет к появлению избыточного трафика IGMP. Для исключения данной ситуации, устройство поддерживает подавление повторных IGMP запросов (режим прокси):

- при получении IGMP-запроса на членство в новой многоадресной группе от хоста устройство отправляет IGMP-запрос многоадресным маршрутизаторам;
- при получении IGMP-запроса на членство в существующей группе от хоста устройство не отправляет IGMP-запрос многоадресным маршрутизаторам;

– при получении IGMP опроса (IGMP Query) от многоадресного маршрутизатора устройство отправляет IGMP-запросы для существующих на нем многоадресных групп.

Независимо от режима прокси устройство преобразует IGMP-запросы от хостов в случае необходимости. Например, если на VLAN обнаружен многоадресный маршрутизатор, работающий в режиме IGMPv2, а хост отправляет IGMP-запрос IGMPv3, то запрос будет преобразован в IGMPv2.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface vlan 1
admin@Switch(config-if-vlan)# ip igmp snooping report-suppression
admin@Switch(config-if-vlan)#
```

17.1.21 deny

Команда настройки профиля IGMP. Добавление запрещающего правила в профиль IGMP.

Синтаксис команды:

[*sequence-number***] deny** *start-address* **[***end-address***]**

no [deny] *sequence-number*

Команда с приставкой «**no**» удаляет запрещающее правило из профиля IGMP.

Параметры команды:

sequence-number	номер правила в списке IGMP. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию, первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
start-address	начальный адрес диапазона
end-address	конечный адрес диапазона. Если параметр не задан, то он приравнивается начальному адресу диапазона

Значение по умолчанию:

Правило отсутствует.

Использование команды:

Команда «**deny**» используется для добавления запрещающего правила в профиль IGMP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp profile 2
admin@Switch(config-igmp-profile)# deny 226.0.0.1 226.0.0.255
admin@Switch(config-igmp-profile)# permit any
admin@Switch(config-igmp-profile)# exit
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip igmp filter 2
admin@Switch(config-if)#
```

17.1.22 permit

Команда настройки профиля IGMP. Добавление разрешающего правила в профиль IGMP.

Синтаксис команды:

[*sequence-number***] permit {***start-address* **| any} [***end-address***]**

no [permit] *sequence-number*

Команда с приставкой «**no**» удаляет разрешающее правило из профиля IGMP.

Параметры команды:

sequence-number	номер правила в списке IGMP. Номер определяет порядок применения правил. Диапазон значений: от 1 до 2147483646. По умолчанию, первое правило добавляется в список с номером 10, а для всех последующих номер увеличивается на 10
any	разрешение всех адресов
start-address	начальный адрес диапазона
end-address	конечный адрес диапазона. Если параметр не задан, то он приравнивается начальному адресу диапазона

Значение по умолчанию:

Правило отсутствует.

Использование команды:

Команда «**permit**» используется для добавления разрешающего правила в профиль IGMP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ip igmp profile 1
admin@Switch(config-igmp-profile)# permit 226.0.0.1 226.0.0.255
admin@Switch(config-igmp-profile)# exit
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# ip igmp filter 1
admin@Switch(config-if)#
```

17.1.23 show ip igmp profile

Команда, доступная из любого режима. Вывод настроек всех или определенного профиля IGMP.

Синтаксис команды:

show ip igmp profile [*number* **|** *name***]**

Параметры команды:

number	номер профиля в диапазоне от 1 до 1024
name	имя профиля в виде текстовой строки. Рекомендуемая длина: до 32 символов

Использование команды:

Команда «**show ip igmp profile**» используется для вывода настроек всех или определенного профиля IGMP. Если команда введена без аргументов, то выводится информация для всех профилей IGMP.

Пример команды:

```
admin@Switch# show ip igmp profile 1
IGMP profile 1
  10 permit 226.0.0.1 226.0.0.255
admin@Switch#
```

17.1.24 show ip igmp snooping

Команда, доступная из любого режима. Вывод общих настроек IGMP Snooping.

Синтаксис команды:

show ip igmp snooping [vlan *vlan-id***]**

Параметры команды:

vlan *vlan-id* вывод настройки по определенному VLAN

Использование команды:

Команда «**show ip igmp snooping**» используется для вывода общих настроек IGMP Snooping.

Пример команды:

```
admin@Switch# show ip igmp snooping
Global IGMP Snooping configuration:
---------------------------
IGMP snooping                : Enabled
Immediate leave              : Enabled
Last member query interval   : 100
Last member query count      : 3
Startup query interval       : 30
Startup query count          : 5
Robustness                   : 2
Version                      : 3
IGMP querier                 : Disabled
IGMP querier address         :

VLAN 1 IGMP Snooping configuration:
---------------------------
IGMP snooping                : Enabled
Immediate leave              : Enabled
Last member query interval   : 100
Last member query count      : 3
Startup query interval       : 30
Startup query count          : 5
Robustness                   : 2
Version                      : 3
IGMP querier                 : Disabled
IGMP querier address
```

17.1.25 show ip igmp snooping groups

Команда, доступная из любого режима. Вывод информации о многоадресных группах IGMP Snooping.

Синтаксис команды:

show ip igmp snooping groups [vlan *vlan-id*] [*ip-address*] **[count | dynamic {count} | user {count}]**

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
ip-address	IP-адрес многоадресной группы
count	общее количество многоадресных групп, отвечающих указанным параметрам команды
dynamic	вывод динамических многоадресных групп IGMP Snooping
user	вывод только настроенных пользователем групп IGMP Snooping

Использование команды:

Команда «**show ip igmp snooping groups**» используется для вывода информации о многоадресных группах IGMP Snooping. Если команда введена без аргументов, то выводится информация о всех многоадресных группах.

Пример команды:

```
admin@Switch# show ip igmp snooping groups
Vlan    Group         Type    Version Port List
----    ---------     ----    ------- ---------
1       224.1.4.4     igmp    v3      gi0/1
1       224.1.4.5     igmp    v3      gi0/2
2       224.0.1.40    igmp    v2      gi0/3
```

17.1.26 show ip igmp snooping mrouter

Команда, доступная из любого режима. Вывод информации об интерфейсах, к которым подключены многоадресные маршрутизаторы.

Синтаксис команды:

show ip igmp snooping mrouter [vlan *vlan-id*]

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Использование команды:

Команда «**show ip igmp snooping mrouter**» используется для вывода информации об интерфейсах, к которым подключены многоадресные маршрутизаторы. Если команда введена без аргументов, то выводится информация для всех VLAN.

Пример команды:

```
admin@Switch# show ip igmp snooping mrouter
Vlan    Ports
----    -------------
1       gi0/1(dynamic)
2       gi0/2(static)
admin@Switch#
```

17.1.27 show ip igmp snooping querier

Команда, доступная из любого режима. Вывод настроек и информации об IGMP querier, включенных на устройстве или обнаруженных на интерфейсах.

Синтаксис команды:

show ip igmp snooping querier [vlan *vlan-id***] [detail]**

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
detail	вывод подробной информации об IGMP querier

Использование команды:

Команда «**show ip igmp snooping querier**» используется для вывода настроек и информации об IGMP querier, включенных на устройстве или обнаруженных на интерфейсах. Если команда введена без аргументов, то выводится информация для всех VLAN.

Пример команды:

```
admin@Switch# show ip igmp snooping querier
Vlan    IP Address   IGMP Version      Port
----    ------------ ------------      -----
1       172.20.50.11 v1                gi0/1
2       172.20.40.20 v2                Switch
admin@Switch#
```

17.2 Настройка MLD Snooping

17.2.1 Общие положения

MLD Snooping – это протокол, отвечающий за управление участниками многоадресной рассылки IPv6. Он используется для установления и поддержания членства в группах многоадресной рассылки между хостами-членами IPv6 и их непосредственно соседними маршрутизаторами многоадресной рассылки.

MLD реализует функцию управления членами группы путем обмена сообщениями MLD между хостами-членами и многоадресными маршрутизаторами, а сообщения MLD инкапсулируются в сообщения IPv6. MLD Snooping работает аналогично IGMP Snooping, но на IPv6 адресах.

MLD Snooping используется для определения активных слушателей многоадресной группы в сети и отправления многоадресного трафика только тем портам, на которых активно прослушивание этого трафика. Это позволяет уменьшить загрузку сети и предотвратить ненужное распространение многоадресного трафика на неактивные (непрослушивающие) порты коммутатора.

Коммутатор обеспечивает:

- включение MLD Snooping глобально или на опрелеленном VLAN с помощью команды «**ipv6 mld snooping**»;
- включение механизма периодического опроса хостов (MLD Querier) на VLAN с помощью команды «**ipv6 mld snooping querier vlan**»;
- установку версии используемого протокола MLD глобально или на опрелеленном VLAN с помощью команды «**ipv6 mld snooping version**»;
- установку интервала опроса хостов механизмом MLD Querier глобально или на опрелеленном VLAN с помощью команды «**ipv6 mld snooping query-interval**»;
- установку интервала времени, в течение которого хосты обязаны ответить на запрос глобально или на опрелеленном VLAN, с помощью команды «**ipv6 mld snooping query-max-response time**»;
- установку чувствительности устройства к потерям пакетов MLD глобально или на опрелеленном VLAN с помощью команды «**ipv6 mld snooping robustness-variable**»;
- установку количества опросов хостов механизмом MLD Querier при его включении глобально или на опрелеленном VLAN с помощью команды «**ipv6 mld snooping startup-query-count**»;
- установку интервала опроса хостов механизмом MLD Querier при его включении глобально или на опрелеленном VLAN с помощью команды «**ipv6 mld snooping startup-query-interval**»;
- установку количества MLD-запросов, отправляемых в порт при получении из него сообщения «Leave» глобально или на опрелеленном VLAN, с помощью команды «**ipv6 mld snooping last-member-query-count**»;

– установку интервала MLD-запросов, отправляемых в интерфейс при получении из него сообщения «Leave» глобально или на опрелеленном VLAN, с помощью команды «**ipv6 mld snooping last-member-query-interval**».

Вывод общих настроек MLD Snooping осуществляется с помощью команды «**show ipv6 mld snooping**».

Вывод информации о многоадресных группах MLD Snooping осуществляется с помощью команды «**show ipv6 mld snooping groups**».

Вывод настроек и информации об MLD querier, включенных на устройстве или обнаруженных на интерфейсах, осуществляется с помощью команды «**show ipv6 mld snooping querier**».

17.2.2 ipv6 mld snooping

Команда глобальной настройки. Включение MLD Snooping глобально или на определенном VLAN.

Синтаксис команды:

ipv6 mld snooping [vlan *vlan-id***]**

no ipv6 mld snooping [vlan *vlan-id***]**

Команда с приставкой «**no**» отключает MLD Snooping.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

MLD Snooping отключен глобально и для всех VLAN по отдельности. При создании VLAN по умолчанию MLD Snooping отключен.

Использование команды:

Команда «**ipv6 mld snooping**» используется для включения MLD Snooping глобально или на определенном VLAN. MLD Snooping будет активен только на тех VLAN, на которых он был включен командой «**ipv6 mld snooping vlan**».

При отключении MLD Snooping с помощью команды «**no ipv6 mld snooping**», MLD Snooping будет отключен на всех VLAN независимо от значения настроек на VLAN.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping
admin@Switch(config)# ipv6 mld snooping vlan 1
```

17.2.3 ipv6 mld snooping querier vlan

Команда глобальной настройки. Включение механизма периодического опроса хостов (MLD Querier) на определенном VLAN.

Синтаксис команды:

ipv6 mld snooping querier vlan *vlan-id*

no ipv6 mld snooping querier vlan *vlan-id*

Команда с приставкой «**no**» отключает механизм периодического опроса хостов на VLAN.

Параметры команды:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Механизмы опроса отключены на всех VLAN.

Использование команды:

Команда «**ipv6 mld snooping querier vlan**» используется для включения механизма периодического опроса хостов (MLD Querier).

Механизм опроса периодически отправляет запросы MLD General Query с интервалом, заданным командой глобальной настройки «**ipv6 mld snooping query-interval**». Интервал времени, в течение которого хосты отвечают на запрос, задается командой «**ipv6 mld snooping query-max-response-time**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping querier vlan 1
admin@Switch(config)#
```

17.2.4 ipv6 mld snooping version

Команда глобальной настройки. Установка версии используемого протокола MLD.

Синтаксис команды:

ipv6 mld snooping version *version* **[vlan** *vlan-id***]**

no ipv6 mld snooping version *version* **[vlan** *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

version	версия MLD: 1 или 2
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Версия MLD v2.

Использование команды:

Команда «**ipv6 mld snooping version**» используется для установки версии используемого протокола MLD. Устройство будет корректно работать с хостами указанной версии и более ранних. Если команда введена без аргумента «*vlan-id*», то значение настройки «*version*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ipv6 mld snooping version vlan**».

При обнаружении хостов (устройств) на VLAN с более ранними версиями протокола по сравнению с настроенной на устройстве, устройство автоматически переходит в режим совместимости с более ранней версией протокола.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping version 1 vlan 1
admin@Switch(config)#
```

17.2.5 ipv6 mld snooping query-interval

Команда глобальной настройки. Установка интервала опроса хостов механизмом MLD Querier.

Синтаксис команды:

ipv6 mld snooping query-interval *interval-count* **[vlan** *vlan-id***]**

no ipv6 mld snooping query-interval [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

interval-count	интервал между опросами MLD в диапазоне от 1 до 18000 секунд
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Интервал между опросами MLD равен 125 секундам.

Использование команды:

Команда «**ipv6 mld snooping query-interval**» используется для установки интервала опроса хостов механизмом MLD Querier. Если команда введена без аргумента «*vlan-id*», то значение параметра «*interval-count*» применяется для VLAN, на которых не установлена собственная настройка с помощью команды «**ipv6 mld snooping query-interval**».

Механизм опроса включается командой «**ipv6 mld snooping querier**». Интервал времени, в течение которого хосты обязаны ответить на запрос, задается командой «**ipv6 mld snooping query-max-responsetime**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping query-interval 100 vlan 1
admin@Switch(config)#
```

17.2.6 ipv6 mld snooping query-max-response-time

Команда глобальной настройки. Установка интервала времени, в течение которого хосты обязаны ответить на запрос.

Синтаксис команды:

ipv6 mld snooping query-max-response-time *response-time* **[vlan** *vlan-id***]**

no ipv6 mld snooping query-max-response-time [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

response-time	максимальное время ожидания ответа на запрос MLD в диапазоне от 1 до 25 секунд
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Максимальное время ожидания ответа на запрос MLD равно 10 секундам.

Использование команды:

Команда «**ipv6 mld snooping query-max-response-time**» используется для установки интервала времени, в течение которого хосты обязаны ответить на запрос.

Если команда введена без аргумента «*vlan-id*», то значение настройки «*response-time*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ipv6 mld snooping query-max-response-time**» (QMRT).

Механизм опроса периодически отправляет запросы MLD General Query с интервалом, заданным командой «**ipv6 mld snooping query-interval**». Для включения механизма опроса используется команда глобальной настройки «**ipv6 mld snooping querier**».

Если в течение интервала QMRT, заданного командой «**ipv6 mld snooping query-max-response-time**», ни один из хостов на порту не ответил на запрос MLD Querier, то устройство автоматически удаляет порт из всех динамических многоадресных групп.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping query-max-response-time 15 vlan 1
admin@Switch(config)#
```

17.2.7 ipv6 mld snooping robustness-variable

Команда глобальной настройки. Установка чувствительности устройства к потерям пакетов MLD.

Синтаксис команды:

ipv6 mld snooping robustness-variable *integer-value* **[vlan** *vlan-id***]**

no ipv6 mld snooping robustness-variable [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

integer-value	порог чувствительности к потерям пакетов MLD в диапазоне от 1 до 7 пакетов
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Порог чувствительности к потерям пакетов MLD равен 2.

Использование команды:

Команда «**ipv6 mld snooping robustness-variable**» используется для установки чувствительности устройства к потерям пакетов MLD. Если команда введена без аргумента «*vlan-id*», то значение настройки «*integer-value*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ipv6 mld snooping robustness-variable**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping robustness-variable 3 vlan 1
admin@Switch(config)#
```

17.2.8 ipv6 mld snooping startup-query-count

Команда глобальной настройки. Установка количества опросов хостов механизмом MLD Querier при его включении.

Синтаксис команды:

ipv6 mld snooping startup-query-count *integer-value* **[vlan** *vlan-id***]**

no ipv6 mld snooping startup-query-count [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

integer-value	количество MLD-запросов, отправляемых механизмом MLD Querier при его включении в диапазоне от 1 до 10
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Количество MLD-запросов, отправляемых механизмом MLD Querier при его включении, равно 2.

Использование команды:

Команда «**ipv6 mld snooping startup-query-count**» используется для установки количества опросов хостов механизмом MLD Querier при его включении. Если команда введена без аргумента «*vlan-id*», то значение настройки «*integer-value*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ipv6 mld snooping startup-query-count**».

При включении механизма опроса (командой пользователя или при включении коммутатора), коммутатор отправляет запросы MLD Query с уменьшенным интервалом для быстрого получения информации о членстве портов в многоадресных группах. Для установки интервала опроса при старте используется команда «**ipv6 mld snooping startup-query-interval**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping startup-query-count 5 vlan 1
admin@Switch(config)#
```

17.2.9 ipv6 mld snooping startup-query-interval

Команда глобальной настройки. Установка интервала опроса хостов механизмом MLD Querier при его включении.

Синтаксис команды:

ipv6 mld snooping startup-query-interval *integer-value* **[vlan** *vlan-id***]**

no ipv6 mld snooping startup-query-interval [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

interval-count	интервал между запросами MLD в диапазоне от 1 до 18000 секунд
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Интервал между запросами MLD равен 30 секундам.

Использование команды:

Команда «**ipv6 mld snooping startup-query-interval**» используется для установки интервала опроса хостов механизмом MLD Querier при его старте. Если команда введена без аргумента «*vlan-id*», то значение настройки «*interval-count*» применяется на всех VLAN, для которых не задана отдельная настройка с помощью команды «**ipv6 mld snooping startup-query-interval**».

При включении механизма опроса (командой пользователя или при включении устройства), устройство отправляет запросы MLD Query с уменьшенным интервалом для быстрого получения информации о членстве интерфейсов в многоадресных группах. Для установки количества опросов при старте используется команда «**ipv6 mld snooping startup-query-count**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping startup-query-interval 25 vlan 1
admin@Switch(config)#
```

17.2.10 ipv6 mld snooping last-member-query-count

Команда глобальной настройки. Установка количества MLD-запросов, отправляемых в порт при получении из него сообщения «Leave».

Синтаксис команды:

ipv6 mld snooping last-member-query-count *count* **[vlan** *vlan-id***]**

no ipv6 mld snooping last-member-query-count [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

count	количество MLD-запросов, отправляемых при получении сообщения «Leave» в диапазоне от 1 до 7
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Количество MLD-запросов, отправляемых при получении сообщения «Leave», равно 2.

Использование команды:

Команда «**ipv6 mld snooping last-member-query-count**» устанавливает количество MLD-запросов, отправляемых в порт при получении из него сообщения «Leave». Если команда введена без аргумента «*vlan-id*», то значение параметра «*count*» применяется для VLAN, на которых не установлена собственная настройка с помощью команды «**ipv6 mld snooping last-member-query-count**».

При получении сообщения «Leave» на каком-либо интерфейсе, которое индицирует о желании подписчика выйти из группы, устройство отправляет MLD-запрос, чтобы удостовериться в отсутствии подписчиков на этом интерфейсе. Количество запросов определяется параметром «**last-member-query-count**» (LMQC), а интервал отправки определяется параметром «**last-member-query-interval**» (LMQI).

Если по истечении времени, равного LMQC * LMQI, устройство не получит ответа от хостов, то передача многоадресного трафика для многоадресной группы будет отключена.

Нежелательно устанавливать параметр «**last-member-query-count**» равным 1, так как при потере MLD-запроса, устройство отключит передачу многоадресного трафика, даже если на нем есть активные подписчики (актуально только при подключении нескольких подписчиков на один интерфейс).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping last-member-query-count 3 vlan 1
admin@Switch(config)#
```

17.2.11 ipv6 mld snooping last-member-query-interval

Команда глобальной настройки. Установка интервала MLD-запросов, отправляемых в интерфейс при получении из него сообщения «Leave».

Синтаксис команды:

ipv6 mld snooping last-member-query-interval *time* **[vlan** *vlan-id***]**

no ipv6 mld snooping last-member-query-interval [vlan *vlan-id***]**

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

time	интервал отправки MLD-запросов в диапазоне от 1 до 255 секунд
vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

Интервал отправки MLD-запросов равен 1 секунде.

Использование команды:

Команда «**ipv6 mld snooping last-member-query-interval**» используется для установки интервала MLD-запросов, отправляемых в интерфейс при получении из него сообщения «Leave». Если команда введена без аргумента «*vlan-id*», то значение параметра «*time*» применяется для VLAN, на которых не установлена собственная настройка с помощью команды «**ipv6 mld snooping last-member-query-interval**».

При получении сообщения «Leave» на каком-либо интерфейсе, которое индицирует о желании подписчика выйти из группы, устройство отправляет MLD-запрос, чтобы удостовериться в отсутствии подписчиков на этом интерфейсе. Количество запросов определяется параметром «**last-member-query-count**» (LMQC), а интервал отправки определяется параметром «**last-member-query-interval**» (LMQI).

Если по истечении времени, равного LMQC * LMQI, устройство не получит ответа от хостов, то передача многоадресного трафика для многоадресной группы на интерфейсе (или нескольких групп) будет отключена.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# ipv6 mld snooping last-member-query-interval 3
admin@Switch(config)#
```

17.2.12 show ipv6 mld snooping

Команда, доступная из любого режима. Вывод общих настроек MLD Snooping.

Синтаксис команды:

show ipv6 mld snooping [vlan *vlan-id***]**

Параметры команды:

vlan *vlan-id* вывод настройки по определенному VLAN

Использование команды:

Команда «**show ipv6 mld snooping**» используется для вывода общих настроек MLD Snooping.

Пример команды:

```
admin@Switch# show ipv6 mld snooping

Global MLD Snooping configuration:
----------------------
MLD snooping : Enabled
Last member query interval : 1
Last member query count : 2
Startup query interval : 0
Startup query count : 2
Robustness : 2
Version : 2
MLD querier : Disabled
MLD querier address : fe80::21b:28ff:fe01:aa60
MLD query interval : 2
MLD query max response time : 2

VLAN 1 MLD Snooping configuration:
----------------------
MLD snooping : Enabled
Last member query interval : 1
Last member query count : 2
Startup query interval : 0
Startup query count : 2
Robustness : 2
Version : 2
MLD querier : Enabled
MLD querier address : fe80::21b:28ff:fe01:aa60
MLD query interval : 2
MLD query max response time : 2
```

17.2.13 show ipv6 mld snooping groups

Команда, доступная из любого режима. Вывод информации о многоадресных группах MLD Snooping.

Синтаксис команды:

show ipv6 mld snooping groups [count]

Параметры команды:

count вывод количества подключенных групп

Использование команды:

Команда «**show ipv6 mld snooping groups**» используется для вывода информации о многоадресных группах MLD Snooping. Если команда введена без аргументов, то выводится информация о всех многоадресных группах. Если введена команда «**show ipv6 mld snooping groups count**» выводится количество подключенных групп.

Пример команды:

```
admin@Switch# show ipv6 mld snooping groups

Vlan    Group                Type         Version Port List
------  ---------            ----------   -----------------
1       ff15::150            dynamic v2   fastethernet0/5
admin@Switch# show ipv6 mld snooping groups count
Groups count: 1
```

17.2.14 show ipv6 mld snooping querier

Команда, доступная из любого режима. Вывод настроек и информации об MLD querier, включенных на устройстве или обнаруженных на интерфейсах.

Синтаксис команды:

show ipv6 mld snooping querier [vlan *vlan-id***]**

Параметры команды:

vlan *vlan-id* вывод настройки по определенному VLAN

Использование команды:

Команда «**show ipv6 mld snooping querier**» используется для вывода настроек и информации об MLD querier, включенных на устройстве или обнаруженных на интерфейсах. Если команда введена без аргументов, то выводится информация для всех VLAN.

Пример команды:

```
admin@Switch# show ipv6 mld snooping querier

Vlan    IPv6 Address               MLD Version  Port
----    -----------------------    -----------  ------
1       fe80::21b:28ff:fe01:aa60   v2           Switch

admin@Switch#
```

17.3 Настройка MVR

17.3.1 mvr

Команда глобальной настройки. Включение регистрации клиентов на многоадресном VLAN.

Синтаксис команды:

mvr

no mvr

Команда с приставкой «**no**» отключает регистрацию клиентов на многоадресном VLAN.

Значение по умолчанию:

Регистрация клиентов на многоадресном VLAN отключена.

Указания по применению:

Используйте команду «**mvr**» для включения регистрации клиентов на многоадресном VLAN.

Механизм регистрации клиентов на многоадресном VLAN (MVR) работает независимо от IGMP Snooping. Регистрация многоадресных VLAN предназначена для применения в крупных сетях, клиенты которых расположены в разных VLAN. В сети используется один VLAN, предназначенный для передачи многоадресных потоков данных (например, IPTV).

Пример команды:

Следующий пример показывает, как включить регистрацию клиентов на многоадресном VLAN:

```
admin@Switch# configure terminal
admin@Switch(config)# mvr
admin@Switch(config)#
```

17.3.2 mvr group

Команда глобальной настройки. Добавление IP-адресов многоадресных групп, ассоциируемых с MVR.

Синтаксис команды:

mvr group { *ip-address* **[** *count* **] | all }**

no mvr group { *ip-address* **[** *count* **] | all }**

Используйте команду «**no mvr group**» для удаления IP-адресов многоадресных групп. Используйте команду «**no mvr group all**» для перехода в режим использования IP-адресов многоадресных групп.

Описание синтаксиса:

all	соответствие любому значению IP-адреса многоадресной группы
ip-address	IP-адрес многоадресной группы в диапазоне от 224.0.1.0 до 239.255.255.255.

count	(опционально) количество последовательно добавляемых IP-адресов многоадресных групп в диапазоне от 1 до 256. Если параметр не задан, то устройство добавляет 1 IP-адрес

Значение по умолчанию:
IP-адреса многоадресных групп, используемых MVR, не заданы.
Указания по применению:
Используйте команду «**mvr group**» для добавления IP-адресов многоадресных групп, ассоциируемых с MVR.
Механизм MVR будет регистрировать интерфейсы в VLAN, предназначенного для передачи многоадресного трафика, только для тех многоадресных групп, которые заданы командой «**mvr group**».
Пример команды:
Следующий пример показывает, как добавить IP-адрес многоадресной группы 225.0.0.1:

```
admin@Switch# configure terminal
admin@Switch(config)# mvr group 225.0.0.1
admin@Switch(config)#
```

17.3.3 mvr mode

Команда глобальной настройки. Установка режима совместимости MVR.
Синтаксис команды:
mvr mode { compatible | dynamic }
no mvr mode
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Описание синтаксиса:

compatible	режим совместимости, при котором отключено создание динамических многоадресных групп для портов-источников
dynamic	режим, обеспечивающий создание динамических многоадресных групп для портов-источников

Значение по умолчанию:
Режим «**compatible**».
Указания по применению:
Используйте команду «**mvr mode**» для установки режима совместимости MVR.
Пример команды:
Следующий пример показывает, как установить динамический режим:

```
admin@Switch# configure terminal
admin@Switch(config)# mvr mode dynamic
admin@Switch(config)#
```

17.3.4 mvr querytime

Команда глобальной настройки. Установка максимального времени ожидания для получения отчета IGMP о членстве на порту получателя, прежде чем порт удалится из членства в группе многоадресной рассылки.

Синтаксис команды:

mvr querytime *value*

no mvr querytime

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Описание синтаксиса:

value	время ожидания ответа (IGMP Report) на опрос механизмом MVR в десятых долях секунды (в диапазоне от 1 до 100)

Значение по умолчанию:

Пять десятых секунды.

Указания по применению:

Используйте команду «**mvr querytime**» для установки времени ожидания ответов клиентов на опрос механизмом MVR.

Пример команды:

Следующий пример показывает, как установить время ожидания ответа равным 1 секунде:

```
admin@Switch# configure terminal
admin@Switch(config)# mvr querytime 10
admin@Switch(config)#
```

17.3.5 mvr vlan

Команда глобальной настройки. Установка номера VLAN, используемого для передачи многоадресных потоков данных.

Синтаксис команды:

mvr vlan *vlan-id*

no mvr vlan

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Описание синтаксиса:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094

Значение по умолчанию:

VLAN 1.

Указания по применению:

Используйте команду «**mvr vlan**» для указания номера VLAN, на который будут приходить многоадресные потоки данных. Все порты источники должны принадлежать этому VLAN.

Пример команды:

Следующий пример показывает, как установить номер VLAN, используемый для передачи многоадресных потоков данных, равным 5:

```
admin@Switch# configure terminal
admin@Switch(config)# mvr vlan 5
admin@Switch(config)#
```

17.3.6 mvr type

Команда настройки интерфейса (Ethernet). Установка типа интерфейса в механизме MVR.

Синтаксис команды:

mvr type { receiver | source }

no mvr type

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Описание синтаксиса:

receiver	принимающий интерфейс, к которому подключены клиенты многоадресного трафика. Принимающий интерфейс не может входить в VLAN, предназначенный для передачи многоадресного трафика
source	передающий интерфейс, к которому подключен многоадресный маршрутизатор, коммутатор или источник многоадресного трафика. Все передающие интерфейсы коммутатора входят в VLAN, предназначенный для передачи многоадресного трафика

Значение по умолчанию:

Интерфейс не является ни передающим, ни принимающим интерфейсом (отключение MVR).

Указания по применению:

Используйте команду «**mvr type**» для установки типа интерфейса в механизме MVR.

Пример команды:

Следующий пример показывает, как установить тип “принимающий интерфейс” для интерфейса gigabitethernet 0/1:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# mvr type receiver
admin@Switch(config-if)#
```

17.3.7 mvr vlan

Команда настройки интерфейса (Ethernet). Статическая настройка интерфеса для приема многоадресного трафика, отправляемого в многоадресную сеть VLAN и IP-адрес многоадресной рассылки.

Синтаксис команды:

mvr vlan *vlan-id* **group** *ip-address* **[source** *source* **]**

no mvr vlan *vlan-id* **group** *ip-address* **[source** *source* **]**

Команда с приставкой «**no**» удаляет IP-адреса многоадресной группы.

Описание синтаксиса:

vlan-id	идентификатор VLAN в диапазоне от 1 до 4094
ip-address	IP-адрес многоадресной группы
source	(опционально) IP-адрес источника

Значение по умолчанию:

IP-адреса не заданы.

Указания по применению:

Используйте команду «**mvr vlan**» для добавления IP-адреса многоадресной группы на указанном VLAN интерфейсе. Интерфейс, статически настроенный как член группы, остается членом группы до статического удаления.

Пример команды:

Следующий пример показывает, как добавить IP-адрес многоадресной группы 225.0.0.1 на VLAN 10 интерфейса gigabitethernet 0/1:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# mvr vlan 10 group 225.0.0.1
admin@Switch(config-if)#
```

17.3.8 mvr immediate

Команда настройки интерфейса (Ethernet). Мнговенное удаление интерфейса из многоадресной группы при получении сообщения IGMPv2 Leave.

Синтаксис команды:

mvr immediate

no mvr immediate

Команда с приставкой «**no**» отключает функцию.

Значение по умолчанию:

Функция отключена.

Указания по применению:

Используйте команду «**mvr immediate**» для мнговенного удаления интерфейса из многоадресной группы при получении сообщения «Leave» на этом интерфейсе сообщения IGMPv2 Leave для этой группы.

Пример команды:

Следующий пример показывает, как добавить IP-адрес многоадресной группы 225.0.0.1 на VLAN 10 интерфейса gigabitethernet 0/1:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# mvr immediate
admin@Switch(config-if)#
```

17.3.9 show mvr

Команда, доступная из любого режима. Вывод глобальных настроек MVR.

Синтаксис команды:

show mvr

Указания по применению:

Используйте команду «**show mvr**» для вывода глобальных настроек MVR.

Пример команды:

Следующий пример показывает, как вывести глобальные настройки MVR:

```
admin@SW2(config)# show mvr

MVR running: Yes
MVR multicast VLAN: 20
MVR max multicast groups: 1024
MVR current multicast groups: 0
MVR global query response time: 5 (tenths of sec)
MVR mode: dynamic
```

17.3.10 show mvr interface

Команда, доступная из любого режима. Вывод информации об интерфейсах MVR.

Синтаксис команды:

show mvr interface [*interface-id* **] members**

Описание синтаксиса:

interface-id (опционально) идентификатор интерфейса (Ethernet)

Указания по применению:

Используйте команду «**show mvr interface**» для вывода информации об интерфейсах MVR. Если команда введена без аргументов, то выводится информация для всех интерфейсов. Если введена команда «**show mvr interface** *interface-id* **members**» выводится информация о многоадресных группах на интерфейсе.

Пример команды:

Следующий пример показывает, как вывести информацию об интерфейсах MVR:

```
admin@SW2(config)# show mvr interface

Port                Type      Status
------------------  --------  ------
gigabitethernet0/2  receiver  up
gigabitethernet0/22 source    up
```

17.3.11 show mvr members

Команда, доступная из любого режима. Вывод информации о многоадресных группах MVR.

Синтаксис команды:

show mvr members [*ip-address* **]**

Описание синтаксиса:

ip-address (опционально) IP-адрес многоадресной группы

Указания по применению:

Используйте команду «**show mvr members**» для вывода информации о многоадресных группах MVR.

Пример команды:

Следующий пример показывает, как вывести информацию о многоадресных группах MVR:

```
admin@SW2(config)# show mvr members

MVR group IP          Members
------------          --------------------
225.0.0.1             gigabitethernet0/2(d)
```

18 Стекирование устройств

18.1 Общие положения

Стек или соединение сетевых коммутаторов в стек – это соединение двух или более коммутаторов, предназначенное для увеличения числа портов; при этом полученная группа идентифицируется остальными сетевыми устройствами как один коммутатор.

Для обеспечения целостности и безопасности конфигурации стека управлять им возможно исключительно с Master-устройства.

18.2 Порядок действий для организации стека

1. Предварительная настройка:

- подключиться к устройству в соответствии с разделом 2 настоящей части РЭ;
- включить устройство (подключить кабель питания);
- дождаться приглашения к авторизации вида “Switch login:”;
- ввести имя пользователя “admin” и пароль “admin”;
- перейти в режим настройки с помощью команды «**configure terminal**»;
- назначить номер устройства с помощью команды «**switch stack id N**», где N – номер устройства в стеке. Необходимо первому устройству назначить номер 1, а остальным назначать последующий номер. Например, если устройств в стеке 2, то необходимо назначить номера 1 и 2;
- сохранить настройки путем ввода команд:

(a) exit;
(b) copy running-config startup-config.

- дождаться завершения команд (вывода приглашения к вводу команд);
- отключить устройство.

2. Подключение устройств в стеке:

- подключить устройства по последним двум портам 10G;
- включить питание на всех устройствах.

ВНИМАНИЕ

Запрещается выключать или перезагружать коммутаторы, находящиеся в стеке, во время обновления ПО. Иначе возможен выход коммутаторов из строя или недоступность функции объединения коммутаторов в стек.

18.3 session

Команда глобальной настройки. Подключение к другому стекированному устройству.

Синтаксис команды:

session *number*

Параметры команды:

number номер членов стека

Пример команды:

```
admin@Switch# session 2
```

18.4 switch stack id

Команда глобальной настройки. Включение стекирования и настройка номера устройства в стеке.

Синтаксис команды:

switch stack id *stack-id*

no switch stack id

Команда с приставкой «**no**» отключает стекирование.

Параметры команды:

stack-id номер устройства в стеке в диапазоне от 1 до 5

Значение по умолчанию:

Стекирование отключено.

Использование команды:

Команда «**switch stack id**» используется для включения стекирования и настройки номера устройства в стеке.

После изменения настроек стекирования необходимо перезагрузить устройство командой «**reload**» для применения изменений.

При удалении конфигурации «**delete starup-config**» режим стекирования не выключается автоматически. Его нужно выключить вручную с помощью команды «**no switch stack id**» и перезагрузить устройство командой «**reload**».

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# switch stack id 10
admin@Switch(config)#
```

18.5 show switch

Команда, доступная из любого режима. Вывод настроек стекирования и информации об устройствах в стеке.

Синтаксис команды:

show switch [*number* | **detail** | **neighbors** | **stack-ports**]

Параметры команды:

number	(опционально) вывод информации для определенного устройства с номером в диапазоне от 1 до 5
detail	вывод подробной информации о стеке
neighbors	вывод топологии стека
stack-ports	вывод состояния стековых портов

Использование команды:

Команда «**show switch**» используется для вывода настроек стекирования и информации об устройствах в стеке. Если команда задана без параметров, то выводится только список устройств в стеке.

Примеры команды:

```
admin@Switch# show switch
Switch#   MAC address         Priority
-------   -----------------   --------
1         00:1B:28:00:91:2A   255
2         00:1B:28:00:91:4E   255
*3        00:1B:28:00:91:5A   255
```

```
admin@Switch# show switch detail

Stack type is ring
Switch#   MAC address         Priority
-------   -----------------   --------
1         00:1B:28:00:91:2A   255
2         00:1B:28:00:91:4E   255
*3        00:1B:28:00:91:5A   255

Neighbors
Switch#   Port A   Port B
-------   ------   ------
1         3        2
2         1        3
3         2        1

Stack port status
Switch#   Port A   Port B
-------   ------   ------
1         UP       UP
2         UP       UP
3         UP       UP
```

19 Статистика и подсчет трафика

19.1 Вывод статистики

19.1.1 Общие положения

Коммутатор обеспечивает вывод счетчиков статистики для порта CPU по команде «**show controllers cpu-interface**».

Вывод информации об интерфейсах осуществляется по команде «**show controllers ethernet-controller**».

Вывод информации об использовании пропускной способности интерфейсов осуществляется по команде «**show controllers utilization**».

19.1.2 show controllers cpu-interface

Команда фундаментального режима. Вывод счетчиков статистики для порта CPU.

Синтаксис команды:

show controllers cpu-interface

Пример команды:

```
admin@Switch# show controllers cpu-interface
cpu-interface1
_____________________________________________________

Rx good octets          64355654
Tx octets               71072047

Rx unicasts             0       Tx unicasts         0
Rx multicasts           0       Tx multicasts       0
Rx broadcasts           0       Tx broadcasts       0
Rx pause                0       Tx pause            0
Rx fcs err              0       Tx fcs err          0
Rx frames 64            0       Tx collisions       0
Rx frames 127           0       Tx multiple         0
Rx frames 255           0       Tx excessive        0
Rx frames 511           0       Tx late collision   0
Rx frames 1023          0       Tx deferred         0
Rx frames max           0
Rx bad octets           0
Rx undersize            0
Rx fragments            0
Rx oversize             0
Rx jabber               0
Rx mac rcv err          0
```

19.1.3 show controllers ethernet-controller

Команда фундаментального режима. Вывод информации об интерфейсах.

Синтаксис команды:

show controllers ethernet-controller [*interface-id***]**

Параметры команды:

interface-id идентификатор интерфейса для вывода информации (tengigabitethernet 0/1, gigabitethernet 0/1)

Значение по умолчанию:

По умолчанию вывод настроек и статистики для всех интерфейсов.

Примеры команды:

```
admin@Switch# show controllers ethernet-controller gigabitethernet 0/1
gigabitethernet 0/2
_____________________________________________

Rx good octets          204301
Tx octets               57171155

Rx unicasts             1475    Tx unicasts         4277
Rx multicasts           778     Tx multicasts       7699
Rx broadcasts           3       Tx broadcasts       808742
Rx pause                0       Tx pause            0
Rx fcs err              0       Tx fcs err          0
Rx frames 64            650     Tx collisions       0
Rx frames 127           816887  Tx multiple         0
Rx frames 255           816     Tx excessive        0
Rx frames 511           4552    Tx late collision   0
Rx frames 1023          16      Tx deferred         0
Rx frames max           53
Rx bad octets           0
Rx undersize            0
Rx fragments            0
Rx oversize             0
Rx jabber               0
Rx mac rcv err          0
admin@Switch#
```

19.1.4 show controllers utilization

Команда фундаментального режима. Вывод информации об использовании пропускной способности интерфейсов.

Синтаксис команды:

show controllers [*interface-id***] utilization**

Параметр команды:

interface-id идентификатор интерфейса для вывода информации (tengigabitethernet 0/1, gigabitethernet 1/1)

Значение по умолчанию:

По умолчанию информация выводится для всех интерфейсов.

Использование команды:

Использование пропускной способности представляет собой среднее значение скорости проходящего потока данных для секунды, предшествовавшей команде вывода.

Пример команды:

```
admin@Switch# show controllers utilization
Port        Receive   Transmit
te0/1       0         0
te0/2       0         0
te0/3       0         0
te0/4       0         0
te0/5       0         0
te0/6       0         0
te0/7       0         0
<output truncated>
admin@Switch#
```

19.2 Настройка sFlow

19.2.1 Общие положения

Технология sFlow предназначена для мониторинга сетевых устройств. Поддерживается версия sFlow V5.

Протокол sFlow предоставляет следующие возможности:

- сэмплинг (выборка) пакетов, входящих и/или исходящих из сетевых интерфейсов;
- отправка статистики по интерфейсам через заданные интервалы.

Система мониторинга sFlow состоит из следующих частей:

- агент sFlow, реализованный на сетевом устройстве;
- приемник sFlow или анализатор sFlow.

sFlow V5 определяет механизмы семплинга, реализованные в агенте sFlow для мониторинга трафика, sFlow MIB для управления агентом sFlow и форматы данных, применяемые для передачи данных на приемник sFlow.

Дейтаграммы sFlow используются для немедленной отправки пакетов или статистики на анализатор sFlow.

sFlow обеспечивает сэмплинг пакетов с заданным интервалом.

Поддерживается следующая статистика по интерфейсам:

- общие счетчики интерфейсов (RFC2233);
- счетчики интерфейсов Ethernet (RFC2358).

Настройки пользователя

sFlow поддерживает следующие настройки:

1. Настройка режима сэмплинга входящих пакетов: сэмплинг всех пакетов или только пакетов, не отброшенных устройством.
2. Настройка sFlow-приемников:

- номер sFlow-приемников;
- IP-адрес;
- номер порта UDP назначения (по умолчанию равен 6343);
- максимальный размер UDP-дейтаграммы (по умолчанию равен 1400).

3. Настройка сэмплинга пакетов для каждого порта:

- номер sFlow-приемника;

- интервал сэмплинга в количестве пакетов «rate» (частота семплинга вычисляется как 1 rate, то есть для каждых rate пакетов на sFlow-приемник в среднем будет отправлен один пакет);
- выбор направления, с которого будет производиться сэмплинг: прием, передача или сразу оба направления (если параметр не задан, то сэмплинг производится для обоих направлений);
- максимальное количество байт, которые будут скопированы из пакета (если параметр не задан, то используется значение 128).

4. Настройка сэмплинга статистики для каждого порта:

- номер sFlow-приемника;
- интервал отправки в секундах.

ПО обеспечивает подсчет, отображение и сброс статистики по пакетам, отправленным на sFlow-приемники и отображение текущей конфигурации.

Дополнения и ограничения

Будьте осторожны при настройке высокой частоты сэмплинга, так как это может вызвать перегрузку CPU.

19.2.2 Порядок настройки

Порядок настройки sFlow на одном из портов устройства приведен в таблице 23.

Таблица 23 – Порядок настройки sFlow на одном из портов устройства

Команда	Назначение
configure terminal	Переход в режим глобальной настройки
sflow receiver *index* {*ipv4-address*}[**udp-port** <*0-65535*>][**max-datagram-size** *bytes*]	Настройка sFlow-приемника
sflow flow-sampling mode {all | nondropped}	(Опционально) Настройка режима сэмплинга входящих пакетов
interface *interface-id*	Переход в режим настройки интерфейса
sflow flow-sampling *rate receiver-index* [**direction {ingress | egress | both}**] [**maxheader-size** *bytes*]	Настройка сэмплинга пакетов на интерфейсе
sflow counters-sampling *interval receiver-index*	Настройка сэмплинга счетчиков на интерфейсе
show sflow configuration	Проверка конфигурации
exit	Переход в предыдущий режим настройки
exit	Переход в предыдущий режим настройки
copy running-config startup-config	Сохранение настроек

19.2.3 clear sflow statistics

Команда фундаментального режима. Сброс статистики sFlow.

Синтаксис команды:

clear sflow statistics [*interface-id*]

Параметры команды:

interface-id	(опционально) идентификатор интерфейса Ethernet

Указания по применению:

Используйте команду «**clear sflow statistics**» для сброса статистики sFlow. Если интерфейс не задан, то сброс производится для всех интерфейсов.

Пример команды:

Следующий пример показывает, как сбросить статистику sFlow на всех интерфейсах:

```
admin@Switch# clear sflow statistics
admin@Switch#
```

19.2.4 sflow flow-sampling mode

Команда глобальной настройки. Настройка режима сэмплинга входящих пакетов.

Синтаксис команды:

sflow flow-sampling mode {all | non-dropped}

no sflow flow-sampling mode

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

all	сэмплинг всех пакетов, за исключением пакетов с ошибками на уровне MAC (например, неверная CRC)
non-dropped	сэмплинг пакетов, которые не были отброшены

Значение по умолчанию:

Сэмплинг пакетов, которые не были отброшены.

Указания по применению:

Используйте команду «**sflow flow-sampling mode**» для режима сэмплинга пакетов.

Пример команды:

Следующий пример показывает, как настроить сэмплинг всех пакетов:

```
admin@Switch# configure terminal
admin@Switch(config)# sflow flow-sampling mode all
admin@Switch(config)#
```

19.2.5 sflow receiver

Команда глобальной настройки. Настройка приемника sFlow.

Синтаксис команды:

sflow receiver *index* {*ipv4-address*}**[udp-port** *<0-65535>***][max-datagram-size** *bytes***]**

no sflow receiver *index*

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

index	номер приемника sFlow в диапазоне 1–8
ipv4-address	IP-адрес sFlow-приемника
udp-port *port*	(опционально) номер порта UDP назначения в диапазоне 0-65535. Если не задан, то используется значение 6343
max-datagram-size *bytes*	(опционально) максимальный размер UDP-дейтаграммы. Если не задан, то используется значение 1400

Значение по умолчанию:

sFlow-приемники не заданы.

Указания по применению:

Используйте команду «**sflow receiver**» для определения и настройки приемника sFlow. Если задан IP-адрес, равный “0.0.0.0”, то отправка пакетов на приемник не производится.

Пример команды:

Следующий пример показывает, как настроить sFlow-приемник:

```
admin@Switch# configure terminal
admin@Switch(config)# sflow receiver 1 10.0.0.1 udp-port 5000 max-datagram-size 1400
admin@Switch(config)#
```

19.2.6 sflow flow-sampling

Команда настройки интерфейса Ethernet. Включение сэмплинга пакетов и настройки средней частоты сэмплинга на интерфейсе.

Синтаксис команды:

sflow flow-sampling *rate receiver-index* **[direction {ingress | egress | both}] [max-header-size** *bytes***]**

no sflow flow-sampling

Команда с приставкой «**no**» отключает сэмплинг.

Параметры команды:

rate	интервал сэмплинга в диапазоне: 512-1073741823 пакетов
receiver-index	номер приемника sFlow в диапазоне 1–8
max-header-size *bytes*	(опционально) максимальное количество байт, которые будут скопированы из пакета в диапазоне 20–256. Если параметр не задан, то используется значение 128

direction {ingress | egress | both} (опционально) выбор направления, для которого производится сэмплинг:

- ingress – сэмплинг входящих пакетов.
- egress – сэмплинг исходящих пакетов.
- both – сэмплинг входящих и исходящих пакетов.

Если параметр не задан, то сэмплинг производится для обоих направлений

Значение по умолчанию:

Сэмплинг пакетов отключен.

Указания по применению:

Используйте команду «**sflow flow-sampling**» для включения сэмплинга пакетов и настройки средней частоты сэмплинга на интерфейсе.

Частота сэмплинга вычисляется как 1 rate, то есть для каждых rate пакетов на sFlow-приемник в среднем будет отправлен один пакет.

Будьте осторожны при настройке высокой частоты сэмплинга, так как это может вызвать перегрузку CPU.

Используйте команду глобальной настройки «**sflow receiver**» для определения и настройки приемника sFlow.

Пример команды:

Следующий пример показывает, как настроить сэмплинг каждого 2000-го пакета на интерфейсе gigabitethernet 0/1 с отправкой на sFlow-приемник с номером 1:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# sflow flow-sampling 2000 1
admin@Switch(config-if)#
```

19.2.7 sflow counters-sampling

Команда настройки интерфейса Ethernet. Включение сэмплинга статистики и настройки интервала сэмплинга на интерфейсе.

Синтаксис команды:

sflow counters-sampling *interval receiver-index*

no sflow counters-sampling

Команда с приставкой «**no**» отключает сэмплинг.

Параметры команды:

interval интервал сэмплинга в диапазоне: 1–86400 сек

receiver-index номер приемника sFlow в диапазоне 1–8

Значение по умолчанию:

Сэмплинг пакетов отключен.

Указания по применению:

Используйте команду «**sflow counters-sampling**» для включения сэмплинга статистики и настройки интервала сэмплинга на интерфейсе.

Используйте команду глобальной настройки «**sflow receiver**» для определения и настройки приемника sFlow.

Пример команды:

Следующий пример показывает, как настроить сэмплинг статистики на интерфейсе gigabitethernet 0/1 с отправкой на sFlow-приемник с номером 1 и интервалом отправки 300 секунд:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# sflow counters-sampling 300 1
admin@Switch(config-if)#
```

19.2.8 show sflow configuration

Команда, доступная из любого режима. Вывод настроек sFlow.

Синтаксис команды:

show sflow configuration [*interface-id*]

Параметры команды:

interface-id (опционально) идентификатор интерфейса Ethernet

Указания по применению:

Используйте команду «**show flow configuration**» для вывода настроек sFlow на всех или определенном интерфейсе. Если идентификатор интерфейса не задан, то выводятся все настройки.

Пример команды:

Следующий пример показывает, как вывести все настройки sFlow:

```
admin@Switch# show sflow configuration
Ingress flow sampling mode: all
Receivers
Index     IP Address   Port      Max Datagram Size
-----     ----------   ----      -----------------
1         10.0.0.1     6343      1400
2         172.16.1.1   5000      1400

          Flow         Counters                            Flow      Counters
Interface Sampling     Sampling  Max Header   Direction    Collector Collector
--------- --------     --------  ----------   ---------    --------- ---------
gi0/1     1/2048       60 sec    128          Both         1         1
gi0/2     1/4096       Disabled  128          Egress       2         2
```

19.2.9 show sflow statistics

Команда, доступная из любого режима. Вывод статистики sFlow на интерфейсах с включенным сэмплингом пакетов или статистики.

Синтаксис команды:

show sflow statistics [interface-id]

Параметры команды:

interface-id (опционально) идентификатор интерфейса Ethernet

Указания по применению:

Используйте команду «**show sflow statistics**» для вывода статистики sFlow на интерфейсах с включенным сэмплингом пакетов или статистики. Если идентификатор интерфейса не задан, то выводится статистика для всех интерфейсов со включенным сэмплингом пакетов или статистики.

Пример команды:

Следующий пример показывает, как вывести статистику sFlow:

```
admin@Switch# show sflow statistics
Total sFlow datagrams sent to collectors: 100
Interface  Packets
           sampled
---------  -------
gi0/1      30
gi0/2      50
```

20 Управление, мониторинг и контроль сетевой инфраструктуры

20.1 Настройка LLDP

20.1.1 Общие положения

Link Layer Discovery Protocol (LLDP) – протокол канального уровня, позволяющий сетевому оборудованию оповещать локальную сеть о своем существовании и характеристиках, а также собирать такие же оповещения, поступающие от соседнего оборудования.

Протокол формально утвержден как стандарт IEEE 802.1AB-2009 в сентябре 2009 года и является независимой (от производителей сетевого оборудования) заменой патентованных протоколов, таких как Cisco Discovery Protocol, Extreme Discovery Protocol, Foundry Discovery Protocol и Nortel Discovery Protocol. Протокол LLDP предназначен для обмена следующей информацией:

- имя и описание системы;
- имя и описание порта;
- имя VLAN;
- IP-адреса управления;
- возможности системы (коммутация, маршрутизация и т.п.);
- информация о MAC и PHY;
- информация о PoE (MDI power);
- агрегация линков.

20.1.2 clear lldp table

Команда фундаментального режима. Очистка информации о соседях для всех или определенного интерфейса.

Синтаксис команды:
clear lldp table interface [*interface-id*]
Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Значение по умолчанию:
Не применимо.
Пример команды:

```
admin@Switch# clear lldp table interface gigabitethernet 0/1
admin@Switch#
```

20.1.3 debug lldp

Команда фундаментального режима. Включение отладки LLDP.
Синтаксис команды:
debug lldp {all | errors | packets}
no debug lldp {all | errors | packets}
Команда с приставкой «**no**» отключает отладку LLDP.
Параметры команды:

all	вывод всей диагностической информации
errors	вывод информации об ошибках LLDP
packets	вывод информации о полученных пакетах LLDP

Пример команды:

```
admin@Switch# debug lldp all
admin@Switch#
```

20.1.4 clear lldp statistics

Команда фундаментального режима. Очистка статистики LLDP для всех или определенного интерфейса.
Синтаксис команды:
clear lldp statistics [interface *interface-id***]**
Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Значение по умолчанию:
Не применимо.
Пример команды:

```
admin@Switch# clear lldp statistics interface gigabitethernet 0/1
admin@Switch#
```

20.1.5 lldp hold-multiplier

Команда глобальной настройки. Установка множителя времени актуальности полученных данных LLDP перед их удалением.
Синтаксис команды:
lldp hold-multiplier *number*
no lldp hold-multiplier
Команда с приставкой «**no**» устанавливает значение по умолчанию.
Параметры команды:

number	множитель времени актуальности полученных данных LLDP в диапазоне от 2 до 10

Значение по умолчанию:

Множитель времени актуальности равен 4.

Использование команды:

Команда «**lldp hold-multiplier**» используется для настройки множителя времени актуальности полученных данных LLDP перед их удалением.

Фактическое время актуальности полученных данных LLDP (Time-to-Live) вычисляется по формуле 1:

$$TTL = min(65535, \backslash LLDP - Timer" * \backslash LLDP - hold - multiplier") \qquad (2)$$

Например, если значение таймера LLDP равно 30 секундам и значение множителя актуальности данных LLDP равно 4, то в поле TTL заголовка пакета LLDP будет записано значение 120. Команда «**lldp hold-multiplier**» используется для настройки интервала отправки обновлений LLDP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp hold-multiplier 5
admin@Switch(config)#
```

20.1.6 lldp med fast-start repeat-count

Команда глобальной настройки. Установка количества пакетов, которые будут отправлены при появлении соединения на порту.

Синтаксис команды:

lldp med fast-start repeat-count *number*

no lldp med fast-start repeat-count

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

number	количество пакетов, которые будут отправлены при появлении соединения на порту, в диапазоне от 1 до 10

Значение по умолчанию:

При появлении соединения на порту отправляется 3 пакета LLDP.

Использование команды:

Команда «**lldp med fast-start repeat-count**» используется для настройки количества пакетов, которые будут отправлены при появлении соединения на порту.

При появлении соединения на порту LLDP может отправлять пакеты с меньшим интервалом для ускорения обмена параметрами с удаленным устройством.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp med fast-start repeat-count 3
admin@Switch(config)#
```

20.1.7 lldp med network-policy (глобальная настройка)

Команда глобальной настройки. Добавление сетевых политик LLDP-MED.

Синтаксис команды:

lldp med network-policy *number application* **[vlan** *vlan-id* **] [vlan-type {tagged | untagged}] [up** *priority***] [dscp** *value***]**

no lldp med network-policy *number*

Команда с приставкой «**no**» удаляет сетевые политики LLDP-MED.

Параметры команды:

number	номер сетевой политики в диапазоне от 1 до 65535
application	название основной функции приложения для сетевой политики: – voice; – voice-signaling; – guest-voice; – guest-voice-signaling; – softphone-voice; – video-conferencing; – streaming-video; – video-signaling.
vlan *vlan-id*	идентификатор VLAN для приложения
vlan-type	тип передаваемого трафика: – tagged – трафик с тегом VLAN; – untagged – трафик без тега VLAN.
up *priority*	приоритет 802.1p для приложения. Имеет смысл только при передаче трафика с тегом VLAN
dscp *value*	приоритет DSCP (TC) для приложения. Имеет смысл только при передаче IP-трафика (IPv4/IPv6)

Значение по умолчанию:

Сетевые политики LLDP-MED отсутствуют.

Использование команды:

Команда «**lldp med network-policy**» используется для добавления сетевых политик LLDP-MED.

Созданные сетевые политики LLDP-MED можно назначить на требуемый интерфейс с помощью команды настройки интерфейса «**lldp med network-policy**». На один порт можно назначить до 32 сетевых политик.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp med network-policy 1 voice-signaling vlan 1
                                vlan-type untagged up 1 dscp 2
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lldp med network-policy add 1
admin@Switch(config-if)#
```

20.1.8 lldp reinit

Команда глобальной настройки. Установка минимального интервала ожидания LLDP перед повторной инициализацией передачи.

Синтаксис команды:

lldp reinit *seconds*

no lldp reinit

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	минимальный интервал ожидания LLDP перед повторной инициализацией передачи в диапазоне от 1 до 10 секунд

Значение по умолчанию:

Интервал равен 2 секундам.

Использование команды:

Команда «**lldp reinit**» используется для установки минимального интервала ожидания LLDP перед повторной инициализацией передачи.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp reinit 3
admin@Switch(config)#
```

20.1.9 lldp run

Команда глобальной настройки. Включение LLDP на устройстве.

Синтаксис команды:

lldp run

no lldp run

Команда с приставкой «**no**» отключает LLDP на устройстве.

Значение по умолчанию:

LLDP включен.

Использование команды:

Команда «**lldp run**» используется для включения LLDP на устройстве.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp run
admin@Switch(config)#
```

20.1.10 lldp timer

Команда глобальной настройки. Установка интервала отправки обновлений LLDP.

Синтаксис команды:

lldp timer *seconds*

no lldp timer

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	интервал отправки обновлений LLDP в диапазоне от 5 до 32768 секунд

Значение по умолчанию:

Интервал отправки обновлений LLDP равен 30 секундам.

Использование команды:

Команда «**lldp timer**» используется для установки интервала отправки обновлений LLDP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp timer 60
admin@Switch(config)#
```

20.1.11 lldp tx-delay

Команда глобальной настройки. Установка задержки перед последовательной отправкой двух пакетов LLDP, инициированной из-за изменений локальных настроек или состояний устройства.

Синтаксис команды:

lldp tx-delay *seconds*

no lldp tx-delay

Команда с приставкой «**no**» устанавливает значение по умолчанию.

Параметры команды:

seconds	задержка перед последовательной отправкой двух пакетов LLDP, инициированной из-за изменений локальных настроек или состояний устройства. Диапазон значений: от 1 до 8192 секунд

Значение по умолчанию:

Задержка перед последовательной отправкой двух пакетов LLDP равна 2 секундам.

Использование команды:

Команда «**lldp tx-delay**» используется для установки задержки перед последовательной отправкой двух пакетов LLDP, инициированной из-за изменений локальных настроек или состояний устройства.

Рекомендуется устанавливать задержку меньше, чем ¼ интервала отправки обновлений LLDP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp tx-delay 2
admin@Switch(config)#
```

20.1.12 lldp management-address

Команда настройки интерфейса (Ethernet). Установка анонсируемого интерфейсом IP-адреса управления.

Синтаксис команды:

lldp management-address {*ip-address* | **none** | **automatic**}

no lldp management-address

Команда с приставкой «**no**» отключает анонсирование IP-адреса управления.

Параметры команды:

ip-address	статический IP-адрес управления
none	отключение анонсирования IP-адреса управления
automatic	автоматическое определение анонсируемого IP-адреса управления из числа IP-адресов, настроенных на VLAN, членами которых является интерфейс

Значение по умолчанию:

Анонсирование IP-адреса управления в режиме «**automatic**».

Использование команды:

Команда «**lldp management-address**» используется для установки анонсируемого интерфейсом IP-адреса управления.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lldp management-address 10.0.0.1
admin@Switch(config-if)#
```

20.1.13 lldp med-select-tlv

Команда настройки интерфейса (Ethernet). Добавление TLV LLDP-MED к списку TLV, анонсируемых на интерфейсе.

Синтаксис команды:

lldp med-select-tlv [*tlv-list*]

no lldp med-select-tlv [*tlv-list*]

Команда с приставкой «**no**» удаляет TLV из списка TLV, анонсируемых на интерфейсе.

Параметры команды:

tlv-list список TLV, которые нужно добавить или удалить из списка TLV, анонсируемых на интерфейсе. Если параметр не указан, то действие применяется ко всем поддерживаемым TLV. Поддерживаемые TLV:

- capabilities;
- network-policy;
- if-location;
- ext-power-via-mdi;
- hw-rev;
- fw-rev;
- sw-rev;
- serial-num;
- manufacturer;
- model-name;
- asset-id.

Значение по умолчанию:

Анонсируются все TLV LLDP-MED.

Использование команды:

Команда «**lldp med-select-tlv**» используется для добавления TLV LLDP-MED к списку TLV, анонсируемых на интерфейсе.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lldp med-select-tlv if-location
admin@Switch(config-if)#
```

20.1.14 lldp med location

Команда настройки интерфейса (Ethernet). Настройка информации о местоположении на интерфейсе.

Синтаксис команды:

lldp med if-location {coordinate *data* **| civic-address** *data* **| ecs-elin** *data***}**

no lldp med if-location {coordinate | civic-address | ecs-elin}

Команда с приставкой «**no**» удаляет информацию о местоположении.

Параметры команды:

coordinate *data*	информация о местоположении в виде координат. Координаты должны быть в шестнадцатеричном формате. Длина: 16 байт
civic-address *data*	информация о местоположении в виде адреса. Адрес должен быть в шестнадцатеричном формате. Длина: от 6 до 160 байт
ecs-elin *data*	информация о местоположении в виде идентификационного номера службы спасения (Emergency Call Service Emergency Location Identification Number). Идентификационный номер должен быть в шестнадцатеричном формате. Длина: от 10 до 25 байт
data	информация о местоположении в формате, соответствующем ANSI/TIA 1057: шестнадцатеричный формат с разделением байтов точкой или двоеточием (каждому байту соответствуют две шестнадцатеричные цифры)

Значение по умолчанию:

Информации о местоположении отсутствует.

Использование команды:

Команда «**lldp med if-location**» используется для настройки информации о местоположении на интерфейсе.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lldp med if-location civic-address 616263646566
admin@Switch(config-if)#
```

20.1.15 lldp med network-policy (настройка интерфейса)

Команда настройки интерфейса (Ethernet). Добавление или удаление сетевой политики LLDP MED на интерфейсе.

Синтаксис команды:

lldp med network-policy {add | remove} *number*

no lldp med network-policy

Команда с приставкой «**no**» удаляет все сетевые политики с интерфейса.

Параметры команды:

number	номер сетевой политики в диапазоне от 1 до 65535
add	добавление сетевой политики LLDP-MED на интерфейс
remove	удаление сетевой политики LLDP-MED с интерфейса

Значение по умолчанию:

На интерфейсах отсутствуют сетевые политики.

Использование команды:

Команда «**lldp med network-policy**» используется для добавления или удаления сетевой политики LLDP-MED на интерфейсе.

На каждый порт можно назначить только одну сетевую политику каждого типа приложения (например, “voice”, “voice-signalling” и т.д.).

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# lldp med network-policy 1 voice-signaling vlan 1
                                vlan-type untagged up 1 dscp 2
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lldp med network-policy add 1
admin@Switch(config-if)#
```

20.1.16 lldp select-tlv

Команда настройки интерфейса (Ethernet). Добавление опциональных TLV LLDP к списку TLV, анонсируемых на интерфейсе.

Синтаксис команды:

lldp select-tlv [*tlv-list*]

no lldp select-tlv [*tlv-list*]

Команда с приставкой «**no**» удаляет опциональные TLV LLDP из списка TLV, анонсируемых на интерфейсе.

Параметры команды:

tlv-list список TLV, которые нужно добавить или удалить из списка TLV, анонсируемых на интерфейсе. Если параметр не указан, то действие применяется ко всем поддерживаемым TLV. Поддерживаемые TLV:

- port-desc;
- sys-name;
- sys-desc;
- sys-cap;
- 802.1-pvid;
- 802.1-vlan-name;
- 802.3-mac-phy;
- 802.3-power-via-mdi;
- 802.3-max-frame-size.

Значение по умолчанию:

Анонсируются все опциональные TLV.

Использование команды:

Команда «**lldp select-tlv**» используется для добавления опциональных TLV LLDP к списку TLV, анонсируемых на интерфейсе.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface tengigabitethernet 0/1
admin@Switch(config-if)# lldp select-tlv port-desc
admin@Switch(config-if)#
```

20.1.17 lldp receive

Команда настройки интерфейса (Ethernet). Включение приема пакетов LLDP на интерфейсе.

Синтаксис команды:

lldp receive

no lldp receive

Команда с приставкой «**no**» отключает прием пакетов LLDP на интерфейсе.

Значение по умолчанию:

Прием пакетов LLDP включен.

Использование команды:

Команда «**lldp receive**» используется для включения приема пакетов LLDP на интерфейсе.

LLDP получает и принимает информацию индивидуально для каждого интерфейса. Параметры LLDP, полученные на портах в группах агрегации (LAG), хранятся независимо для каждого интерфейса.

Прием пакетов LLDP не зависит от состояния Spanning Tree на порту, то есть пакеты LLDP принимаются на портах, заблокированных Spanning Tree.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lldp receive
admin@Switch(config-if)#
```

20.1.18 lldp transmit

Команда настройки интерфейса (Ethernet). Включение передачи пакетов LLDP на интерфейсе.

Синтаксис команды:

lldp transmit

no lldp transmit

Команда с приставкой «**no**» отключает передачу пакетов LLDP на интерфейсе.

Значение по умолчанию:

Передача пакетов LLDP включена.

Использование команды:

Команда «**lldp transmit**» используется для включения передачи пакетов LLDP на интерфейсе.

LLDP получает и принимает информацию индивидуально для каждого интерфейса. Параметры LLDP, полученные на портах в группах агрегации (LAG), хранятся независимо для каждого интерфейса.

Передача пакетов LLDP не зависит от состояния Spanning Tree на порту, то есть пакеты LLDP передаются на портах, заблокированных Spanning Tree.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# lldp transmit
admin@Switch(config-if)#
```

20.1.19 show lldp configuration

Команда фундаментального режима. Вывод конфигурации LLDP на всех или определенном интерфейсе.

Синтаксис команды:

show lldp configuration interface [*interface-id*]

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show lldp configuration**» используется для вывода конфигурации LLDP на всех или определенном интерфейсе. Если введена команда без аргументов, то выводится информация для всех интерфейсов.

Примеры команды:

```
admin@Switch# show lldp configuration gigabitethernet 0/1
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5

Port    State   Optional TLVs      Address      Notifications
-----   -----   -------------      ----------   -------------
gi0/1   RX,TX   PD,SN,SD,SC        172.16.1.1   Disabled
802.3 optional TLVs: 802.3-mac-phy, 802.3-lag, 802.3-max-frame-size
802.1 optional TLVs:
  PVID: Enabled
  PPVIDs: 0, 1, 92
  VLANs: 1, 92
  Protocols: 802.1x
```

```
admin@Switch# show lldp configuration
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
Notifications interval: 5

Port    State   Optional TLVs      Address       Notifications
-----   -----   -------------      ----------    -------------
gi0/1   RX,TX   PD,SN,SD,SC        172.16.1.1    Disabled
gi0/2   TX      PD,SN              172.16.1.1    Disabled
gi0/3   RX,TX   PD,SN              None          Disabled
gi0/4   RX,TX   PD,SN              automatic     Disabled
```

20.1.20 show lldp local

Команда фундаментального режима. Вывод информации, которая анонсируется устройством на всех или определенном интерфейсе.

Синтаксис команды:

show lldp local [interface *interface-id* **]**

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show lldp local**» используется для вывода информации, которая анонсируется устройством на всех или определенном интерфейсе. Если введена команда без аргументов, то выводится информация для всех интерфейсов.

Примеры команды:

```
    LLDP-MED Inventory
      Hardware Revision: B1
      Firmware Revision: A1
      Software Revision: 2.3.0
      Serial number: 123456
      Manufacturer name: Polygon JSC
      Model name: Акманай-2xxx
      Asset ID: 123
```

```
admin@Switch# show lldp local gigabitethernet 0/1
LLDP is disabled.
```

```
admin@Switch# show lldp local gigabitethernet 0/1
Local LLDP information on gigabitethernet 0/1
  LLDP:
    Device ID: 00:1B:28:00:00:01
    Port ID: gi0/1
    Capabilities: Bridge
    System Name: Акманай-2xxx
    System description:
    Port description:
    Management address: 10.0.0.1
  LLDP IEEE 802.3:
    802.3 MAC/PHY Configuration/Status
    Auto-negotiation support: Supported
    Auto-negotiation status: Enabled
    Auto-negotiation Advertised Capabilities: 100BASE-TX full duplex,
    1000BASE-T full duplex
    Operational MAU type: 1000BaseTFD
    802.3 Link Aggregation
    Aggregation capability: Capable of being aggregated
    Aggregation status: Not currently in aggregation
    Aggregation port ID: 1
    802.3 Maximum Frame Size: 10000
    802.3 EEE
    Local Tx: 30 usec
    Local Rx: 25 usec
    Remote Tx Echo: 30 usec
    Remote Rx Echo: 25 usec
  LLDP IEEE 802.1:
    802.1 PVID: 1
    802.1 PPVID: 2 supported, enabled
    802.1 VLAN: 2 (VLAN2)
    802.1 Protocol: 88 8E 01
  LLDP-MED:
    LLDP-MED capabilities: Network Policy, Location Identification
    LLDP-MED Device type: Network Connectivity
    LLDP-MED Network policy
      Application type: Voice
      Flags: Tagged VLAN
      VLAN ID: 2
      Layer 2 priority: 0
      DSCP: 0
    LLDP-MED Power over Ethernet
      Device Type: Power Sourcing Entity
      Power source: Primary Power Source
      Power priority: High
      Power value: 9.6 Watts
    LLDP-MED Location
      Coordinates: 54:53:c1:f7:51:57:50:ba:5b:97:27:80:00:00:67:01
```

20.1.21 show lldp med configuration

Команда фундаментального режима. Вывод конфигурации LLDP-MED на всех или определенном интерфейсе.

Синтаксис команды:

show lldp med configuration [interface *interface-id***]**

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show lldp med configuration**» используется для вывода конфигурации LLDP-MED на всех или определенном интерфейсе. Если введена команда без аргументов, то выводится информация для всех интерфейсов.

Примеры команды:

```
admin@Switch# show lldp med configuration
Fast Start Repeat Count: 4.
Network policy 1
----------
Application type: voiceSignaling
VLAN ID: 1 untagged
Layer 2 priority: 0
DSCP: 0

Port    Capabilities Network Policy    Location     Notifications      Inventory
-----   ------------ --------------    --------     -------------      ---------
gi0/1   Yes          Yes               Yes          Enabled            Yes
gi0/2   Yes          Yes               Yes          Enabled            No
gi0/3   No           No                Yes          Enabled            No
gi0/4   Yes          No                Yes          Disabled           Yes
```

```
admin@Switch# show lldp med configuration gigabitethernet 0/1
Port    Capabilities Network Policy    Location     Notifications      Inventory
-----   ------------ --------------    --------     -------------      ---------
gi0/1   Yes          Yes               Yes          Enabled            Yes

Network policies:
Location:
Civic-address: 61:62:63:64:65:66
```

20.1.22 show lldp neighbors

Команда фундаментального режима. Вывод информации о соседних устройствах, обнаруженных протоколом LLDP, на всех или определенном интерфейсе.

Синтаксис команды:

show lldp neighbors [interface *interface-id*]

Параметры команды:

interface-id	идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show lldp neighbors**» используется для вывода информации о соседних устройствах, обнаруженных протоколом LLDP, на всех или определенном интерфейсе. Если введена команда без аргументов, то выводится информация для всех интерфейсов.

Пример команды:

```
admin@Switch(config)# show lldp neighbors interface gigabitethernet 0/2
Neighbor LLDP information on gigabitethernet0/2
  LLDP:
    Device ID: 00:1B:28:02:60:40
    Port ID: gi 0/1
    Capabilities:
    System Name:
    System Description:
    Port Description:
    Management Address: 192.168.10.225
  LLDP-MED:
    LLDP-MED capabilities: Inventory, Location Identification, Network Policy
    LLDP-MED Device type: Network Connectivity
    LLDP-MED Inventory
    Hardware Revision: 2.0
    Firmware Revision: 2.0
    Software Revision: 2.3.11-d13
    Serial Number: 907505
    Manufacturer Name: Polygon JSC
    Model Name: Акманай-2xxx
    Asset ID:
```

20.1.23 show lldp statistics

Команда фундаментального режима. Вывод статистики LLDP для всех или определенного интерфейса.

Синтаксис команды:

show lldp statistics [interface *interface-id***]**

Параметры команды:

interface-id идентификатор интерфейса (Ethernet)

Использование команды:

Команда «**show lldp statistics**» используется для вывода статистики LLDP для всех или для определенного интерфейса.

Пример команды:

```
admin@Switch(config)# show lldp statistics

LLDP global counters:
Neighbors entries was last changed at 17:40:00 Dec 25 2020.
Total Neighbors Entries Added 0.
Total Neighbors Entries Deleted 0.
Total Neighbors Entries Dropped 0.
Total Neighbors Entries Aged Out 0.

LLDP local counters:
Interface                   Rx Frames    Tx Frames    Rx Unknown   Organiz      Aged
--------------------        ---------    ---------    ----------   -------      ----
TenGigabitEthernet0/1       0            0            0            0            0
TenGigabitEthernet0/2       0            0            0            0            0
TenGigabitEthernet0/3       0            0            0            0            0
TenGigabitEthernet0/4       0            0            0            0            0
```

20.2 Настройка CFM OAM

20.2.1 ethernet cfm domain

Команда глобальной настройки. Создание домена обслуживания CFM определенного уровня и переход в режим настройки домена CFM.

Синтаксис команды:

ethernet cfm domain *domain-name* **level** *level-id*

no ethernet cfm domain *domain-name* **level** *level-id*

Используйте команду «**no ethernet cfm domain**» для удаления домена обслуживания CFM.

Описание синтаксиса:

domain-name	имя домена длиной от 1 до 154 символов
level-id	уровень обслуживания в диапазоне от 0 до 7

Значение по умолчанию:

Домены управления CFM не заданы.

Указания по применению:

Используйте команду «**ethernet cfm domain**» для создания домена обслуживания CFM определенного уровня и перехода в режим настройки домена CFM. Для одного и того же уровня обслуживания можно создать несколько доменов, однако один домен может принадлежать только одному уровню обслуживания.

Пример команды:

Следующий пример показывает, как создать домен обслуживания “TEST”, назначить уровень обслуживания “5”, создать привязки имени сообщества точек обслуживания “10” и включить отправку сообщений проверки связности:

```
admin@Switch# configure terminal
admin@Switch(config)# ethernet cfm domain TEST level 5
admin@Switch(config-cfm)# service 10 vlan 1000
admin@Switch(config-cfm-srv)# continuity-check
admin@Switch(config-cfm-srv)#
```

20.2.2 service instance ethernet

Команда настройки интерфейса (Ethernet). Создание экземпляра сервиса на интерфейсе.

Синтаксис команды:

service instance *id* **ethernet** *ma-num*

no service instance *id* **ethernet** *ma-num*

Используйте команду «**no service instance ethernet**» для удаления экземпляра сервиса с интерфейса.

Описание синтаксиса:

id	идентификатор экземпляра сервиса в диапазоне от 1 до 4294967295
ma-num	номер сообщества точек обслуживания от 0 до 65535

Значение по умолчанию:

Экземпляры сервисов отсутствуют.

Указания по применению:

Используйте команду «**service instance ethernet**» для создания экземпляра сервиса на интерфейсе.

Пример команды:

Следующий пример показывает, как создать экземпляр сервиса “100” на интерфейсе gigabitethernet 0/1 для сообщества точек обслуживания “10”:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# service instance 100 ethernet 10
admin@Switch(config-if-srv)#
```

20.2.3 service

Команда настройки домена CFM. Создание привязки имени сообщества точек обслуживания и переход в режим настройки сервиса CFM.

Синтаксис команды:

service *ma-name* **vlan** *vlan-id* **[direction down]**

no service *ma-name* **vlan** *vlan-id* **[direction down]**

Используйте команду «**no service**» для удаления сервиса.

Описание синтаксиса:

ma-name	имя сообщества точек обслуживания длиной от 1 до 32 символов
vlan-id	номер VLAN в диапазоне от 1 до 4094
direction down	(опционально) направление сервиса в сторону порта (для создания Down MEP). По умолчанию направление сервиса в сторону устройства (для создания Up MEP)

Значение по умолчанию:

Привязки отсутствуют.

Указания по применению:

Используйте команду «**service**» для создания привязки имени сообщества точек обслуживания и перехода в режим настройки сервиса CFM.

Одно имя сообщства «*ma-name*» может быть привязано только к одному VLAN.

Пример команды:

Следующий пример показывает, как создать домен обслуживания “TEST”, назначить уровень обслуживания “5”, создать привязки имени сообщества точек обслуживания “10” и включить отправку сообщений проверки связности:

```
admin@Switch# configure terminal
admin@Switch(config)# ethernet cfm domain TEST level 5
admin@Switch(config-cfm)# service 10 vlan 1000
admin@Switch(config-cfm-srv)# continuity-check
admin@Switch (config-cfm-srv)#
```

20.2.4 continuity-check

Команда глобальной настройки. Включение и настройка параметров сообщений проверки связности (Continuity Check Messages).

Синтаксис команды:

continuity-check [interval *time* **| loss-threshold** *threshold* **]**

no continuity-check [interval *time* **| loss-threshold** *threshold* **]**

Используйте команду «**no continuity-check**» для отключения сообщений проверки связности или установки настроек в значения по умолчанию.

Описание синтаксиса:

time — интервал отправки сообщений CFM:

1. 3.3ms – 3.3 миллисекунды;
2. 10ms – 10 миллисекунд;
3. 100ms – 100 миллисекунд;
4. 1s – 1 секунда;
5. 10s – 10 секунд;
6. 1m – 1 минута;
7. 10m – 10 минут

По умолчанию параметр равен 100 миллисекундам

threshold — количество подряд потерянных фреймов, после которых удаленная точка обслуживания считается вышедшей из строя. Диапазон значений от 2 до 255. По умолчанию параметр равен 3

Значение по умолчанию:

Передача сообщений проверки связности отключена.

Указания по применению:

Используйте команду «**continuity-check**» для включения и настройки параметров сообщений проверки связности (Continuity Check Messages).

Команды «**continuity-check**» или «**no continuity-check**» с параметрами «**interval**» или «**loss-threshold**» только изменяют значения соответствующих параметров. Режим передачи сообщений проверки связности при этом не изменяется.

Пример команды:

Следующий пример показывает, как создать домен обслуживания “TEST”, назначить уровень обслуживания “5”, создать привязки имени сообщества точек обслуживания “MA_1” и включить отправку сообщений проверки связности:

```
admin@Switch# configure terminal
admin@Switch(config)# ethernet cfm domain TEST level 5
admin@Switch(config-cfm)# service MA_1 vlan 1000
admin@Switch(config-cfm-srv)# continuity-check
admin@Switch(config-cfm-srv)#
```

20.2.5 cfm mep domain

Команда настройки экземпляров сервисов CFM. Создание точки обслуживания (maintenance point) на определенном домене.

Синтаксис команды:

cfm mep domain *domain-name* **mpid** *mpid-value* **[cos** *cos-value* **]**

no cfm mep domain *domain-name* **mpid** *mpid-value*

Используйте команду «**no cfm mep domain**» для удаления точки обслуживания.

Описание синтаксиса:

domain-name	имя домена длиной от 1 до 154 символов
mpid-value	номер точки обслуживания (maintenance point ID) в диапазоне от 1 до 8192
cos-value	(опционально) класс обслуживания пакетов CFM в диапазоне от 0 до 7

Значение по умолчанию:

Точки обслуживания отсутствуют.

Указания по применению:

Используйте команду «**cfm mep domain**» для создания точки обслуживания (maintenance point) на определенном домене.

Пример команды:

Следующий пример показывает, как настроить точку обслуживания “100” на интерфейсе gigabitethernet 0/1 в домене “TEST”:

```
admin@Switch# configure terminal
admin@Switch(config)# interface gigabitethernet 0/1
admin@Switch(config-if)# service instance 100 ethernet 10
admin@Switch(config-if-srv)# cfm mep domain TEST mpid 100
admin@Switch(config-if-srv)#
```

20.2.6 show ethernet cfm errors

Команда, доступная из любого режима. Вывод информации об ошибках связности.

Синтаксис команды:

show ethernet cfm errors [domain *domain-name* **| level** *level-id* **]**

Описание синтаксиса:

domain-name	(опционально) имя домена длиной от 1 до 154 символов
level-id	уровень обслуживания в диапазоне от 0 до 7

Указания по применению:

Используйте команду «**show ethernet cfm errors**» для вывода информации об ошибках связности. Если команда введена без аргументов, то происходит вывод информации обо всех ошибках.

Пример команды:

Следующий пример показывает, как вывести информацию об ошибках связности:

```
admin@Switch# show ethernet cfm errors

MPID    Domain ID                                       MAC Address             Lvl
        MA Name                                         Reason                  Age
        Local MEP Identifier (MPID, Domain, MA)
----    ------------------------------------       --------------------    ---
1       TEST                                            00:1B:28:01:98:40       0
        MA_1                                            Remote MEP available    10s
1       TEST MA_1

admin@Switch#
```

20.3 Настройка SNMP

20.3.1 Общие положения

Коммутатор обеспечивает управление и мониторинг по протоколу SNMP (Simple Network Management Protocol) версии v3. Для SNMP версий v1, v2c доступен только мониторинг.

Включение управления и мониторинга по протоколу SNMP осуществляется с помощью команды «**snmp-server protocol enable**».

Установка версии протокола SNMP для управления и мониторинга осуществляется с помощью команды «**snmp-server protocol version**».

На коммутаторе реализованы следующие настройки SNMP:

- имя сообщества для чтения параметров в виде текстовой строки (рекомендуемая длина до 16 символов). Установка имени сообщества для чтения осуществляется с помощью команды «**snmp-server community**»;
- контактная информация ответственного лица в виде текстовой строки (рекомендуемая длина до 32 символов). Установка контактной информации ответственного лица осуществляется с помощью команды «**snmp-server contact**»;
- информация о местоположении аппаратуры в виде текстовой строки (рекомендуемая длина до 32 символов). Установка информация о местоположении аппаратуры осуществляется с помощью команды «**snmp-server location**»;
- имя контекста для SNMP-агента в виде текстовой строки (рекомендуемая длина до 32 символов). Установка имени контекста для SNMP-агента осуществляется с помощью команды «**snmp-server context**»;
- идентификатор движка SNMP в виде 5–32 пар шестнадцатеричных цифр, разделенных двоеточием. Установка идентификатор движка SNMP осуществляется с помощью команды «**snmp-server engineid**»;
- имя сообщества для отправки ловушек в виде текстовой строки (рекомендуемая длина до 16 символов). Задается в команде установки IP-адреса SNMP-менеджера. Включение отправки SNMP-ловушек по различным событиям осуществляется с помощью команды «**snmp-server traps**»;
- набор IP-адресов SNMP-менеджеров, на которые осуществляется отправка ловушек. Установка IP-адреса SNMP-менеджера осуществляется с помощью команды «**snmp-server host**»;
- настройки пользователей для SNMPv3: имя пользователя, пароль, режим авторизации и шифрования. Добавление и изменение параметров пользователей для протокола SNMPv3 осуществляется с помощью команды «**snmp-server user**».

Отображение настроек SNMP-агента осуществляется с помощью команды «**show snmp**».

20.3.2 snmp-server community

Команда глобальной настройки. Установка имени сообщества для чтения.

Синтаксис команды:

snmp-server community *name*

no snmp-server community

Команда с приставкой «**no**» устанавливает имя сообщества в значении «public».

Параметры команды:

name	имя сообщества в виде текстовой строки

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server community somename
admin@Switch(config)# end
admin@Switch#
```

20.3.3 snmp-server contact

Команда глобальной настройки. Установка контактной информации ответственного лица. Данный параметр доступен для чтения и записи по протоколу SNMP (параметр system.sysContact.0).

Синтаксис команды:

snmp-server contact *contact-info*

no snmp-server contact

Команда с приставкой «**no**» устанавливает контактную информацию в значении «no contact».

Параметры команды:

contact-info	контактная информация в виде текстовой строки (рекомендуемая длина до 32 символов)

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server contact Ivanov Ivan Ivanovich
admin@Switch(config)# end
admin@Switch#
```

20.3.4 snmp-server context

Команда глобальной настройки. Установка имени контекста для SNMP-агента. Имя контекста используется только для обмена между SNMP-агентом и SNMP-менеджером. Рекомендуется оставить данную настройку в значении по умолчанию (пустая строка).

Синтаксис команды:

snmp-server context *context-name*

no snmp-server context

Команда с приставкой «**no**» устанавливает имя контекста в виде пустой строки.

Параметры команды:

context- name	имя контекста в виде текстовой строки (рекомендуемая длина до 32 символов)

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server context somecontext
admin@Switch(config)# end
admin@Switch#
```

20.3.5 snmp-server engineid

Команда глобальной настройки. Установка идентификатора движка SNMP, используемого для обмена между SNMP-агентом и SNMP-менеджером. Рекомендуется оставить данную настройку в значении по умолчанию.

Синтаксис команды:

snmp-server engineid local *id*

no snmp-server engineid local

Команда с приставкой «**no**» устанавливает значение идентификатора в следующем виде: «80:00:3A:25:03», дополненным текстовым представлением MAC-адреса коммутатора (например, «80:00:3A:25:03:00:1B:28:00:00:01»).

Параметры команды:

id	идентификатор движка SNMP в виде 5–32 пар шестнадцатеричных цифр, разделенных двоеточием

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server engineid 80:00:3A:25:06
admin@Switch(config)# end
admin@Switch#
```

20.3.6 snmp-server host

Команда глобальной настройки. Установка IP-адреса SNMP-менеджера, на который будут отправляться ловушки, и параметров отправки.

Синтаксис команды:

snmp-server host *host-addr community-string*

no snmp-server host *host-addr*

Команда с приставкой «**no**» удаляет IP-адрес SNMP-менеджера.

Параметры команды:

host-addr	IP-адрес SNMP-менеджера
community-string	имя сообщества, используемого в ловушках (рекомендуемая длина до 16 символов)

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server host 10.0.0.1 community
admin@Switch(config)#
```

20.3.7 snmp-server location

Команда глобальной настройки. Позволяет ввести информацию о местоположении аппаратуры для SNMP-агента. Данный параметр доступен для чтения и записи по протоколу SNMP (параметр system.sysLocation.0).

Синтаксис команды:

snmp-server location *location-info*

no snmp-server location

Команда с приставкой «**no**» выводит информацию о местоположении в виде «no location».

Параметры команды:

location-info	информация о местоположении аппаратуры в виде текстовой строки (рекомендуемая длина: до 32 символов)

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server location Ufa, Russia
admin@Switch(config)# end
admin@Switch#
```

20.3.8 snmp-server protocol enable

Команда глобальной настройки. Включение управления и мониторинга по протоколу SNMP.

Синтаксис команды:

snmp-server protocol enable

no snmp-server protocol enable

Команда с приставкой «**no**» отключает управление и мониторинг по протоколу SNMP.

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server protocol enable
admin@Switch(config)# end
admin@Switch#
```

20.3.9 snmp-server protocol version

Команда глобальной настройки. Установка версии протокола SNMP для управления и мониторинга.

Синтаксис команды:
snmp-server protocol version {**all | v1 | v2 | v3**}
no snmp-server protocol version
Команда с приставкой «**no**» устанавливает версию протокола в значении «all».
Параметры команды:

all	доступны все версии протокола (v1, v2c, v3)
v1	доступен только протокол SNMPv1
v2	доступен только протокол SNMPv2
v3	доступен только протокол SNMPv3

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server protocol version all
admin@Switch(config)# end
admin@Switch#
```

20.3.10 snmp-server source-interface

Команда глобальной настройки. Выбор интерфейса источника для SNMP-агента.
Синтаксис команды:
snmp-server source-interface traps vlan *vlan-id*
no snmp-server source-interface traps
Команда с приставкой «**no**» удаляет выбранное значение.
Параметры команды:

vlan-id	идентификатор интерфейса VLAN в диапазоне от 1 до 4094

Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server source-interface traps vlan 10
admin@Switch(config)#
```

20.3.11 snmp-server traps

Команда глобальной настройки. Включение отправки SNMP-ловушек по различным событиям.
Синтаксис команды:
snmp-server traps [**authorization | ethernet | snmp**]
no snmp-server traps [**authorization | ethernet | snmp**]
Команда с приставкой «**no**» отключает отправку SNMP-ловушек для соответствующих событий.
Параметры команды:

authorization	отправка ловушек при неудачной авторизации через CLI или SNMP

ethernet	отправка ловушек при изменении состояния портов Ethernet
snmp	отправка ловушек при включении аппаратуры (cold start)

Значение по умолчанию:
По умолчанию включена отправка SNMP-ловушек для всех событий.
Использование команды:
Команда без параметров включает отправку SNMP-ловушек для всех событий.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server traps ethernet
admin@Switch(config)# end
admin@Switch#
```

20.3.12 snmp-server user

Команда глобальной настройки. Добавление пользователей для протокола SNMPv3. Если указанный пользователь существует, то его настройки будут заменены настройками, указанными в параметрах команды.

Синтаксис команды:
snmp-server user *username* **group** [**read** | **write**] [**auth** {**md5** | **sha**} *password* [**priv** {**aes-128** | **des**} *password*]]
no snmp-server user *username*
Команда с приставкой «**no**» удаляет имя пользователя.
Параметры команды:

username	имя пользователя в виде текстовой строки
group [**read** | **write**]	выбор группы пользователя. «**read**» – данный пользователь может только читать параметры по SNMP. «**write**» – данный пользователь может читать и изменять параметры по SNMP
auth {**md5** | **sha**}	алгоритм хеширования при авторизации: MD5 или SHA1
password	пароль для авторизации пользователя
priv {**aes-128** | **des**}	использование алгоритма шифрования
password	пароль шифрования пользователя

Значение по умолчанию:
По умолчанию пользователи для протокола SNMPv3 отсутствуют.
Пример команды:

```
admin@Switch# configure terminal
admin@Switch(config)# snmp-server user User group read
admin@Switch(config)# end
admin@Switch#
```

20.3.13 show snmp

Фундаментальная команда. Отображение настроек SNMP-агента.

Синтаксис команды:

show snmp

Пример команды:

```
admin@Switch# show snmp
SNMP configuration:
-------------
SNMP protocol: Enabled
Contact: no contact
Location: no location
SNMPv1 community: public
Context:
Engine ID: 80:00:3A:25:03:00:01:02:03:04:24
Version: All

Host address    Version   Community
-------------   -------   ---------
192.168.0.117    v1        public

SNMPv3 user name   Group   Auth   Priv
----------------   -----   ----   ----
guest               read    no     no
sysop               write   md5    no
admin@Switch#
```

20.4 Управление и мониторинг по протоколу SNMP

20.4.1 Общие положения

Управление по протоколу SNMP производится с помощью SNMP-менеджеров. В настоящем документе описано управление коммутатором с помощью SNMP-менеджера SNMPc.

Настоящее описание предполагает, что:

1. Администратор является специалистом, сертифицированным для управления вышеуказанным ПО;
2. Пользователь является сертифицированным оператором ПЭВМ, имеющим навыки работы с вышеуказанным ПО;
3. Администратор имеет соответствующие знания стандартов и рекомендаций:
   - RFC1155-1157 – «описание протокола SNMPv1 и SMIv1»;
   - RFC3410-3418 – «описание протокола SNMPv3 и SMIv2»;
   - RFC1213 – «описание MIB-базы для сетевого управления».

Управление по SNMP поддерживает следующие MIB-базы:

- RFC-1213 MIB-2;
- RFC-1659 RS-232-MIB;
- RFC-2863 Interface MIB;
- RFC-2819 RMON MIB (Group 1);
- POLYGON-MIB.

20.4.2 Подготовка к управлению и мониторингу по протоколу SNMP

Управление коммутатором производится через интерфейс Ethernet 10/100/1000BASE-T.

Для управления коммутатором с помощью SNMP необходимо:

1. Установить SNMP.
2. Добавить MIB-базу «polygon-mib.mib» (меню Config\Mib database. . .).
3. Скомпилировать, нажав кнопку «Compile» (рисунок 12).

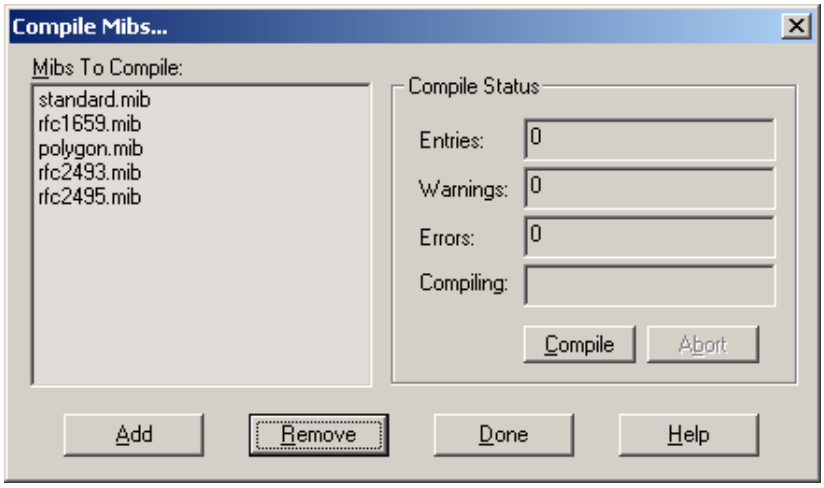

Рисунок 12 – Настройка списка MIB-баз

4. Вручную добавить коммутатор в общую карту (если не включен режим поиска SNMPc): меню Insert\Map object\Device.
5. Настроить все параметры (рисунки 13, 14):

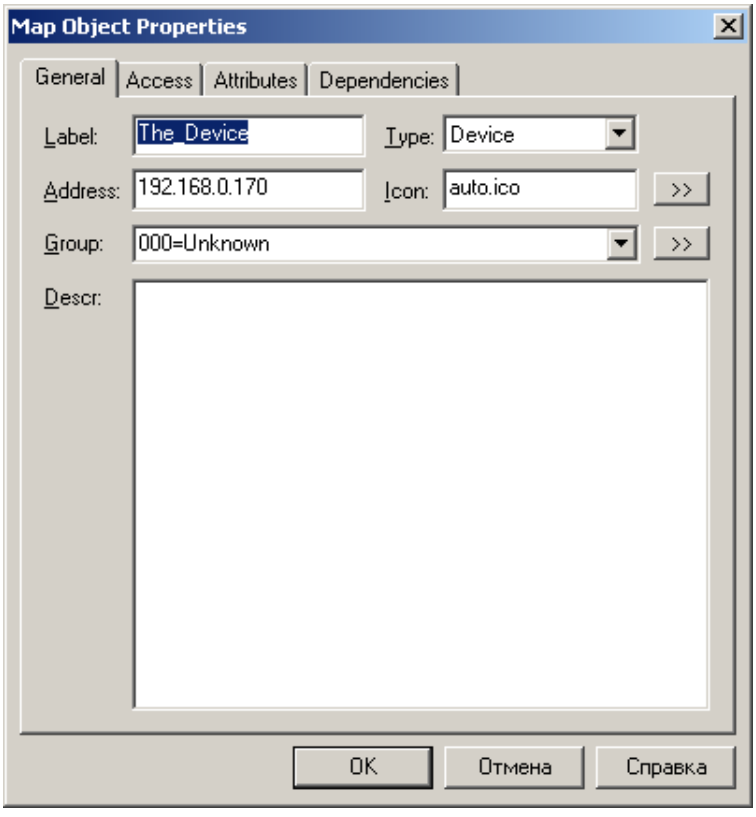

Рисунок 13 – Настройка основных параметров устройства

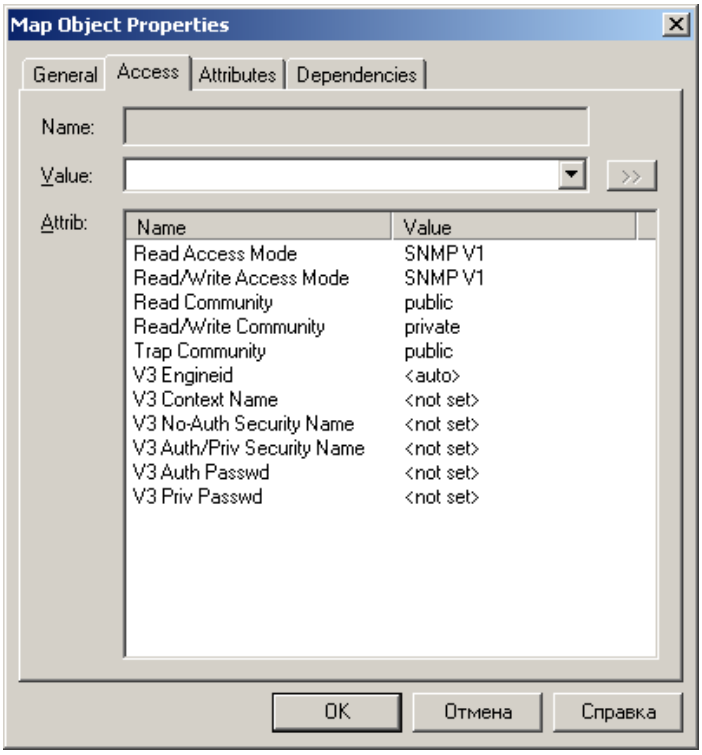

Рисунок 14 – Настройка параметров доступа

6. При этом главное окно SNMPc после включения коммутатора (и настройки IP-адреса SNMP-менеджера) примет вид (рисунок 15):

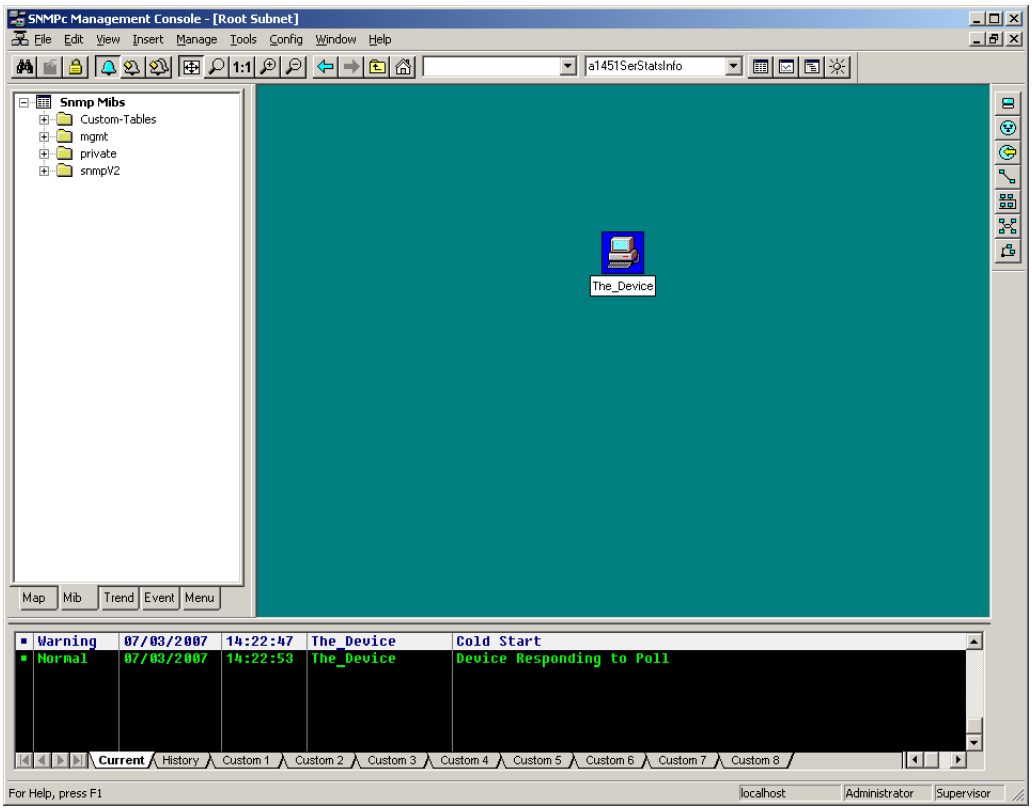

Рисунок 15 – Пример главного окна с добавленным объектом

20.4.3 Управление общей информацией о системе

Для управления общей информацией о системе на вкладке «MIB» левой панели необходимо найти ветку SystemInfo: путь mgmt→System→SystemInfo.

Изменяемые параметры:

- Contact – контактная информация ответственного лица (физического или юридического);
- Name – название для конкретного коммутатора;
- Location – местоположение коммутатора.

Информационные параметры:

- Descr – текстовое название типа коммутатора.

20.4.4 Получение информации об интерфейсах системы

Для получения информации об интерфейсах системы на вкладке MIB левой панели необходимо найти ветку IfEntry: путь mgmt→interfaces→ifTable→IfEntry.

Данная таблица не содержит изменяемых параметров.

Информационные параметры:

- Index – порядковый номер интерфейса (возможны разрывы нумерации);
- Descr – текстовое название физического интерфейса;
- Type – тип интерфейса;
- Mtu – максимально допустимый размер поля данных для интерфейса (для канальных интерфейсов равен нулю);
- Speed – пропускная способность интерфейса в бит/с;
- PhysAddress – физический адрес, равный пустой строке;
- AdminStatus – административное состояние интерфейса (значение параметра всегда равно 1 (up));
- OperStatus – текущее состояние интерфейса (значение параметра всегда равно 1 (up));
- LastChange – время последнего изменения состояния интерфейса (равно значению sysUpTime во время последнего изменения состояния интерфейса);
- InOctets – количество принятых октетов;
- InUcastPkts – количество принятых пакетов с обычным адресом назначения;
- InNUcastPkts – количество принятых пакетов с мультикастовым или широковещательным адресом назначения;
- InDiscards – количество пакетов, отброшенных при приеме (значение параметра всегда равно 0);

– InErrors – количество ошибок при приеме (пакеты меньше минимального размера, больше минимального размера, фрагменты, ошибки CRC);
– InUnknownProtos – количество пакетов с неизвестным протоколом (значение параметра всегда равно 0);
– OutOctets – количество отправленных октетов;
– OutUcastPkts – количество отправленных пакетов с обычным адресом назначения.

20.4.5 Настройка портов RS-232/485

1) Для настройки портов RS-232/485 на вкладке MIB левой панели необходимо найти ветку Rs232PortEntry: путь mgmt → transmission → rs232 → rs232PortTable → Rs232PortEntry.

Информационные параметры:

1. Index – индекс порта RS-232 в таблице интерфейсов;
2. Type – тип интерфейса (всегда «rs232»);
3. InsSigNumber – количество входящих сигнальных линий порта RS-232, представленных в таблице «rs232InSigTable»;
4. OutSigNumber – количество исходящих сигнальных линий порта RS-232, представленных в таблице «rs232OutSigTable».

Изменяемые параметры:

1. InSpeed, OutSpeed – входящая и исходящая скорости порта RS-232;
2. InFlowType, OutFlowType – режим входящего и исходящего управления потоком порта RS-232. Поддерживаются два значения:
   (a) «none» – управление потоком отключено;
   (b) «ctsRts» – включено аппаратное управление потоком с помощью линий RTS/CTS.

2) Также необходимо найти ветку Rs232AsyncPortEntry: путь mgmt → transmission → rs232 → rs232AsyncPortTable → Rs232AsyncPortEntry.

Информационные параметры:

1. Index – индекс порта RS-232 в таблице интерфейсов;
2. Autobaud – режим автоподстройки частоты порта RS-232 (отключен).

Изменяемые параметры:

1. Bits – количество бит данных в диапазоне от 5 до 8;

2. StopBits – количество стоповых бит. Поддерживаемые значения:

   (a) «one» – используется 1 стоповый бит;
   (b) «oneAndHalf» – используется 1,5 стоповых бита;
   (c) «two» – используется 2 стоповых бита.

3. Parity – режим контроля четности. Поддерживаемые значения:

   (a) «none» – контроль четности отключен;
   (b) «even» – режим контроля четного количества единиц («чет»);
   (c) «odd» – режим контроля нечетного количества единиц («нечет»);
   (d) «mark» – режим контроля четности «маркер» (бит четности всегда равен единице);
   (e) «space» – режим контроля четности «пробел» (бит четности всегда равен нулю).

20.4.6 Настройка интерфейсов Ethernet

Для настройки портов Ethernet на вкладке MIB левой панели необходимо найти ветку Eth1ConfigEntry: путь mgmt → private → Polygon → polygonTransmission → eth → ethConfigEntry.

Информационные параметры:

– PortStatus – состояние линейного тракта.

Возможные значения:

– linkUp10 – установлено соединение на скорости 10 Мбит/с;
– linkUp100 – установлено соединение на скорости 100 Мбит/с;
– linkUp1000 – установлено соединение на скорости 1 Гбит/с;
– linkDown – соединение на порту отсутствует.

Изменяемые параметры:

1. PortSpeed – управление настройкой скорости. Возможные значения:

   – spd10 – установлена скорость 10 Мбит/с;
   – spd100 – установлена скорость 100 Мбит/с;
   – spd1000 – установлена скорость 1 Гбит/с.

2. PortMode – управление настройкой режима дуплекса. Возможные значения:

   – fullDuplex – установлен режим полного дуплекса;
   – halfDuplex – установлен режим полудуплекса.

3. PortAutonegotiation – управление настройкой режима автосогласования. Возможные значения:
   - enabled – режим автосогласования включен;
   - disabled – режим автосогласования отключен.
4. PortFlowControl – настройка режима управления потоком. Возможные значения:
   - enabled – режим управления потоком включен;
   - disabled – режим управления потоком отключен.

20.4.7 Описание SNMP-ловушек

Система управления коммутатором отравляет SNMP-ловушки при изменении состояния портов Ethernet, ошибке авторизации через CLI или SNMP, а также при включении питания.

Для порта Ethernet SNMP-ловушка содержит информацию о:

- идентификаторе события «ethLineStatusChange»;
- состоянии порта на момент возникновения события «ethPortStatus».

20.4.8 Получение информации о счетчиках статистики RMON

Для получения информации о счетчиках статистики RMON на вкладке MIB левой панели необходимо найти ветку EtherStatsEntry: путь mgmt → rmon → statistics → EtherStatsEntry. Данная таблица не содержит изменяемых параметров. Описание параметров приведено в стандарте RFC2819.

21 Обновление программного обеспечения через TFTP-сервер

21.1 Настройка TFTP-сервера

Файлы обновления ПО необходимо поместить в выделенный каталог, например «C:\PolygonUpdates\». Если данного каталога нет, то необходимо его создать. Перед обновлением ПО необходимо установить TFTP-сервер на ПК. В качестве TFTP-сервера для ОС Windows® XP рекомендуется использовать tftpd32.

21.2 Порядок настройки tftpd32:

1. После запуска появится главное окно программы примерно следующего вида (рисунок 16):

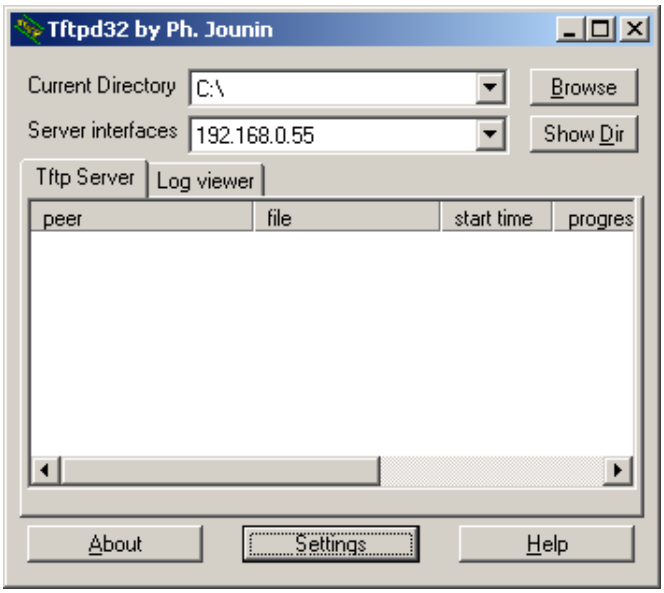

Рисунок 16 – Главное окно tftpd32

2. Если сетевых карт на ПК несколько, то необходимо выбрать сетевой адрес сетевой карты, используемой в данный момент в ниспадающем списке «Server interfaces».

3. После этого необходимо открыть окно настроек программы нажатием на кнопку «Settings» («настройки»). Рекомендуемые настройки параметров приведены на рисунке 17.

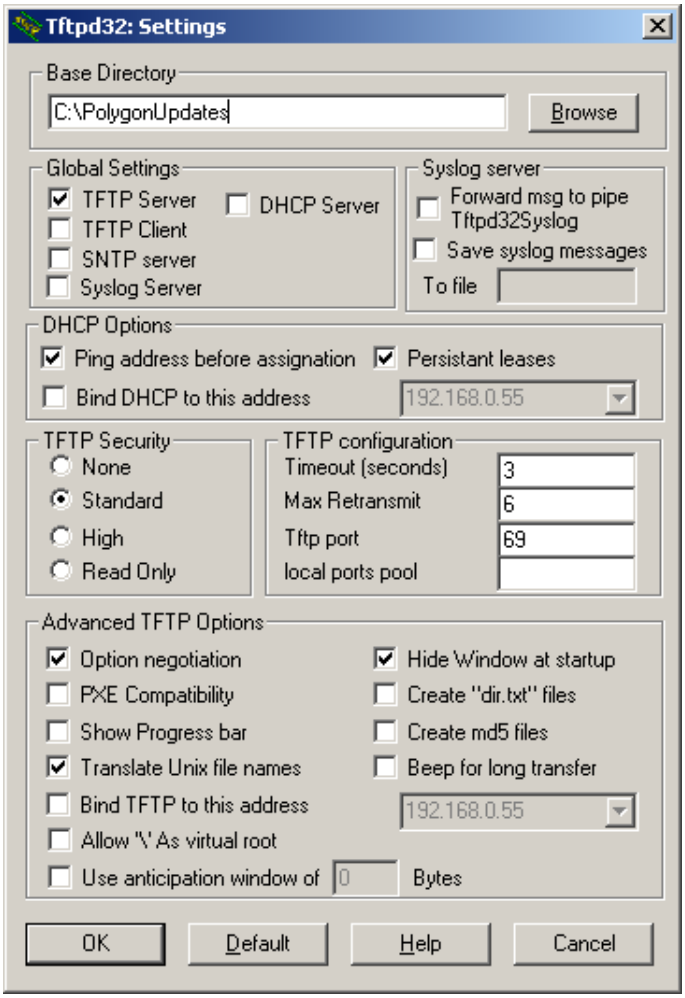

Рисунок 17 – Настройки tftpd32

21.3 Загрузка программного обеспечения

1. Подключить кабель Ethernet к порту 10/100/1000BASE-T коммутатора и сетевому коммутатору или напрямую к ПК.

2. Выбрать тип подключения для управления коммутатором и выполнить подключение:

2.1 Подключиться по порту «F»:

1) Подключить кабель управления к порту «F» коммутатора (RS-232) и COM-порту ПК;
2) Запустить программу PuTTY или HyperTerminal на ПК и настроить на выбранный COM-порт с параметрами: скорость –115200, количество битов данных – 8, количество стоповых бит – 1, режим проверки четности – нет;
3) Задать IP-адрес коммутатора и маску подсети командой «**ip address**»;
4) Задать IP-адрес шлюза коммутатора (при необходимости) командой «**ip default-gateway**»;

5) Проверить доступность коммутатора программой ping на ПК: «ping ххх.ххх .ххх.ххх». В случае недоступности коммутатора необходимо убедиться в том, что:

   – установленный IP-адрес не совпадает с IP-адресом существующего сетевого устройства;
   – есть физическое соединение;
   – горят светодиоды на порту 10/100/1000BASE-T коммутатора.

2.2 Подключиться по протоколу Telnet с помощью PuTTY или иного Telnet-клиента, указав IP-адрес коммутатора. По умолчанию на коммутаторе не настроен IP-адрес на VLAN 1. Для настройки адреса 192.168.0.225/24 используется команда «**interface vlan 1**», а затем команда «**ip address 192.168.0.225 /24**». Так же протокол Telnet отключен, поэтому если необходимо управление по протоколу Telnet, то его нужно включить с помощью команды «**ip telnet server**» (подключившись по порту «F»).

2.3 Подключиться по протоколу SSH с помощью PuTTY или иного SSH-клиента, указав IP-адрес коммутатора. По умолчанию на коммутаторе не настроен IP-адрес на VLAN 1. Для настройки адреса 192.168.0.225/24 используется команда «**interface vlan 1**», а затем команда «**ip address 192.168.0.225 /24**». Так же для протокола SSH необходимо предварительно создать ключ RSA или DSA. Для этого необходимо создать ключ RSA или DSA с помощью команды «**ssh key**» (подключившись по порту «F»).

3. Загрузить файл обновления ПО командой «enumerate», где «A» – URL загружаемого файла обновления ПО. В случае вывода сообщения об ошибке, необходимо убедиться, что TFTP-сервер запущен и аргументы команды введены правильно.

4. В процессе обновления ПО коммутатор может перезагружаться несколько раз.

ПРИЛОЖЕНИЕ А
ТАБЛИЦЫ ПРЕОБРАЗОВАНИЙ COS – PRIO, DSCP – PRIO

(справочное)

Таблица А.1 – Преобразования CoS – Prio

Приоритеты	Значения приоритетов							
CoS	0	1	2	3	4	5	6	7
Prio	1	0	2	3	4	5	6	7

Таблица А.2 – Преобразования DSCP – Prio

Приоритеты	Значения приоритетов							
DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Prio	2	0	1	3	4	5	6	7

ПРИЛОЖЕНИЕ Б
ТИПЫ И ФОРМАТ ЖУРНАЛИРУЕМЫХ СОБЫТИЙ

(справочное)

Коммутатор журналирует следующие события:

1. Изменение состояния интерфейса Ethernet. Формат события: «Имя интерфейса» «Состояние интерфейса». Значения параметров события приведены в таблице Б.1.
2. Изменение состояния STP на интерфейсе Ethernet. Формат события: «Имя интерфейса» «Состояние STP». Значения параметров события приведены в таблице Б.1.

Таблица Б.1 – Типы и формат журналируемых событий

Тип события	Параметры события	Значения параметров
Изменение состояния интерфейса Ethernet	Имя интерфейса	tengigabitethernet N/M
		gigabitethernet N/M
	Состояние интерфейса	«link up 10» – установлено соединение 10 Мбит/с
		«link up 100» – установлено соединение 100 Мбит/с
		«link up 1000» – установлено соединение 1000 Мбит/с
		«link up 10000» – установлено соединение 10000 Мбит/с
		«link down» – отсутствует соединение
Изменение состояния STP на интерфейсе Ethernet	Имя интерфейса	tengigabitethernet N/M
		gigabitethernet N/M
	Состояние STP	«disabled» – интерфейс блокирует трафик
		«blocking» – интерфейс блокирует трафик
		«learning» – интерфейс блокирует трафик
		«forwarding» – интерфейс передает и принимает трафик

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопрово-дительного документа и дата	Подп.	Дата
Изм.	изменен-ных	заме-ненных	новых	аннули-рован-ных					