OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Управление коммутатором с помощью интерфейса командной строки (CLI)

www.osnovo.ru

SEC.RU | Короткий путь к информации Скачано с sec.ru

Оглавление

1.Введение.....14

1.1 Подключение к коммутатору через консольный порт (Console Port Connection) 14

1.2 Распиновка разъема RJ-45 16

1.3 Распиновка разъема DB9..... 17

2. Интерфейс управления через командную строку (CLI) 18

2.1 Режимы CLI (CLI Modes) 18

2.2 Горячие клавиши (Quick Keys)..... 21

2.3 Синтаксис команд (Command Syntax)..... 23

2.4 Базовые конфигурации (Basic Configurations) 26

2.4.1 Настройка IPv4-адреса (Configuring IPv4 Address) 26

2.4.2 Вход в режим конфигурации интерфейса (Enter Config Interface Mode)..... 28

2.4.3 Сохранение конфигурации (Save Configurations) 30

2.4.4 Перезагрузка устройства (Restart the Device)..... 30

2.4.5 Загрузка заводских настроек по умолчанию (Load Factory Defaults) 32

2.4.6 Просмотр системной информации и информации о ПО (Show System and Software Information) 33

2.4.7 Просмотр текущей рабочей конфигурации (Show Running Configurations) 35

2.4.8 Просмотр истории команд (Show History Commands) 37

2.4.9 Справка (Help) 39

2.4.10 Выход из системы (Logout)..... 41

2.5 Команды в пользовательском режиме (Commands in User Mode)..... 43

2.5.1 Очистка ARP-кэша (> clear ip arp) 44

2.5.2 Очистка статистики LLDP (> clear lldp statistics) 45

2.5.3 Очистка статистики интерфейсов (> clear statistics)..... 46

2.5.4 Переход в привилегированный режим (> enable)..... 48

2.5.5 Выход/Возврат (> exit)..... 49

2.5.6 Справка (> help)..... 50

2.5.7 Выход из системы (> logout)..... 51

2.5.8 Проверка связи (ping) до IPv4-адреса (> ping ip)..... 52

2.5.9 Проверка связи (ping) до IPv6-адреса (> ping ipv6) 53

2.6 Команды в привилегированном режиме EXEC (Commands in EXEC Mode) 55

2.6.1 Очистка статистики управления доступом (# clear access management statistics) 55

2.6.2 Очистка статистики записей ACL (# clear access-list ace statistics) 56

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.3 Очистка статистики 802.1X (# clear dot1x statistics) 57
2.6.4 Очистка статистики ERPS (# clear erps statistics) 58
2.6.5 Очистка ARP-кэша (# clear ip arp) 59
2.6.6 Очистка детальной статистики IP DHCP (# clear ip dhcp detailed statistics) 60
2.6.7 Очистка статистики IP DHCP Relay (# clear ip dhcp relay statistics) 61
2.6.8 Очистка статистики IP DHCP Snooping (# clear ip dhcp snooping statistics) 62
2.6.9 Очистка статистики IP IGMP Snooping (# clear ip igmp snooping statistics) 63
2.6.10 Очистка IP-статистики (# clear ip statistics) 64
2.6.11 Очистка статистики IPv6 MLD Snooping (# clear ipv6 mld snooping statistics) 66
2.6.12 Очистка таблицы устройств «соседей» IPv6 (# clear ipv6 neighbors) 67
2.6.13 Очистка IPv6-статистики (# clear ipv6 statistics) 68
2.6.14 Очистка статистики LACP (# clear lacp statistics) 69
2.6.15 Очистка статистики LLDP (# clear lldp statistics) 70
2.6.16 Очистка журналов системных сообщений (# clear logging) 71
2.6.17 Очистка таблицы MAC-адресов (# clear mac address-table) 72
2.6.18 Очистка информации MEP (# clear mep) 73
2.6.19 Очистка информации протокола Spanning Tree (# clear spanning-tree) 74
2.6.20 Очистка статистики интерфейсов (# clear statistics) 76
2.6.21 Вход в режим глобальной конфигурации (# config terminal) 77
2.6.22 Копирование (# copy) 78
2.6.23 Удаление файла (# delete) 79
2.6.24 Просмотр содержимого каталога (# dir) 80
2.6.25 Переключение между пользовательским и привилегированным режимами (# disable & # enable) 82
2.6.26 Инициализация 802.1X (# dot1x initialize) 83
2.6.27 Управление ERPS (# erps) 84
2.6.28 Переключение на резервную прошивку (# firmware swap) 86
2.6.29 Обновление прошивки (# firmware upgrade) 87
2.6.30 Повторный запрос DHCP для интерфейса VLAN (# ip dhcp retry interface vlan) 88
2.6.31 Просмотр содержимого файла (# more) 89
2.6.32 Проверка связи (ping) до IPv4-адреса (# ping ip) 90
2.6.33 Проверка связи (ping) до IPv6-адреса (# ping ipv6) 92
2.6.34 Выполнение полной (холодной) перезагрузки (# reload cold) 93
2.6.35 Сброс к заводским настройкам по умолчанию (# reload defaults) 94

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.6.36 Отправка сообщения (# send) 95
2.6.37 Редактирование командной строки в терминале (# terminal editing) 96
2.6.38 Тайм-аут бездействия для терминальной сессии (# terminal exec-timeout) 97
2.6.39 Размер истории команд для терминала (# terminal history size) 99
2.6.40 Длина страницы терминала (# terminal length) 100
2.6.41 Ширина терминала (# terminal width) 101
2.6.42 Разблокировка портов, отключенных функцией Port Security (# no port-security shutdown) 103
2.6.43 Команды show (show commands) 104
2.7 Команды в режиме конфигурации (Commands in Config Mode) 105
2.7.1 Настройка метода аутентификации для входа (login) (config)# aaa authentication login 105
2.7.2 Правило управления доступом (config)# access management 107
2.7.3 Конфигурация списков контроля доступа (Access Control Lists - ACL) (config)# access-list 110
2.7.4 Настройка агрегирования каналов (Link Aggregation) (config)# aggregation 113
2.7.5 Настройка баннеров (Banners) (config)# banner 117
2.7.6 Настройка часов и времени (config)# clock 120
2.7.7 Сброс настроек ограничителя скорости ACL (config)# default access-list rate-limiter 123
2.7.8 Настройка 802.1X (IEEE Port-Based Network Access Control) (config)# dot1x 125
2.7.9 Настройка режима дуплекса на интерфейсе (config-if)# duplex 129
2.7.10 Настройка пароля привилегированного режима (config)# enable password 131
2.7.10.1 Настройка пароля для уровня привилегий (config)# enable password level 132
2.7.10.2 Настройка защищенного пароля для уровня привилегий (config)# enable secret) 134
2.7.11 Настройка параметров ERPS (Ethernet Ring Protection Switching) (config)# erps 135
2.7.11.1 (config)# erps <group> guard 135
2.7.11.2 (config)# erps <group> holdoff 137
2.7.11.3 (config)# erps <group> major port0 interface port1 interface 139
2.7.11.4 (config)# erps <group> mep 141
2.7.11.5 (config)# erps <group> revertive 143
2.7.11.6 (config)# erps <group> rpl 145
2.7.11.7 (config)# erps <group> sub 147
2.7.11.8 (config)# erps <group> topology-change propagate 149
2.7.11.9 (config)# erps <group> version 151

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7.11.10 (config)# erps <group> vlan 152
2.7.12 Включение алгоритма отсрочки перезапуска после избыточных коллизий (config-if)# excessive-restart 154
2.7.13 Включение/выключение управления потоком на интерфейсе (config-if)# flowcontrol 156
2.7.14 Настройка энергосберегающих функций Green Ethernet (config)# green-ethernet .. 158
2.7.14.1 (config)# green-ethernet led interval 158
2.7.14.2 (config)# green-ethernet led on-event 160
2.7.14.3 (config)# green-ethernet eee optimize-for-power 162
2.7.14.4 (config-if)# green-ethernet eee 164
2.7.14.5 (config-if)# green-ethernet eee urgent-queues 166
2.7.14.6 (config-if)# green-ethernet energy-detect 168
2.7.14.7 (config-if)# green-ethernet short-reach 170
2.7.15 Глобальное включение GVRP (config)# gvrp 171
2.7.15.1(config)# gvrp 171
2.7.15.2 (config)# gvrp max-vlans 173
2.7.15.3 (config)# gvrp time 174
2.7.15.4 (config-if)# gvrp 177
2.7.16 Настройка имени устройства (hostname) 179
2.7.17 Вход в режим конфигурации интерфейса (interface) 180
2.7.17.1 (config)# interface (<port_type> [<plist>]) 180
2.7.17.2 (config)# interface vlan 182
2.7.18 Настройка IP-протоколов (config)# ip 184
2.7.18.1 (config)# ip arp inspection 184
2.7.18.2 (config)# ip arp inspection entry interface 186
2.7.18.3 (config)# ip arp inspection translate 188
2.7.18.4 (config)# ip arp inspection vlan 189
2.7.18.5 (config)# ip arp inspection vlan <in_vlan_list> logging 191
2.7.18.6 (config)# ip dhcp relay 193
2.7.18.7 (config)# ip dhcp relay information option 194
2.7.18.8 (config)# ip dhcp relay information policy 196
2.7.18.9 (config)# ip dhcp snooping 198
2.7.18.10 (config)# ip dns proxy 200
2.7.18.11 (config)# ip helper-address 202
2.7.18.12 (config)# ip http secure-server 204

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.13 (config)# ip http secure-redirect 206
2.7.18.14 (config)# ip igmp host-proxy..... 208
2.7.18.15 (config)# ip igmp snooping..... 210
2.7.18.16 (config)# ip igmp snooping vlan 212
2.7.18.17 (config)# ip igmp ssm-range 214
2.7.18.18 (config)# ip igmp unknown-flooding..... 216
2.7.18.19 (config)# ip name-server..... 217
2.7.18.20 (config)# ip route 219
2.7.18.21 (config)# ip routing..... 221
2.7.18.22 (config)# ip source binding interface 223
2.7.18.23 (config)# ip ssh..... 225
2.7.18.24 (config)# ip verify source..... 227
2.7.18.25 (config)# ip verify source translate 229
2.7.18.26 (config-if)# ip arp inspection check-vlan 230
2.7.18.27 (config-if)# ip arp inspection logging..... 232
2.7.18.28 (config-if)# ip arp inspection trust 234
2.7.18.29 (config-if)# ip dhcp snooping trust 235
2.7.18.30 (config-if)# ip igmp snooping filter 237
2.7.18.31 (config-if)# ip igmp snooping immediate-leave 239
2.7.18.32 (config-if)# ip igmp snooping max-groups 241
2.7.18.33 (config-if)# ip igmp snooping mrouter..... 243
2.7.18.34 (config-if)# ip verify source..... 245
2.7.18.35 (config-if)# ip verify source limit..... 247
2.7.18.36 (config-if-vlan)# ip address 249
2.7.18.37 (config-if-vlan)# ip igmp snooping 251
2.7.18.38 (config-if-vlan)# ip igmp snooping compatibility 253
2.7.18.39 (config-if-vlan)# ip igmp snooping last-member-query-interval..... 255
2.7.18.40 (config-if-vlan)# ip igmp snooping priority..... 257
2.7.18.41 (config-if-vlan)# ip igmp snooping querier address 258
2.7.18.42 (config-if-vlan)# ip igmp snooping querier election..... 260
2.7.18.43 (config-if-vlan)# ip igmp snooping query-interval 262
2.7.18.44 (config-if-vlan)# ip igmp snooping query-max-response-time..... 264
2.7.18.45 (config-if-vlan)# ip igmp snooping robustness-variable..... 265
2.7.18.46 (config-if-vlan)# ip igmp snooping unsolicited-report-interval 267

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.47 (config-if-vlan)# ipv6 address 269
2.7.18.48 (config-if-vlan)# ipv6 mld snooping 271
2.7.18.49 (config-if-vlan)# ipv6 mld snooping compatibility 273
2.7.18.50 (config-if-vlan)# ipv6 mld snooping last-member-query-interval 275
2.7.18.51 (config-if-vlan)# ipv6 mld snooping priority 277
2.7.18.52 (config-if-vlan)# ipv6 mld snooping query-interval 278
2.7.18.53 (config-if-vlan)# ipv6 mld snooping query-max-response-time 280
2.7.18.54 (config-if-vlan)# ipv6 mld snooping robustness-variable 281
2.7.18.55 (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval 283
2.7.19 Настройка профилей IP-многоадресной рассылки (IPMC) (config)# ipmc 286
2.7.19.1 (config)# ipmc profile 286
2.7.19.2 (config)# ipmc profile <profile_name> 287
2.7.19.3 (config)# ipmc range 289
2.7.19.4 (config-ipmc-profile)# default range 291
2.7.19.5 (config-ipmc-profile)# description 293
2.7.19.6 (config-ipmc-profile)# range 295
2.7.20 Настройка MLD-прокси для IPv6 (config)# ipv6 mld host-proxy 297
2.7.20.1 (config)# ipv6 mld host-proxy 297
2.7.20.2 (config)# ipv6 mld host-proxy leave-proxy 299
2.7.20.3 (config)# ipv6 mld snooping 301
2.7.20.4 (config)# ipv6 mld snooping vlan 303
2.7.20.5 (config)# ipv6 mld ssm-range 305
2.7.20.6 (config)# ipv6 mld unknown-flooding 307
2.7.20.7 (config)# ipv6 route 309
2.7.20.8 (config-if)# ipv6 mld snooping filter 311
2.7.20.9 (config-if)# ipv6 mld snooping immediate-leave 313
2.7.20.10 (config-if)# ipv6 mld snooping max-groups 316
2.7.21 Настройка LACP (Link Aggregation Control Protocol) (config)# lacp 318
2.7.21.1 (config)# lacp system-priority 318
2.7.21.2 (config-if)# lacp 320
2.7.21.3 (config-if)# lacp key 322
2.7.21.4 (config-if)# lacp port-priority 324
2.7.21.5 (config-if)# lacp role 326
2.7.21.6 (config-if)# lacp timeout 328

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7.22 Настройка линий (терминалов) (config)# line 330
2.7.22.1 (config)# line 330
2.7.22.2 (config-line)# do 332
2.7.22.3 (config-line)# exec-banner 333
2.7.22.4 (config-line)# exec-timeout 335
2.7.22.5 (config-line)# help 337
2.7.22.6 (config-line)# history size 337
2.7.22.7 (config-line)# length 339
2.7.22.8 (config-line)# location 341
2.7.22.9 (config-line)# motd-banner 342
2.7.22.10 (config-line)# privilege level 344
2.7.22.11 (config-line)# width 346
2.7.23 Настройка LLDP (Link Layer Discovery Protocol) (config)# lldp 348
2.7.23.1 (config)# lldp holdtime 348
2.7.23.2 (config)# lldp reinit 350
2.7.23.3 (config)# lldp timer 351
2.7.23.4 (config)# lldp transmission-delay 353
2.7.23.5 (config)# lldp med datum 354
2.7.23.6 (config)# lldp med fast 357
2.7.23.7 (config)# lldp med location-tlv altitude 360
2.7.23.8 (config)# lldp med location-tlv civic-addr 361
2.7.23.9 (config)# lldp med location-tlv elin-addr 364
2.7.23.10 (config)# lldp med location-tlv latitude 366
2.7.23.11 (config)# lldp med location-tlv longitude 368
2.7.23.12 (config)# lldp med media-vlan-policy 369
2.7.23.13 (config-if)# lldp cdp-aware 372
2.7.23.14 (config-if)# lldp med media-vlan policy-list 374
2.7.23.15 (config-if)# lldp med transmit-tlv 376
2.7.23.16 (config-if)# lldp receive 379
2.7.23.17 (config-if)# lldp tlv-select 381
2.7.23.18 (config-if)# lldp transmit 383
2.7.24 Настройка журналирования (logging) (config)# logging 385
2.7.24.1 (config)# logging on 385
2.7.24.2 (config)# logging host 387

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7.24.3 (config)# logging level 389
2.7.25 Настройка защиты от петель (loop-protect) (config)# loop-protect 391
2.7.25.1 (config)# loop-protect 391
2.7.25.2 (config)# loop-protect shutdown-time 393
2.7.25.3 (config)# loop-protect transmit-time 395
2.7.25.4 (config-if)# loop-protect 396
2.7.25.5 (config-if)# loop-protect action 398
2.7.25.6 (config-if)# loop-protect tx-mode 400
2.7.26 Настройка таблицы MAC-адресов (mac) (config)# mac 402
2.7.26.1 (config)# mac address-table aging-time 402
2.7.26.2 (config)# mac address-table static 405
2.7.26.3 (config-if)# mac address-table learning 407
2.7.27 (config-if)# media-type 410
2.7.28 (config-if)# mtu 412
2.7.29 Настройка MEP (Maintenance End Point) (config)# mep 414
2.7.29.1 (config)# mep <inst> 414
2.7.29.2 (config)# mep <inst> ais 416
2.7.29.3 (config)# mep <inst> aps 418
2.7.29.4 (config)# mep <inst> cc 421
2.7.29.5 (config)# mep <inst> client domain 423
2.7.29.6 (config)# mep <inst> client flow 425
2.7.29.7 (config)# mep <inst> dm 427
2.7.29.8 (config)# mep <inst> dm ns 430
2.7.29.9 (config)# mep <inst> dm overflow-reset 432
2.7.29.10 (config)# mep <inst> dm proprietary 434
2.7.29.11 (config)# mep <inst> dm synchronized 436
2.7.29.12 (config)# mep <inst> lb 438
2.7.29.13 (config)# mep <inst> lck 441
2.7.29.14 (config)# mep <inst> level 443
2.7.29.15 (config)# mep <inst> lm 445
2.7.29.16 (config)# mep <inst> lt 447
2.7.29.17 (config)# mep <inst> meg-id 450
2.7.29.18 (config)# mep <inst> peer-mep-id 452
2.7.29.19 (config)# mep <inst> performance-monitoring 453

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7.29.20 (config)# mep <inst> tst 455
2.7.29.21 (config)# mep <inst> tst rx 458
2.7.29.22 (config)# mep <inst> tst tx 460
2.7.29.23 (config)# mep <inst> vid 462
2.7.29.24 (config)# mep <inst> voe 463
2.7.30 Настройка мониторинга трафика (config)# monitor 466
2.7.30.1 (config)# monitor destination interface 466
2.7.30.2 (config)# monitor source 467
2.7.31 Настройка NTP (Network Time Protocol) (config)# ntp 470
2.7.31.1 (config)# ntp 470
2.7.31.2 (config)# ntp server 471
2.7.32 Настройка PoE (Power over Ethernet) (config)# poe 473
2.7.32.1 (config)# poe management mode 473
2.7.32.2 (config)# poe supply 477
2.7.33 Настройка безопасности портов (Port Security) (config)# port-security 479
2.7.33.1 (config)# port-security 479
2.7.33.2 (config)# port-security aging 481
2.7.33.3 (config)# port-security aging time 483
2.7.33.4 (config-if)# port-security 485
2.7.33.5 (config-if)# port-security maximum 487
2.7.33.6 (config-if)# port-security violation 489
2.7.34 Настройка уровней привилегий для команд (config)# privilege 492
2.7.35 Настройка QoS (Quality of Service) (config)# qos 495
2.7.35.1 (config)# qos map cos-dscp 495
2.7.35.2 (config)# qos map dscp-classify 497
2.7.35.3 (config)# qos map dscp-cos 500
2.7.35.4 (config)# qos map dscp-egress-translation 502
2.7.35.5 (config)# qos map dscp-ingress-translation 505
2.7.35.6 (config)# qos qce refresh 507
2.7.35.7 (config)# qos qce update 509
2.7.35.8 (config)# qos storm 512
2.7.35.9 (config-if)# qos cos 515
2.7.35.10 (config-if)# qos dei 517
2.7.35.11 (config-if)# qos dpl 519

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7.35.12 (config-if)# qos dscp-classify 521
2.7.35.13 (config-if)# qos dscp-remark 524
2.7.35.14 (config-if)# qos dscp-translate 527
2.7.35.15 (config-if)# qos map cos-tag cos 529
2.7.35.16 (config-if)# qos map tag-cos pcp 531
2.7.35.17 (config-if)# qos pcp 533
2.7.35.18 (config-if)# qos policer 535
2.7.35.19 (config-if)# qos queue-policer queue 537
2.7.35.20 (config-if)# qos queue-shaper queue 539
2.7.35.21 (config-if)# qos shaper 542
2.7.35.22 (config-if)# qos tag-remark 544
2.7.35.23 (config-if)# qos trust dscp 546
2.7.35.24 (config-if)# qos trust tag 548
2.7.35.25 (config-if)# qos wrr 550
2.7.36 Настройка RADIUS-сервера (config)# radius-server 553
2.7.36.1 (config)# radius-server attribute 32 553
2.7.36.2 (config)# radius-server attribute 4 555
2.7.36.3 (config)# radius-server attribute 95 557
2.7.36.4 (config)# radius-server deadtime 559
2.7.36.5 (config)# radius-server host 561
2.7.36.6 (config)# radius-server key 564
2.7.36.7 (config)# radius-server retransmit 566
2.7.37 Настройка RMON (Remote Network Monitoring) (config)# rmon 568
2.7.37.1 (config)# rmon alarm 568
2.7.37.2 (config)# rmon event 572
2.7.37.3 (config-if)# rmon collection history 574
2.7.37.4 (config-if)# rmon collection stats 576
2.7.38 Настройка Spanning Tree Protocol (STP) (config)# spanning-tree 578
2.7.38.1 (config)# spanning-tree aggregation 578
2.7.38.2 (config-stp-aggr)# spanning-tree 580
2.7.38.3 (config-stp-aggr)# spanning-tree auto-edge 582
2.7.38.4 (config-stp-aggr)# spanning-tree bpdu-guard 584
2.7.38.5 (config-stp-aggr)# spanning-tree edge 586
2.7.38.6 (config-stp-aggr)# spanning-tree link-type 588

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7.38.7 (config-stp-aggr)# spanning-tree mst <instance> cost 590
2.7.38.8 (config-stp-aggr)# spanning-tree mst <instance> port-priority 592
2.7.38.9 (config-stp-aggr)# spanning-tree restricted-role 595
2.7.38.10 (config-stp-aggr)# spanning-tree restricted-tcn 597
2.7.38.11 (config)# spanning-tree edge bpdu-filter 599
2.7.38.12 (config)# spanning-tree edge bpdu-guard 601
2.7.38.13 (config)# spanning-tree mode 603
2.7.38.14 (config)# spanning-tree mst <instance> priority 605
2.7.38.15 (config)# spanning-tree mst <instance> vlan 607
2.7.38.16 (config)# spanning-tree mst forward-time 609
2.7.38.17 (config)# spanning-tree mst max-age 611
2.7.38.18 (config)# spanning-tree mst max-hops 614
2.7.38.19 (config)# spanning-tree mst name 616
2.7.38.20 (config)# spanning-tree recovery interval 619
2.7.38.21 (config)# spanning-tree transmit hold-count 621
2.7.38.22 (config-if)# spanning-tree 624
2.7.38.23 (config-if)# spanning-tree auto-edge 626
2.7.38.24 (config-if)# spanning-tree bpdu-guard 628
2.7.38.25 (config-if)# spanning-tree edge 630
2.7.38.26 (config-if)# spanning-tree link-type 632
2.7.38.27 (config-if)# spanning-tree mst <instance> cost 634
2.7.38.29 (config-if)# spanning-tree mst <instance> port-priority 637
2.7.39 (config-if)# speed 643
2.7.40 (config)# switchport 647
2.7.41.1 (config)# switchport vlan mapping 647
2.7.41.2 (config-if)# switchport access vlan 650
2.7.41.3 (config-if)# switchport forbidden vlan 652
2.7.41.4 (config-if)# switchport hybrid acceptable-frame-type 655
2.7.41.5 (config-if)# switchport hybrid allowed vlan 658
2.7.41.6 (config-if)# switchport hybrid egress-tag 661
2.7.41.7 (config-if)# switchport hybrid ingress-filtering 664
2.7.41.8 (config-if)# switchport hybrid native vlan 666
2.7.41.9 (config-if)# switchport hybrid port-type 669
2.7.41.10 (config-if)# switchport mode 673

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7.41.11 (config-if)# switchport trunk allowed vlan 677
2.7.41.12 (config-if)# switchport trunk native vlan 680
2.7.41.13 (config-if)# switchport trunk vlan tag native 682
2.7.41.14 (config-if)# switchport vlan ip-subnet id 685
2.7.41.15 (config-if)# switchport vlan mac 688
2.7.41.16 (config-if)# switchport vlan mapping 691
2.7.41.17 (config-if)# switchport vlan protocol group 693
2.7.42 Настройка TACACS+ сервера (config)# tacacs-server 696
2.7.42.1 (config)# tacacs-server timeout 696
2.7.42.2 (config)# tacacs-server deadtime 698
2.7.42.3 (config)# tacacs-server key 701
2.7.42.4 (config)# tacacs-server host 703
2.7.43 Настройка UPnP (Universal Plug and Play) (config)# upnp 706
2.7.43.1 (config)# upnp 706
2.7.43.2 (config)# upnp advertising-duration 708
2.7.43.3 (config)# upnp ttl 711
2.7.44 Настройка учетных записей пользователей (username) (config)# username 713
2.7.44.1 (config)# username <username> privilege <priv> password encrypted 713
2.7.44.2 (config)# username <username> privilege <priv> password none 716
2.7.44.3 (config)# username <username> privilege <priv> password unencrypted 719
2.7.45 Настройка VLAN (config)# vlan 721
2.7.45.1 (config)# vlan 721
2.7.45.2 (config)# vlan ethertype s-custom-port 724
2.7.45.3 (config)# vlan protocol 726
2.7.46 (config)# web privilege group 730

SEC.RU | Короткий путь к информации
Скачано с sec.ru

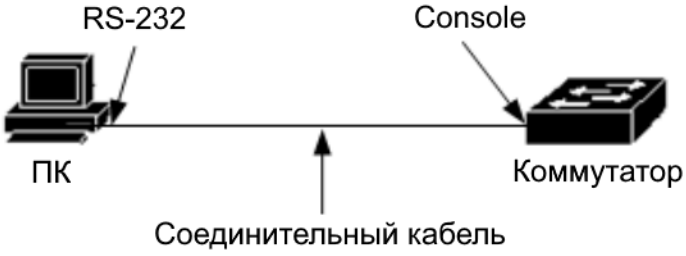
1. Введение

Управление коммутатором через консольный порт (чаще всего физический COM порт или виртуальный (USB=>COM)) или Telnet/SSH с помощью командной строки (CLI или Command Line Interface) предоставляет пользователю широкие возможности по настройке и управлению режимами работы коммутатора, или в случае, если по каким-либо причинам управление через WEB-интерфейс недоступно (ограничено).

1.1 Подключение к коммутатору через консольный порт (Console Port Connection)

Управляемые коммутаторы OSNOVO оснащены асинхронным консольным портом (Console) для локального управления через последовательный терминал. Подключение выполняется с помощью стандартного кабеля RJ-45 – DB9, который поставляется вместе с коммутатором или приобретается отдельно.

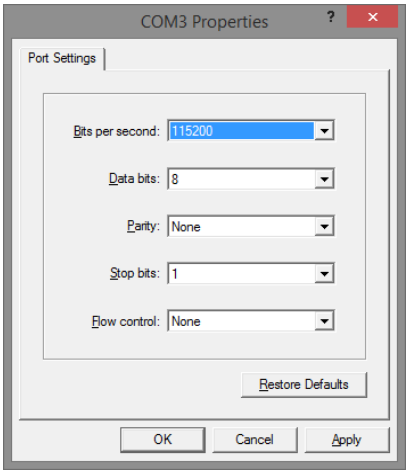
Терминал предоставляет доступ к интерфейсу командной строки (CLI, Command Line Interface), который хорошо знаком многим сетевым инженерам. Для большинства пользователей CLI может быть использован для первоначальной настройки доступа по TCP/IP, чтобы дальнейшая конфигурация могла быть выполнена через графический веб-интерфейс (WEB GUI) в любом браузере.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Порядок подключения:

1. Соедините порт Console коммутатора с COM-портом компьютера с помощью кабеля;
2. Запустите клиент терминала (putty, mobaXterm, secureCRT и др.);
3. Задайте имя для нового консольного подключения;
4. Выберите COM-порт, к которому подключен коммутатор;
5. Настройте COM-порт следующим образом:



- ✓ Скорость передачи данных (Baud Rate) – 115200;
- ✓ Биты данных (Data bits) – 8;
- ✓ Четность (Parity) – нет (no);
- ✓ Стоп биты (Stop bits) – 1;
- ✓ Управление потоком (flow control) – нет (no).

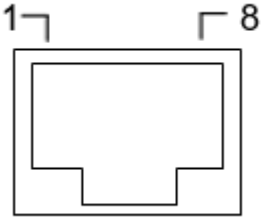
6. Включите коммутатор, система предложит войти в интерфейс CLI (управление через командную строку), используя логин (username) и пароль (password). Логин и пароль новых коммутаторов вы можете узнать из комплектного руководства по эксплуатации или на коробке/корпусе коммутатора.

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
+Luton10 board detected  (8539 Rev. D).
--Welcome to use our system
--Software version V2.00
== Executing boot scipt in 1.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x81016178
RedBoot> go
Press ENTER to get started
Username: admin
Password:
```

1.2 Распиновка разъема RJ-45

Данный разъем позволяет подключать коммутатор к ПК, на котором установлен терминал или программа (putty, mobaXterm, secureCRT и др.) с помощью кабеля RJ-45 – DB9.



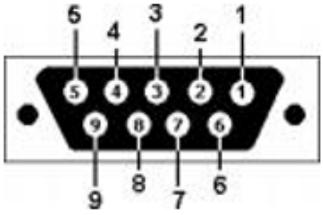
Контакт	Обозначение	Назначение	Направление сигнала
3	RxD	Принимаемые данные	Исходящий, в сторону DTE*
6	TxD	Передаваемые данные	Входящий, от DTE
5	SG	Сигнальная земля	–

*DTE – Data Terminal Equipment, обычно это ПК с установленным клиентом терминала

SEC.RU | Короткий путь к информации Скачано с sec.ru

1.3 Распиновка разъема DB9

Данный разъем позволяет подключать ПК, на котором установлен терминал или программа (putty, mobaXterm, secureCRT и др.) к коммутатору с помощью кабеля RJ-45 – DB9.



Контакты		Обозначение	Назначение	Направление сигнала
DB9	RJ-45			
2	3	RxD	Принимаемые данные	Исходящий от устройства в сторону DTE (ПК)
3	6	TxD	Передаваемые данные	Входящий в устройство от DTE (ПК)
5	5	SG	Сигнальная земля	–

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Интерфейс управления через командную строку (CLI)

2.1 Режимы CLI (CLI Modes)

Интерфейс командной строки (CLI) в основном разделен на четыре базовых режима:

- Пользовательский режим (User)
- Режим EXEC
- Режим глобальной конфигурации (Config)
- Режим конфигурации интерфейса (Config Interface).

После ввода имени пользователя и пароля вы начинаете работу в режиме EXEC (подсказка «#») по умолчанию. Команды, доступные в Пользовательском режиме и режиме EXEC, ограничены. Для выполнения расширенных конфигураций необходимо перейти в Режим глобальной конфигурации (Config) или Режим конфигурации интерфейса (Config Interface). В каждом режиме можно ввести знак вопроса (?) в командной строке, чтобы получить список доступных команд для данного режима. В следующей таблице представлен краткий обзор режимов, доступных коммутаторах OSNOVO.

Режим	Подсказка (Prompt)	Метод входа (Enter Method)	Метод выхода (Exit Method)
Пользовательский (User)	>	enable	disable

SEC.RU | Короткий путь к информации Скачано с sec.ru

Режим	Подсказка (Prompt)	Метод входа (Enter Method)	Метод выхода (Exit Method)
EXEC (Привилегированный)	#	Ввод авторизованного имени пользователя и пароля	exit, logout
Глобальной конфигурации (Global Config)	(config)#	Ввод configure terminal после #	end, exit, do logout
Конфигурации интерфейса (Config Interface)	(config-if)#	Указание типа и номера интерфейса после (config)# (например, interface ethernet 1/0/1)	end, exit, do logout

Рекомендации:

- Режимы CLI имеют иерархическую структуру. Для перехода на более глубокий уровень конфигурации требуется вводить определенные команды (например, configure terminal).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Важно обращать внимание на приглашение (символ/ы) командной строки (>, #, (config)#), так как оно указывает на текущий уровень доступа и набор доступных команд.
- Команда ? является контекстно-зависимой справкой и показывает команды, доступные именно в текущем режиме или начинающиеся с уже набранной последовательности символов.
- Для выхода из текущего режима в более высокий (например, из (config-if)# в (config)#) используется команда exit. Для немедленного возврата в привилегированный режим EXEC (#) из любого режима конфигурации используется команда end или комбинация клавиш Ctrl+Z.

Примеры настройки:

```
Switch> enable
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# description Uplink_to_Router
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

В этом примере:

1. Команда enable переводит из Пользовательского режима (>) в Привилегированный режим EXEC (#).
2. Команда configure terminal (сокр. conf t) переводит в Режим глобальной конфигурации ((config)#).
3. Команда interface ethernet 1/0/1 переводит в Режим конфигурации конкретного интерфейса ((config-if)#).

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. Команда exit в режиме интерфейса возвращает в режим глобальной конфигурации. Еще один exit возвращает в режим EXEC.
5. Команда end, выполненная в режиме (config-if)# или (config)#, сразу вернула бы пользователя в режим #.

2.2 Горячие клавиши (Quick Keys)

При редактировании командных строк доступно несколько полезных горячих клавиш.

Клавиша / Символ	Действие
?	Вывод списка команд, доступных в текущем режиме.
Стрелка вверх	Просмотр предыдущих введенных команд (переход назад по истории команд).
Стрелка вниз	Просмотр следующих введенных команд (переход вперед по истории команд).
Tab	Автодополнение (завершение) неполной команды или имени файла.

Рекомендации:

- Клавиша **?** (знак вопроса) является основным средством контекстной справки. Если ввести ? в командной строке, система отобразит все команды, доступные на данном уровне иерархии.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Если ввести часть команды и затем ? (например, show ?), система покажет все возможные продолжения или аргументы для этой команды.

- Использование **стрелок вверх/вниз** для навигации по истории команд значительно ускоряет работу, позволяя повторно использовать или модифицировать ранее выполненные команды без их повторного набора.
- Клавиша **Tab** — мощный инструмент для предотвращения опечаток и ускорения ввода. Достаточно набрать несколько уникальных начальных символов команды и нажать Tab, чтобы система автоматически дописала полное имя команды или параметра. Если вариантов несколько, двойное нажатие Tab отобразит все возможные варианты.

Примеры:

1. **Использование справки (?):**

```
Switch> ?
```

Покажет все команды, доступные в Пользовательском режиме.

```
Switch# show ?
```

Покажет все возможные аргументы для команды show *в Привилегированном режиме (например,* running-config*,* interfaces*,* version*).*

2. **Навигация по истории команд:**

    - Находясь в режиме #, нажатие **стрелки вверх** отобразит последнюю выполненную команду.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Повторные нажатия **стрелки вверх** позволяют перемещаться дальше по истории.

3. **Автодополнение команды (Tab):**

```
Switch# conf<Tab>
```

Система автоматически дополнит команду до configure.

```
Switch# configure t<Tab>
```

Система автоматически дополнит команду до configure terminal

2.3 Синтаксис команд (Command Syntax)

Команды, представленные в данном руководстве, записываются с использованием единообразных символов и простого для понимания синтаксиса. Хотя пользователи могут использовать команду справки (Help) для завершения нужной команды в CLI, полезно понимать часто используемые символы и синтаксические соглашения. В следующей таблице перечислены синтаксические соглашения, используемые в данном руководстве, вместе с примером.

Пример синтаксиса:

(config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }

SEC.RU | Короткий путь к информации Скачано с sec.ru

Символ	Функция	Пример	Объяснение (Explanation)
< > (Угловые скобки)	Введите значение, буквенно-цифровую строку или ключевое слово.	<address> <netmask>	Введите IP-адрес и маску подсети.
[ ] (Квадратные скобки)	Обозначает необязательный параметр.	[fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]	Параметр fallback является необязательным элементом.
{ } (Фигурные скобки)	Фигурная скобка выполняет две функции: 1. Если доступно более двух опций, фигурная скобка используется для их группировки. 2. Внешняя фигурная скобка означает, что это обязательный блок. Должен быть указан хотя бы один вариант из представленных.	{ { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	Чтобы завершить команду, необходимо указать как минимум одну опцию из предложенных (статический IP или DHCP).
| (Вертикальная черта)	Используйте вертикальную черту для разделения	{ { <address> <netmask> } | { dhcp [fallback	Выберите одну из опций: либо введите IP-адрес

SEC.RU | Короткий путь к информации Скачано с sec.ru

Символ	Функция	Пример	Объяснение (Explanation)
	взаимоисключающих опций внутри блока.	<fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	вручную, либо используйте DHCP для автоматического назначения IP-адреса.

Рекомендации:

- Элементы в **угловых скобках** < > никогда не вводятся буквально. Они являются заполнителями (placeholders) для конкретных значений, которые должен предоставить пользователь (например, 192.168.1.1 или 255.255.255.0).
- Элементы в **квадратных скобках** [ ] можно полностью опустить при вводе команды.
- **Фигурные скобки** { } и **вертикальная черта** \| используются вместе для обозначения выбора между обязательными опциями. При вводе команды ни фигурные скобки, ни вертикальная черта не печатаются.
- Чтение синтаксиса следует начинать с самого внешнего уровня (главных фигурных скобок), чтобы понять обязательный выбор, а затем углубляться в детали каждой опции.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.4 Базовые конфигурации (Basic Configurations)

В данном разделе пользователям показано, как изменить IP-адрес по умолчанию на желаемый и сохранить текущую рабочую конфигурацию (running configuration) в стартовую конфигурацию (startup configuration).

2.4.1 Настройка IPv4-адреса (Configuring IPv4 Address)

IP-адрес (IP address): 192.0.3.254

Маска подсети (Subnet mask): 255.255.255.0

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.0.3.254 255.255.255.0
(config-if-vlan)# exit
(config)# exit
# show ip interface brief
Vlan   Address              Method   Status
1      192.0.3.254/24       Manual   DOWN
```

Команды показаны в порядке их выполнения для достижения цели (назначение IP-адреса управлению).

1. **Переход в режим глобальной конфигурации:**
    - `# configure terminal` – Переход из привилегированного режима EXEC (`#`) в режим глобальной конфигурации (`(config)#`).
2. **Выбор интерфейса для настройки:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- (config)# interface vlan 1 – Переход в режим конфигурации интерфейса VLAN 1 ((config-if-vlan)#).

3. **Назначение IP-адреса:**
   - (config-if-vlan)# ip address 192.0.3.254 255.255.255.0 – Ключевая команда для задания статического IP-адреса и маски подсети на выбранном интерфейсе.
4. **Выход из режимов конфигурации:**
   - (config-if-vlan)# exit – Возврат в режим глобальной конфигурации.
   - (config)# exit – Возврат в привилегированный режим EXEC.
5. **Проверка конфигурации:**
   - # show ip interface brief – Команда проверки, которая отображает настроенный адрес и текущий статус интерфейса.

Рекомендации:

- Интерфейс **VLAN 1** (Management VLAN) по умолчанию используется для удаленного управления коммутатором.
- После присвоения IP-адреса интерфейс может оставаться в состоянии **DOWN**. Для перевода его в состояние **UP** необходимо подключить активное устройство (например, ПК или маршрутизатор) к любому порту коммутатора, который

SEC.RU | Короткий путь к информации Скачано с sec.ru

принадлежит VLAN 1 (по умолчанию это все порты), либо явно настроить этот порт как член VLAN 1.

- Команда show ip interface brief является важным средством диагностики. Она выводит краткий список всех интерфейсов уровня 3 (в данном случае VLAN-интерфейсов) с их IP-адресами и статусами (UP/DOWN).

2.4.2 Вход в режим конфигурации интерфейса (Enter Config Interface Mode)

Вход в режим конфигурации для диапазона портов (Port 1 – Port 3):

```
# configure terminal
(config)# interface GigabitEthernet 1/1-3
(config-if)#
```

Примечание: Запись 1/1-3 означает порты с 1 по 3 на интерфейсном модуле (или блоке портов) 1.

Вход в режим конфигурации для нескольких портов (Port 1 – Port 3 и Port 5):

```
# configure terminal
(config)# interface GigabitEthernet 1/1-3,5
(config-if)#
```

Примечание: Запись 1/1-3,5 означает порты с 1 по 3 и отдельно порт 5 на интерфейсном модуле 1.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Данный метод позволяет применять одинаковые настройки (например, описание, режим дуплекса, скорость, настройки VLAN) сразу к нескольким портам одновременно, что экономит время и обеспечивает единообразие конфигурации.
- Важно помнить, что в данном режиме ((config-if)#) любая введенная команда будет применена ко **всем** указанным в диапазоне портам.
- Для выхода из этого группового режима конфигурации и возврата в режим глобальной конфигурации используется команда exit. Для немедленного возврата в привилегированный режим EXEC (#) используется команда end или комбинация клавиш Ctrl+Z.

Примеры настройки:

Пример применения настроек к диапазону портов:

```
# configure terminal
(config)# interface GigabitEthernet 1/1-3
(config-if)# description ACCESS_PORTS_FOR_PCs
(config-if)# speed 100
(config-if)# duplex full
(config-if)# switchport access vlan 10
(config-if)# exit
```

*В этом примере портам 1, 2 и 3 на модуле 1 одновременно задаются: описание, скорость 100

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.4.3 Сохранение конфигурации (Save Configurations)

Пример успешного сохранения:

```
# copy running-config startup-config
Building configuration...
% Saving 1520 bytes to flash:startup-config
#
```

Рекомендации:

- После внесения любых изменений в конфигурацию коммутатора они сохраняются только в рабочей (текущей) конфигурации (running-config), которая хранится в оперативной памяти (RAM). При перезагрузке устройства эти изменения будут утеряны.
- Для сохранения изменений на постоянной основе необходимо скопировать рабочую конфигурацию в стартовую (startup-config), которая хранится в энергонезависимой памяти (flash).
- Сообщение % Saving ... bytes to flash:startup-config указывает на успешное завершение операции.

2.4.4 Перезагрузка устройства (Restart the Device)

Пример выполнения перезагрузки:

```
# reload cold
% Cold reload in progress, please standby.
#
+Luton10 board detected (8539 Rev. D).
--Welcome to use our system
--Software version V2.00
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
== Executing boot script in 1.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x810156c8
RedBoot> go
Press ENTER to get started
```

Рекомендации:

- Команда reload cold инициирует **полную («холодную») перезагрузку** устройства. Это эквивалентно выключению питания и его повторному включению. Все аппаратные компоненты проходят повторную инициализацию.
- **Внимание!** Использование этой команды приведет к **прерыванию работы сети** на всех портах коммутатора на время перезагрузки (обычно 1-3 минуты).
- Перед выполнением перезагрузки **всегда рекомендуется сохранить текущую конфигурацию** с помощью команды copy running-config startup-config, чтобы изменения не были утеряны.
- Во время перезагрузки на консоли отображаются сообщения загрузчика (RedBoot) и процесса инициализации системы. После завершения загрузки появится приглашение командной строки (Press ENTER to get started или приглашение входа в систему).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.4.5 Загрузка заводских настроек по умолчанию (Load Factory Defaults)

Примеры выполнения сброса настроек:

1. *Полный сброс к заводским настройкам (включая IP-адрес):*

```
# reload defaults
% Reloading defaults. Please standby.
```

После перезагрузки коммутатор будет иметь IP-адрес по умолчанию (указан в руководстве, например, 192.168.2.1) и потребует полной перенастройки.

2. *Сброс к заводским настройкам с сохранением IP-адреса управления:*

```
# reload defaults keep-ip
% Reloading defaults, attempting to keep IP address. Please standby.
```

После перезагрузки коммутатор вернет все настройки (пароли, VLAN, порты) к заводским, но интерфейс управления (например, VLAN 1) сохранит ранее заданный статический IP-адрес, что позволит подключиться к нему для настройки

Рекомендации:

- **Команда** `reload defaults` **выполняет полный сброс** всех параметров конфигурации коммутатора к состоянию «из коробки». Это включает сброс паролей, IP-адресов, настроек VLAN, параметров портов и т.д. Устройство перезагрузится с чистой конфигурацией.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Команда** reload defaults keep-ip **является более безопасным вариантом**, если необходимо исправить ошибочную конфигурацию, но при этом сохранить возможность удаленного доступа к устройству по известному IP-адресу после перезагрузки. Она сбрасывает все настройки, кроме IP-адреса, маски подсети и шлюза по умолчанию, назначенных на интерфейс управления (обычно VLAN 1).
- **Важное предупреждение:** Обе эти операции являются **деструктивными**. Перед их выполнением убедитесь, что у вас есть физический (консольный) доступ к устройству, либо вы уверены в сохранении IP-доступа (при использовании keep-ip). Все текущие конфигурации будут безвозвратно утеряны.

2.4.6 Просмотр системной информации и информации о ПО (Show System and Software Information)

Пример выполнения команды:

```
# show version
MEMORY: Total=87066 KBytes, Free=73379 KBytes, Max=73286 KBytes
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
MAC Address: 00-02-c1-93-9a-35
Previous Restart: Cold
System Contact:
System Name:
System Location  :
System Time: 06-06-2019T02:04:31- 10:00
System Uptime: 00:03:33
Active Image
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Image: ce_switch_caracal1_l10_ref.dat (primary)
Version: CEServicesCEServices---V1.00
Date: 09-2019
Alternate Image
Image: ce_switch_caracal1_l10_ref.dat (backup)
Version: CEServicesCEServices---V1.00
Date: 09-2019
Bootloader
Image: RedBoot (bootloader)
Version: version 1_20-Vitesse
Date: 12:02:42, Aug 19 2019

Рекомендации:

- Команда show version является одной из основных диагностических команд. Она предоставляет сводную информацию о состоянии оборудования и программного обеспечения устройства.
- **Ключевые параметры для внимания:**
    - **MAC Address:** Базовый MAC-адрес устройства, часто используемый для идентификации в сети.
    - **System Uptime:** Время работы системы с последней перезагрузки. Полезно для диагностики проблем, возникающих после длительной работы.
    - **Active Image Version:** Версия работающего системного ПО (прошивки). Критически важна при обновлении или поиске известных ошибок конкретной версии.
    - **Bootloader Version:** Версия загрузчика (RedBoot).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Previous Restart:** Причина последней перезагрузки (Cold — полная перезагрузка, Warm — мягкая перезагрузка ПО).

- Поля System Contact, Name, Location пусты, так как они предназначены для заполнения администратором с помощью соответствующих команд конфигурации (например, snmp-server contact, hostname).

2.4.7 Просмотр текущей рабочей конфигурации (Show Running Configurations)

Пример выполнения команды (сокращенный вывод):

```
# show running-config
Building configuration...
username admin privilege 15 password encrypted YWRtaW4=
!
vlan 1
!
!
!
!
clock timezone sz1111 -10
spanning-tree mst name 02-00-c1-93-4a-01 revision 0
poe management mode allocation-reserved-power
voice vlan oui 00-01-E3 description Siemens AG phones
voice vlan oui 00-03-6B description Cisco phones
voice vlan oui 00-0F-E2 description H3C phones
voice vlan oui 00-60-B9 description Philips and NEC AG phones
voice vlan oui 00-D0- 1E description Pingtel phones
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
voice vlan oui 00-E0-75 description Polycom phones
voice vlan oui 00-E0-BB description 3Com phones
!
interface GigabitEthernet 1/1
 poe mode plus
 poe power limit 90.0
 poe delay limit 1.3
!
interface GigabitEthernet 1/2
 poe mode plus
 poe power limit 90.0
 poe delay limit 1.2
!
interface GigabitEthernet 1/3
 poe mode plus
 poe power limit 50.0
 poe delay limit 1.1
!
```

Рекомендации:

- Команда show running-config отображает полную текущую активную конфигурацию устройства, хранящуюся в оперативной памяти (RAM).
- Это **основной инструмент** для проверки, аудита, копирования конфигурации или диагностики проблем. Вывод показывает все примененные настройки в том виде, в котором их необходимо вводить в CLI.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Формат вывода:** Конфигурация разделена на секции (глобальные настройки, настройки интерфейсов и т.д.). Восклицательный знак (!) используется как разделитель для улучшения читаемости.
- **Внимание:**
    - ✓ Пароли по умолчанию отображаются в зашифрованном виде (например, password encrypted ...).
    - ✓ Настройки, которые не были изменены с заводских значений, обычно не отображаются в выводе этой команды. Показываются только настроенные параметры.
    - ✓ Изменения, внесенные в режиме конфигурации, немедленно отражаются в выводе этой команды.

2.4.8 Просмотр истории команд (Show History Commands)

Пример выполнения команды в разных режимах:

1. *Просмотр истории в привилегированном режиме EXEC (#):*

```
# show history
config t
exit
config t
ip arp ex
exit
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2. *Просмотр истории в пользовательском режиме (>):*

```
> show history
config t
interface GigabitEthernet 1/3
exit
interface GigabitEthernet 1/1-5
exit
interface GigabitEthernet 1/1-3,5,7
flowcontrol on
exit
show interface * status
disable
show clock detail
show dot1x
show history
```

Рекомендации:

- Команда show history отображает список ранее введенных команд в текущей сессии терминала для **текущего режима доступа** (User или EXEC). История команд в режимах конфигурации (например, (config)#) обычно не сохраняется или сохраняется отдельно.
- История является мощным инструментом для:
    - ✓ Повторного выполнения длинных или сложных команд (используя клавиши **Стрелка вверх**).
    - ✓ Анализа своих действий, особенно при отладке конфигурации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Восстановления последовательности команд после случайного выхода из сессии.

- Размер буфера истории ограничен (обычно 10-20 последних команд) и **сбрасывается при завершении сессии терминала** (выходе из коммутатора). История не сохраняется между сессиями.

2.4.9 Справка (Help)

Команда *Help* может быть выполнена в пользовательском режиме (User), привилегированном режиме EXEC и режиме глобальной конфигурации (Global Config) для получения подсказки с описанием того, как использовать команду show для получения справки в CLI.

```
# help
```

Рекомендации:

- Встроенная система справки CLI, активируемая символом ?, является основным инструментом для изучения доступных команд и их синтаксиса без необходимости обращения к руководству.
- **Полная справка (**команда ?**)** выводит список **всех** возможных продолжений или аргументов для текущей позиции в команде. Это особенно полезно на верхних уровнях иерархии (например, # ? или # show ?).
- **Частичная справка (**часть_команды?**)** используется для автодополнения. Если введенная последовательность символов

SEC.RU | Короткий путь к информации Скачано с sec.ru

уникальна, система может автоматически дописать команду. Если вариантов несколько, будет показан список всех команд, начинающихся с этих символов.

- Если после ? ничего не выводится, это означает, что набранная последовательность не является валидным началом ни одной команды в текущем режиме, либо вы пытаетесь ввести аргумент в неправильном контексте.

Примеры использования:

Примеры использования контекстной справки:

1. **Полная справка на корневом уровне режима EXEC:**

```
# ?
```

Покажет все команды, доступные в привилегированном режиме (например, show*,* configure*,* copy*,* reload*).*

2. **Полная справка для конкретной команды:**

```
# show ?
```

Покажет все возможные объекты для отображения с помощью команды show *(например,* interface*,* running-config*,* vlan*,* ip*).*

3. **Частичная справка для автодополнения:**

```
# show int<Tab>
```

или

```
# show int?
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Если ввод int *является уникальным, система может автоматически дополнить команду до* show interface*. Если нет, будет показан список всех команд, начинающихся с* show int *(например,* show interface*,* show interfaces*).*

4. **Справка внутри режима конфигурации интерфейса:**

```
(config-if)# speed ?
```

Покажет все доступные значения для команды speed *в данном режиме (например,* 10*,* 100*,* 1000*,* auto*).*

2.4.10 Выход из системы (Logout)

Для завершения активной терминальной сессии выполните команду logout в пользовательском (User) или привилегированном (EXEC) режиме.

Пример 1: Выход из привилегированного режима EXEC.

```
(config)# exit
# logout
Press ENTER to get started
```

Пример 2: Выход из пользовательского режима.

```
# disable
> logout
Press ENTER to get started
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда logout является корректным и безопасным способом завершения сессии управления коммутатором. Она закрывает текущее соединение (консольное или удаленное по Telnet/SSH) и возвращает устройство в состояние, при котором для нового доступа требуется аутентификация.
- В отличие от выключения питания или разрыва кабеля, этот метод гарантирует, что все процессы завершатся штатно, а системные логи будут корректно зафиксированы.
- После выполнения команды logout в консольном сеансе обычно появляется приглашение Press ENTER to get started, указывающее на то, что система готова к началу новой сессии (потребуется ввести логин и пароль, если они настроены).
- Команда exit также может завершить сессию, когда выполняется в верхнем уровне иерархии (пользовательском или привилегированном режиме), и является синонимом logout в этом контексте.

Примеры настройки:

Корректная последовательность завершения работы с устройством после настройки:

```
# copy running-config startup-config
Building configuration...
[OK]
# logout
Press ENTER to get started
```

SEC.RU | Короткий путь к информации Скачано с sec.ru

В этом примере:

1. *Сначала сохраняется конфигурация, чтобы все изменения были записаны.*
2. *Затем безопасно завершается сессия управления с помощью команды* `logout`.
3. *Теперь можно физически отключить консольный кабель или закрыть окно терминальной программы (Putty и т.д.)*

2.5 Команды в пользовательском режиме (Commands in User Mode)

Когда вы успешно входите в интерфейс командной строки, вы оказываетесь в привилегированном режиме EXEC (с приглашением `#`). Чтобы перейти в пользовательский режим (User mode), выполните команду `disable` после приглашения `#`. После этого вы перейдете в пользовательский режим с приглашением `>`.

Пример перехода в пользовательский режим:

```
Username: admin
Password: admin
#
# disable
>
```

В пользовательском режиме доступен только ограниченный набор команд. Эти команды используются для очистки статистики, перехода в привилегированный режим EXEC и проверки связи (ping) с указанным адресом назначения. Для настройки функций необходимо перейти в

SEC.RU | Короткий путь к информации Скачано с sec.ru

режим глобальной конфигурации (Config mode) или режим конфигурации интерфейса (Config Interface mode).

Рекомендации:

- Пользовательский режим (>) — это режим с **минимальными привилегиями**. Его основное назначение — предоставить базовые возможности мониторинга и диагностики сети без риска случайного изменения конфигурации устройства.
- Для возврата в режим с полными привилегиями (#) из пользовательского режима используется команда `enable`, после которой потребуется ввести пароль (если он настроен).
- Типичные команды, доступные в этом режиме (помимо `enable` и `logout`), могут включать:
    - `ping` — проверка доступности сетевого узла.
    - `traceroute` — определение маршрута к узлу.
    - `show` — только для просмотра **некоторых** (обычно наиболее общих) параметров, без доступа к конфиденциальной информации вроде конфигурации.
    - `clear counters` — сброс статистики интерфейсов.

2.5.1 Очистка ARP-кэша (> clear ip arp)

Синтаксис:

```
> clear ip arp
```

Объяснение: Очищает кэш ARP-таблицы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда clear ip arp удаляет все динамические записи из ARP-таблицы коммутатора. Статические ARP-записи (если они настроены) при этом не затрагиваются.
- ARP-таблица (Address Resolution Protocol) используется для сопоставления IP-адресов (уровень 3) с MAC-адресами (уровень 2) в локальной сети. Со временем в ней могут накапливаться устаревшие или неверные записи.
- Очистка ARP-кэша может помочь при устранении проблем со связью в локальной сети, например, если у устройства изменился MAC-адрес или IP-адрес был назначен другому устройству. После выполнения команды коммутатор будет заново узнавать MAC-адреса, отправляя ARP-запросы.
- Команда **не требует подтверждения** и выполняется немедленно. Временная потеря связи с узлами возможна на очень короткий период (миллисекунды), пока не будет выполнен новый ARP-запрос.

2.5.2 Очистка статистики LLDP (> clear lldp statistics)

Синтаксис:

```
> clear lldp statistics
```

Объяснение: Очищает статистику, собранную протоколом LLDP (Link Layer Discovery Protocol).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда clear lldp statistics сбрасывает все счетчики статистики, связанные с работой протокола LLDP, на всех интерфейсах коммутатора.
- LLDP — это стандартный протокол обнаружения соседних устройств уровня 2 (канального уровня). Он собирает информацию о количестве отправленных (transmitted) и полученных (received) кадров LLDP, а также о различных ошибках.
- Очистка статистики полезна для:
    - ✓ **Диагностики проблем** с LLDP-соседством. После сброса можно наблюдать за накоплением статистики заново, чтобы выявить потенциальные ошибки передачи.
    - ✓ **«Обнуления»** счетчиков перед началом нового этапа мониторинга или тестирования, чтобы получить актуальные данные за определенный период.
- Важно понимать, что команда очищает **только статистические счетчики**. Она **не прерывает и не перезапускает** сам процесс работы LLDP, не влияет на таблицу соседей LLDP (show lldp neighbors) и на конфигурацию протокола.

2.5.3 Очистка статистики интерфейсов (> clear statistics)

Синтаксис:

```
> clear statistics {[ interface ] ( <port_type> [ <v_port_type_list> ] )}
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

- <port_type>: Укажите тип интерфейса (например, GigabitEthernet).
- [<v_port_type_list>]: Укажите порты, статистику которых нужно очистить (необязательный параметр).

Объяснение: Очищает статистику (счетчики) указанных интерфейсов.

Рекомендации:

- Команда clear statistics сбрасывает все счетчики ввода-вывода (I/O statistics) на указанных физических интерфейсах (портах). Это включает счетчики переданных/принятых байтов и пакетов, ошибок, сброшенных пакетов и т.д.
- Эта операция **не влияет** на работу самого порта (он не отключается и не перезапускается), а лишь обнуляет данные для мониторинга.
- **Основные случаи применения:**
    1. **Диагностика:** Если на порту наблюдаются ошибки, очистка статистики позволяет начать отсчет «с чистого листа» и определить, продолжают ли ошибки накапливаться, что помогает локализовать проблему (порт, кабель, подключенное устройство).
    2. **Мониторинг:** Для сбора «чистых» данных о нагрузке на порт за определенный период (например, после настройки или в часы пик).
- Если не указывать конкретные порты (<v_port_type_list>), статистика будет очищена для **всех портов** указанного типа. Если не указывать и тип интерфейса, команда может очистить статистику для всех интерфейсов (поведение может зависеть от реализации).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.5.4 Переход в привилегированный режим (> enable)

Синтаксис:

```
> enable [ <new_priv> ]
```

- [<new_priv>]: Уровень привилегий от 0 до 15 (необязательный параметр).

Объяснение: Переход из пользовательского режима (User mode) в привилегированный режим EXEC (Exec mode).

Рекомендации:

- Команда enable является основным способом повышения уровня привилегий в CLI. Без ее выполнения большинство команд настройки и отображения детальной информации будут недоступны.
- По умолчанию, при успешной аутентификации с паролем (если он настроен), команда переводит пользователя на **максимальный уровень привилегий (обычно 15)**, что предоставляет полный доступ ко всем командам.
- **Необязательный аргумент** [<new_priv>] позволяет перейти на определенный, заранее настроенный уровень привилегий (от 0 до 15). Это используется в моделях управления доступом на основе ролей (RBAC), где разным пользователям или задачам назначаются разные уровни. Например, уровень 5 может разрешать только команды show, но не configure.
- Если для привилегированного режима настроен пароль (команда enable secret в глобальной конфигурации), система запросит его после ввода команды enable.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.5.5 Выход/Возврат (> exit)

Синтаксис:

```
> exit
```

Объяснение: Возврат в предыдущий режим. Выполнение этой команды в пользовательском режиме (User mode) завершает сеанс работы с интерфейсом командной строки (выход из системы).

Рекомендации:

- Команда exit является **контекстно-зависимой**. Ее поведение меняется в зависимости от текущего режима CLI:
    - ✓ В **режимах конфигурации** ((config)#, (config-if)# и т.д.) команда exit возвращает пользователя на один уровень вверх в иерархии конфигурации.
    - ✓ В **пользовательском режиме (>)** или **привилегированном режиме EXEC (#)** команда exit завершает текущую сессию управления (выполняет logout).
- Это самый распространенный и безопасный способ пошагового выхода из глубоких уровней конфигурации, в отличие от команды end, которая немедленно возвращает в привилегированный режим EXEC (#) из любого режима конфигурации.
- В пользовательском режиме команды exit и logout абсолютно идентичны по действию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.5.6 Справка (> help)

Синтаксис:

```
> help
```

Объяснение: Выводит справочные сообщения.

Рекомендации:

- Команда help предоставляет краткую текстовую справку о том, как использовать встроенную систему помощи интерфейса командной строки. Она объясняет основной принцип работы контекстной справки с помощью символа ?.
- Фактически, команда help и ввод символа ? (без предшествующего текста) в командной строке **часто являются синонимами** и выводят одинаковую информацию.
  Однако ? является более универсальным и мощным инструментом, так как его можно использовать в любой позиции при вводе команды.
- Сообщение, выводимое командой help, обычно статично и не меняется в зависимости от текущего режима. Для получения конкретного списка доступных команд в текущем режиме всегда используйте ?.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.5.7 Выход из системы (> logout)

Синтаксис:

```
> logout
```

Объяснение: Завершает сеанс работы с интерфейсом командной строки (выход из системы).

Рекомендации:

- Команда logout является **предпочтительным и корректным** способом завершения любой активной сессии управления (консольной, Telnet или SSH). Она гарантирует штатное закрытие сессии на стороне коммутатора.
- После выполнения команды текущее соединение разрывается. При консольном подключении обычно появляется приглашение к началу новой сессии (например, Press ENTER to get started).
- В пользовательском режиме (>) команды logout и exit абсолютно идентичны по своему действию и приводят к одному результату – завершению сессии.
- Использование этой команды вместо простого закрытия окна терминала или обрыва соединения позволяет:
    - ✓ Корректно освободить ресурсы сессии на устройстве.
    - ✓ Четко зафиксировать время окончания сессии в системных журналах (log).
    - ✓ Избежать потенциальных проблем с блокировкой сессии или виртуальных терминальных линий (VTY) в некоторых случаях.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.5.8 Проверка связи (ping) до IPv4-адреса (> ping ip)

Синтаксис:

```
> ping ip <v_ip_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ]
```

- <v_ip_addr>: Укажите IPv4-адрес, до которого нужно проверить связь.
- [repeat <count>]: Количество отправляемых эхо-запросов (пакетов).
- [size <size>]: Размер отправляемого пакета (в байтах).
- [interval <seconds>]: Таймаут ожидания ответа. Тест считается успешным, только если эхо-ответ от узла назначения получен в течение указанного времени.

Объяснение: Выполнение проверки связи (ping-теста) до указанного IPv4-адреса или имени хоста.

Рекомендации:

- Команда ping ip — это основной инструмент диагностики IP-соединения на уровне 3. Она проверяет доступность удаленного узла, измеряет время прохождения пакетов (RTT) и обнаруживает потери пакетов.
- **Базовое использование:** При указании только адреса (ping ip 192.168.1.1) отправляется стандартное количество пакетов (обычно 4 или 5) с интервалом по умолчанию.
- **Расширенные параметры:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ repeat — позволяет отправить определенное количество запросов, что полезно для статистики (например, repeat 100).
- ✓ size — позволяет увеличить размер пакета для проверки фрагментации или производительности сети с большими кадрами (MTU). Размер указывается без учета служебных заголовков.
- ✓ interval — задает паузу (в секундах) между отправкой пакетов. Увеличение интервала снижает нагрузку на сеть при массовой проверке.

- Успешный ping требует корректной маршрутизации. Если маршрут до адреса назначения неизвестен, проверка не удастся, даже если у коммутатора есть IP-адрес в той же подсети.

2.5.9 Проверка связи (ping) до IPv6-адреса (> ping ipv6)

Синтаксис:

```
> ping ipv6 <v_ipv6_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ]
```

- <v_ipv6_addr>: Укажите IPv6-адрес, до которого нужно проверить связь.
- [repeat <count>]: Количество отправляемых эхо-запросов (пакетов).
- [size <size>]: Размер отправляемого пакета (в байтах).
- [interval <seconds>]: Таймаут ожидания ответа. Тест считается успешным, только если эхо-ответ от узла назначения получен в течение указанного времени.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Выполнение проверки связи (ping-теста) до указанного IPv6-адреса или имени хоста.

Рекомендации:

- Команда `ping ipv6` является IPv6-аналогом команды `ping ip` и служит для диагностики связности в сетях IPv6.
- **Критически важно**, чтобы на интерфейсе управления коммутатора (обычно VLAN 1) был настроен глобальный IPv6-адрес и/или адрес link-local, а также корректно настроена IPv6-маршрутизация (статические маршруты или протоколы маршрутизации), если целевой адрес находится в другой подсети.
- Для проверки связи по IPv6 в локальном сегменте (link-local) может потребоваться указание исходящего интерфейса, поскольку адреса link-local не являются глобально уникальными. Синтаксис для этого может отличаться (например, `ping ipv6 fe80::1%Vlan1`).
- Параметры `repeat`, `size` и `interval` работают аналогично IPv4-версии команды и используются для расширенной диагностики и нагрузочного тестирования.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6 Команды в привилегированном режиме EXEC (Commands in EXEC Mode)

2.6.1 Очистка статистики управления доступом (# clear access management statistics)

Синтаксис:

```
# clear access management statistics
```

Объяснение: Очищает статистику управления доступом (HTTP, HTTPS, SNMP, Telnet, SSH).

Рекомендации:

- Команда clear access management statistics сбрасывает внутренние счетчики, связанные с попытками подключения и аутентификации по различным протоколам управления: **HTTP, HTTPS, SNMP, Telnet и SSH**.
- Статистика может включать в себя количество успешных и неудачных попыток входа, количество запросов, ошибки аутентификации и авторизации. Эта информация полезна для **мониторинга активности** и **выявления подозрительных событий** (например, множественных неудачных попыток входа по SSH).
- Очистка статистики не влияет на текущие активные сессии управления, настройки протоколов или параметры безопасности (такие как ACL или пароли). Она лишь обнуляет счетчики, позволяя начать сбор данных заново.
- Команда полезна администраторам для сброса «лишних» данных перед началом периода активного мониторинга или после изменения политик безопасности для оценки их эффекта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.2 Очистка статистики записей ACL (# clear access-list ace statistics)

Синтаксис:

```
# clear access-list ace statistics
```

Объяснение: Очищает статистику записей списков контроля доступа (Access Control List entries).

Рекомендации:

- Команда clear access-list ace statistics сбрасывает все счетчики совпадений (match counters), связанные с **отдельными записями (entries)** в сконфигурированных ACL (как IPv4, так и IPv6, если поддерживается).
- Статистика ACL полезна для:
    1. **Верификации работы ACL:** Подтверждения, что трафик действительно фильтруется ожидаемым образом.
    2. **Оптимизации ACL:** Выявления наиболее часто используемых (или, наоборот, бесполезных) записей для реорганизации списков (самые частые правила должны быть вверху для повышения производительности).
    3. **Диагностики проблем сетевого доступа.**
- Очистка статистики **не удаляет и не изменяет** сами ACL или их записи. Она только обнуляет счетчики совпадений. После сброса новые совпадения начнут накапливаться с нуля.
- Используйте эту команду перед началом тестирования нового ACL или для получения «чистой» статистики за определенный период мониторинга.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.3 Очистка статистики 802.1X (# clear dot1x statistics)

Синтаксис:

```
# clear dot1x statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Параметры:

- [interface (<port_type> [<v_port_type_list>])]: Укажите интерфейс (порт), для которого нужно очистить статистику.

Объяснение: Очищает статистику протокола 802.1X (для указанных интерфейсов).

Рекомендации:

- Команда clear dot1x statistics сбрасывает счетчики, связанные с работой протокола аутентификации **IEEE 802.1X** (Port-Based Network Access Control). Это включает статистику успешных/неудачных аутентификаций, запросов на повторную аутентификацию (reauth), логаутов, тайм-аутов и различных ошибок протокола.
- Статистика 802.1X критически важна для **мониторинга и отладки** системы контроля доступа к сети (NAC). Она помогает выявлять проблемы с клиентами, сервером аутентификации (RADIUS) или настройками портов.
- Если не указывать конкретный интерфейс, статистика будет очищена **для всех портов**, на которых включен 802.1X.
- Очистка статистики **не прерывает** текущие сеансы аутентификации на портах и **не изменяет** конфигурацию 802.1X. Она лишь обнуляет счетчики для последующего наблюдения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.4 Очистка статистики ERPS (# clear erps statistics)

Синтаксис:

```
# clear erps [ <groups> ] statistics
```

Параметр:

- [<groups>]: Укажите группу ERPS, статистику которой нужно очистить.

Объяснение: Очищает статистику (для указанной группы) протокола ERPS.

Рекомендации:

- Команда clear erps statistics сбрасывает счетчики, связанные с работой протокола **Ethernet Ring Protection Switching (ERPS или G.8032)**. Этот протокол обеспечивает резервирование и быстрое восстановление (менее 50 мс) в кольцевых топологиях Ethernet.
- Статистика ERPS может включать счетчики количества изменений состояния кольца (Ring State Changes), полученных/отправленных служебных кадров (R-APS), тайм-аутов и различных ошибок. Она используется для **мониторинга стабильности** кольца и **диагностики** проблем со сходимостью.
- Если параметр [<groups>] не указан, статистика будет очищена для **всех** сконфигурированных групп ERPS.
- Очистка статистики **не влияет** на текущее рабочее состояние кольца (блокированные/разблокированные порты), конфигурацию протокола или трафик данных. Она только обнуляет счетчики мониторинга.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.5 Очистка ARP-кэша (# clear ip arp)

Синтаксис:

```
# clear ip arp
```

Объяснение: Очищает ARP-кэш.

Рекомендации:

- Команда # clear ip arp идентична по действию команде > clear ip arp, но доступна в привилегированном режиме EXEC. Она удаляет **все динамические записи** из таблицы ARP (Address Resolution Protocol) коммутатора. Статические ARP-записи, если они были предварительно настроены, сохраняются.
- ARP-таблица сопоставляет IP-адреса (слой 3) с MAC-адресами (слой 2) в локальной сети. Очистка кэша заставляет коммутатор заново узнавать MAC-адреса соседних устройств при следующей необходимости отправки данных, отправляя ARP-запросы.
- **Типичные случаи использования:**
    - ✓ Устранение проблем со связью, когда MAC-адрес устройства изменился (например, замена сетевой карты), а в кэше осталась старая запись.
    - ✓ Сброс устаревших записей при изменении IP-адресации в сети.
    - ✓ Диагностика проблем ARP-спуфинга или других аномалий.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Команда выполняется немедленно и без подтверждения. Временная потеря пакетов (на время выполнения нового ARP-запроса) возможна, но обычно незаметна.

2.6.6 Очистка детальной статистики IP DHCP (# clear ip dhcp detailed statistics)

Синтаксис:

```
# clear ip dhcp detailed statistics { server | client | snooping | relay | helper | a
ll } [ interface ( <port_type> [ <in_port_list> ] ) ]
```

Параметр:

- { server | client | snooping | relay | helper | all }: Укажите тип информации, которую нужно очистить.
- [interface (<port_type> [<in_port_list>])]: Укажите тип интерфейса и номер порта.

Объяснение: Очищает статистику IP DHCP.

Рекомендации:

- Команда clear ip dhcp detailed statistics предоставляет детальный контроль над сбросом счетчиков для различных DHCP-функций коммутатора. Это мощный инструмент для мониторинга и отладки работы DHCP.
- **Выбор компонента для очистки (обязательный выбор одного из):**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ server – Статистика встроенного DHCP-сервера (если функция включена).
- ✓ client – Статистика DHCP-клиента (например, на интерфейсе управления).
- ✓ snooping – Статистика DHCP Snooping (безопасность).
- ✓ relay – Статистика DHCP Relay Agent (ретранслятора).
- ✓ helper – Статистика DHCP Helper (обычно синоним relay).
- ✓ all – Статистика всех перечисленных выше компонентов.

- **Очистка на уровне интерфейса (необязательно):** Позволяет сбросить статистику не глобально, а только для указанных портов, что полезно для точечной диагностики.
- Статистика может включать количество отправленных/полученных DHCP-сообщений каждого типа (DISCOVER, OFFER, REQUEST, ACK, NAK), ошибок, отброшенных пакетов (snooping) и т.д.

2.6.7 Очистка статистики IP DHCP Relay (# clear ip dhcp relay statistics)

Синтаксис:

```
# clear ip dhcp relay statistics
```

Объяснение: Очищает статистику ретранслятора IP DHCP (DHCP Relay Agent).

Рекомендации:

- Команда clear ip dhcp relay statistics является **частным случаем** более общей команды clear ip dhcp detailed statistics

SEC.RU | Короткий путь к информации Скачано с sec.ru

relay. Она сбрасывает счетчики, специфичные для функции **DHCP Relay Agent**.

- **DHCP Relay Agent** — это функция, которая позволяет клиентам из одной IP-подсети (VLAN) получать адреса от DHCP-сервера, находящегося в другой подсети, путем ретрансляции широковещательных DHCP-сообщений в виде unicast на указанный сервер.
- Статистика обычно включает количество принятых и пересланных DHCP-сообщений различных типов (DISCOVER, REQUEST, OFFER, ACK), количество сгенерированных ответов, а также ошибок (например, отсутствие настроенного адреса сервера).
- Очистка статистики не влияет на работоспособность самой функции relay, ее конфигурацию (например, ip helper-address) или текущие сессии аренды адресов. Она лишь обнуляет счетчики для последующего наблюдения за активностью.

2.6.8 Очистка статистики IP DHCP Snooping (# clear ip dhcp snooping statistics)

Синтаксис:

```
# clear ip dhcp snooping statistics [ interface ( <port_type> [ <in_port_list> ] ) ]
```

Объяснение: Очищает статистику IP DHCP Snooping.

Рекомендации:

- Команда clear ip dhcp snooping statistics является **частным случаем** более общей команды clear ip dhcp detailed statistics

SEC.RU | Короткий путь к информации Скачано с sec.ru

snooping. Она сбрасывает счетчики, специфичные для функции **DHCP Snooping** — механизма безопасности, который проверяет DHCP-сообщения и строит базу данных о соответствии IP-MAC-Port (Binding Database).

- **DHCP Snooping** защищает сеть от атак, связанных с DHCP (например, rogue DHCP-серверы). Его статистика включает количество обработанных пакетов, отброшенных пакетов (из-за нарушений политики доверия, несоответствия binding и пр.), а также количество записей в binding table.
- **Очистка на уровне интерфейса:** Необязательный параметр [interface ...] позволяет очистить статистику только для указанных портов, что удобно для диагностики проблем на конкретном линке.
- Важно: Эта команда **не очищает саму базу данных привязок (binding database)**. Она сбрасывает только счетчики операций. Для очистки базы данных привязок используется другая команда (например, clear ip dhcp snooping binding).

2.6.9 Очистка статистики IP IGMP Snooping (# clear ip igmp snooping statistics)

Синтаксис:

```
# clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
```

Объяснение: Очищает статистику IP IGMP Snooping.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда clear ip igmp snooping statistics сбрасывает счетчики, связанные с работой функции **IGMP Snooping**. Этот протокол позволяет коммутаторам уровня 2 «прослушивать» IGMP-сообления между маршрутизаторами и хостами, чтобы эффективно управлять многоадресным (multicast) трафиком, перенаправляя его только на те порты, где есть подписчики.
- Статистика может включать количество полученных IGMP-запросов (Queries), отчетов (Reports), покиданий группы (Leaves), ошибок, а также количество отслеживаемых многоадресных групп.
- **Очистка на уровне VLAN:** Необязательный параметр [vlan <v_vlan_list>] позволяет очистить статистику не для всей системы, а только для указанных VLAN. Это полезно, если IGMP Snooping включен только в определенных VLAN.
- Очистка статистики **не влияет** на текущее состояние подписок (группы, порты), таблицы многоадресной фильтрации или конфигурацию IGMP Snooping. Она лишь обнуляет счетчики для последующего мониторинга.

2.6.10 Очистка IP-статистики (# clear ip statistics)

Синтаксис:

```
# clear ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
```

Объяснение: Очищает IPv4-статистику для системы, интерфейса и ICMP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда clear ip statistics предоставляет гибкий инструмент для сброса различных счетчиков, связанных с обработкой IPv4-трафика. Можно очищать статистику выборочно или все сразу.
- **Ключевые параметры (можно комбинировать):**
    - ✓ system – Сброс глобальной системной статистики IP (общее количество полученных/переданных пакетов, ошибок).
    - ✓ interface vlan <v_vlan_list> – Сброс статистики IP для указанных интерфейсов VLAN (например, interface vlan 1). Это влияет на счетчики уровня 3 для этих интерфейсов.
    - ✓ icmp – Сброс глобальной статистики протокола ICMP (количество отправленных/полученных эхо-запросов и ответов, ошибок и т.д.).
    - ✓ icmp-msg <type> – Сброс статистики для сообщений ICMP определенного типа (например, icmp-msg echo для эхо-запросов).
- Если **ни один параметр не указан**, команда может очистить всю IP-статистику (поведение может зависеть от реализации устройства).
- Очистка не влияет на таблицы маршрутизации, ARP-кэш или состояние интерфейсов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.11 Очистка статистики IPv6 MLD Snooping (# clear ipv6 mld snooping statistics)

Синтаксис:

```
# clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics
```

Объяснение: Очищает статистику для IPv6 MLD Snooping.

Рекомендации:

- Команда clear ipv6 mld snooping statistics является IPv6-аналогом команды для IGMP Snooping. Она сбрасывает счетчики, связанные с функцией **MLD (Multicast Listener Discovery) Snooping**. Этот протокол позволяет коммутаторам уровня 2 эффективно управлять многоадресным трафиком IPv6, отслеживая подписчиков.
- Статистика может включать количество полученных MLD-запросов (Queries), отчетов (Reports), выполненных действий (Done), ошибок, а также количество отслеживаемых IPv6 многоадресных групп.
- **Очистка на уровне VLAN:** Необязательный параметр [vlan <v_vlan_list>] позволяет очистить статистику только для указанных VLAN. Используйте его, если MLD Snooping включен не во всех VLAN.
- Как и в случае с IGMP, очистка статистики **не затрагивает** текущее состояние подписок (активные группы, порты-получатели) или конфигурацию MLD Snooping. Она обнуляет только счетчики мониторинга.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.12 Очистка таблицы устройств «соседей» IPv6 (# clear ipv6 neighbors)

Синтаксис:

```
# clear ipv6 neighbors
```

Объяснение: Очищает таблицу устройств «соседей» IPv6.

Рекомендации:

- Команда clear ipv6 neighbors удаляет все **динамические записи** из таблицы соседей IPv6 (Neighbor Discovery Cache), которая является аналогом ARP-таблицы для IPv6. Статические записи соседей (если они были настроены) сохраняются.
- Таблица соседей IPv6 создается протоколом NDP (Neighbor Discovery Protocol) и содержит соответствия между IPv6-адресами и MAC-адресами устройств в локальном сетевом сегменте (link-local или одной подсети).
- **Типичные случаи использования:**
  - ✓ Устранение проблем со связью при изменении MAC-адреса устройства в сети IPv6.
  - ✓ Принудительное обновление информации о соседях, если старые записи стали некорректными.
  - ✓ Диагностика проблем, связанных с протоколом NDP.
- Команда выполняется немедленно. После ее выполнения коммутатору потребуется заново выполнить процедуру обнаружения соседей (отправить NS-запросы) при следующей необходимости связи с этими IPv6-адресами, что вызовет небольшую задержку.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.13 Очистка IPv6-статистики (# clear ipv6 statistics)

Синтаксис:

```
# clear ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
```

Объяснение: Очищает IPv6-статистику для системы, интерфейса и ICMPv6.

Рекомендации:

- Команда clear ipv6 statistics является IPv6-аналогом команды clear ip statistics. Она сбрасывает различные счетчики, связанные с обработкой IPv6-трафика, с возможностью выборочной очистки.
- **Ключевые параметры (можно комбинировать):**
  - ✓ system – Сброс глобальной системной статистики IPv6 (общее количество полученных/переданных IPv6-пакетов, ошибок, отброшенных пакетов).
  - ✓ interface vlan <v_vlan_list> – Сброс статистики IPv6 для указанных интерфейсов VLAN уровня 3.
  - ✓ icmp – Сброс глобальной статистики протокола ICMPv6. Сюда входят все типы ICMPv6-сообщений (Echo, Neighbor Discovery, MLD и т.д.).
  - ✓ icmp-msg <type> – Сброс статистики для сообщений ICMPv6 определенного типа (например, icmp-msg echo-request).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Если **ни один параметр не указан**, команда, очистит всю IPv6-статистику (системную, интерфейсную и ICMPv6) — аналогично поведению команды для IPv4.
- Очистка статистики не влияет на таблицы маршрутизации IPv6, кэш соседей (NDP) или состояние интерфейсов.

2.6.14 Очистка статистики LACP (# clear lacp statistics)

Синтаксис:

```
# clear lacp statistics
```

Объяснение: Очищает статистику протокола LACP.

Рекомендации:

- Команда clear lacp statistics сбрасывает все счетчики, связанные с работой протокола **LACP (Link Aggregation Control Protocol, IEEE 802.3ad/802.1ax)**. Этот протокол используется для автоматического объединения нескольких физических портов в один логический агрегированный канал (LAG, порт-канал).
- Статистика LACP обычно включает:
    - ✓ Количество отправленных и полученных LACPDU (Protocol Data Units).
    - ✓ Количество ошибок в LACPDU.
    - ✓ Счетчики различных событий протокола (изменения состояния порта, тайм-ауты).
- Очистка статистики **не влияет** на:
    - ✓ Текущее состояние агрегированных групп (up/down).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Состав и настройки агрегированных каналов.
- ✓ Передачу пользовательского трафика через агрегированный канал.

- Команда полезна для сбора «чистых» данных о работе LACP после настройки или изменения агрегации, а также для диагностики проблем со стабильностью порт-канала.

2.6.15 Очистка статистики LLDP (# clear lldp statistics)

Синтаксис:

```
# clear lldp statistics
```

Объяснение: Очищает статистику LLDP.

Рекомендации:

- Команда `# clear lldp statistics` идентична по действию команде `> clear lldp statistics` (раздел 2.7.2), но доступна в привилегированном режиме EXEC. Она полностью обнуляет все счетчики протокола **LLDP (Link Layer Discovery Protocol)** на всех интерфейсах устройства.
- Статистика LLDP включает количество отправленных (transmitted) и полученных (received) кадров LLDP, количество ошибок приема, отброшенных кадров, а также неподдерживаемых или нераспознанных TLV.
- Команда сбрасывает **только статистические счетчики**. Она **не** влияет на:
  - ✓ Работу самого протокола LLDP (он продолжает работать).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Таблицу LLDP-соседей (show lldp neighbors).
- ✓ Конфигурацию LLDP (интервалы, тайм-ауты, включение/выключение на портах).

- Очистка статистики — стандартная процедура перед началом нового этапа мониторинга или для диагностики проблем со стабильностью обмена LLDP-сообщениями с соседями.

2.6.16 Очистка журналов системных сообщений (# clear logging)

Синтаксис:

```
# clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]
```

Объяснение: Очищает указанные системные события (syslog).

Рекомендации:

- Команда clear logging управляет внутренним буфером системных сообщений (syslog) коммутатора. Этот буфер хранит записи о событиях (информационных, предупреждениях, ошибках), которые еще не были отправлены на внешний syslog-сервер или просмотрены администратором.
- **Выборочная очистка по уровню серьезности (severity):**
  - ✓ info – Очищает информационные сообщения.
  - ✓ warning – Очищает предупреждения.
  - ✓ error – Очищает сообщения об ошибках.
- Если **ни один параметр не указан**, команда очистит весь внутренний буфер сообщений.
- **Важно:** Эта команда очищает только **внутренний буфер** на устройстве. Она **не затрагивает** сообщения, уже переданные на внешний syslog-сервер, и не влияет на настройки логирования (logging host и т.д.).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.17 Очистка таблицы MAC-адресов (# clear mac address-table)

Синтаксис:

```
# clear mac address-table
```

Объяснение: Очищает таблицу MAC-адресов.

Рекомендации:

- Команда clear mac address-table удаляет **все динамически изученные записи** из таблицы MAC-адресов коммутатора (Content Addressable Memory, CAM). Статические MAC-адреса, настроенные вручную, при этом **не удаляются**.
- Таблица MAC-адресов — это фундаментальная база данных коммутатора уровня 2. Она сопоставляет MAC-адреса устройств с конкретными портами коммутатора, что позволяет ему интеллектуально пересылать кадры только на нужный порт, а не на все (flooding).
- **Внимание:**
    - ✓ **Временное нарушение связи:** После очистки таблицы коммутатор временно будет вынужден *затоплять* (flood) трафик неизвестных назначений во всех портах VLAN, пока не изучит новые расположения MAC-адресов. Это может вызвать кратковременный всплеск широковещательного трафика и небольшие задержки.
    - ✓ **Диагностика и безопасность:** Команда используется для:

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Устранения проблем, связанных с устаревшими или неверными записями MAC (например, после перемещения устройства).
2. Сброса таблицы перед тестированием сети или сбором данных об изучении адресов.
3. Очистки таблицы в рамках мер безопасности (например, после инцидента).

- Для очистки только на определенном порту или в определенной VLAN используйте более конкретные варианты команды (например, clear mac address-table dynamic interface GigabitEthernet 1/1).

2.6.18 Очистка информации MEP (# clear mep)

Синтаксис:

```
# clear mep <inst> { lm | dm | tst }
```

- <inst>: Укажите идентификатор (ID) экземпляра MEP.
- { lm | dm | tst }: Укажите тип информации MEP для очистки.

Объяснение: Очищает информацию определенного экземпляра MEP (Maintenance End Point).

Рекомендации:

- Команда clear mep управляет данными, связанными с конечными точками обслуживания (**MEP**) в рамках стандартов IEEE 802.1ag (CFM - Connectivity Fault Management) и ITU-T Y.1731 (OAM - Operations, Administration and Maintenance). Эти протоколы используются для диагностики,

SEC.RU | Короткий путь к информации Скачано с sec.ru

мониторинга и измерения производительности в Ethernet-сетях (например, в сетях провайдеров или крупных предприятий).

- Типы очищаемой информации (обязательный выбор одного):
  - ✓ lm – Очищает статистику и данные **Loss Measurement (Измерение потерь)** для указанного MEP.
  - ✓ dm – Очищает статистику и данные **Delay Measurement (Измерение задержки)** для указанного MEP.
  - ✓ tst – Очищает информацию, связанную с тестовыми кадрами (**Test frames**) для указанного MEP.
- MEP идентифицируется по номеру экземпляра (<inst>), который должен быть предварительно сконфигурирован. Команда не удаляет сам экземпляр MEP и его конфигурацию, а лишь очищает накопленные оперативные данные измерений и тестов.
- Используется для сброса счетчиков перед началом нового цикла измерений или после изменения конфигурации сети.

2.6.19 Очистка информации протокола Spanning Tree (# clear spanning-tree)

Синтаксис:

```
# clear spanning-tree { { statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ] } | { detected-protocols [ interface ( <port_type> [ <v_port_type_list_1> ] ) ] } }
```

Объяснение: Очищает статистику Spanning Tree для указанных интерфейсов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда clear spanning-tree предоставляет два основных варианта очистки данных, связанных с протоколом **Spanning Tree Protocol (STP)** и его расширениями (RSTP, MSTP).
- **Вариант 1: Очистка статистики (**statistics**)**
    - ✓ Сбрасывает счетчики протокола STP на портах. Это может включать количество полученных/отправленных BPDU, количество изменений топологии (TCN), ошибок BPDU и т.д.
    - ✓ Если не указать конкретные интерфейсы ([interface ...]), статистика будет очищена на **всех** портах.
    - ✓ Полезно для сбора «чистых» данных после изменения конфигурации или для диагностики.
- **Вариант 2: Очистка обнаруженных протоколов (**detected-protocols**)**
    - ✓ Сбрасывает внутренний кэш информации о типе протокола STP (**STP, RSTP, MSTP**), обнаруженном на соседних портах. Это заставляет коммутатор заново определять, какой протокол используется на линке.
    - ✓ Применяется в ситуациях, когда тип протокола на соседнем порту изменился, но коммутатор не обновил эту информацию автоматически.
- Эти команды **не влияют** на состояние портов (blocking/forwarding), конфигурацию STP (приоритеты, стоимости) и саму работу протокола.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.20 Очистка статистики интерфейсов (# clear statistics)

Синтаксис:

```
# clear statistics [ interface ] ( <port_type> [ <v_port_type_list> ] )
```

Объяснение: Очищает статистику интерфейсов Fast Ethernet и/или Gigabit Ethernet.

Рекомендации:

- Команда `# clear statistics` является аналогом команды `> clear statistics` (раздел 2.7.3), но доступна в привилегированном режиме EXEC. Она сбрасывает все счетчики ввода-вывода (**I/O statistics**) на указанных физических Ethernet-портах.
- Очищаемая статистика включает: количество переданных/принятых байтов и пакетов, ошибок (CRC, выравнивания, гигантских/карликовых кадров), отброшенных пакетов и т.д.
- Если не указывать конкретные порты ([<v_port_type_list>]), статистика будет очищена для **всех портов** указанного типа (например, всех портов `GigabitEthernet`).
- Эта операция **не влияет** на административное состояние порта (up/down), настройки скорости/дуплекса или конфигурацию VLAN. Она лишь обнуляет счетчики мониторинга.
- Основное назначение — **диагностика** (например, определение, продолжают ли накапливаться ошибки после очистки) и сбор статистики нагрузки за определенный период.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.21 Вход в режим глобальной конфигурации (# config terminal)

Синтаксис:

```
# config terminal
или
# conf t
```

Объяснение: Переход в режим глобальной конфигурации (Global Config mode).

Рекомендации:

- Команда config terminal является **ключевой командой** для перехода из привилегированного режима EXEC (режима мониторинга и диагностики, #) в режим глобальной конфигурации ((config)#), где можно вносить изменения в настройки системы.
- В этом режиме становятся доступны команды для настройки глобальных параметров коммутатора, таких как:
    - ✓ Имя устройства (hostname)
    - ✓ Пароли (enable secret)
    - ✓ Параметры SNMP, системного времени, DNS
    - ✓ Создание VLAN и т.д.
- Это **первый уровень** иерархии конфигурации. Для настройки конкретных интерфейсов (портов, VLAN) из этого режима необходимо перейти на более глубокий уровень, например, с помощью команды interface.
- Для выхода из режима глобальной конфигурации обратно в привилегированный режим EXEC используйте команду exit или end (команда end возвращает сразу на уровень # из любого уровня конфигурации).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.22 Копирование (# copy)

Синтаксис:

```
# copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [ syntax-check ]
```

- { startup-config | running-config | <source_path> }: Укажите тип файла или путь к исходному файлу для копирования. Это может быть startup-config, running-config или конкретный файл во flash-памяти или на TFTP-сервере.
- { startup-config | running-config | <destination_path> }: Укажите тип файла или путь к файлу назначения. Это может быть startup-config, running-config или конкретный файл во flash-памяти или на TFTP-сервере.
- [syntax-check]: Проверка синтаксиса перед сохранением (необязательный параметр).

Объяснение: Сохраняет рабочую конфигурацию в стартовую конфигурацию.

Рекомендации:

- Команда copy — это **универсальная команда для управления файлами** в системе, аналогичная команде copy в ОС Cisco IOS. Ее основное назначение — копирование файлов между различными источниками и приемниками.
- **Наиболее частые сценарии использования:**
    1. **Сохранение конфигурации:** # copy running-config startup-config — сохраняет текущую активную конфигурацию (RAM) в загрузочную конфигурацию

SEC.RU | Короткий путь к информации Скачано с sec.ru

(flash). **Это обязательное действие для сохранения изменений после настройки.**

2. **Резервное копирование конфигурации на TFTP-сервер:** `# copy running-config tftp://192.168.1.100/backup.cfg`
3. **Восстановление конфигурации с TFTP-сервера:** `# copy tftp://192.168.1.100/backup.cfg running-config`
4. **Копирование файлов прошивки (образов ПО).**

- **Параметр** `syntax-check`**:** При копировании конфигурации в `running-config` или `startup-config` этот параметр заставляет систему проверить синтаксис загружаемых команд перед их применением, что помогает избежать ошибок.
- При копировании конфигурации поверх `running-config` изменения применяются немедленно (и могут вызвать разрыв соединения). При копировании поверх `startup-config` изменения вступят в силу только после следующей перезагрузки.

2.6.23 Удаление файла (# delete)

Синтаксис:

```
# delete <path>
```

Объяснение: Удаляет файл, сохраненный во флеш-памяти (Flash).

Параметры (Parameters):

- `<path>`: Имя файла во флеш-памяти, который необходимо удалить.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `delete` предназначена для **безвозвратного удаления файлов** из флеш-памяти (flash:) коммутатора.
- **Примеры удаляемых файлы:**
  - ✓ Устаревшие образы операционной системы (прошивки).
  - ✓ Резервные копии конфигураций (`startup-config.backup`, `config.bak`).
  - ✓ Файлы журналов (log files).
  - ✓ Загруженные, но неиспользуемые файлы.
- **Внимание:** Перед удалением убедитесь, что файл **не является активным** (например, текущей загрузочной прошивкой `primary.dat` или текущей стартовой конфигурацией `startup-config`). Удаление активных системных файлов может сделать устройство неработоспособным.
- Для безопасного удаления рекомендуется сначала просмотреть содержимое флеш-памяти с помощью команды `dir` или `show flash:`.

2.6.24 Просмотр содержимого каталога (# dir)

Синтаксис:

```
# dir
```

Объяснение: Отображает файлы во флеш-памяти.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `dir` (directory) используется для просмотра содержимого файловой системы устройства, в первую очередь — встроенной флеш-памяти (`flash:`). Это аналог команды `ls` в Linux или `dir` в Windows.
- Команда выводит список файлов с ключевой информацией:
    - ✓ **Индекс/номер** файла.
    - ✓ **Атрибуты** (например, `-rw-` — обычный файл, доступный для чтения и записи).
    - ✓ **Размер** файла в байтах.
    - ✓ **Дата и время** последнего изменения.
    - ✓ **Имя файла**.
- **Основное применение:**
    1. **Проверка доступных образов ПО:** Определение текущей активной (`primary.dat`) и резервной (`backup.dat`) прошивки.
    2. **Управление конфигурациями:** Поиск файлов конфигураций (`startup-config`, резервные копии).
    3. **Подготовка к операциям:** Проверка наличия и размера файла перед его удалением (`delete`), копированием (`copy`) или обновлением ПО.
- Для просмотра файлов в других файловых системах (например, `usb:`, если поддерживается) может потребоваться указать путь: `dir usb:`.

```
# dir
Directory of flash:

                                    default-config
    r-  01-01-1970 00:00:00      284
                                    startup-config
    rw  06-06-1970 01:56:32     1487


2 files, 3258 bytes total.
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.25 Переключение между пользовательским и привилегированным режимами (# disable & # enable)

Синтаксис:

```
# disable
#enable
```

Объяснение: Возврат в пользовательский режим или вход в привилегированный режим EXEC.

Рекомендации:

- Команды # disable и # enable используются для переключения между двумя основными уровнями доступа в CLI:
  - ✓ # disable – Переход из привилегированного режима EXEC (#) в пользовательский режим (>). Эта команда не требует пароля и просто понижает уровень привилегий.
  - ✓ # enable – Переход из привилегированного режима EXEC (#) на заданный или максимальный уровень привилегий (оставаясь в режиме #). Если для максимального уровня привилегий (обычно 15) настроен пароль (enable secret), система запросит его. Эта команда также позволяет перейти на конкретный уровень (например, enable 5), если модель RBAC настроена.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.26 Инициализация 802.1X (# dot1x initialize)

Синтаксис:

```
# dot1x initialize [ interface ( <port_type> [ <plist> ] ) ]
```

- [interface (<port_type> [<plist>])]: Укажите тип интерфейса, который вы хотите использовать. Символ * означает все интерфейсы.
- <plist>: Укажите порты, к которым применяется эта команда.

Объяснение: Немедленная инициализация функции 802.1X на интерфейсе.

Рекомендации:

- Команда dot1x initialize выполняет **принудительную переинициализацию (сброс состояния) протокола 802.1X** на указанных портах. Это приводит к немедленному завершению текущей сессии аутентификации (если она есть) и началу нового цикла аутентификации.
- Типичные сценарии использования:
    1. **Диагностика проблем с аутентификацией:** Если подключенное устройство (супликант) не запускает процесс аутентификации или завис, принудительная инициализация на стороне коммутатора (аутентификатора) может заставить его начать процесс заново.
    2. **Применение изменений конфигурации:** После изменения настроек 802.1X (например, параметров тайм-аутов, контрольных точек (checkpoints) или VLAN)

SEC.RU | Короткий путь к информации Скачано с sec.ru

на работающем порту, эта команда позволяет немедленно применить новые настройки к существующей сессии.

3. **Ручной сброс сессии:** Для отключения аутентифицированного устройства без физического отключения кабеля.

- Если порт не указан (используется * или параметр опущен), инициализация выполняется **для всех портов**, на которых включен 802.1X.
- Команда не изменяет постоянную конфигурацию 802.1X и не очищает статистику.

2.6.27 Управление ERPS (# erps)

Синтаксис:

```
# erps <group> command { clear | force | manual } { port0 | port1 }
```

Объяснение: Настройка ERPS.

Параметры (Parameters):

- <group: 1-64>: Укажите номер группы от 1 до 64.
- { clear | force | manual }: Укажите действие.
- { port0 | port1 }: Укажите порт port0 (восточный, east) или port1 (западный, west), к которому применяется команда.

Рекомендации:

- Команда erps <group> command используется для ручного управления состоянием защиты в кольце Ethernet Ring

SEC.RU | Короткий путь к информации Скачано с sec.ru

Protection Switching (ERPS). Она позволяет администратору влиять на логику блокировки портов вручную, что требуется для обслуживания или принудительного изменения маршрута трафика.

- **Ключевые действия (Actions):**
  - ✓ clear – **Очистка** ручной команды. Возвращает указанный порт в автоматический режим работы, управляемый протоколом ERPS.
  - ✓ force – **Принудительная** блокировка (Force Switch) указанного порта. Коммутатор немедленно переводит порт в состояние Blocked, независимо от состояния кольца. Используется для приоритетного обслуживания или экстренного изменения пути.
  - ✓ manual – **Ручная** блокировка (Manual Switch) указанного порта. Порт блокируется, но если в кольце произойдет реальная ошибка (Signal Fail), протокол переопределит ручную команду для разблокировки порта и восстановления связи. Это менее приоритетная команда, чем force.
- Параметры port0 и port1 соответствуют портам, назначенным в конфигурации данной группы ERPS (обычно это два порта, образующие часть кольца).
- Используйте эти команды с осторожностью, так как они могут вызвать плановый или внеплановый разрыв трафика в кольце.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.28 Переключение на резервную прошивку (# firmware swap)

Синтаксис:

```
# firmware swap
```

Объяснение: Использовать другой резервный файл образа прошивки, загруженный во флеш-память.

Рекомендации:

- Команда firmware swap выполняет **переключение активного образа прошивки** на устройстве. Она меняет роли между текущей основной (primary) и резервной (backup) прошивками, которые должны быть предварительно загружены во флеш-память.
- Эта команда используется для отката к предыдущей, стабильной версии прошивки, если после обновления на новую версию возникли проблемы (ошибки, нестабильная работа).
- **Внимание:** После выполнения этой команды для применения изменений **требуется перезагрузка устройства** (команда reload). Переключение само по себе не перезагружает коммутатор.
- Перед выполнением команды рекомендуется:
    1. Проверить наличие двух валидных образов прошивки во флеш-памяти с помощью dir.
    2. Сохранить текущую конфигурацию (copy running-config startup-config).
    3. Убедиться, что резервный образ действительно является работоспособной и совместимой версией.
- После перезагрузки с резервным образом новая (проблемная) прошивка станет резервной и может быть удалена или перезаписана.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.29 Обновление прошивки (# firmware upgrade)

Синтаксис:

```
# firmware upgrade <TFTPServer_path_file : word>
```

- <TFTPServer_path_file : word>: Укажите IP-адрес TFTP-сервера и имя файла прошивки.

Объяснение: Обновление образа прошивки.

Рекомендации:

- Команда firmware upgrade выполняет **загрузку нового образа системного ПО (прошивки) с TFTP-сервера** во флеш-память коммутатора и его активацию. Это основной способ обновления программного обеспечения устройства.
- **Важные шаги перед обновлением:**
    1. **Резервное копирование:** Сохраните текущую конфигурацию (copy running-config startup-config) и, желательно, скопируйте ее на внешний сервер.
    2. **Проверка файла:** Убедитесь, что файл прошивки является корректным, совместимым с моделью коммутатора и загружен в корневой каталог TFTP-сервера.
    3. **Сетевая доступность:** Убедитесь, что у коммутатора есть IP-соединение с TFTP-сервером.
- **Процесс:** После выполнения команды коммутатор загрузит указанный файл, сохранит его во флеш-памяти (обычно как резервный образ), а затем автоматически перезагрузится для

SEC.RU | Короткий путь к информации Скачано с sec.ru

активации новой прошивки. Время простоя сети зависит от размера файла и скорости загрузки.

- После перезагрузки рекомендуется проверить версию прошивки (`show version`) и убедиться в работоспособности всех критически важных функций.

2.6.30 Повторный запрос DHCP для интерфейса VLAN (# ip dhcp retry interface vlan)

Синтаксис:

```
# ip dhcp retry interface vlan <vlan_id>
```

- `<vlan_id>`: Укажите допустимый идентификатор VLAN для DHCP-запроса.

Объяснение: Выполняет повторный DHCP-запрос для указанного интерфейса VLAN.

Рекомендации:

- Команда `ip dhcp retry interface vlan` используется для **принудительного повторного запуска процесса получения IP-адреса по DHCP** на указанном интерфейсе VLAN уровня 3 (обычно интерфейсе управления).
- **Типичные сценарии использования:**
    1. **Устранение сбоев:** Если интерфейс не смог получить адрес (остался в состоянии `0.0.0.0` или с конфликтным адресом `169.254.x.x`), эта команда заставляет его отправить новый DHCPDISCOVER.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. **Обновление аренды вручную:** Для немедленного обновления DHCP-аренды до истечения срока текущей.
3. **Применение изменений:** После изменения конфигурации сети или DHCP-сервера для получения новых параметров (шлюз, DNS) без ожидания перезагрузки.

- Команда отправляет новый широковещательный DHCP-запрос. Для его успеха DHCP-сервер должен быть доступен в той же широковещательной области (broadcast domain), что и интерфейс VLAN, либо должен быть настроен DHCP Relay (`ip helper-address`).
- Эта команда не изменяет конфигурацию и не очищает статистику DHCP.

2.6.31 Просмотр содержимого файла (# more)

Синтаксис:

```
# more <path>
```

- `<path>`: Укажите имя файла.

Объяснение: Отображает содержимое файла во флеш-памяти или на TFTP-сервере.

Рекомендации:

- Команда `more` используется для **просмотра содержимого текстовых файлов**, хранящихся в файловой системе коммутатора (обычно во флеш-памяти) или на удаленном TFTP-

SEC.RU | Короткий путь к информации Скачано с sec.ru

сервере. Это аналог команды more в Unix/Linux или type в Windows.

- **Типичные просматриваемые файлы:**
  - ✓ Файлы конфигурации (startup-config, резервные копии .cfg).
  - ✓ Текстовые файлы журналов (log files).
  - ✓ Файлы с информацией о лицензиях или других текстовых данных.
- Команда не предназначена для просмотра бинарных файлов (таких как образы прошивки .dat), их содержимое будет отображено как "trash".
- Для постраничного просмотра длинных файлов обычно можно использовать:
  - ✓ **Пробел** – переход на следующую страницу.
  - ✓ **Enter** – переход на следующую строку.
  - ✓ **Q** – выход из режима просмотра.
- Для просмотра файлов на TFTP-сервере укажите полный URL (например, more tftp://192.168.1.100/config_backup.txt).

2.6.32 Проверка связи (ping) до IPv4-адреса (# ping ip)

Синтаксис:

```
# ping ip <v_ip_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ]
```

Объяснение: Проверка связи (ping) с указанным IP-адресом.

Параметры:

- <v_ip_addr>: Укажите IPv4-адрес для проведения ping-теста.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда # ping ip функционально идентична команде > ping ip (раздел 2.7.8), но доступна в привилегированном режиме EXEC. Она отправляет эхо-запросы ICMP для проверки доступности и качества соединения с указанным IPv4-узлом.
- **Дополнительные параметры (необязательные):**
    - ✓ repeat <count> – Количество отправляемых эхо-запросов. Позволяет собрать статистику (например, repeat 100).
    - ✓ size <size> – Размер полезной нагрузки пакета в байтах. Используется для тестирования MTU, фрагментации и производительности (например, size 1500).
    - ✓ interval <seconds> – Задержка в секундах между отправкой пакетов. Увеличение интервала снижает нагрузку на сеть.
- Для успешного ping требуется, чтобы у коммутатора был маршрут до целевого адреса (включая шлюз по умолчанию, если адрес в другой подсети) и чтобы промежуточные устройства не блокировали ICMP-трафик.
- Команда является основным инструментом оперативной диагностики сетевых проблем (доступность, потери пакетов, задержка).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.33 Проверка связи (ping) до IPv6-адреса (# ping ipv6)

Синтаксис:

```
# ping ipv6 <v_ipv6_addr> [ repeat <count> ] [ size <size> ] [ interval <seconds> ] [ interface vlan <v_vlan_id> ]
```

- <v_ipv6_addr>: Укажите IPv6-адрес для проведения ping-теста.
- [repeat <count>]: Количество отправляемых эхо-пакетов.
- [size <size>]: Размер или длина эхо-пакетов.
- [interval <seconds>]: Временной интервал между каждым ping-запросом.
- [interface vlan <v_vlan_id>]: Укажите идентификатор VLAN.

Объяснение: Проверка связи (ping) с указанным IPv6-адресом.

Рекомендации:

- Команда # ping ipv6 является аналогом команды # ping ip для сетей IPv6 и позволяет отправлять эхо-запросы ICMPv6. Она также расширяет функциональность команды > ping ipv6 (раздел 2.7.9), добавляя параметр указания исходного интерфейса.
- **Ключевой дополнительный параметр:** [interface vlan <v_vlan_id>] – Критически важен для проверки связи с **адресами link-local** (fe80::/10). Поскольку link-local адреса уникальны только в пределах одного сетевого интерфейса, необходимо явно указать, через какой интерфейс VLAN отправлять пакеты (например, interface vlan 1).
- Для проверки связи с глобальными IPv6-адресами (2001:db8::/32 и т.д.) указание интерфейса обычно не требуется, если у коммутатора настроен IPv6-адрес и маршрутизация.
- Параметры repeat, size и interval работают аналогично IPv4-версии команды.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.34 Выполнение полной (холодной) перезагрузки (# reload cold)

Синтаксис:

```
# reload cold
```

Объяснение: Выполняет полную («холодную») перезагрузку системы.

Рекомендации:

- Команда # reload cold инициирует полную перезагрузку коммутатора, идентичную команде # reload cold, описанной в разделе 2.6.4. Этот процесс эквивалентен отключению питания и его повторному включению, при котором все аппаратные компоненты проходят полную процедуру инициализации (POST - Power-On Self-Test).
- **Внимание!** Выполнение этой команды приводит к **полному прерыванию сетевого трафика** через коммутатор на время перезагрузки (обычно 1-3 минуты). Все текущие сессии (Telnet, SSH, веб-интерфейс) будут разорваны.
- **Обязательное действие перед перезагрузкой:** Сохранение текущей конфигурации с помощью команды copy running-config startup-config. В противном случае все изменения, внесенные с последнего сохранения, будут утеряны.
- Система может запросить подтверждение на сохранение конфигурации, если обнаружит несохраненные изменения. Рекомендуется явно сохранить конфигурацию до выполнения команды reload cold.
- Эта команда используется для применения изменений, требующих полной перезагрузки (например, обновление прошивки, сброс к заводским настройкам), или для восстановления работы устройства в случае серьезных сбоев.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.35 Сброс к заводским настройкам по умолчанию (# reload defaults)

Синтаксис:

```
# reload defaults [keep-ip]
```

Объяснение: Восстановление устройства к заводским настройкам по умолчанию.

Параметры:

- [keep-ip]: Сохранить настройки IP интерфейса VLAN 1.

Рекомендации:

- Команда # reload defaults выполняет **полный сброс** всей конфигурации устройства к состоянию «из коробки». Она идентична команде, описанной в разделе 2.6.5.
- **Ключевое различие между вариантами:**
    - # reload defaults – Выполняет **полный сброс**, включая IP-адрес, маску и шлюз по умолчанию на интерфейсе управления (обычно VLAN 1). После перезагрузки устройство вернется к IP-адресу по умолчанию (например, 192.168.1.1). Для доступа потребуется прямое подключение или знание этого адреса.
    - # reload defaults keep-ip – Выполняет сброс **всех настроек, кроме статического IP-адреса, маски и шлюза по умолчанию, назначенных на VLAN 1**. Это позволяет сохранить возможность удаленного доступа к

SEC.RU | Короткий путь к информации Скачано с sec.ru

устройству после сброса, что критически важно, если нет физического (консольного) доступа.

- **Внимание:** Обе операции **необратимы**. Все настройки (пароли, VLAN, порты, SNMP и т.д.) будут безвозвратно утеряны. Убедитесь, что у вас есть резервная копия конфигурации или физический доступ к устройству.
- После выполнения команды устройство автоматически перезагрузится.

2.6.36 Отправка сообщения (# send)

Синтаксис:

```
# send { * | <session_list> | console 0 | vty <vty_list> } <message>
```

Объяснение: Отправка сообщений другим tty-линиям (терминальным сессиям).

Параметры:

- { * | <session_list> | console 0 | vty <vty_list> }: Выберите один из вариантов:
  - ✓ * – Обозначает всех пользователей терминальных сессий.
  - ✓ <session_list> – Укажите номер сессии от 0 до 16.
  - ✓ console 0 – Основная (консольная) терминальная линия.
  - ✓ <vty_list> – Отправить сообщение на виртуальный терминал (VTY, например, Telnet/SSH сессию).
- <message>: Введите сообщение длиной до 128 символов, которое вы хотите отправить.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `send` позволяет администратору отправлять широковещательные или адресные текстовые уведомления другим пользователям, которые в данный момент работают с устройством через консоль, Telnet или SSH.
- **Типичные сценарии использования:**
    1. **Уведомление о плановых работах:** Предупреждение всех администраторов (`send *`) о предстоящей перезагрузке или изменении конфигурации.
    2. **Координация действий:** Связь с другим администратором, работающим параллельно.
    3. **Экстренное оповещение:** Сообщение о критическом событии или необходимости освободить сессию.
- Сообщение появится в терминале целевого пользователя, возможно, прервав его текущий ввод. Используйте команду вежливо.
- Для просмотра активных сессий и их номеров можно использовать команду `show users`.

2.6.37 Редактирование командной строки в терминале (# terminal editing)

Синтаксис:

```
# terminal editing
```

Объяснение: Включение редактирования командной строки.
Просмотр текущих настроек терминала: `> show terminal` или `# show terminal`
Отключение функции: `# no terminal editing`

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда terminal editing включает **расширенные возможности редактирования и навигации** в командной строке текущей сессии терминала. Когда эта функция включена (что обычно установлено по умолчанию), становятся доступны:
    - ✓ **Клавиши со стрелками** (вверх/вниз) для навигации по истории команд.
    - ✓ Клавиши **Влево/Вправо** для перемещения курсора по строке.
    - ✓ Клавиши **Backspace** и **Delete** для удаления символов.
    - ✓ **Автодополнение (Tab)** для завершения команд.
- **Внимание:** Эта настройка является **локальной для текущей сессии** (например, для вашего текущего Telnet/SSH-подключения или консоли) и не сохраняется в конфигурации устройства.
- Команда no terminal editing отключает эти функции, что может быть полезно в некоторых скриптах или при работе с терминальными программами, которые некорректно обрабатывают управляющие последовательности.
- Для просмотра всех текущих параметров терминала (ширина, длина, редактирование и т.д.) используйте команду show terminal.

2.6.38 Тайм-аут бездействия для терминальной сессии (# terminal exec-timeout)

Синтаксис:

```
# terminal exec-timeout <0-1440> [<0-3600>]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <0-1440>: Укажите значение тайм-аута в минутах (от 0 до 1440, где 0 означает "без тайм-аута").
- [<0-3600>]: Укажите значение тайм-аута в секундах (необязательно, от 0 до 3600).

Объяснение: Настройка значения тайм-аута для терминала.
Просмотр текущих настроек терминала: > show terminal или # show terminal
Сброс тайм-аута к значению по умолчанию: # no terminal exec-timeout

Рекомендации:

- Команда terminal exec-timeout устанавливает **максимальное время бездействия** для текущей терминальной сессии (консоль, Telnet, SSH). Если в течение указанного периода пользователь не вводит никаких команд, сессия автоматически разрывается.
- **Значения:**
  - ✓ 0 0 – Тайм-аут **отключен**. Сессия никогда не будет разорвана по причине бездействия (не рекомендуется по соображениям безопасности).
  - ✓ 5 0 – 5 минут, 0 секунд.
  - ✓ 0 30 – 0 минут, 30 секунд.
- Эта настройка является **локальной для текущей сессии** и не влияет на другие сессии и не сохраняется в конфигурации устройства. Для установки глобального тайм-аута для всех сессий необходимо настроить параметры линий (line console 0, line vty 0 15) в режиме глобальной конфигурации.
- Команда no terminal exec-timeout сбрасывает тайм-аут для текущей сессии к **значению по умолчанию**, которое определено в глобальной конфигурации линий.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.39 Размер истории команд для терминала (# terminal history size)

Синтаксис:

```
# terminal history size <0-32>
```

Параметры:

- <0-32>: Укажите текущий размер истории. Значение 0 означает отключение.

Объяснение: Настройка размера истории команд для терминала.
Просмотр текущих настроек терминала: > show terminal или # show terminal
Сброс размера истории к значению по умолчанию: # no terminal history size

Рекомендации:

- Команда terminal history size устанавливает **максимальное количество команд**, которые будут сохраняться в истории для текущей терминальной сессии. Эта история доступна для навигации с помощью клавиш **Стрелка вверх** и **Стрелка вниз**.
- **Значения:**
  - ✓ 0 – История команд **отключена**. Навигация по предыдущим командам невозможна.
  - ✓ 32 – Максимальное количество записей в истории (максимум может варьироваться в зависимости от модели).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Размер истории по умолчанию обычно равен 10 или 16 командам. Увеличение этого размера полезно для длительных сеансов настройки, когда требуется доступ к большому числу ранее введенных команд.
- Эта настройка является **локальной для текущей сессии** и не сохраняется в конфигурации устройства. Для установки глобального размера истории необходимо настроить параметры линий (line console 0, line vty 0 15) в режиме глобальной конфигурации.
- Команда no terminal history size сбрасывает размер истории для текущей сессии к **значению по умолчанию**.

2.6.40 Длина страницы терминала (# terminal length)

Синтаксис:

```
# terminal length <0 or 3-512>
```

Параметры:

- <0 or 3-512>: Укажите количество строк, отображаемых на экране перед паузой. Значение 0 означает отсутствие паузы.

Объяснение: Настройка длины страницы терминала.
Просмотр текущих настроек терминала: > show terminal или # show terminal

Рекомендации:

- Команда terminal length управляет **разбиением на страницы (постраничным выводом)** для длинных выводов команд (например, show running-config, show interfaces).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Параметры:**
  - ✓ 0 – **Отключает постраничный вывод**. Вся информация выводится непрерывно, без пауз. Это удобно при копировании вывода или работе через скрипты.
  - ✓ 24 (или другое значение, например, 30) – Устанавливает паузу после указанного количества строк. Для продолжения вывода необходимо нажать Пробел (следующая страница) или Enter (следующая строка).
- Стандартное значение по умолчанию обычно равно 24 строкам, что соответствует размеру стандартного терминала.
- Эта настройка является **локальной для текущей сессии** и не сохраняется в конфигурации устройства. Для установки глобальной длины используется команда length в режиме конфигурации линии.
- Отключение постраничного вывода (terminal length 0) — одна из самых полезных команд при активной настройке, так как позволяет сразу видеть весь вывод.

2.6.41 Ширина терминала (# terminal width)

Синтаксис:

```
# terminal width <0 or 40-512>
```

Параметры:

- <0 or 40-512>: Укажите ширину, отображаемую на экране. Значение 0 означает неограниченную ширину.

Объяснение: Настройка ширины отображения терминала.

Скачано с sec.ru

Просмотр текущих настроек терминала: > show terminal или # show terminal
Сброс ширины к значению по умолчанию: # no terminal width

Рекомендации:

- Команда terminal width задает максимальную ширину строки вывода (в символах) для текущей терминальной сессии. Если вывод команды (например, таблица из show interface status) превышает эту ширину, он будет переноситься на следующую строку, что может ухудшить читаемость.
- **Ключевые значения:**
    - ✓ 0 – **Неограниченная ширина**. Вывод никогда не переносится, позволяя отображать очень широкие таблицы в одну строку. Это полезно при работе с широкими мониторами или для сохранения форматирования при копировании.
    - ✓ 80 – Стандартная ширина, соответствующая традиционным терминалам.
    - ✓ 132 – Ширина, подходящая для широкоформатных дисплеев.
- Ширина по умолчанию обычно определяется настройками вашего клиента терминала (например, PuTTY) и "согласовывается" с коммутатором при подключении.
- Эта настройка является **локальной для текущей сессии** и не сохраняется в конфигурации устройства.
- Команда no terminal width сбрасывает ширину для текущей сессии к зафиксированному по умолчанию значению или значению, полученному от клиента.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.6.42 Разблокировка портов, отключенных функцией Port Security (# no port-security shutdown)

Синтаксис:

```
# no port-security shutdown [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Объяснение: Повторное открытие портов, которые были отключены (shutdown) или заблокированы функцией Port Security.

Параметры:

- [interface (<port_type> [<v_port_type_list>])]: Укажите тип порта и номера портов, которые вы хотите открыть заново.

Рекомендации:

- Команда no port-security shutdown используется для ручного восстановления работы порта, который был автоматически переведен в состояние **errdisable** (ошибка отключения) функцией безопасности портов (Port Security) из-за нарушения политики (например, обнаружение неразрешенного MAC-адреса).
- **Port Security** — это функция защиты уровня 2, которая ограничивает подключаемые MAC-адреса. При нарушении порт часто блокируется, переводится в состояние errdisable и административно отключается (shutdown).
- **Процесс снятия блокировки двухэтапный:**
    1. **Шаг 1:** Выполнить no port-security shutdown для снятия блокировки.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. **Шаг 2:** Включить порт командой `no shutdown` в режиме конфигурации интерфейса.

- Если порты не указаны, команда может применяться ко всем портам, заблокированным Port Security.
- Эта команда не очищает таблицу изученных безопасных MAC-адресов на порту и не изменяет конфигурацию Port Security

2.6.43 Команды show (show commands)

В привилегированном режиме EXEC (Exec mode) можно выполнять команды `show` для отображения текущего состояния или настроек определенной функции. Они будут представлены в **Разделе 3.9 «Команды в режиме конфигурации (Commands in Config Mode)»**.

Рекомендации:

- Команды `show` являются основным инструментом **мониторинга, проверки конфигурации и диагностики** на устройстве. Они предоставляют доступ только для чтения (read-only) и не вносят изменений в настройки.
- Эти команды доступны как в **привилегированном режиме EXEC (`#`)**, так и часто в **пользовательском режиме (`>`)**, хотя в последнем вывод может быть ограниченным.
- **Обширная функциональность:** Существуют десятки команд `show`, охватывающих все аспекты работы устройства:
  - ✓ `show running-config` – Текущая конфигурация.
  - ✓ `show interfaces` – Статус и статистика портов.
  - ✓ `show vlan` – Информация о VLAN.
  - ✓ `show mac address-table` – Таблица MAC-адресов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ show ip route – Таблица маршрутизации.
- ✓ show version – Информация о системе и ПО.
- ✓ И многие другие.

- Используйте символ ? после show для просмотра всех доступных вариантов в текущем режиме: # show ?.
- Многие команды show поддерживают фильтрацию вывода с помощью ключевых слов (например, show ip interface brief, show interfaces GigabitEthernet 1/1 status).

2.7 Команды в режиме конфигурации (Commands in Config Mode)

2.7.1 Настройка метода аутентификации для входа (login) (config)# aaa authentication login

Синтаксис:

(config)# aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }

Объяснение: Настройка метода аутентификации для клиента.

Параметры:

- { console | telnet | ssh | http }: Укажите один из клиентов аутентификации (способ доступа).
- { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }: Укажите один из методов аутентификации для указанного клиента. Необходимо указать как минимум один метод. Пользователи могут указать максимум три метода.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ local: Использовать локальную базу пользователей на коммутаторе для аутентификации.
- ✓ radius: Использовать удаленный сервер RADIUS для аутентификации.
- ✓ tacacs: Использовать удаленный сервер TACACS+ для аутентификации.

Рекомендации:

- Команда aaa authentication login является частью системы AAA (Authentication, Authorization, Accounting) и определяет последовательность (список) методов, которые будут использоваться для проверки учетных данных пользователей при входе через различные интерфейсы.
- **Клиенты (интерфейсы входа):**
  - ✓ console – Консольный доступ (физический порт).
  - ✓ telnet – Сессии Telnet.
  - ✓ ssh – Сессии SSH.
  - ✓ http – Доступ к веб-интерфейсу.
- **Важность порядка методов:** Методы проверяются в указанном порядке. Если первый метод недоступен (например, тайм-аут RADIUS-сервера), система переходит к следующему. Рекомендуется настраивать local в качестве последнего (резервного) метода, чтобы гарантировать доступ при недоступности внешних серверов.
- Для использования radius или tacacs необходимо предварительно настроить соответствующие серверы AAA (команды radius-server host, tacacs-server host).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Удаление конфигурации:** (config)# no aaa authentication login { console | telnet | ssh | http } – удаляет список методов аутентификации для указанного клиента, возвращая его к поведению по умолчанию (обычно local или запрос пароля, если он не настроен).

Пример настройки:

Настройка клиента Console на использование удаленного RADIUS-сервера для аутентификации.

```
# configure terminal
(config)# aaa authentication login console radius
```

2.7.2 Правило управления доступом (config)# access management

Синтаксис:

```
(config)# access management <access_id> <access_vid> <start_addr> [ to <end_addr> ] { [ web ] [ snmp ] [ telnet ] | all }
```

Объяснение: Создание правила управления доступом.

Параметры:

- <access_id: 1-16>: Укажите идентификатор (ID) для этой записи управления доступом.
- <access_vid>: Указывает идентификатор VLAN (VLAN ID) для записи управления доступом.
- <start_addr> [to <end_addr>]: Указывает начальный и конечный IP-адрес для записи управления доступом.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- { [web] [snmp] [telnet] | all }: Укажите, с каких интерфейсов (протоколов) соответствующие хосты могут получать доступ к коммутатору.

Пример настройки:

Разрешить IP с 192.0.3.1 по 192.0.3.10 доступ к устройству через Web, SNMP и Telnet.

```
# configure terminal
(config)# access management 1 1 192.0.3.1 to 192.0.3.10 all
```

Удаление конфигурации (Negation):

- (config)# no access management – удаляет все правила управления доступом.
- (config)# no access management <access_id> – удаляет правило с указанным ID.

Просмотр (Show):

```
# show access management [ statistics | <access_id_list> ]
```

Очистка статистики (Clear):

```
# clear access management statistics
```

Рекомендации:

- Команда access management создает правило контроля доступа на основе IP-адреса и VLAN, которое разрешает или запрещает доступ к интерфейсам управления коммутатора (Web, SNMP,

SEC.RU | Короткий путь к информации Скачано с sec.ru

Telnet). Это базовая форма ACL (Access Control List) для управления.

- **Внимание:**
  - ✓ **VLAN ID (**<access_vid>**)**: Правило применяется только к трафику, приходящему из указанной VLAN. Это добавляет проверку уровня 2.
  - ✓ **Диапазон IP-адресов**: Можно указать одиночный адрес (<start_addr>) или диапазон (to <end_addr>).
  - ✓ **Протоколы управления**: Можно выборочно разрешить доступ по конкретным протоколам (web, snmp, telnet) или сразу по всем (all).
  - ✓ **Идентификатор правила (**<access_id>**)**: Каждому правилу присваивается уникальный номер (1-16) для последующего управления.
- **Поведение по умолчанию:** Если ни одно правило не настроено, доступ по управляющим протоколам может быть разрешен со всех адресов. После создания хотя бы одного правила доступ будет разрешен ТОЛЬКО тем адресам и протоколам, которые явно описаны в правилах. Весь остальной трафик управления будет запрещен (неявное deny any).
- Правила не влияют на трафик данных (forwarding plane) и консольный доступ (console).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.3 Конфигурация списков контроля доступа (Access Control Lists - ACL) (config)# access-list

Этот раздел описывает комплексную систему ACL на основе правил (ACE - Access Control Entries), которая позволяет фильтровать и управлять трафиком на уровнях 2-4 с расширенными функциями.

(config)# access-list ace

Создание/изменение записи контроля доступа (ACE)

Синтаксис:

(config)# access-list ace <AceId: 1-256> [action {deny | filter | permit}] [dmac-type {any | broadcast | multicast | unicast}] [frame-type {any | arp | etype | ipv4 | ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp}] [ingress {any | interface <PORT_TYPE>}] [logging] [mirror] [next {<AceId:1-256> | last}] [policy <PolicyId: 0-255>] [rate-limiter {<RateLimiterId: 1-16> | disable}] [redirect {disable | interface <PORT_TYPE>}] [shutdown] [tag {any | tagged | untagged}] [tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority: 0-7> | any}] [vid {<Vid: 1-4095> | any}]

Объяснение: Настройка записи списка контроля доступа.

Ключевые параметры:

- <AceId>: Уникальный идентификатор правила (1-256).
- action:
  Действие: deny (заблокировать), filter (фильтровать), permit (разрешить).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- frame-type: Тип трафика для фильтрации (ARP, IPv4, IPv6, TCP, UDP, ICMP).
- vid: Фильтр по VLAN ID.
- ingress: Фильтр по входящему порту.
- rate-limiter: Привязка к ограничителю скорости.
- redirect / mirror: Перенаправление или зеркалирование трафика.
- shutdown: Отключение порта при срабатывании правила.
- next: Управление порядком правил (вставка перед другим правилом или перемещение в конец).

Просмотр (Show):

```
# show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]]
```

Удаление (Negation):

```
(config)# no access-list ace <ace_list>
```

Очистка статистики (Clear):

```
# clear access-list ace statistics
```

(config)# access-list ace update

Обновление существующей записи ACE

Синтаксис: Аналогичен access-list ace, но используется для изменения уже созданного правила с указанным <AceId>.

SEC.RU | Короткий путь к информации Скачано с sec.ru

(config)# access-list rate-limiter

Настройка ограничителя скорости

Синтаксис:

(config)# access-list rate-limiter [<rate_limiter_list>] {pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate>}

Объяснение: Создание ограничителя скорости с указанным ID (1-16) и лимитом (пакеты/сек или килобиты/сек).

Команды применения ACL к интерфейсам (config-if)#

Эти команды применяются в режиме конфигурации интерфейса для активации функций ACL на конкретном порту.

1. (config-if)# access-list action {permit | deny}
    - ✓ Глобальное действие по умолчанию для неподходящего трафика на порту: разрешить или запретить.
2. (config-if)# access-list logging
    - ✓ Включение логирования срабатываний ACL на порту.
3. (config-if)# access-list mirror
    - ✓ Включение зеркалирования трафика порта на порт-назначение.
4. (config-if)# access-list policy <policy_id>
    - ✓ Применение набора правил ACL (политики) к порту.
5. (config-if)# access-list port-state
    - ✓ Включение обработки ACL на порту (активация фильтрации).

SEC.RU | Короткий путь к информации Скачано с sec.ru

6. (config-if)# access-list rate-limiter <rate_limiter_id>
    - ✓ Применение ограничителя скорости к порту.
7. (config-if)# access-list shutdown
    - ✓ Включение функции отключения порта при нарушении правил ACL.
8. (config-if)# access-list {redirect | port-copy} interface {<port_type> <port_type_id> | (<port_type> [<port_type_list>])}
    - ✓ Перенаправление или копирование трафика с порта на другие порты.

Рекомендации: Данная система ACL предоставляет очень детальный контроль. Для ее эффективного использования необходимо:

1. Сначала создать **ограничители скорости** (access-list rate-limiter), если требуется.
2. Затем создать **правила (ACE)** (access-list ace) с нужными критериями и действиями.
3. Далее **применить политики и функции** к конкретным портам, используя команды в режиме (config-if)#.
4. **Активировать обработку ACL** на порту командой (config-if)# access-list port-state.

2.7.4 Настройка агрегирования каналов (Link Aggregation) (config)# aggregation

Данный раздел описывает команды для настройки агрегирования каналов (объединения портов, LAG, EtherChannel) и алгоритма распределения нагрузки.

SEC.RU | Короткий путь к информации Скачано с sec.ru

(config)# aggregation mode

Настройка алгоритма распределения нагрузки в агрегированном канале

Синтаксис:

```
(config)# aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }
```

Объяснение: Настройка режима агрегирования.

Параметры:

- [smac]: Весь трафик с одинаковым **исходным MAC-адресом (Source MAC)** передается по одному и тому же линку в агрегате.
- [dmac]: Весь трафик с одинаковым **MAC-адресом назначения (Destination MAC)** передается по одному и тому же линку в агрегате.
- [ip]: Весь трафик с одинаковой парой **исходный и конечный IP-адрес (source and destination IP)** передается по одному и тому же линку в агрегате.
- [port]: Весь трафик с одинаковыми номерами **TCP/UDP портов источника и назначения** передается по одному и тому же линку в агрегате.

Рекомендации:

- Команда задает **алгоритм хеширования**, который определяет, как распределять потоки трафика между физическими линками внутри логического агрегированного канала. Это необходимо

SEC.RU | Короткий путь к информации Скачано с sec.ru

для гарантии, что все пакеты одного потока будут идти по одному пути, избегая нарушения порядка пакетов.

- Параметры можно **комбинировать** (например, aggregation mode smac dmac), чтобы создать более сложный и эффективный критерий хеширования, обеспечивающий лучшее распределение нагрузки.
- Выбор оптимального режима зависит от структуры трафика:
    - ✓ dmac: Часто используется по умолчанию, хорошо работает, когда коммутатор является "ядром" и имеет много получателей (например, серверов).
    - ✓ smac: Эффективен, когда много клиентов обращаются к нескольким целям.
    - ✓ ip **или** ip port: Наиболее "интеллектуальное" распределение на уровне 3/4, подходит для балансировки нагрузки между множеством TCP/UDP сессий (например, трафик маршрутизатора или файрвола).

Удаление конфигурации (Negation):

```
(config)# no aggregation mode
```

Сбрасывает режим агрегирования к значению по умолчанию (зависит от модели устройства).

Просмотр (Show):

```
# show aggregation [mode]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

(config-if)# aggregation group

Добавление интерфейса в агрегированную группу

Синтаксис:

```
(config-if)# aggregation group <unit>
```

Объяснение: Добавить данный конкретный интерфейс в указанную агрегированную группу.

Параметры:

- <unit>: Укажите идентификатор (ID) агрегированной группы.

Рекомендации:

- Эта команда, выполненная в режиме конфигурации интерфейса ((config-if)#), **вручную** добавляет порт в статическую агрегированную группу (Static LAG). Для использования динамических протоколов (LACP, PAgP) требуются другие команды.
- Все порты, добавленные в одну группу с одинаковым <unit>, образуют один логический канал.
- **Внимание:** Перед добавлением порта в группу убедитесь, что его настройки (скорость, дуплекс, режим VLAN) **идентичны** у всех портов в этой группе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.5 Настройка баннеров (Banners) (config)# banner

Данный раздел описывает команды для настройки информационных сообщений (баннеров), которые отображаются пользователям при подключении к устройству.

(config)# banner [motd]

Настройка баннера "Сообщение дня" (Message of the Day)

Синтаксис:

```
(config)# banner [ motd ] <banner>
```

Объяснение: Настройка сообщения дня.

Параметры:

- [motd]: Введите сообщение дня (необязательный ключевой параметр, часто подразумевается по умолчанию).
- <banner>: Текст баннера. Текст должен быть заключен в **разделительный символ** (delimiter character), например, знак решетки #. Текст между двумя разделителями будет считаться баннером.

Рекомендации:

- **MOTD (Message of the Day)** отображается **после** входа в систему, но **перед** появлением приглашения командной строки (> или #).
- Используется для отображения общей информации, предупреждений или уведомлений для всех авторизованных

SEC.RU | Короткий путь к информации Скачано с sec.ru

пользователей (например, о плановых работах, политиках безопасности компании).

- Важный элемент безопасности — баннер не должен содержать информацию, которая может помочь злоумышленнику (тип устройства, версия ПО и т.д.).

Удаление конфигурации (Negation):

```
(config)# no banner [motd]
```

(config)# banner exec

Настройка баннера, отображаемого при входе в режим EXEC

Синтаксис:

```
(config)# banner exec <banner>
```

Объяснение: Отображать настроенное сообщение при успешном входе в режим EXEC.

Рекомендации:

- Этот баннер отображается **после** MOTD, непосредственно перед появлением приглашения командной строки в режиме EXEC.
- Может использоваться для отображения **правил использования** или информации, актуальной уже после аутентификации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации (Negation):

```
(config)# no banner exec
```

(config)# banner login

Настройка баннера, отображаемого при запросе логина и пароля

Синтаксис:

```
(config)# banner login <banner>
```

Объяснение: Отображать настроенное сообщение при запросе логина и пароля.

Рекомендации:

- **Login Banner** (иногда называемый **MOTD Banner** в других системах) отображается до запроса имени пользователя и пароля.
- Часто настраивается как "баннер авторизованного доступа" (Authorization Banner)**,** предупреждающий, что несанкционированный доступ запрещен, и действия пользователя могут контролироваться и регистрироваться. Во многих организациях его содержание регламентируется политикой безопасности.
- Для корректного отображения многострочного баннера используйте разделительный символ.

Удаление конфигурации (Negation):

```
(config)# no banner login
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Пример настройки:

Настройка баннера авторизованного доступа (login banner) с разделителем #:

```
(config)# banner login #
**********************************************
*   WARNING: Authorized Access Only!    *
*   All activities are logged and monitored. *
*   Unauthorized access is prohibited.       *
**********************************************#
```

2.7.6 Настройка часов и времени (config)# clock

Данный раздел описывает команды для настройки временной зоны и правил перехода на летнее/зимнее время (Daylight Saving Time - DST).

(config)# clock timezone

Настройка часового пояса

Синтаксис:

```
(config)# clock timezone <word> <-23-23> [<0-59>]
```

Объяснение: Настройка часового пояса, используемого на коммутаторе.

Параметры:

- <word>: Укажите название часового пояса (например, MSK, EST, GMT+3).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- <-23-23>: Смещение в часах относительно UTC (Coordinated Universal Time). Для восточных полушарий используется положительное значение, для западных — отрицательное.
- [<0-59>]: Смещение в минутах относительно UTC (необязательно).

Рекомендации:

- Эта настройка определяет местное время для всех временных меток (логи, отображение времени в CLI) на устройстве.
- UTC (время по Гринвичу) используется как базовое. Например, для московского времени (MSK) зимой смещение +3, командой будет clock timezone MSK 3.

Удаление конфигурации (Negation):

```
(config)# no clock timezone
```

Сбрасывает часовой пояс к UTC (смещение 0).

(config)# clock summer-time (две формы: date и recurring)

Настройка правил перехода на летнее время

Объяснение: Настройка летнего времени. Используется для перевода часов вперед или назад в соответствии с заданной конфигурацией на определенный период. Команда recurring используется для повторения конфигурации каждый год.

Форма 1: Указание конкретных дат (date)

Синтаксис:

SEC.RU | Короткий путь к информации Скачано с sec.ru

(config)# clock summer-time <word16> date [<start_month> <start_date> <start_year> <start_hour> <end_month> <end_date> <end_year> <end_hour> [<offset>]]

- summer-time <word16>: Описание для данного правила летнего времени.
- date: Указывает на использование абсолютных дат.
- Параметры начала (<start_*>) и окончания (<end_*>) периода.
- [<offset>]: Количество минут, добавляемых во время действия летнего времени (обычно 60).

Форма 2: Указание повторяющегося правила (recurring)

Синтаксис:

(config)# clock summer-time <word16> recurring [<start_week> <start_day> <start_month> <start_hour> <end_week> <end_day> <end_month> <end_hour> [<offset>]]

- recurring: Указывает на ежегодное повторение правила.
- Параметры используют относительные определения: неделя месяца (<start_week>, 1=первая, 5=последняя), день недели (<start_day>, например, Sun, Mon). Эта форма более удобна для правил типа "последнее воскресенье марта".

Общие рекомендации:

- Летнее время автоматически переводит часы вперед на указанное количество минут (<offset>) в момент начала периода и обратно в момент его окончания.
- Предпочтительно использовать форму recurring, так как она не требует ежегодного обновления конфигурации.
- Обязательно сверьтесь с актуальными правилами вашего региона.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации (Negation):

```
(config)# no clock summer-time
```

Полностью отключает настройку летнего времени.

Просмотр (Show):

```
# show clock
# show clock detail
```

Команда show clock detail *отображает информацию о настройках часового пояса и летнего времени.*

2.7.7 Сброс настроек ограничителя скорости ACL (config)# default access-list rate-limiter

Синтаксис:

```
(config)# default access-list rate-limiter [ <rate_limiter_list> ]
```

Объяснение: Сбросить настройки указанного идентификатора ограничителя скорости (rate-limiter ID).

Параметры:

- [<rate_limiter_list: 1-16>]: Укажите идентификатор ограничителя скорости (Rate Limiter ID).

Пример: Сбросить ограничитель скорости 1.

```
# configure terminal
(config)# default access-list rate-limiter 1
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда default access-list rate-limiter **сбрасывает настройки указанного ограничителя скорости к значениям по умолчанию** (обычно это означает, что ограничение скорости становится неактивным или сбрасывается до нулевой конфигурации).
- Ограничитель скорости — это объект, создаваемый командой access-list rate-limiter (раздел 2.9.3), который определяет лимит пропускной способности (в пакетах в секунду или килобитах в секунду). Эта команда удаляет это конкретное определение лимита.
- **Отличие от команды** no**:**
    - ✓ no access-list rate-limiter <ID> обычно **полностью удаляет** объект ограничителя скорости из конфигурации.
    - ✓ default access-list rate-limiter <ID> **сбрасывает параметры объекта** к состоянию по умолчанию, но может оставлять сам объект (с пустой или нулевой конфигурацией). Точное поведение может зависеть от реализации.
- Эта команда **не влияет** на правила ACL (access-list ace), которые могут ссылаться на данный ограничитель. После сброса ограничителя соответствующие правила могут перестать функционировать должным образом.
- Перед выполнением убедитесь, что сброс не нарушит политики контроля трафика.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.8 Настройка 802.1X (IEEE Port-Based Network Access Control) (config)# dot1x

Этот раздел описывает комплексную настройку протокола аутентификации 802.1X. Команды сгруппированы по уровню конфигурации: глобальные настройки системы и настройки на уровне интерфейсов (портов).

Глобальные настройки 802.1X (config)#

(config)# dot1x system-auth-control

Объяснение: Глобальное включение службы 802.1X на коммутаторе. Без этой команды все остальные настройки 802.1X неактивны.

Удаление конфигурации**:**

(config)# no dot1x system-auth-control

(config)# dot1x re-authentication

Объяснение: Включает функцию периодической повторной аутентификации (re-authentication) для всех клиентов. Это позволяет обнаружить замену устройства на порту.

Удаление конфигурации**:**

(config)# no dot1x re-authentication

Таймеры аутентификации (важные для работы и безопасности):

- ✓ (config)# dot1x authentication timer re-authenticate <1-3600> – Интервал повторной аутентификации в секундах (по умолчанию 3600). no – сброс к значению по умолчанию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ (config)# dot1x timeout tx-period <1-65535> – Время ожидания ответа от клиента (супликанта) перед повторной отправкой EAP-запроса (по умолчанию 30 сек).
- ✓ (config)# dot1x authentication timer inactivity <10-1000000> – Таймер неактивности. Возраст записи об авторизованном клиенте, после которого она удаляется (по умолчанию 300 сек).
- ✓ (config)# dot1x timeout quiet-period <10-1000000> – Период "тишины". Время, в течение которого порт не будет пытаться аутентифицировать клиента после неудачной попытки (по умолчанию 10 сек).

Глобальные функции (Features):

- ✓ (config)# dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }
  - Глобальное включение расширенных функций:
    - guest-vlan – VLAN для гостевого доступа (непрошедшие аутентификацию).
    - radius-qos – Назначение параметров QoS (приоритет, полоса) с RADIUS-сервера.
    - radius-vlan – Назначение VLAN с RADIUS-сервера (динамическое изменение VLAN порта).
- ✓ (config)# dot1x guest-vlan <1-4095> – Назначение номера VLAN, используемой в качестве гостевой.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ (config)# dot1x guest-vlan supplicant – Изменяет логику работы гостевой VLAN, позволяя клиентам, которые не отправили ни одного EAPOL-пакета, попадать в нее.
- ✓ (config)# dot1x max-reauth-req <1-255> – Максимальное количество EAP-запросов, отправляемых до перевода порта в гостевую VLAN (если она включена).

Настройки 802.1X на интерфейсе (порту) (config-if)#

(config-if)# dot1x port-control { force-authorized | force-unauthorized | auto | single | multi | mac-based }

Ключевая команда. Определяет режим контроля доступа на порту:

- force-authorized – Порт всегда открыт (аутентификация отключена).
- force-unauthorized – Порт всегда закрыт.
- auto – **Порт-базированный 802.1X.** Требует аутентификацию для доступа к порту. Не-802.1X клиенты блокируются.
- single – **Одиночный 802.1X.** На порту может быть авторизован только **один** клиент. Наиболее безопасный режим.
- multi – **Множественный 802.1X.** На порту могут быть авторизованы несколько клиентов, каждый индивидуально.
- mac-based – **MAC-базированная аутентификация.** Коммутатор сам отправляет учетные данные (MAC-адрес) на RADIUS-сервер. Не требует поддержки 802.1X на клиенте.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Отмена:** (config-if)# no dot1x port-control (сброс к force-authorized).

6. **Включение расширенных функций на порту:**
   - ✓ (config-if)# dot1x guest-vlan – Разрешить использование гостевой VLAN на этом порту.
   - ✓ (config-if)# dot1x radius-qos – Разрешить назначение QoS с RADIUS для этого порта.
   - ✓ (config-if)# dot1x radius-vlan – Разрешить назначение VLAN с RADIUS для этого порта.
7. (config-if)# dot1x re-authenticate
   - ✓ Запускает немедленную повторную аутентификацию для всех клиентов на порту.

Просмотр состояния и статистики (Show):

- # show dot1x status [interface ...] [brief] – Общий статус и статус портов.
- # show dot1x statistics { eapol | radius | all } [interface ...] – Статистика EAPOL или RADIUS сообщений.

Рекомендации:

- **Последовательность настройки:**
  1. Настроить RADIUS-серверы (radius-server host).
  2. Включить глобальный контроль (dot1x system-auth-control).
  3. Настроить глобальные таймеры и функции (guest-vlan и т.д.).

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. На каждом порту настроить режим контроля (dot1x port-control) и при необходимости включить функции.

- Режим single или multi требуют, чтобы на порту была также включена и настроена **Port Security** для закрепления MAC-адресов.

Пример настройки порта доступа с 802.1X и гостевой VLAN:

```
(config)# dot1x system-auth-control
(config)# dot1x feature guest-vlan
(config)# dot1x guest-vlan 100
(config)# interface GigabitEthernet 1/1
(config-if)# dot1x port-control auto
(config-if)# dot1x guest-vlan
```

2.7.9 Настройка режима дуплекса на интерфейсе (config-if)# duplex

Синтаксис:

```
(config-if)# duplex { half | full | auto [ half | full ] }
```

Объяснение: Настройка режима дуплекса для порта.

Параметры:

- { half | full | auto [half | full] }: Укажите режим дуплекса для данного конкретного интерфейса.

Пример: Установить режим дуплекса для порта 1 в режим автосогласования (auto).

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
# configure terminal
(config)# interface gigabitethernet 1/1-10
(config-if)# duplex auto
```

Удаление конфигурации:

```
(config-if)# no duplex
```

Просмотр:

```
> show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface ( <port_type> [ <v_port_type_list> ] ) status
```

Рекомендации:

- Команда duplex определяет метод двусторонней связи на физическом Ethernet-порту:
  - ✓ half **(Полудуплекс)**: Устройство может либо передавать, либо принимать данные в любой момент времени, но не одновременно. Устаревший режим, может вызывать коллизии.
  - ✓ full **(Полный дуплекс)**: Устройство может передавать и принимать данные одновременно. Это стандартный и предпочтительный режим для современного оборудования.
  - ✓ auto **(Автосогласование)**: Порт автоматически согласовывает (negotiates) с подключенным устройством наилучший общий режим дуплекса (и скорости).
    Это **рекомендуемая настройка по умолчанию** для большинства портов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Уточнение автосогласования:** В некоторых реализациях параметр `auto` может иметь уточнения [`half` | `full`], которые задают предпочтительный режим при автосогласовании (например, `auto full` пытается согласовать полный дуплекс).
- **Критически важно** для стабильной связи, чтобы режим дуплекса (и скорости) **полностью совпадал** на обоих концах соединения (коммутатор и подключенное устройство). Несоответствие приводит к дуплексным несоответствиям (duplex mismatch), вызывающим высокий уровень коллизий, ошибок CRC и катастрофическое падение производительности.
- **Когда задавать явно (`full` или `half`):**
    - ✓ При подключении к старому устройству, не поддерживающему автосогласование.
    - ✓ Для критически важных линков (например, uplink между коммутаторами), где требуется гарантировать полнодуплексный режим.
    - ✓ По указанию документации или политики сети.
- Команда `no duplex` возвращает порт к автосогласованию без предпочтений.

2.7.10 Настройка пароля привилегированного режима (config)# enable password

Синтаксис:

```
(config)# enable password <password>
```

Объяснение: Настройка пароля для входа в привилегированный режим.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры (Parameters):

- <password>: Укажите пароль для режима enable.

2.7.10.1 Настройка пароля для уровня привилегий (config)# enable password level

Синтаксис:

```
(config)# enable password [level <priv: 1-15>] <password>
```

Объяснение: Настройка пароля и уровня привилегий для входа в привилегированный режим.

Параметры:

- [level <priv: 1-15>]: Укажите уровень привилегий для данного пароля.
- <password>: Укажите пароль для режима enable.

Удаление конфигурации:

```
(config)# no enable password [ level <priv> ]
```

Рекомендации:

- Эта команда расширяет базовую команду enable password, позволяя назначить **разные пароли для разных уровней привилегий** (Role-Based Access Control, RBAC). Это позволяет создавать иерархию доступа среди администраторов.
- **Уровни привилегий (Privilege Levels):**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Уровень 1:** Пользовательский режим (>). Команды только для просмотра.
- ✓ **Уровни 2-14:** Пользовательские уровни. Администратор может назначить определенным командам эти уровни, чтобы ограничить доступ.
- ✓ **Уровень 15:** Привилегированный режим (#). Полный доступ ко всем командам (по умолчанию).

- **Как это работает:**

  1. Пользователь вводит enable.
  2. Система запрашивает пароль.
  3. Если введен пароль уровня 15, пользователь переходит на уровень 15.
  4. Если введен пароль уровня 5, пользователь переходит на уровень 5 и имеет доступ только к командам, назначенным уровням 1-5.

- Если параметр [level <priv>] не указан, пароль назначается для **уровня по умолчанию (обычно 15)**.
- **Проблема безопасности сохраняется:** Пароли, заданные этой командой, также могут храниться в незашифрованном виде. Для безопасной реализации RBAC следует использовать комбинацию enable secret (для уровня 15) и AAA-сервер (TACACS+/RADIUS) с профилями авторизации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.10.2 Настройка защищенного пароля для уровня привилегий (config)# enable secret)

Синтаксис:

```
(config)# enable secret { 0 | 5 } [ level <priv: 1-15> ] <password>
```

Параметры:

- { 0 | 5 }: Укажите 0 для обозначения незашифрованного секрета (открытый текст). Укажите 5 для обозначения зашифрованного секрета (MD5).
- [level <priv: 1-15>]: Укажите уровень привилегий для данного пароля.
- <password>: Укажите пароль для режима enable.

Объяснение: Настройка защищенного пароля (secret) и уровня привилегий для входа в привилегированный режим.

Удаление конфигурации (Negation):

```
(config)# no enable secret { [ 0 | 5 ] } [ level <priv> ]
```

Рекомендации:

- Команда enable secret является **безопасной альтернативой** команде enable password. Она хранит пароль в конфигурации в **зашифрованном виде**, что предотвращает его чтение из файла конфигурации.
- **Ключевые параметры:**
    - ✓ 5 **(рекомендуется):** Пароль будет **зашифрован** с использованием алгоритма MD5. В конфигурации

SEC.RU | Короткий путь к информации Скачано с sec.ru

отображается только его хеш, например: enable secret 5 1mERr$XYZ123...

- ✓ 0 **(не рекомендуется):** Пароль будет сохранен в **открытом тексте (cleartext)**, аналогично enable password. Используйте этот вариант только для совместимости или если устройство не поддерживает шифрование.

- **Уровни привилегий (**level <priv>**):** Как и в команде enable password level, позволяет назначить зашифрованный пароль для конкретного уровня привилегий (1-15) для реализации RBAC.
- **Приоритет:** Если настроены и enable secret, и enable password для одного уровня, система будет использовать пароль из enable secret.
- Для максимальной безопасности **всегда используйте** enable secret 5 для паролей всех уровней. Это стандартная практика для сетевой безопасности.

2.7.11 Настройка параметров ERPS (Ethernet Ring Protection Switching) (config)# erps

2.7.11.1 (config)# erps <group> guard

Настройка защитного таймера (guard timer) для группы ERPS

Синтаксис:

```
(config)# erps <group> guard <guard_time_ms>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Настройка защитного времени (guard time) для указанной группы.

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- <guard_time_ms: 10-2000>: Укажите время защиты (guard time). Допустимый диапазон от 10 до 2000 мс.

Рекомендации:

- Команда erps <group> guard устанавливает **защитный таймер (Guard Timer)** для указанной группы протокола ERPS.
- **Назначение Guard Timer:** Этот таймер предотвращает **нестабильность (flapping)** кольца при временных сбоях или во время процесса сходимости (convergence) после изменения топологии. Он задает минимальный интервал между изменениями состояния (state changes) на порту кольца.
- **Принцип работы:** После того как порт меняет свое состояние (например, разблокируется), он не сможет изменить его снова (например, заблокироваться) до истечения времени, заданного Guard Timer. Это дает сети время стабилизироваться.
- **Выбор значения:** Стандартное значение (по умолчанию) обычно составляет **200 мс** или **500 мс**. Значение должно быть достаточно большим, чтобы пропустить возможные временные всплески или задержки в сети, но не чрезмерным, чтобы не замедлять восстановление. Типичный диапазон в рабочих сетях: **200-1000 мс**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Отключение или настройка слишком малого значения может привести к нестабильной работе кольца.

Удаление конфигурации (Negation):

```
(config)# no erps <group> guard
```

Сбрасывает значение защитного таймера для указанной группы к значению по умолчанию.

Просмотр состояния ERPS:

```
# show erps [ <groups> ] [ detail | statistics ]
```

2.7.11.2 (config)# erps <group> holdoff

Синтаксис:

```
(config)# erps <group> holdoff <holdoff_time_ms>
```

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- <holdoff_time_ms: 0-10000>: Укажите время отложенного действия (holdoff time). Допустимый диапазон от 0 до 10000 мс.

Объяснение: Настройка времени отложенного действия для указанной группы.

Рекомендации:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Команда erps <group> holdoff устанавливает **таймер отложенного действия (Hold-off Timer)** для указанной группы протокола ERPS.
- **Назначение Hold-off Timer:** Когда на порту кольца обнаруживается **сигнальный отказ (Signal Fail, SF)** — физическая потеря сигнала (например, обрыв), этот таймер вводит преднамеренную задержку перед тем, как протокол начнет реагировать на это событие и менять состояние кольца.
- **Принцип работы:** Если отказ устраняется в течение времени, заданного Hold-off Timer (например, кратковременный сбой или мигание линка), ERPS **не инициирует процесс переключения защиты**, что предотвращает ненужные и потенциально дестабилизирующие операции восстановления.
- **Выбор значения:** Значение по умолчанию часто равно **0 мс** (немедленная реакция). Увеличение этого значения (например, до **100-500 мс**) полезно в сетях, подверженных кратковременным сбоям, для повышения устойчивости и уменьшения количества ложных срабатываний защиты.
- Этот таймер применяется **только к событиям Signal Fail (SF)**. На события Signal Degrade (SD, деградация сигнала) он не влияет.

Удаление конфигурации:

```
(config)# no erps <group> holdoff
```

Сбрасывает значение таймера отложенного действия для указанной группы к значению по умолчанию (обычно 0 мс).

Просмотр состояния ERPS:

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
# show erps [ <groups> ] [ detail | statistics ]
```

2.7.11.3 (config)# erps <group> major port0 interface port1 interface

Синтаксис:

```
(config)# erps <group> major port0 interface <port_type> <port0> port1 interface <port_type> <port1> [ interconnect ]
```

Объяснение: Создание экземпляра ERPS.

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- <port_type> <port0>: Укажите тип порта и номер порта для Port0. Port0 также известен как E-port (Восточный порт), используемый некоторыми производителями.
- <port_type> <port1>: Укажите тип порта и номер порта для Port1. Port1 также известен как W-port (Западный порт), используемый некоторыми производителями. Если этот порт соединен с другим подкольцом, в этом поле указывается 0, что означает отсутствие западного порта для данного экземпляра.
- [interconnect]: Укажите этот параметр, если данный узел является узлом межсоединения (interconnected node) для этого экземпляра.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Это **основная команда для создания кольца ERPS**. Она определяет, какие два физических порта на коммутаторе являются частью одного кольца (группы) и будут участвовать в протоколе защиты.
- **Порты кольца:**
    - ✓ **Port0 (E-port):** Один из портов кольца.
    - ✓ **Port1 (W-port):** Второй порт того же кольца.
    - ✓ Коммутатор должен быть подключен к соседним коммутаторам в кольце через эти порты.
- **Параметр** [interconnect] используется в **сложных топологиях с несколькими кольцами (многокольцевых, interconnected rings)**. Он указывает, что данный экземпляр (и, следовательно, один из его портов) является связующим звеном с другим кольцом. В этом случае один из портов (обычно port1) может быть указан как 0, если он физически не существует на данном коммутаторе для этого конкретного кольца.
- Перед выполнением этой команды необходимо убедиться, что:

    1. Создан и настроен Control VLAN для этой группы ERPS (обычно командой vlan <id> и назначением его на порты).
    2. Порты находятся в режиме доступа (access) или транка (trunk) с разрешенным Control VLAN.

Просмотр состояния ERPS (Show):

```
# show erps [ <groups> ] [ detail | statistics ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.11.4 (config)# erps <group> mep

Синтаксис:

```
(config)# erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>
```

Объяснение: Настройка параметров MEP (Maintenance End Point) и APS (Automatic Protection Switching) для указанной группы.

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- <p0_sf>: Это также известно как Восточная конечная точка отчетности об отказах сигнала (East Signal Fail APS MEP). Назначьте MEP для отчетов об отказах сигнала на Восточном порту в этом поле.
- <p0_aps>: Укажите MEP для обработки APS PDU на Восточном порту.
- <p1_sf>: Это также известно как Западная конечная точка отчетности об отказах сигнала (West Signal Fail APS MEP). При соединении с другим подкольцом в этом поле указывается 0, что означает отсутствие западного SF MEP для данного экземпляра. Назначьте MEP для отчетов об отказах сигнала на Западном порту в этом поле.
- <p1_aps>: Укажите MEP для обработки APS PDU на Западном порту. При соединении с другим подкольцом в этом поле указывается 0, что означает отсутствие западного APS MEP для данного экземпляра.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Эта команда выполняет **тонкую настройку внутренних идентификаторов MEP** для протокола ERPS. MEP (Maintenance End Point) — это логические точки в сети, которые генерируют и обрабатывают служебные сообщения протокола (APS PDU).
- **Назначение параметров:**
    - ✓ sf **MEP (Signal Fail MEP):** Отвечает за обнаружение и отправку сообщений об **отказах сигнала (Signal Fail)** в кольцо.
    - ✓ aps **MEP:** Отвечает за обработку и передачу **служебных APS-сообщений (Automatic Protection Switching PDU)**, которые управляют состоянием кольца.
- Значения <p0_sf>, <p0_aps>, <p1_sf>, <p1_aps> представляют собой **идентификаторы (ID) MEP**, которые должны быть уникальными в рамках данного кольца. Часто для простоты используются небольшие целые числа (например, 1, 2, 3, 4).
- В **многокольцевых (interconnected) топологиях** для порта, который является точкой соединения, соответствующие MEP могут отсутствовать. В этом случае для <p1_sf> и/или <p1_aps> указывается 0.
- Обычно эти параметры не требуют ручной настройки, если не возникает специфических проблем интеграции или не требуется соответствие строгим требованиям другого вендора. В большинстве случаев система автоматически назначает ID MEP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no erps <group> mep
```

Удаляет ручную конфигурацию MEP для указанной группы, позволяя системе использовать автоматически назначенные значения.

Просмотр состояния ERPS:

```
# show erps [ <groups> ] [ detail | statistics ]
```

2.7.11.5 (config)# erps <group> revertive

Синтаксис:

```
(config)# erps <group> revertive <wtr_time_minutes>
```

Объяснение: Настройка таймера "Ожидание-Восстановления" (Wait-to-Restore) в режиме с возвратом.

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- <wtr_time_minutes>: Укажите таймер "Ожидание-Восстановления" в минутах. Допустимый диапазон от 1 до 12 минут.

Рекомендации:

- Команда erps <group> revertive активирует **режим с возвратом (revertive mode)** и задает значение **таймера ожидания восстановления (Wait-to-Restore, WTR timer)** для указанной группы ERPS.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Режим с возвратом (Revertive Mode):**
    - ✓ **Включен (данной командой):** После устранения исходной неисправности (обрыва) и стабилизации кольца, трафик автоматически вернется (revert) на первоначальный (оптимальный) путь через определенный интервал (WTR timer). Этот режим обеспечивает оптимальную маршрутизацию трафика после восстановления.
    - ✓ **Выключен (non-revertive):** После переключения на резервный путь трафик продолжает идти по нему, даже если основной путь восстановлен. Возврат происходит только при новой неисправности на резервном пути. Этот режим минимизирует количество переключений.
- **Таймер WTR (Wait-to-Restore):** Это задержка (в минутах) между моментом восстановления основного пути и фактическим возвратом трафика на него. Таймер нужен для того, чтобы убедиться, что восстановленный путь стабилен, прежде чем снова выполнять переключение, которое само по себе вызывает кратковременный разрыв связи.
- **Типичные значения WTR:** 1, 5, 10 минут. Выбор зависит от требований к стабильности сети.

Удаление конфигурации (Negation):

```
(config)# no erps <group> revertive
```

*Отключает режим с возвратом для указанной группы (устанавливает **non-revertive mode**).*

Просмотр состояния ERPS (Show):

```
# show erps [ <groups> ] [ detail | statistics ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.11.6 (config)# erps <group> rpl

Синтаксис:

```
(config)# erps <group> rpl { owner | neighbor } { port0 | port1 }
```

Объяснение: Укажите порт Ethernet-кольца на локальном узле в качестве владельца (owner) или соседа (neighbor) RPL (Ring Protection Link).

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- { owner | neighbor }: Укажите, является ли порт кольца владельцем (owner) или соседом (neighbor). RPL (Ring Protection Link) отвечает за блокировку трафика через RPL, чтобы в Ethernet-трафике не образовывались петли.
- { port0 | port1 }: Укажите порт, к которому применяется это правило.

Рекомендации:

- Команда erps <group> rpl является **ключевой для настройки логики защиты кольца**. Она определяет, какой порт в кольце будет выполнять роль **защитного звена (RPL - Ring Protection Link)**.
- **RPL (Ring Protection Link):** Это логическое звено в кольце, которое в нормальном (рабочем) состоянии **заблокировано (Blocked)** для трафика данных, чтобы предотвратить образование широковещательной петли уровня 2. При обрыве в

SEC.RU | Короткий путь к информации Скачано с sec.ru

другом месте кольца RPL разблокируется, обеспечивая альтернативный путь для трафика.

- **Роли RPL:**
  - ✓ owner **(владелец):** Узел, на котором порт **активно управляет** состоянием блокировки RPL. В кольце должен быть ровно **один RPL owner**. Это главный узел для защиты.
  - ✓ neighbor **(сосед):** Узел, который находится на **противоположном конце** того же звена RPL от владельца. Порт RPL neighbor также будет заблокирован в нормальном состоянии.
- **Важность правильного назначения:** Обычно RPL назначается на **наиболее слабое или наименее загруженное** звено в кольце, так как в нормальном режиме оно не передает трафик данных. Неправильная настройка (отсутствие owner или несколько owners) нарушит работу протокола.
- Port0 и Port1 — это порты, указанные при создании экземпляра командой erps <group> major port0 interface ....

Удаление конфигурации (Negation):

```
(config)# no erps <group> rpl
```

Удаляет конфигурацию RPL для указанной группы (порт перестает быть owner/neighbor). Это может нарушить работу кольца.

Просмотр состояния ERPS (Show):

```
# show erps [ <groups> ] [ detail | statistics ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.11.7 (config)# erps <group> sub

Синтаксис:

```
(config)# erps <group> sub port0 interface <port_type> <port0> { { port1 interface <port_type> <port1> } | { interconnect <major_ring_id> [ virtual-channel ] } }
```

Объяснение: Создание профиля и настройка портов 0 и 1 для подкольца (Sub ERPS).

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- <port_type> <port0>: Укажите тип порта и номер порта для подпорта 0.
- { { port1 interface <port_type> <port1> } | { interconnect <major_ring_id> [virtual-channel] } }: Укажите тип порта и номер порта для порта 1 ИЛИ укажите ID группы главного кольца.

Рекомендации:

- Команда erps <group> sub используется для конфигурации **подколец (sub-rings)** в сложных **многокольцевых топологиях ERPS (interconnected rings)**. Подкольцо обычно соединяется с главным кольцом (major ring) через общий узел.
- **Два основных сценария использования:**
    1. **Создание независимого подкольца (как обычного кольца, но с типом 'sub'):** Используется, когда необходимо логически выделить часть сети. В этом

SEC.RU | Короткий путь к информации Скачано с sec.ru

случае указываются оба порта (port0 и port1), аналогично команде erps <group> major.

```
(config)# erps 20 sub port0 interface Gi2/1 port1 interface Gi2/2
```

2. **Соединение подкольца с главным кольцом (interconnect):** Используется, когда данный узел является точкой соединения между подкольцом и главным кольцом. В этом случае указывается только port0 (порт, принадлежащий подкольцу), а параметр interconnect связывает это подкольцо с уже существующим главным кольцом (<major_ring_id>).
    - virtual-channel **(необязательно):** Активирует **виртуальный канал (VC)**, который позволяет служебным сообщениям подкольца (R-APS PDU) проходить через главное кольцо, не затрагивая его трафик данных. Это стандартный метод взаимодействия колец в G.8032.

```
(config)# erps 30 sub port0 interface Gi3/1 interconnect 10 virtual-channel
```

Удаление конфигурации:

```
(config)# no erps <group>
```

Полностью удаляет конфигурацию ERPS для указанной группы (как major, так и sub).

Просмотр состояния ERPS (Show):

```
# show erps [ <groups> ] [ detail | statistics ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.11.8 (config)# erps <group> topology-change propagate

Синтаксис:

```
(config)# erps <group> topology-change propagate
```

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.

Объяснение: Разрешить распространение уведомлений об изменении топологии.

Рекомендации:

- Команда erps <group> topology-change propagate управляет распространением **уведомлений об изменении топологии (Topology Change Notifications, TCN)** при срабатывании механизма защиты ERPS.
- **Что такое TCN?** Когда ERPS выполняет переключение (например, разблокирует RPL при обрыве), это изменяет активную топологию сети уровня 2. Чтобы другие протоколы (в первую очередь, **Spanning Tree Protocol - STP**) узнали об этом изменении и соответствующим образом обновили свои таблицы, необходимо сгенерировать и распространить TCN BPDU.
- **Назначение команды:**
    - ✓ **Включено (**topology-change propagate**):** Коммутатор будет **генерировать и отправлять** TCN BPDU на все свои порты (кроме порта, где произошло изменение) при

SEC.RU | Короткий путь к информации Скачано с sec.ru

срабатывании защиты ERPS. Это необходимо для корректной работы STP в сети.

- ✓ **Выключено (**`no topology-change propagate`**):** Коммутатор **не будет распространять** TCN при изменениях в кольце ERPS. Это может использоваться в строго контролируемых сетях, где обновление таблиц STP не требуется или является нежелательным.

- **В большинстве случаев эту опцию следует оставлять включенной.** Выключение может привести к тому, что другие коммутаторы в сети будут использовать устаревшие пути (старые MAC-адреса в своих таблицах), что вызовет временную потерю связности.
- Эта настройка применяется на уровне конкретной группы ERPS.

Удаление конфигурации (Negation):

```
(config)# no erps <group> topology-change propagate
```

Отключает распространение уведомлений об изменении топологии для указанной группы.

Просмотр состояния ERPS (Show):

```
# show erps [ <groups> ] [ detail | statistics ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.11.9 (config)# erps <group> version

Синтаксис:

(config)# erps <group> version { 1 | 2 }

Объяснение: Настройка версии ERPS для определенного профиля.

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- { 1 | 2 }: Укажите версию ERPS 1 или 2.

Рекомендации:

- Команда erps <group> version позволяет выбрать, какую **версию (ревизию) протокола G.8032 (ERPS)** использовать для конкретного кольца.
- **Различия версий:**
  - ✓ **Версия 1 (G.8032v1):** Базовая версия стандарта, поддерживающая одиночные кольца.
  - ✓ **Версия 2 (G.8032v2):** Расширенная версия, включающая поддержку **сложных топологий**, таких как **многокольцевые (interconnected rings)** и **подкольца (sub-rings)**, а также **виртуальные каналы (virtual channels)** для их взаимодействия.
- **Выбор версии:**
  - ✓ Для **простых одиночных колец** можно использовать любую версию, но для совместимости со старым оборудованием может потребоваться версия 1.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Для построения **сложных топологий с несколькими пересекающимися кольцами (interconnected rings) обязательно** необходимо использовать **версию 2**.

- **Важно**, чтобы **все коммутаторы в одном кольце (группе ERPS) были настроены на использование одинаковой версии протокола.** Несоответствие версий приведет к неработоспособности защиты.
- После изменения версии протокола может потребоваться перезагрузка кольца или повторное применение конфигурации.

Удаление конфигурации (Negation):

```
(config)# no erps <group> version
```

Сбрасывает настройку версии для указанной группы к значению по умолчанию (зависит от модели и ПО устройства, часто это версия 1).

Просмотр состояния ERPS (Show):

```
# show erps [ <groups> ] [ detail | statistics ]
```

2.7.11.10 (config)# erps <group> vlan

Синтаксис:

```
(config)# erps <group> vlan { none | [ add | remove ] <vlans> }
```

Объяснение: Настройка VLAN для определенного профиля ERPS.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <group: 1-64>: Укажите номер группы. Допустимый диапазон от 1 до 64.
- { none | [add | remove] <vlans> }: Укажите опцию.
    - ✓ none: Не включать какие-либо VLAN.
    - ✓ [add | remove] <vlans>: Добавить или удалить определенную VLAN.

Рекомендации:

- Команда erps <group> vlan управляет **списком VLAN, защищаемых (переносимых) данным кольцом ERPS**. Это позволяет сегментировать трафик и применять механизм защиты только к определенным VLAN, а не ко всему трафику на портах кольца.
- **Control VLAN и Protected VLANs:** Важно отличать эти понятия:
    - ✓ **Control VLAN:** Служебная VLAN (обычно один ID), по которой передаются сообщения протокола ERPS (R-APS PDU). Настраивается отдельно (часто через interface vlan и назначение на порты).
    - ✓ **Protected VLANs (Data VLANs):** Пользовательские VLAN, трафик которых должен защищаться механизмом ERPS (т.е., переключаться при обрыве). Их список задается данной командой.
- **Параметры:**
    - ✓ none: Указывает, что кольцо **не защищает ни одну VLAN данных**. Используется, если кольцо настроено только для служебных целей или для подготовки.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ add <vlans>: **Добавляет VLAN(ы)** в список защищаемых. Можно указать одну VLAN, диапазон (например, 10-20) или список через запятую (10,20,30).
- ✓ remove <vlans>: **Удаляет VLAN(ы)** из списка защищаемых.

- Для корректной работы трафик защищаемых VLAN должен быть разрешен (tagged или untagged) на всех портах кольца.
- По умолчанию, после создания кольца ERPS, список защищаемых VLAN, вероятно, пуст (none). Его необходимо явно заполнить.

Удаление конфигурации (Negation):

```
(config)# no erps <group> vlan
```

Полностью очищает список защищаемых VLAN для указанной группы (устанавливает none*).*

Просмотр состояния ERPS (Show):

```
# show erps [ <groups> ] [ detail | statistics ]
```

2.7.12 Включение алгоритма отсрочки перезапуска после избыточных коллизий (config-if)# excessive-restart

Синтаксис:

```
(config-if)# excessive-restart
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Перезапуск алгоритма отсрочки после 16 коллизий (Отключение excessive-restart означает отбрасывание кадров после 16 коллизий).

Удаление конфигурации (Negation):

```
(config-if)# no excessive-restart
```

Просмотр (Show):

```
> show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface ( <port_type> [ <v_port_type_list> ] ) status
```

Рекомендации:

- Команда excessive-restart управляет поведением Ethernet-порта в **полудуплексном (half-duplex) режиме** при возникновении последовательных коллизий (collisions).
- **Пояснение:** В сетях Ethernet с полудуплексом используется алгоритм CSMA/CD (Carrier Sense Multiple Access with Collision Detection). При обнаружении коллизии устройство запускает алгоритм отсрочки (backoff algorithm) — случайное ожидание перед повторной попыткой передачи.
- **Что делает команда:**
    - ✓ **Включено (**excessive-restart**):** Если на порту обнаруживается 16 последовательных коллизий при попытке передать один кадр, он не отбрасывает этот кадр, а перезапускает алгоритм отсрочки с нуля (начинает отсчет коллизий заново),

SEC.RU | Короткий путь к информации Скачано с sec.ru

продолжая попытки отправить тот же кадр. Это повышает вероятность доставки в условиях сильной загрузки среды, но может увеличить задержку.

- ✓ **Выключено (**`no excessive-restart`**):** После 16-й последовательной коллизии порт отбрасывает (discard) проблемный кадр и переходит к обработке следующего кадра из очереди. Это стандартное поведение, определенное в исходном стандарте IEEE 802.3.

- **Внимание:** Эта настройка **имеет значение только для портов, работающих в полудуплексном режиме (**`half`**)**. В современном полнодуплексном (`full`) Ethernet коллизии отсутствуют, и команда не оказывает никакого эффекта.
- В большинстве современных сетей, где порты работают в полнодуплексном режиме, эта настройка не требуется и может быть оставлена по умолчанию (`no excessive-restart`).

2.7.13 Включение/выключение управления потоком на интерфейсе (config-if)# flowcontrol

Синтаксис:

```
(config-if)# flowcontrol { on | off }
```

Объяснение: Включить или выключить управление потоком (flow control) для данного конкретного интерфейса.

Параметры:

- { on | off }: Включить или выключить управление потоком.

Удаление конфигурации (Negation):

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
(config-if)# no flowcontrol
```

Сбрасывает настройку управления потоком к значению по умолчанию (как правило off *или зависит от автосогласования).*

Просмотр (Show):

```
> show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface ( <port_type> [ <v_port_type_list> ] ) status
```

Рекомендации:

- Команда flowcontrol управляет функцией **управления потоком (flow control) на уровне канала передачи данных (Data Link Layer, IEEE 802.3x)** для полнодуплексного Ethernet.
- **Принцип работы:** Когда буфер приема порта заполняется, он может отправить специальный кадр "паузы" (PAUSE frame) на соседнее устройство, запрашивая временную приостановку передачи на указанный интервал времени. Это помогает предотвратить переполнение буфера (buffer overflow) и потерю пакетов.
- **Когда использовать:**
  - ✓ on **(включено):** Рекомендуется включать на высокоскоростных линках (например, 10 Гбит/с) и в сценариях, где возможен дисбаланс скорости (например, подключение высокоскоростного сервера). Помогает справиться с кратковременными всплесками трафика.
  - ✓ off **(выключено):** Частая настройка по умолчанию. Рекомендуется для большинства обычных портов доступа и в сетях, где используется контроль перегрузок

SEC.RU | Короткий путь к информации Скачано с sec.ru

на более высоких уровнях (TCP, QoS). Избыточные PAUSE-кадры могут негативно влиять на производительность.

- **Внимание:** Для корректной работы управление потоком должно быть согласовано (включено или выключено) на обоих концах соединения. При использовании автосогласования (auto-negotiation) этот параметр также согласуется.
- Управление потоком для полудуплекса (backpressure) реализуется иначе.

2.7.14 Настройка энергосберегающих функций Green Ethernet (config)# green-ethernet

2.7.14.1 (config)# green-ethernet led interval

Настройка интервала и интенсивности свечения светодиодов (LED) для снижения энергопотребления

Синтаксис:

```
(config)# green-ethernet led interval <v_0_to_24> intensity <v_0_to_100>
```

Объяснение: Настройка временного интервала и интенсивности свечения светодиодов для снижения энергопотребления.

Параметры:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- led interval <v_0_to_24>: Укажите временной интервал для работы светодиодов. Первое значение — время начала, второе — время окончания. Допустимые значения от 0 до 24.
- intensity <v_0_to_100>: Интенсивность свечения светодиодов. Значение от 0 до 100.

Рекомендации:

- Команда *green-ethernet led interval* позволяет управлять яркостью и, соответственно, энергопотреблением светодиодных индикаторов (LED) на передней панели коммутатора.
- **Принцип работы:** Вы определяете временной интервал (например, ночное время, когда в помещении мало людей) и задаете сниженную интенсивность свечения (например, 30% от максимальной яркости) в этот период. В остальное время LED работают на полную яркость (100%).
- Если временной интервал не указан, настройка не применяется. Команда *no green-ethernet led interval* отключает эту функцию для указанного интервала.

Удаление конфигурации:

```
(config)# no green-ethernet led interval <0~24>
```

Удаляет настройку снижения яркости для указанного временного интервала.

Примеры настройки:

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. **Снижение интенсивности LED до 80% в рабочее время (с 9:00 до 18:00):**

```
(config)# green-ethernet led interval 9 intensity 80
(config)# green-ethernet led interval 18 intensity 100
```

В 9:00 яркость LED снижается до 80%, в 18:00 возвращается к 100%.

2. **Снижение яркости LED до 30% в ночное время (с 22:00 до 7:00):**

```
(config)# green-ethernet led interval 22 intensity 30
(config)# green-ethernet led interval 7 intensity 100
```

3. **Отключение функции снижения яркости для ночного интервала:**

```
(config)# no green-ethernet led interval 22
```

2.7.14.2 (config)# green-ethernet led on-event

Настройка поведения светодиодов при возникновении событий

Синтаксис:

```
(config)# green-ethernet led on-event { [ link-change <v_0_to_65535> ] [ erro
r ] }
```

Объяснение: Коммутатор будет увеличивать интенсивность свечения светодиодов до 100% в течение указанного периода при возникновении любого события (например, отключения линка).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- [link-change <v_0_to_65535>]: Укажите, как долго (в секундах) интенсивность свечения LED будет 100% при возникновении ошибок. Допустимые значения от 0 до 65535.
- [error]: Увеличить интенсивность свечения LED до 100% при возникновении ошибок.

Рекомендации:

- Команда *green-ethernet led on-event* дополняет функцию управления энергопотреблением LED, позволяя временно **повышать яркость индикаторов до 100%** в случае возникновения определенных событий, даже если в данный момент действует интервал сниженной яркости.
- Позволяет обеспечить визуальную индикацию проблем (например, обрыва линка, ошибок на порту) для администратора, даже если в обычном режиме яркость LED снижена для экономии энергии.
- **Параметры:**
    - ✓ error**:** Активирует данное поведение (повышение яркости) при возникновении любых ошибок.
    - ✓ link-change <v_0_to_65535>**:** Определяет длительность (в секундах), на которую яркость будет повышена до 100% после наступления события. Например, если задано 600 (10 минут), LED будут гореть ярко в течение 10 минут после обрыва линка.
- Комбинация *green-ethernet led interval* (снижение яркости в заданное время) и *green-ethernet led on-event* (временное

SEC.RU | Короткий путь к информации Скачано с sec.ru

повышение яркости при событиях) позволяет достичь баланса между энергосбережением и оперативной визуальной диагностикой.

Удаление конфигурации:

```
(config)# no green-ethernet led on-event [ link-change ] [ error ]
```

Отключает функцию временного повышения яркости LED при указанных событиях.

Примеры настройки:

1. **Настройка: при любой ошибке повышать яркость LED до 100% на 10 минут (600 секунд):**

   ```
   (config)# green-ethernet led on-event link-change 600 error
   ```

   Теперь, даже если LED приглушены по расписанию, при обрыве кабеля они загорятся на полную мощность на 10 минут, привлекая внимание.

2. **Настройка только на повышение яркости при ошибках без указания длительности (используется значение по умолчанию):**

   ```
   (config)# green-ethernet led on-event error
   ```

2.7.14.3 (config)# green-ethernet eee optimize-for-power

Глобальное включение энергоэффективного Ethernet (EEE)

Синтаксис:

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
(config)# green-ethernet eee optimize-for-power
```

Объяснение: Включает функцию EEE (Energy-Efficient Ethernet) для данного коммутатора.

Рекомендации:

- Команда *green-ethernet eee optimize-for-power* глобально активирует стандарт **IEEE 802.3az (Energy-Efficient Ethernet, EEE)** на коммутаторе.
- **EEE** функция, которая позволяет физическим портам Ethernet переходить в режим пониженного энергопотребления (Low Power Idle, LPI) в периоды низкой сетевой активности. Когда трафик отсутствует или его интенсивность мала, передатчик "засыпает", экономя электроэнергию. При появлении трафика порт быстро "просыпается" и возобновляет передачу.
- EEE особенно эффективен на портах, подключенных к клиентским устройствам (ПК, телефоны), которые большую часть времени не генерируют интенсивный трафик. На высоконагруженных магистральных линках (uplink) эффект от EEE будет минимальным, а иногда даже может внести незначительную задержку при выходе из спящего режима.
- Влияние на производительность: Переход в режим LPI и выход из него занимает некоторое время (микросекунды), что теоретически может добавить небольшую задержку первому пакету после простоя. В современных сетях это влияние обычно незаметно для приложений.
- Взаимодействие с автосогласованием: Для работы EEE необходимо, чтобы функция была поддержана и согласована на

SEC.RU | Короткий путь к информации Скачано с sec.ru

обоих концах соединения (обычно в процессе автосогласования).

Удаление конфигурации:

```
(config)# no green-ethernet eee optimize-for-power
```

Глобально отключает функцию EEE.

Просмотр:

```
# show green-ethernet [ interface ( <port_type> [ <port_list> ] ) ]
# show green-ethernet eee [ interface ( <port_type> [ <port_list> ] ) ]
# show green-ethernet energy-detect [ interface ( <port_type> [ <port_list> ] ) ]
# show green-ethernet short-reach [ interface ( <port_type> [ <port_list> ] ) ]
```

2.7.14.4 (config-if)# green-ethernet eee

Включение EEE на выбранном интерфейсе

Синтаксис:

```
(config-if)# green-ethernet eee
```

Объяснение: Включает EEE (Energy-Efficient Ethernet) на выбранном интерфейсе.

Рекомендации:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Команда *green-ethernet eee*, выполняемая в режиме конфигурации интерфейса ((config-if)#), включает поддержку EEE на конкретном порту.
- Взаимосвязь с глобальной командой: Для того чтобы EEE работал на порту, необходимо выполнить оба условия:
    1. Глобально включен EEE на коммутаторе (*green-ethernet eee optimize-for-power*).
    2. На порту включен EEE данной командой.
- Если EEE не включен на порту (или отключен командой *no green-ethernet eee*), порт будет работать в обычном режиме без энергосбережения, даже если глобально функция активирована. Это позволяет гибко настраивать EEE только на тех портах, где это действительно необходимо.
- EEE обычно работает в паре с автосогласованием (auto-negotiation). Для успешной активации EEE на линке, подключенное устройство (свитч, ПК, сервер) также должно поддерживать и иметь включенный EEE.

Удаление конфигурации:

```
(config-if)# no green-ethernet eee
```

Отключает EEE на указанном интерфейсе.

Просмотр:

```
# show green-ethernet eee [ interface ( <port_type> [ <port_list> ] ) ]
```

Примеры настройки:

SEC.RU | Короткий путь к информации Скачано с sec.ru

Включение EEE на порту GigabitEthernet 1/1 (после глобального включения):

```
(config)# interface GigabitEthernet 1/1
(config-if)# green-ethernet eee
```

2.7.14.5 (config-if)# green-ethernet eee urgent-queues

Настройка "срочных" очередей для минимизации задержек при работе EEE

Синтаксис:

```
(config-if)# green-ethernet eee urgent-queues [ <urgent_queue_range_list> ]
```

Объяснение:

Можно минимизировать задержку для определенных кадров, назначая кадры в конкретную очередь (с помощью QoS) и затем помечая эту очередь как "срочную" (urgent). Когда в срочную очередь поступают данные для передачи, схемы питания незамедлительно активируются, и задержка сокращается до времени пробуждения (wakeup time). Очереди, не помеченные как срочные, будут откладывать передачу до тех пор, пока не накопится пачка кадров для передачи.

Параметры:

- [<urgent_queue_range_list>]: Укажите диапазон "срочных" очередей. Допустимый диапазон от 1 до 8.

Рекомендации:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Эта команда предоставляет тонкую настройку взаимодействия EEE и QoS (Quality of Service). Она позволяет определить, трафик из каких очередей приоритетов должен немедленно "будить" порт из энергосберегающего режима (LPI), а трафик из каких очередей может подождать.
- Когда порт находится в режиме пониженного энергопотребления (LPI), для отправки первого пакета требуется время на "пробуждение" (wakeup time). Для чувствительного к задержкам трафика (например, VoIP, видеоконференции) эта дополнительная задержка нежелательна. Для менее чувствительного трафика (например, массовые загрузки, email) небольшая задержка приемлема
- **Как настроить:**
    1. С помощью механизмов QoS (например, `qos map`) определенный тип трафика направляется в определенную очередь (например, голосовой трафик в очередь 5, а данные в очередь 2).
    2. На порту с помощью данной команды очереди, содержащие важный трафик, помечаются как **срочные (**`urgent-queues`**)**. Например: `green-ethernet eee urgent-queues 5,6`.
    3. Когда в срочную очередь (5 или 6) попадает кадр, порт немедленно просыпается и отправляет его.
    4. Когда кадр попадает в обычную очередь (2), порт может подождать, накопить больше кадров из этой очереди и отправить их одним этапом, экономя энергию.
- Если параметр не указан, ни одна очередь не считается срочной.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no green-ethernet eee urgent-queues [ <urgent_queue_range_list > ]
```

Если указан диапазон, удаляет отметку "срочности" для этих очередей. Если диапазон не указан, удаляет настройку для всех очередей (возврат к состоянию "нет срочных очередей").

Примеры настройки:

Назначение очередей 5 и 6 (обычно для голоса и видео) как "срочных" на порту Gi1/1:

```
(config)# interface GigabitEthernet 1/1
(config-if)# green-ethernet eee urgent-queues 5,6
```

2.7.14.6 (config-if)# green-ethernet energy-detect

Включение энергосбережения при отсутствии линка

Синтаксис:

```
(config-if)# green-ethernet energy-detect
```

Объяснение: Включение функции энергосбережения для данного конкретного интерфейса, когда нет подключенного устройства (линк-партнера).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда *green-ethernet energy-detect* активирует режим **Energy Detect** на порту.
- Принцип работы: Когда кабель не подключен к порту или подключенное устройство выключено (линк отсутствует), коммутатор переводит передатчик порта в режим пониженного энергопотребления. Вместо постоянной отправки импульсов для поддержания линка (или их полного отсутствия), порт периодически "просыпается" и проверяет, не появился ли линк-партнер. Как только подключение обнаруживается, порт мгновенно возвращается к нормальной работе. Эта функция позволяет существенно снизить энергопотребление на портах, которые большую часть времени простаивают (например, резервные порты, порты в неиспользуемых розетках).

Удаление конфигурации:

```
(config-if)# no green-ethernet energy-detect
```

Отключает функцию энергосбережения при отсутствии линка на указанном интерфейсе. Порт будет потреблять больше энергии в ожидании подключения.

Просмотр:

```
# show green-ethernet energy-detect [ interface ( <port_type> [ <port_list> ] ) ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.14.7 (config-if)# green-ethernet short-reach

Включение энергосбережения для коротких кабелей

Синтаксис:

```
(config-if)# green-ethernet short-reach
```

Объяснение: Включение энергосбережения для портов, которые подключены к линк-партнеру с помощью короткого кабеля.

Рекомендации:

- Команда *green-ethernet short-reach* активирует режим Short Reach на порту. Эта функция основана на том, что для передачи сигнала на короткое расстояние требуется меньше мощности, чем на длинное.
- Когда порт устанавливает линк с подключенным устройством, он анализирует длину кабеля (на основе затухания сигнала или других параметров). Если кабель короткий (обычно менее 30-50 метров), порт автоматически снижает мощность передатчика до уровня, достаточного для надежной связи. Это снижает энергопотребление порта и электромагнитное излучение. Эта функция особенно полезна в типовых офисных сетях, где большинство кабелей от коммутатора до рабочей станции не превышают нескольких десятков метров. На длинных линиях (близких к пределу в 100 метров для витой пары) мощность остается на нормальном уровне.
- Рекомендуется включать на всех портах доступа по умолчанию. Функция безопасна и не влияет на работу, даже если кабель окажется длинным — порт автоматически подстроит мощность.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Для корректной работы функция может требовать, чтобы на порту было включено автосогласование (auto-negotiation).

Удаление конфигурации:

```
(config-if)# no green-ethernet short-reach
```

Отключает функцию энергосбережения для коротких кабелей на указанном интерфейсе. Порт всегда будет использовать полную мощность передатчика независимо от длины кабеля.

Просмотр:

```
# show green-ethernet short-reach [ interface ( <port_type> [ <port_list> ] ) ]
```

2.7.15 Глобальное включение GVRP (config)# gvrp

2.7.15.1(config)# gvrp

Синтаксис:

```
(config)# gvrp
```

Объяснение: Глобальное включение функции GVRP (GARP VLAN Registration Protocol).

Удаление конфигурации (Negation):

```
(config)# no gvrp
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда *gvrp* (без дополнительных параметров) глобально активирует протокол **GVRP (GARP VLAN Registration Protocol)** на коммутаторе.
- **GVRP** это протокол, основанный на GARP (Generic Attribute Registration Protocol), который позволяет коммутаторам автоматически обмениваться информацией о VLAN и динамически создавать VLAN на портах, где это необходимо. Упрощенно: если на одном коммутаторе настроена VLAN 10, и к нему подключен другой коммутатор с включенным GVRP, второй коммутатор может автоматически узнать о VLAN 10 и добавить ее в свой список разрешенных VLAN на линковом порту.
- Зачем нужно:
    - ✓ Упрощение администрирования VLAN в крупных сетях.
    - ✓ Автоматическое распространение информации о VLAN.
    - ✓ Снижение риска ошибок при ручной настройке транков.
- **Внимание!** GVRP может представлять угрозу безопасности, так как позволяет динамически создавать VLAN без ведома администратора. Злоумышленник, подключившись к порту, где GVRP включен, может анонсировать свою VLAN и получить доступ к соответствующим сетям. Поэтому GVRP рекомендуется включать только в доверенной среде (например, в ядре сети) или не включать вовсе, используя статическую конфигурацию.
- После глобального включения GVRP, необходимо также включить его на конкретных портах (в режиме конфигурации интерфейса), чтобы они участвовали в обмене информацией о VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.15.2 (config)# gvrp max-vlans

Настройка максимального количества VLAN, изучаемых через GVRP

Синтаксис:

```
(config)# gvrp max-vlans <maxvlans>
```

Объяснение: Установка максимального количества VLAN, которые могут быть изучены через GVRP.

Параметры:

- <maxvlans>: Укажите количество VLAN, изучаемых через GVRP.

Рекомендации:

- Команда *gvrp max-vlans* устанавливает верхний предел на количество VLAN, которые коммутатор может динамически запомнить через протокол GVRP. VLAN, созданные администратором вручную (статически), в этот лимит обычно не входят.
- Зачем нужно:
    - ✓ Защита от исчерпания ресурсов (DoS-атака): предотвращает ситуацию, когда злоумышленник или неправильно настроенное устройство начнет рассылать большое количество GVRP-сообщений, пытаясь создать множество VLAN и исчерпать память или процессорные ресурсы коммутатора.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Контроль сети: позволяет администратору контролировать сеть, и предотвращает случайное создание избыточного количества VLAN.

- Выбор значения: Значение должно быть достаточно большим, чтобы вместить все VLAN, которые могут появиться в сети динамически, но достаточно маленьким, чтобы обеспечить защиту. Например, если в сети ожидается не более 50 динамических VLAN, можно установить лимит 60 или 70.
- Команда имеет смысл только в том случае, если GVRP глобально включен (gvrp).

Удаление конфигурации:

```
(config)# no gvrp max-vlans <maxvlans>
```

Сбрасывает ограничение на максимальное количество изучаемых VLAN к значению по умолчанию (зависит от модели устройства, часто это максимально возможное количество VLAN).

2.7.15.3 (config)# gvrp time

Настройка таймеров GVRP

Синтаксис:

```
(config)# gvrp time { [ join-time <jointime> ] [ leave-time <leavetime> ] [ leave-all-time <leavealltime> ] }
```

Объяснение: Установка таймеров для протокола GVRP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- [join-time <jointime>]: Укажите время (в сантисекундах), с которым передаются PDU (блоки данных протокола). Значение по умолчанию — 20 сантисекунд. Допустимые значения: 1~20.
- [leave-time <leavetime>]: Укажите время (в сантисекундах), которое устройство ожидает перед удалением соответствующей записи. Время ожидания удаления активируется сообщением "Leave All-time", отправленным/полученным, и отменяется сообщением Join. Значение по умолчанию — 60 сантисекунд.
- [leave-all-time <leavealltime>]: Укажите время (в сантисекундах), через которое создаются PDU "LeaveAll". PDU LeaveAll указывает, что все регистрации будут вскоре сняты с регистрации. Участникам потребуется повторно присоединиться, чтобы сохранить регистрацию. Допустимые значения: от 1000 до 5000 сантисекунд. Значение по умолчанию — 1000 сантисекунд.

Внимание: Параметр "LeaveAll-time" должен быть больше параметра "Leave-time".

Рекомендации:

- Команда gvrp time позволяет настроить **таймеры протокола GVRP**. Корректная настройка этих таймеров важна для стабильной и эффективной работы динамического распространения VLAN.
- **Таймеры GVRP:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Join-time (Таймер присоединения):** Определяет, как часто устройство отправляет Join-сообщения для подтверждения своей заинтересованности в VLAN. Меньшие значения ускоряют распространение информации, но увеличивают служебный трафик.
- ✓ **Leave-time (Таймер ожидания удаления):** Время, в течение которого устройство ждет подтверждения (Join) после получения LeaveAll-сообщения, прежде чем удалить запись о VLAN. Должен быть **больше**, чем Join-time.
- ✓ **LeaveAll-time (Таймер массового удаления):** Период, с которым устройство генерирует LeaveAll-сообщения, инициируя процесс "перерегистрации" всех VLAN. Это механизм "сброса" и обновления информации. Должен быть **значительно больше**, чем Leave-time (обычно в 10 и более раз).

- Существует правило LeaveAll-time > Leave-time > Join-time. Нарушение этого правила приведет к нестабильной работе GVRP.
- **Настройка по умолчанию:**
  - ✓ Join-time: 20 cc (0.2 секунды)
  - ✓ Leave-time: 60 cc (0.6 секунды)
  - ✓ LeaveAll-time: 1000 cc (10 секунд)
- В большинстве сетей значения по умолчанию работают хорошо. Изменять их может потребоваться в очень больших сетях с множеством VLAN, чтобы снизить служебный трафик (увеличив таймеры), или, наоборот, в сетях, где топология VLAN меняется очень часто (уменьшив таймеры).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no gvrp time { [join-time <jointime> ] [ leave-time <leavetime> ] [ leave-all-time <leavealltime> ] }
```

Сбрасывает указанный таймер к значению по умолчанию.

2.7.15.4 (config-if)# gvrp

Включение GVRP на указанных интерфейсах

Синтаксис:

```
(config-if)# gvrp
```

Объяснение: Включение функции GVRP на указанных интерфейсах.

Рекомендации:

- Команда *gvrp* в режиме конфигурации интерфейса включает протокол GVRP на конкретном порту (или диапазоне портов). После глобального включения GVRP на коммутаторе, эта команда необходима для того, чтобы порт начал участвовать в обмене GVRP-сообщениями и динамически изучал VLAN.
- Как это работает:
    1. Порт с включенным GVRP прослушивает GVRP-объявления от соседних устройств.
    2. Когда он слышит объявление о VLAN, которой у него нет в списке разрешенных, он может динамически добавить эту VLAN в список разрешенных на этом порту (порт становится членом VLAN).

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Он также может передавать информацию о VLAN, настроенных статически, дальше по сети.

- **Внимание:** Включайте GVRP только на портах, которые ведут к другим доверенным коммутаторам в управляемой сети (обычно на транковых портах между коммутаторами). Никогда не включайте GVRP на портах доступа, к которым подключаются конечные пользователи, так как это создает серьезную уязвимость (пользователь может анонсировать свою VLAN и получить несанкционированный доступ).
- Порты, на которых включен GVRP, должны быть настроены как транковые, чтобы пропускать тегированные кадры нескольких VLAN.

Удаление конфигурации:

```
(config-if)# no gvrp
```

Отключает GVRP на указанном интерфейсе. Порт перестанет участвовать в динамическом обмене информацией о VLAN и удалит все динамически изученные VLAN.

Примеры настройки:

Включение GVRP на портах 1-5 (например, для связи с другими коммутаторами):

```
# configure terminal
(config)# interface GigabitEthernet 1/1-5
(config-if)# gvrp
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.16 Настройка имени устройства (hostname)

Синтаксис:

```
(config)# hostname <WORD>
```

Объяснение: Укажите описательное имя для данного коммутатора.

Параметры:

- <WORD>: Укажите описательное имя для данного устройства. Укажите имя хоста для этого устройства. Можно использовать буквы (A-Z; a-z), цифры (0-9) и знак минуса (-). Однако пробелы не допускаются. Первый символ должен быть буквой. Первый и последний символы не могут быть знаком минуса. Допустимая длина строки от 0 до 255 символов.

Удаление конфигурации:

```
(config)# no hostname
```

Сбрасывает имя устройства к значению по умолчанию (обычно "Switch").

Просмотр:

```
> show version
# show version
```

Имя устройства отображается в приглашении командной строки, а также в выводе команд show version*.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда *hostname* задает имя для коммутатора. Это имя отображается в приглашении командной строки, помогая администратору идентифицировать устройство, с которым он работает.
- Для чего нужно
    - ✓ **Идентификация:** Критически важно для управления в сети с несколькими устройствами. Позволяет быстро понять, на каком коммутаторе вы находитесь
    - ✓ **Логи и сообщения:** Имя устройства включается в системные сообщения и логи, что облегчает поиск источника событий.
    - ✓ **SNMP:** Имя устройства часто используется в SNMP-запросах как *sysName*.
- После смены имени приглашение командной строки изменится немедленно

2.7.17 Вход в режим конфигурации интерфейса (interface)

2.7.17.1 (config)# interface (<port_type> [<plist>])

Синтаксис:

```
(config)# interface ( <port_type> [ <plist> ] )
```

Объяснение: Переход в режим конфигурации интерфейса (Config Interface mode) для данного конкретного интерфейса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- *<port_type> [<plist>]:* Укажите тип порта и номер порта (или список/диапазон портов).

Просмотр: (Широкий набор команд для просмотра статуса, статистики и возможностей интерфейсов)

```
> show interface ( <port_type> [ <in_port_list> ] ) switchport [ access | trunk | hybrid ]
> show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
> show interface ( <port_type> [ <v_port_type_list> ] ) statistics [{ packets | bytes | errors | discards | filtered | { priority [ <priority_0_to_7> ] } } ] [ { up | down } ]
> show interface ( <port_type> [ <v_port_type_list> ] ) status
> show interface vlan [ <vlist> ]
# show interface ( <port_type> [<in_port_list> ] ) switchport [access | trunk | hybrid ]
# show interface ( <port_type> [ <v_port_type_list> ] ) capabilities
# show interface ( <port_type> [ <v_port_type_list> ] ) statistics [{ packets | bytes | errors | discards | filtered | { priority [ <priority_0_to_7> ] } } ] [ { up | down } ]
# show interface ( <port_type> [ <v_port_type_list> ] ) status
# show interface vlan [ <vlist> ]
```

Очистка статистики:

```
# clear statistics { [ interface ] ( <port_type> [ <v_port_type_list> ] ) }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда *interface* является основным способом перехода в режим конфигурации конкретного порта (или группы портов). В этом режиме ((config-if)#) применяются все настройки, специфичные для физического интерфейса: скорость, дуплекс, VLAN, описание, управление потоком, Port Security и т.д.
- После входа в этот режим все последующие команды применяются ко всем указанным портам, если не указано иное. Это мощный инструмент для массовой настройки.
- Для выхода из режима конфигурации интерфейса обратно в глобальную конфигурацию используется команда exit. Для немедленного возврата в привилегированный режим EXEC (#) — команда end или Ctrl+Z.
- Команды *show interface* (в пользовательском и привилегированном режимах) являются основными инструментами для мониторинга состояния, статистики и возможностей портов.

2.7.17.2 (config)# interface vlan

Вход в режим конфигурации интерфейса VLAN (SVI)

Синтаксис:

```
(config)# interface vlan <vlist>
```

Объяснение: Переход в режим конфигурации интерфейса VLAN (Config Interface VLAN mode) для данного конкретного интерфейса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <vlist>: Укажите идентификатор VLAN (VLAN ID) для интерфейса уровня 3.

Рекомендации:

- Команда *interface vlan* используется для создания и настройки виртуального интерфейса уровня 3 (SVI — Switch Virtual Interface), связанного с определенной VLAN.
- Назначение SVI:
    - ✓ Обеспечение IP-связности (маршрутизации) между VLAN на коммутаторе уровня 3 (или L2+). Коммутатор может выступать в роли шлюза по умолчанию для устройств в этой VLAN.
    - ✓ Предоставление интерфейса управления (management interface) для самого коммутатора. По умолчанию это обычно VLAN 1.
    - ✓ Участие в протоколах маршрутизации (OSPF, RIP, статические маршруты), если поддерживаются
- Внимание:
    - ✓ Прежде чем настраивать интерфейс VLAN, сама VLAN должна быть создана
    - ✓ Физические порты должны быть назначены в эту VLAN (как access или trunk), чтобы трафик мог достичь SVI.
    - ✓ Для того чтобы SVI работал (был в состоянии UP/UP), в этой VLAN должен быть хотя бы один активный (линк UP) порт коммутатора.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- В режиме *(config-if-vlan)#* вы можете настроить IP-адрес (статический или DHCP, если поддерживается), описание, параметры протоколов маршрутизации и другие свойства, присущие интерфейсу уровня 3.

Просмотр:

```
> show interface vlan [ <vlist> ]
# show interface vlan [ <vlist> ]
```

2.7.18 Настройка IP-протоколов (config)# ip

2.7.18.1 (config)# ip arp inspection

Глобальное включение проверки ARP (ARP Inspection)

Синтаксис:

```
(config)# ip arp inspection
```

Объяснение: Включение функции проверки ARP (ARP Inspection).

Рекомендации:

- Команда ip arp inspection глобально активирует функцию безопасности **Dynamic ARP Inspection (DAI)** на коммутаторе.
- **DAI** – это механизм защиты от **ARP-спуфинга**. DAI перехватывает все ARP-пакеты на ненадежных портах и проверяет их валидность, сверяя информацию (IP-MAC) с доверенной базой данных, создаваемой DHCP Snooping. ARP-пакеты с несоответствующими адресами отбрасываются.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Принцип работы:**
    1. Коммутатор, используя базу данных привязок DHCP Snooping (DHCP Snooping binding table), знает, какой IP-адрес должен принадлежать какому MAC-адресу и на каком порту.
    2. Когда на порт, где включена проверка, приходит ARP-пакет, коммутатор проверяет соответствие (IP, MAC, порт) по этой базе.
    3. Если пакет не соответствует записи в базе (например, злоумышленник пытается выдать себя за шлюз), он отбрасывается, и может быть зарегистрировано нарушение.
- Для работы DAI необходимо включить DHCP Snooping (ip dhcp snooping) на коммутаторе, так как DAI использует его базу данных привязок.
- DAI обычно настраивается на портах доступа. Порты, ведущие к другим коммутаторам или маршрутизаторам, должны быть настроены как доверенные (trusted), чтобы не блокировать легитимный ARP-трафик между ними.

Удаление конфигурации (Negation):

```
(config)# no ip arp inspection
```

Глобально отключает Dynamic ARP Inspection.

Просмотр:

```
> show ip arp inspection [ interface ( <port_type> [ <in_port_type_list> ] ) |
vlan <in_vlan_list> ]
# show ip arp inspection [ interface ( <port_type> [ <in_port_type_list> ] ) |
vlan <in_vlan_list> ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Очистка:

```
# clear ip arp
```

2.7.18.2 (config)# ip arp inspection entry interface

Создание статической записи для ARP Inspection

Синтаксис:

```
(config)# ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>
```

Объяснение: Создание статической записи для ARP Inspection.

Параметры:

- <port_type> <in_port_type_id>: Укажите тип порта и номер порта.
- <vlan_var>: Укажите настроенный идентификатор VLAN.
- <mac_var>: Укажите разрешенный исходный MAC-адрес в ARP-запросах.
- <ipv4_var>: Укажите разрешенный исходный IP-адрес в ARP-запросах.

Рекомендации:

- Команда *ip arp inspection entry interface* создает статическую запись в базе данных привязок, используемую функцией **Dynamic ARP Inspection (DAI)**.
- DAI для проверки ARP-пакетов использует базу данных, созданную DHCP Snooping. Однако устройства со статическими

SEC.RU | Короткий путь к информации Скачано с sec.ru

IP-адресами (серверы, принтеры, сетевое оборудование) не проходят процесс DHCP и, следовательно, не имеют динамической записи в этой базе. Чтобы DAI не блокировал ARP-трафик от таких устройств, для них необходимо вручную создать статические записи.

- Запись связывает конкретный порт, VLAN, MAC-адрес и IP-адрес. Когда на указанном порту приходит ARP-пакет, DAI проверяет, соответствует ли его (Source MAC, Source IP) этой статической записи.
- Без статической записи DAI будет отбрасывать ARP-пакеты от таких устройств, нарушая связь.

Удаление конфигурации:

```
(config)# no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>
```

Удаляет указанную статическую запись ARP Inspection.

Просмотр:

```
# show ip arp inspection entry [ dhcp-snooping | static ] [ interface ( <port_type> [ <in_port_type_list> ] ) ]
```

*Позволяет просмотреть статические (*static*) или динамические (*dhcp-snooping*) записи, используемые DAI.*

Очистка (Clear):

```
# clear ip arp
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.3 (config)# ip arp inspection translate

Преобразование динамической записи ARP Inspection в статическую

Синтаксис:

```
(config)# ip arp inspection translate [ interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var> ]
```

Объяснение: Преобразование динамической записи в статическую.

Параметры:

- <port_type> <in_port_type_id>: Укажите тип порта и номер порта.
- <vlan_var>: Укажите настроенный идентификатор VLAN.
- <mac_var>: Укажите разрешенный исходный MAC-адрес в ARP-запросах.
- <ipv4_var>: Укажите разрешенный исходный IP-адрес в ARP-запросах.

Рекомендации:

- Команда *ip arp inspection translate* позволяет преобразовать существующую динамическую запись из базы данных DHCP Snooping в статическую запись для ARP Inspection.
- Зачем это нужно:
    1. **Устройства со статическим IP:** Если устройство изначально получало адрес по DHCP (и поэтому имеет динамическую запись), но затем было переведено на статический IP-адрес, можно преобразовать его последнюю известную корректную динамическую запись

SEC.RU | Короткий путь к информации Скачано с sec.ru

в статическую, чтобы ARP Inspection продолжал его пропускать. Это удобнее, чем создавать запись вручную с нуля.

2. **Миграция и резервирование:** Полезно, когда нужно зафиксировать привязку для критически важного устройства, которое ранее работало по DHCP, гарантируя, что оно не будет заблокировано DAI после перезагрузки или изменения аренды.

- Преобразованная статическая запись ведет себя так же, как и созданная вручную командой *ip arp inspection entry interface*.

Просмотр:

```
# show ip arp inspection entry [ dhcp-snooping | static ] [ interface ( <port_type> [ <in_port_type_list> ] ) ]
```

Используется для просмотра как динамических (dhcp-snooping), так и статических записей, чтобы найти нужную для преобразования.

2.7.18.4 (config)# ip arp inspection vlan

Включение ARP Inspection в указанных VLAN

Синтаксис:

```
(config)# ip arp inspection vlan <in_vlan_list>
```

Объяснение: Указывает, в каких VLAN включена проверка ARP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <in_vlan_list>: Укажите список идентификаторов VLAN, для которых будет включена проверка ARP.

Рекомендации:

- Команда *ip arp inspection vlan* активирует функцию **Dynamic ARP Inspection (DAI)** не глобально на всех VLAN, а только в указанных VLAN. Это позволяет более гибко применять защиту от ARP-спуфинга.
- После глобального включения DAI (ip arp inspection), необходимо явно указать, какие VLAN будут защищены. Трафик в незащищенных VLAN не будет проверяться.
- Для работы DAI в указанных VLAN также необходимо, чтобы в этих VLAN был включен DHCP Snooping (команда ip dhcp snooping vlan <vlan_list>), так как DAI использует его базу данных.

Удаление конфигурации (Negation):

```
(config)# no ip arp inspection vlan <in_vlan_list>
```

Отключает проверку ARP в указанных VLAN. Для полного отключения DAI также потребуется глобальная команда no ip arp inspection*.*

Просмотр:

```
> show ip arp inspection
# show ip arp inspection
```

Показывает статус DAI глобально и по VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Очистка:

```
# clear ip arp
```

2.7.18.5 (config)# ip arp inspection vlan <in_vlan_list> logging

Настройка логирования для ARP Inspection в указанных VLAN

Синтаксис:

```
(config)# ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }
```

Объяснение: Включение функции логирования.

Параметры:

- { deny | permit | all }: Укажите один из типов логирования.
    - ✓ deny: Логировать заблокированные (отклоненные) записи.
    - ✓ permit: Логировать разрешенные записи.
    - ✓ all: Логировать все записи.

Рекомендации:

- Команда *ip arp inspection vlan logging* управляет тем, какие события, связанные с проверкой ARP, будут записываться в системный журнал (syslog) для указанных VLAN.
- Зачем нужно логирование:
    - ✓ **Обнаружение атак:** Логирование отклоненных (deny) ARP-пакетов — это основной способ обнаружения попыток ARP-спуфинга или других аномалий в сети. Вы

SEC.RU | Короткий путь к информации Скачано с sec.ru

сможете увидеть, откуда (с какого порта и с какими адресами) приходили подозрительные пакеты.

- ✓ **Отладка и мониторинг:** Логирование разрешенных (permit) пакетов может быть полезно для отладки, но в рабочей сети оно создаст огромное количество избыточных записей.

- **Выбор уровня логирования:**
  - ✓ deny (рекомендуется): Включает запись только отклоненных пакетов. Это позволяет отслеживать нарушения, не перегружая журнал.
  - ✓ permit**:** Включает запись разрешенных пакетов. Используйте крайне осторожно и только для кратковременной отладки.
  - ✓ all**:** Включает запись всех ARP-пакетов (и разрешенных, и отклоненных). Может быстро заполнить буфер логов.
- Логируемые события обычно содержат информацию о порте, VLAN, MAC-адресе источника и IP-адресе источника.

Удаление конфигурации:

```
(config)# no ip arp inspection vlan <in_vlan_list> logging
```

Отключает логирование ARP Inspection для указанных VLAN.

Просмотр:

```
> show ip arp inspection
# show ip arp inspection
```

Показывает статус логирования для каждого VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Очистка:

```
# clear ip arp
```

2.7.18.6 (config)# ip dhcp relay

Глобальное включение функции DHCP Relay

Синтаксис:

```
(config)# ip dhcp relay
```

Объяснение: Включение функции ретрансляции DHCP (DHCP Relay).

Рекомендации:

- Команда ip dhcp relay глобально активирует функцию **DHCP Relay** на коммутаторе.
- DHCP Relay – Это функция, которая позволяет ретранслировать широковещательные (broadcast) DHCP-запросы от клиентов в unicast-запросы и пересылать их на указанный DHCP-сервер, находящийся в другой подсети (другой VLAN). Это избавляет от необходимости иметь DHCP-сервер в каждом широковещательном домене.
- Внимание:
    1. Необходимо настроить IP-адрес DHCP-сервера (или нескольких серверов) на интерфейсе VLAN, с которого нужно ретранслировать запросы.
    2. Функция relay должна быть включена на интерфейсах VLAN (настраивается отдельно).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no ip dhcp relay
```

Глобально отключает функцию DHCP Relay.

Просмотр:

```
> show ip dhcp relay [statistics]
# show ip dhcp relay [statistics]
```

Показывает статус relay и статистику ретранслированных сообщений.

Очистка:

```
# clear ip dhcp relay statistics
```

2.7.18.7 (config)# ip dhcp relay information option

Включение опции 82 (Relay Agent Information Option) для DHCP Relay

Синтаксис:

```
(config)# ip dhcp relay information option
```

Объяснение: Включение функции опции 82 для DHCP Relay. Обратите внимание, что "Режим Relay" должен быть включен, прежде чем эта функция сможет вступить в силу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда ip dhcp relay information option активирует добавление опции 82 (Relay Agent Information Option, RFC 3046) в DHCP-пакеты, ретранслируемые коммутатором.
- опция 82 – Это дополнительная информация, которую DHCP Relay Agent (коммутатор) может вставить в DHCP-запрос перед отправкой его на сервер. Эта информация помогает DHCP-серверу более точно идентифицировать клиента и принимать решения о выдаче IP-адреса.
- опция 82:
    - ✓ Circuit ID (Идентификатор схемы): Обычно идентифицирует порт и VLAN, с которого пришел запрос (например, GigabitEthernet 1/1).
    - ✓ Remote ID (Идентификатор удаленного устройства): Обычно это MAC-адрес или IP-адрес самого Relay Agent (коммутатора).
- Зачем нужна опция 82:
    - ✓ Политики IP-адресации: DHCP-сервер может назначать IP-адреса на основе того, с какого порта или коммутатора пришел запрос (например, выделять определенный пул адресов для конкретного этажа здания).
    - ✓ Безопасность: Позволяет отследить физическое местоположение клиента.
    - ✓ Предотвращение атак: Помогает бороться с атаками типа "DHCP Starvation", связывая запросы с конкретным портом.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Внимание: Как указано в описании, для работы этой функции необходимо, чтобы глобально был включен DHCP Relay (ip dhcp relay).

Удаление конфигурации:

```
(config)# no ip dhcp relay information option
```

Отключает добавление опции 82 в ретранслируемые DHCP-пакеты

2.7.18.8 (config)# ip dhcp relay information policy

Настройка политики обработки существующей информации ретрансляции (опции 82)

Синтаксис:

```
(config)# ip dhcp relay information policy { drop | keep | replace }
```

Объяснение: Укажите действие политики для информации ретрансляции DHCP.

Параметры:

- { drop | keep | replace }: Укажите один из вариантов политики обработки информации ретрансляции.
    - ✓ drop**:** Отбросить пакет, когда он получает DHCP-сообщение, которое уже содержит информацию ретрансляции (опцию 82).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ keep**:** Сохранить существующую DHCP-информацию клиента (не изменять её).
- ✓ replace**:** Заменить информацию в пакете DHCP-клиента на информацию ретрансляции коммутатора. Это настройка по умолчанию.

Рекомендации:

- Команда *ip dhcp relay information policy* определяет, как коммутатор (выступающий в роли DHCP Relay Agent) должен поступать, если входящий DHCP-пакет уже содержит опцию 82 (Relay Agent Information). Такая ситуация может возникнуть, если пакет прошел через другое устройство, также выполняющее функции ретрансляции (например, в многоуровневой сети).
- **Варианты политик:**
  - ✓ drop (Отбросить): Самая строгая политика. Если в пакете уже есть опция 82, коммутатор считает это подозрительным и отбрасывает пакет. Это предотвращает возможные манипуляции, но может нарушить работу в сетях со сложной топологией, где несколько relay-агентов законны.
  - ✓ keep (Сохранить): Коммутатор оставляет существующую опцию 82 нетронутой и пересылает пакет дальше. Это полезно, если нижестоящее устройство (например, другой коммутатор) уже добавило свою информацию, и её нужно сохранить для передачи на сервер.
  - ✓ replace (Заменить): Поведение по умолчанию. Коммутатор заменяет существующую опцию 82 своей собственной информацией (идентификатор

SEC.RU | Короткий путь к информации Скачано с sec.ru

порта, MAC и т.д.). Это гарантирует, что DHCP-сервер получит актуальную информацию от последнего устройства в цепочке ретрансляции.

- Выбор политики зависит от топологии сети и требований к идентификации клиентов. В простых сетях с одним relay-агентом достаточно настроек по умолчанию (replace).

Удаление конфигурации:

```
(config)# no ip dhcp relay information policy
```

*Сбрасывает политику к значению по умолчанию (*replace*).*

2.7.18.9 (config)# ip dhcp snooping

Глобальное включение функции DHCP Snooping

Синтаксис:

```
(config)# ip dhcp snooping
```

Объяснение: Глобальное включение функции DHCP Snooping. Когда режим работы DHCP Snooping включен, DHCP-запросы будут перенаправляться на доверенные (trusted) порты, а ответы разрешено получать только с доверенных портов.

Рекомендации:

- Команда *ip dhcp snooping* глобально активирует функцию безопасности **DHCP Snooping** на коммутаторе.
- DHCP Snooping – Это механизм защиты. Он предотвращает ряд атак, таких как:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Подмена DHCP-сервера (Rogue DHCP Server): Злоумышленник может запустить свой DHCP-сервер и раздавать клиентам неправильные настройки (подмененный шлюз, DNS). DHCP Snooping блокирует ответы от DHCP-серверов на ненадежных портах.
- ✓ DHCP Starvation (истощение): Атака, при которой злоумышленник отправляет множество DHCP-запросов с разными MAC-адресами, чтобы исчерпать пул адресов.
- ✓ ARP Spoofing: Создает базу данных привязок (Binding Table), которая используется другими функциями, такими как Dynamic ARP Inspection (DAI).

- **Принцип работы:**

1. Коммутатор делит порты на доверенные (trusted) и ненадежные (untrusted).
2. По умолчанию все порты считаются ненадежными.
3. DHCP-ответы (OFFER, ACK, NAK) разрешены только с доверенных портов (где сидит настоящий DHCP-сервер). Ответы с ненадежных портов блокируются.
4. DHCP Snooping строит и поддерживает базу данных (Binding Table), содержащую записи (MAC-адрес, IP-адрес, VLAN, порт, время аренды) для всех клиентов, успешно получивших адрес.

- **Внимание:**

1. Настроить порты, ведущие к DHCP-серверам (или uplink к другому коммутатору, за которым есть сервер), как доверенные (ip dhcp snooping trust).
2. Включить DHCP Snooping для конкретных VLAN

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no ip dhcp snooping
```

Глобально отключает DHCP Snooping.

Просмотр:

```
> show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
# show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
# show ip dhcp snooping table
```

Очистка:

```
# clear ip dhcp snooping statistics [ interface ( <port_type> [ <in_port_list> ] ) ]
```

2.7.18.10 (config)# ip dns proxy

Включение функции DNS-прокси

Синтаксис:

```
(config)# ip dns proxy
```

Объяснение: Включение функции DNS-прокси (Domain Name System proxy).

Рекомендации:

- Команда ip dns proxy активирует функцию **DNS-прокси (DNS proxy)** на коммутаторе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- DNS-прокси – Когда эта функция включена, коммутатор выступает в роли посредника между клиентами и внешними DNS-серверами. Он принимает DNS-запросы от устройств в локальной сети, сам выполняет рекурсивный запрос к настроенным DNS-серверам и возвращает ответ клиенту.
- **Зачем это нужно:**
    - ✓ **Упрощение конфигурации клиентов:** Клиентам нужно знать только IP-адрес коммутатора как DNS-сервер. Им не нужно знать адреса внешних DNS-серверов (например, 8.8.8.8, 1.1.1.1).
    - ✓ **Кэширование:** Коммутатор может кэшировать результаты DNS-запросов. Если несколько клиентов запрашивают один и тот же домен, коммутатор может ответить из кэша, не отправляя повторный запрос во внешнюю сеть, что ускоряет ответ и снижает внешний трафик.
    - ✓ **Централизованное управление:** Администратор настраивает DNS-серверы только на коммутаторе, а не на каждом клиенте.
- **Внимание:**
    1. На коммутаторе должен быть настроен хотя бы один DNS-сервер
    2. Коммутатор должен иметь IP-связность с этими DNS-серверами.
    3. Клиенты должны быть настроены на использование IP-адреса коммутатора (обычно его интерфейса управления) в качестве DNS-сервера.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- DNS-прокси на коммутаторе уровня 2/3 обычно обладает ограниченной производительностью по сравнению с выделенным DNS-сервером и подходит для небольших и средних сетей.

Удаление конфигурации:

```
(config)# no ip dns proxy
```

Отключает функцию DNS-прокси.

2.7.18.11 (config)# ip helper-address

Настройка адреса DHCP-сервера для ретрансляции

Синтаксис:

```
(config)# ip helper-address <v_ipv4_ucast>
```

Объяснение: Настройка IPv4-адреса DHCP Relay сервера.

Параметры:

- <v_ipv4_ucast>: Укажите IPv4-адрес DHCP Relay сервера, который используется агентом ретрансляции DHCP коммутатора.

Рекомендации:

- Команда ip helper-address выполняется в режиме конфигурации интерфейса VLAN (например, после interface vlan 10) и служит

SEC.RU | Короткий путь к информации Скачано с sec.ru

для указания IP-адреса удаленного DHCP-сервера, которому будут перенаправляться широковещательные DHCP-запросы из этой VLAN.

- Это ключевая команда для настройки DHCP Relay. Без неё, даже при глобально включенном relay, запросы не будут знать, куда их отправлять.
- Как работает:
    1. Клиент в VLAN 10 отправляет широковещательный DHCPDISCOVER.
    2. Коммутатор, видя, что на интерфейсе VLAN 10 настроен ip helper-address <IP_сервера>, преобразует широковещательный запрос в unicast и пересылает его на указанный IP-адрес.
    3. Сервер отвечает коммутатору, а коммутатор ретранслирует ответ клиенту.
- Можно настроить несколько helper-адресов на одном интерфейсе VLAN, если требуется, чтобы запросы уходили на разные DHCP-серверы (для отказоустойчивости или разных пулов).
- Функция должна быть глобально включена командой ip dhcp relay.

Удаление конфигурации:

```
(config)# no ip helper-address
```

Удаляет адрес DHCP-сервера для ретрансляции. Если адресов несколько, может потребоваться указать конкретный удаляемый адрес (синтаксис может зависеть от реализации).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.12 (config)# ip http secure-server

Включение защищенного HTTPS-сервера

Синтаксис:

(config)# ip http secure-server

Объяснение: Включение режима работы HTTPS (защищенный HTTP). Если текущее соединение осуществляется по HTTPS, а режим HTTPS отключен, веб-браузер будет автоматически перенаправлен на HTTP-соединение.

Рекомендации:

- Команда *ip http secure-server* активирует веб-сервер для защищенного доступа (HTTPS) на коммутаторе. Это позволяет администраторам управлять устройством через веб-интерфейс (GUI) с использованием шифрования SSL/TLS.
- **Зачем нужно:**
  - ✓ Безопасность: HTTPS шифрует весь трафик между браузером администратора и коммутатором, включая передаваемые учетные данные (логин/пароль) и конфигурационные данные. Это предотвращает их перехват злоумышленниками в локальной сети (в отличие от обычного HTTP).
  - ✓ Соответствие стандартам: Многие корпоративные политики безопасности и стандарты (например, PCI DSS) требуют использования шифрованных протоколов для управления сетевым оборудованием.
- **Принцип работы:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Администратор подключается к коммутатору по адресу `https://<IP_коммутатора>`.
2. Коммутатор использует сертификат (самоподписанный или загруженный) для установления защищенного соединения.
3. Весь последующий обмен данными шифруется.

- **Внимание:** Как указано в описании, если соединение установлено по HTTPS, а затем администратор отключает HTTPS-сервер (`no ip http secure-server`), браузер может быть автоматически перенаправлен на нешифрованное HTTP-соединение (если HTTP-сервер включен), что создает угрозу безопасности. Поэтому при отключении HTTPS следует быть внимательным.
- Обычно команда `ip http secure-server` включает HTTPS, а отдельная команда `ip http server` включает обычный HTTP.

Удаление конфигурации:

```
(config)# no ip http secure-server
```

Отключает HTTPS-сервер. Доступ по HTTPS становится невозможен.

Просмотр:

```
# show ip http server secure status
```

Отображает статус HTTPS-сервера (включен/отключен) и, возможно, информацию о сертификате.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.13 (config)# ip http secure-redirect

Включение автоматического перенаправления с HTTP на HTTPS

Синтаксис:

```
(config)# ip http secure-redirect
```

Объяснение: Включение режима перенаправления на HTTPS. Это применимо только в том случае, если режим HTTPS включен. Автоматически перенаправляет HTTP-запросы веб-браузера на HTTPS-соединение, когда включены как режим HTTPS, так и автоматическое перенаправление.

Рекомендации:

- Команда *ip http secure-redirect* включает функцию автоматического перенаправления (redirect) всех попыток подключения к веб-интерфейсу по незащищенному протоколу HTTP на защищенный протокол HTTPS.
- Зачем это нужно:
    - ✓ **Принудительное шифрование:** Гарантирует, что администраторы и любые другие пользователи веб-интерфейса всегда будут использовать шифрованное соединение, даже если они случайно введут в браузере http:// вместо https:// или перейдут по старой ссылке.
    - ✓ **Улучшение безопасности:** Исключает возможность случайного незашифрованного соединения, при котором учетные данные могли бы быть переданы в открытом виде.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Условия работы:**

    1. **HTTPS-сервер должен быть включен** (ip http secure-server).
    2. Данная функция (ip http secure-redirect) включена.
    3. HTTP-сервер также может быть включен (или отключен, перенаправление все равно сработает, если HTTP-запрос принят).
- **Принцип работы:** Когда пользователь пытается открыть http://<IP_коммутатора>, коммутатор отправляет HTTP-ответ с кодом перенаправления (например, 301 или 302) и новым URL https://<IP_коммутатора>. Браузер автоматически переходит по защищенному адресу.

Удаление конфигурации:

```
(config)# no ip http secure-redirect
```

Отключает автоматическое перенаправление с HTTP на HTTPS. Пользователи, зашедшие по HTTP, останутся на HTTP-соединении (если HTTP-сервер включен).

Просмотр:

```
# show ip http server secure status
```

Отображает статус HTTPS-сервера и, вероятно, статус функции перенаправления.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.14 (config)# ip igmp host-proxy

Включение проксирования IGMP-сообщений (Host Proxy и Leave Proxy)

Синтаксис:

(config)# ip igmp host-proxy [leave-proxy]

Объяснение: При включении коммутатор подавляет (не пересылает) сообщения о выходе из группы (Leave), если они не получены от последнего порта-участника группы. IGMP leave proxy подавляет все ненужные IGMP-сообщения о выходе, так что коммутатор, не являющийся запросчиком (non-querier), пересылает пакет IGMP Leave только тогда, когда последний динамический порт-участник покидает многоадресную группу.

Параметры:

- [leave-proxy]: Необязательный параметр. Включает функцию проксирования выхода (leave-proxy).

Рекомендации:

- Команда *ip igmp host-proxy* управляет поведением коммутатора в отношении подавления (проксирования) IGMP-сообщений, что помогает оптимизировать трафик управления многоадресной рассылкой (multicast).
- **Две функции:**
    - ✓ ip igmp host-proxy **(Host Proxy):** Базовая функция. Коммутатор выступает в роли прокси для хостов, подключенных к его портам. Он отвечает на IGMP-запросы (Queries) от маршрутизатора от имени всех

SEC.RU | Короткий путь к информации Скачано с sec.ru

своих клиентов, вместо того чтобы пересылать все их ответы. Это снижает нагрузку на маршрутизатор.

- ✓ ip igmp host-proxy leave-proxy (Leave Proxy): Расширение Host Proxy. Коммутатор пересылает сообщение IGMP Leave только в том случае, если это сообщение исходит от последнего участника группы в данном VLAN. Если в группе остаются другие подписчики, Leave-сообщение подавляется. Это предотвращает ненужные запросы группы (Group-Specific Queries) от маршрутизатора и, как следствие, излишний трафик.

- Зачем это нужно:
  - ✓ **Снижение служебного трафика (overhead):** Уменьшает количество IGMP-пакетов, циркулирующих в сети.
  - ✓ **Повышение эффективности:** Снижает нагрузку на маршрутизаторы и коммутаторы за счет агрегации IGMP-ответов.
- Эти функции обычно включаются глобально и работают на основе информации, собранной IGMP Snooping.

Удаление конфигурации:

```
(config)# no ip igmp host-proxy [leave-proxy]
```

Отключает указанную функцию проксирования.

Просмотр:

```
# show ip igmp snooping detail
```

Детальная информация о состоянии IGMP Snooping, включая статус прокси-функций.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.15 (config)# ip igmp snooping

Глобальное включение функции IGMP Snooping

Синтаксис:

```
(config)# ip igmp snooping
```

Объяснение: Глобальное включение функции IGMP Snooping. При включении это устройство будет отслеживать сетевой трафик и определять, какие хосты должны получать многоадресный (multicast) трафик. Коммутатор может пассивно отслеживать IGMP-пакеты Query и Report, передаваемые между IP-маршрутизаторами многоадресной рассылки и подписчиками IP-многоадресных служб, для идентификации членов многоадресной группы. Коммутатор отслеживает проходящие через него IGMP-пакеты, извлекает информацию о регистрации групп и соответствующим образом настраивает фильтры многоадресной рассылки.

Рекомендации:

- Команда ip igmp snooping глобально активирует функцию **IGMP Snooping** на коммутаторе.
- IGMP Snooping – Это ключевая функция для управления многоадресным (multicast) трафиком в сетях Ethernet на коммутаторах уровня 2. Без неё коммутатор обрабатывал бы многоадресный трафик как широковещательный (broadcast) — рассылая его во все порты VLAN. Это крайне неэффективно и создает избыточную нагрузку.
- Зачем это нужно:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Оптимизация пропускной способности:** Экономит полосу пропускания, особенно для приложений, чувствительных к трафику (IP-телевидение, видеонаблюдение, онлайн-игры).
- ✓ **Повышение производительности:** Снижает нагрузку на конечные устройства, которые не должны обрабатывать ненужный им многоадресный трафик.

- Внимание: Для работы IGMP Snooping в VLAN должен присутствовать IGMP Querier (запросчик). Обычно это многоадресный маршрутизатор. В его отсутствие коммутатор может выступать в роли Querier, если эта функция настроена.

Удаление конфигурации:

```
(config)# no ip igmp snooping
```

Глобально отключает IGMP Snooping. Многоадресный трафик будет рассылаться во все порты VLAN.

Просмотр:

```
# show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```

Очистка:

```
# clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.16 (config)# ip igmp snooping vlan

Включение IGMP Snooping в указанных VLAN

Синтаксис:

```
(config)# ip igmp snooping vlan <v_vlan_list>
```

Объяснение: Включение функции IGMP для определенных VLAN.

Параметры:

- <v_vlan_list>: Укажите допустимые VLAN для IGMP.

Рекомендации:

- Команда *ip igmp snooping vlan* активирует IGMP Snooping не глобально на всех VLAN, а только в указанном списке VLAN. Это позволяет гибко применять оптимизацию многоадресного трафика только там, где это необходимо.
- **Зачем нужно указывать VLAN:**
  - ✓ **Выборочная оптимизация:** Многоадресный трафик может быть не во всех VLAN. Например, в VLAN для передачи данных может не быть multicast-приложений. Включение IGMP Snooping в таких VLAN не даст преимуществ, но будет потреблять ресурсы коммутатора.
  - ✓ **Изоляция трафика:** В некоторых VLAN может требоваться, чтобы multicast-трафик распространялся широковещательно (например, в тестовых средах или

SEC.RU | Короткий путь к информации Скачано с sec.ru

для устаревших протоколов). В таких VLAN IGMP Snooping можно отключить.

- **Последовательность настройки:**
    1. Сначала IGMP Snooping включается глобально (ip igmp snooping).
    2. Затем с помощью этой команды указываются VLAN, в которых он должен работать.
- Если VLAN не указан в списке, IGMP Snooping в нем будет отключен, даже если включен глобально. (Поведение может зависеть от реализации; в некоторых системах глобальное включение автоматически включает его во всех существующих VLAN, и эта команда используется для отключения в конкретных).

Удаление конфигурации:

```
(config)# no ip igmp snooping vlan [ <v_vlan_list> ]
```

Отключает IGMP Snooping в указанных VLAN. Если список не указан, может отключить во всех VLAN, где он был включен этой командой.

Просмотр:

```
# show ip igmp snooping
```

Показывает статус IGMP Snooping глобально и по VLAN.

Очистка:

```
# clear ip igmp snooping [ vlan <v_vlan_list> ] statistics
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.17 (config)# ip igmp ssm-range

Настройка диапазона адресов для Source-Specific Multicast (SSM)

Синтаксис:

```
(config)# ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>
```

Объяснение: Диапазон SSM (Source-Specific Multicast, многоадресная рассылка с указанием источника) позволяет хостам и маршрутизаторам, поддерживающим SSM, использовать модель обслуживания SSM для групп в указанном диапазоне адресов.

Параметры:

- <v_ipv4_mcast>: Укажите допустимый IPv4-адрес многоадресной рассылки (в пределах диапазона 232.0.0.0/8, если используется стандартный SSM).
- <ipv4_prefix_length>: Укажите длину префикса (маску) в диапазоне от 4 до 32.

Рекомендации:

- Команда ip igmp ssm-range определяет диапазон многоадресных (multicast) IPv4-адресов, для которых будет применяться модель Source-Specific Multicast (SSM).
- **SSM**
    - ✓ В стандартной ASM (Any-Source Multicast) клиент подписывается на группу (например, 239.1.1.1) и получает трафик от любого источника, передающего в эту группу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ В модели SSM клиент подписывается на **конкретный источник** и группу одновременно (например, (192.168.1.10, 232.1.1.1)). Это повышает безопасность и упрощает управление, так как исключает возможность получения трафика от нежелательных источников.

- **Как работает:** Для IGMP-запросов, попадающих в указанный диапазон, коммутатор и подключенные к нему маршрутизаторы будут ожидать и обрабатывать сообщения в формате IGMPv3 (который поддерживает указание источника). Более старые версии IGMP (v1/v2) не будут корректно работать в этом диапазоне.
- Эта команда обычно требуется только в том случае, если необходимо использовать нестандартный диапазон адресов для SSM. По умолчанию устройства могут поддерживать стандартный диапазон 232.0.0.0/8 без дополнительной настройки.

Удаление конфигурации:

```
(config)# no ip igmp ssm-range
```

Удаляет настройку нестандартного диапазона SSM, возвращаясь к поведению по умолчанию (вероятно, отключение или использование стандартного диапазона).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.18 (config)# ip igmp unknown-flooding

Настройка обработки неизвестного (незарегистрированного) многоадресного трафика

Синтаксис:

(config)# ip igmp unknown-flooding

Объяснение: Установка режима пересылки для незарегистрированного (к которому не присоединились) IP-многоадресного трафика. Установите флажок (выполните команду), чтобы затоплять (flood) трафик.

Рекомендации:

- Команда ip igmp unknown-flooding определяет, как коммутатор должен обрабатывать многоадресный (multicast) трафик, для которого в таблице IGMP Snooping нет ни одного подписчика (незарегистрированный трафик).
- **Два режима работы:**
  - ✓ Режим flooding - команда включена **(**ip igmp unknown-flooding**):** Если для многоадресной группы нет подписчиков, коммутатор будет рассылать этот трафик во все порты VLAN. Это поведение похоже на широковещательную рассылку (broadcast).
  - ✓ Режим dropping - команда отключена **(**no ip igmp unknown-flooding**):** Если для многоадресной группы нет подписчиков, коммутатор будет отбрасывать этот трафик. Он не будет отправлен ни на один порт.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- В большинстве современных сетей, где IGMP Snooping настроен корректно, рекомендуется отключать эту функцию (no ip igmp unknown-flooding).

Удаление конфигурации:

```
(config)# no ip igmp unknown-flooding
```

Отключает режим затопления (включает режим отбрасывания) для неизвестного многоадресного трафика.

2.7.18.19 (config)# ip name-server

Настройка адресов DNS-серверов

Синтаксис:

```
(config)# ip name-server { <v_ipv4_ucast> | dhcp [ interface vlan <v_vlan_id> ] }
```

Объяснение: Ручная установка IP-адреса DNS или получение IP-адреса DNS через DHCP-сервер в определенной VLAN.

Параметры:

- <v_ipv4_ucast>: Вручную укажите адрес unicast IPv4-сервера имен (DNS).
- dhcp [interface vlan <v_vlan_id>]: Настройка IP-адреса DNS через DHCP-сервер в указанной VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда ip name-server задает IP-адреса DNS-серверов, которые коммутатор будет использовать для разрешения доменных имен (например, при выполнении команд ping google.com или traceroute).
- Существует два способа настройки:
    - ✓ **Статический (**<v_ipv4_ucast>**):** Администратор вручную вводит IP-адрес одного или нескольких DNS-серверов. Для нескольких серверов команда выполняется несколько раз или указывается список через запятую (зависит от реализации).
    - ✓ **Динамический (**dhcp [interface vlan <v_vlan_id>]**):** Коммутатор получает адрес DNS-сервера от DHCP-сервера, когда его интерфейс управления (указанная VLAN) получает IP-адрес по DHCP. Это удобно в сетях, где DNS-серверы могут меняться.
- **Зачем это нужно:**
    - ✓ **Удобство администрирования:** Позволяет использовать доменные имена в командах вместо запоминания IP-адресов.
    - ✓ **Интеграция:** Необходимо для работы некоторых протоколов и функций (например, отправка логов на сервер по имени).
- После настройки DNS-серверов коммутатор может выполнять разрешение имен.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no ip name-server
```

Удаляет все настроенные DNS-серверы.

Просмотр:

```
> show ip name-server
# show ip name-server
```

2.7.18.20 (config)# ip route

Настройка статического IP-маршрута

Синтаксис:

```
(config)# ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
```

Объяснение: Настройка статического IP-маршрута.

Параметры:

- <v_ipv4_addr>: Укажите IPv4-адрес. IP-маршрут — это сеть назначения или адрес хоста для данного маршрута. Допустимый формат — десятичная запись с точками.
- <v_ipv4_netmask>: Маска маршрута — это маска сети назначения или хоста. Она определяет, какая часть сетевого адреса должна совпадать, чтобы маршрут был применим. Только маршрут по умолчанию (default route) будет иметь маску длиной 0 (так как он соответствует чему угодно).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- <v_ipv4_gw>: Это IP-адрес шлюза (gateway). Допустимый формат — десятичная запись с точками. Шлюз и сеть должны быть одного типа.

Рекомендации:

- Команда ip route создает статический маршрут в таблице маршрутизации коммутатора уровня 3 (L3). Она указывает, через какой шлюз (next-hop) необходимо отправлять пакеты для достижения определенной IP-сети или хоста.
- Наиболее важное применение — маршрут по умолчанию (default route):
    - ✓ Если сеть назначения не совпадает ни с одним из более конкретных маршрутов и не является непосредственно подключенной сетью, используется маршрут по умолчанию.
    - ✓ Синтаксис для маршрута по умолчанию: ip route 0.0.0.0 0.0.0.0 <IP_шлюза>. Маска 0.0.0.0 означает "совпадает с любым адресом".
- Статические маршруты необходимы в сетях, где не используются динамические протоколы маршрутизации (OSPF, RIP), или для определения маршрутов к конкретным изолированным сетям.
- Шлюз (<v_ipv4_gw>) должен быть доступен с коммутатора, т.е. его IP-адрес должен принадлежать одной из непосредственно подключенных сетей (к одному из интерфейсов VLAN коммутатора).
- Для удаления статического маршрута используется та же команда с ключевым словом no.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
```

Просмотр:

```
> show ip route
# show ip route
```

2.7.18.21 (config)# ip routing

Глобальное включение IP-маршрутизации

Синтаксис:

```
(config)# ip routing
```

Объяснение: Включение маршрутизации IPv4 и IPv6.

Рекомендации:

- Команда *ip routing* является ключевой для превращения коммутатора уровня 2 (L2) в коммутатор уровня 3 (L3). Она глобально активирует функцию IP-маршрутизации на устройстве, если поддерживается последним.
- **Что происходит после включения:**
  - ✓ Коммутатор начинает выполнять функции маршрутизатора: он может пересылать IP-пакеты между различными VLAN (подсетями).
  - ✓ Становятся доступны для настройки команды, связанные с маршрутизацией, такие как ip

SEC.RU | Короткий путь к информации Скачано с sec.ru

route (статические маршруты), а также протоколы динамической маршрутизации.

- ✓ Интерфейсы VLAN (SVI) начинают вести себя как маршрутизируемые интерфейсы (с IP-адресами).

- **Зачем это нужно:**
  - ✓ **Взаимодействие типа Inter-VLAN Routing:** Устройства в разных VLAN могут обмениваться данными через коммутатор, без необходимости во внешнем маршрутизаторе (схема "router-on-a-stick").
  - ✓ **Подключение к внешним сетям:** Коммутатор может выступать в роли шлюза для своих VLAN и иметь статические или динамические маршруты во внешние сети.
  - ✓ **Поддержка IPv6:** Команда также включает маршрутизацию IPv6.
- **Важное условие:** Для работы маршрутизации необходимо, чтобы на интерфейсах VLAN (SVI) были настроены корректные IP-адреса и маски подсети.
- **Отключение (**no ip routing**)** возвращает коммутатор к поведению уровня 2. Он будет пересылать трафик между VLAN только с помощью своих функций коммутации (L2), но не будет выполнять IP-маршрутизацию (L3). Это может нарушить связь между VLAN.

Удаление конфигурации:

```
(config)# no ip routing
```

Глобально отключает IP-маршрутизацию (как IPv4, так и IPv6)

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
> show ip route
> show ipv6 route [interface vlan <vlan_list>]
# show ip route
# show ipv6 route [interface vlan <vlan_list>]
```

Эти команды показывают таблицы маршрутизации IPv4 и IPv6, которые будут заполнены только при включенной маршрутизации.

2.7.18.22 (config)# ip source binding interface

Создание статической привязки для IP Source Guard

Синтаксис:

```
(config)# ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>
```

Объяснение: Создание статической записи.

Параметры:

- <port_type> <in_port_type_id>: Укажите тип порта и номер порта, к которому привязывается статическая запись.
- <vlan_var>: Укажите идентификатор VLAN, который был настроен.
- <ipv4_var>: Укажите допустимый IPv4-адрес.
- <mask_var>: Укажите маску подсети для введенного IP-адреса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда *ip source binding interface* создает статическую запись в базе данных привязок (binding table), которая используется функцией **IP Source Guard**.
- Source Guard – Это функция безопасности уровня доступа, которая фильтрует IP-трафик на ненадежных портах, пропуская только те пакеты, источник (source IP и source MAC) которых соответствует записям в базе привязок. Это предотвращает атаки с подменой IP-адреса (IP spoofing).
- IP Source Guard для своей работы использует базу данных, созданную DHCP Snooping (для DHCP-клиентов).
  Однако устройства со статическими IP-адресами (серверы, принтеры) не проходят процесс DHCP и, следовательно, не имеют динамической записи. Чтобы IP Source Guard не блокировал трафик от таких устройств, для них необходимо вручную создать статические записи.
- Запись связывает конкретный порт, VLAN, IP-адрес и маску (а также может включать MAC-адрес, хотя в данном синтаксисе MAC не указан явно, возможно, он подразумевается или берется из других источников). Когда на указанном порту появляется IP-пакет, IP Source Guard проверяет, соответствует ли его исходный IP-адрес этой статической записи.

Удаление конфигурации:

```
(config)# no ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаляет указанную статическую запись.

Просмотр:

```
# show ip source binding [ dhcp-snooping | static ] [ interface ( <port_type> [ <in_port_type_list> ] ) ]
```

*Позволяет просмотреть статические (*static*) или динамические (*dhcp-snooping*) записи в базе привязок.*

2.7.18.23 (config)# ip ssh

Включение SSH-сервера

Синтаксис:

```
(config)# ip ssh
```

Объяснение: Включение режима SSH.

Рекомендации:

- Команда ip ssh активирует SSH-сервер на коммутаторе, позволяя безопасное удаленное управление устройством по протоколу SSH.
- **Почему стоит использовать SSH:**
    - ✓ **SSH предпочтительнее Telnet**, если сеть управления не является полностью доверенной.
    - ✓ **Telnet** передает учетные данные (логин и пароль) в открытом текстовом виде, что делает их уязвимыми

SEC.RU | Короткий путь к информации Скачано с sec.ru

для перехвата и анализа (снифинга) злоумышленниками в локальной сети.

- ✓ **SSH** предоставляет безопасный метод аутентификации и шифрует весь сеанс связи (включая передачу паролей и команд), защищая от перехвата.

- SSH на данном устройстве использует версию 2 протокола SSH, которая является современной и безопасной (в отличие от устаревшей и уязвимой версии 1).
- Для работы SSH на коммутаторе также могут потребоваться:
  - ✓ Настройка имени хоста (hostname).
  - ✓ Настройка домена (ip domain-name), если требуется генерация ключей.
  - ✓ Генерация криптографических ключей (часто происходит автоматически или отдельной командой).
  - ✓ Настройка пользователей (например, username).
- После включения SSH, администраторы могут подключаться к коммутатору, используя SSH-клиенты (например, PuTTY, OpenSSH) по IP-адресу устройства.

Удаление конфигурации:

```
(config)# no ip ssh
```

Отключает SSH-сервер. Удаленное управление по SSH становится невозможным.

Просмотр:

```
# show ip ssh
```

Отображает статус SSH-сервера, используемую версию, таймауты, количество попыток и другую информацию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.24 (config)# ip verify source

Глобальное включение функции IP Source Guard

Синтаксис:

```
(config)# ip verify source
```

Объяснение: Включение функции защиты источника IP (IP Source Guard).

Рекомендации:

- Команда *ip verify source* глобально активирует функцию безопасности **IP Source Guard** на коммутаторе.
- **IP Source Guard –** Это механизм защиты на уровне портов, предназначенный для предотвращения атак с подменой IP-адреса (IP spoofing). Он фильтрует IP-трафик на ненадежных портах, пропуская только те пакеты, чей исходный IP-адрес соответствует записям в базе данных привязок (binding table).
- **Принцип работы:**
    1. IP Source Guard использует базу данных привязок, создаваемую **DHCP Snooping** (для динамических адресов) и статические записи (ip source binding, созданные администратором).
    2. На каждом порту, где функция включена (обычно через ip verify source port-security в режиме интерфейса), коммутатор проверяет все входящие IP-пакеты.
    3. Если исходный IP-адрес пакета (и, опционально, MAC-адрес) не соответствует ни одной записи в базе для данного порта и VLAN, пакет отбрасывается.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Для работы IP Source Guard необходимо предварительно включить DHCP Snooping (ip dhcp snooping), так как именно он создает динамическую часть базы данных. Также могут потребоваться статические записи для устройств с фиксированными IP-адресами.
- IP Source Guard обычно настраивается на портах доступа. На транковых портах или портах, ведущих к другим коммутаторам, эта функция не применяется.
- Существует два основных режима работы: проверка только IP-адреса (ip verify source) или проверка IP-адреса и MAC-адреса (ip verify source port-security).

Удаление конфигурации:

```
(config)# no ip verify source
```

Глобально отключает IP Source Guard.

Просмотр:

```
> show ip verify source [ interface ( <port_type> [<in_port_type_list> ] ) ]
# show ip verify source [ interface ( <port_type> [<in_port_type_list> ] ) ]
```

Отображает статус IP Source Guard глобально и на конкретных портах, а также фильтры, применяемые к портам.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.25 (config)# ip verify source translate

Преобразование динамических записей IP Source Guard в статические

Синтаксис:

```
(config)# ip verify source translate
```

Объяснение: Преобразование динамических записей в статические.

Рекомендации:

- Команда ip verify source translate позволяет преобразовать все существующие динамические записи из базы данных привязок, созданной DHCP Snooping, в статические записи для IP Source Guard.
- **Зачем это нужно:**
    1. **Фиксация привязок для статических устройств:** Если устройство изначально получало адрес по DHCP (и поэтому имеет динамическую запись), но затем было переведено на статический IP-адрес, можно преобразовать его последнюю известную корректную динамическую запись в статическую, чтобы IP Source Guard продолжал его пропускать.
    2. **Миграция и резервирование:** Полезно, когда нужно зафиксировать привязку для критически важного устройства, гарантируя, что оно не будет заблокировано после перезагрузки коммутатора или истечения аренды DHCP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. **Быстрое создание множества статических записей:** Вместо ручного создания десятков статических записей для устройств в сети, можно позволить им получить адреса по DHCP, а затем одним действием преобразовать всю динамическую базу в статическую.

- **Как это работает:** Коммутатор берет текущее содержимое таблицы привязок DHCP Snooping (которая содержит пары "порт - VLAN - MAC - IP" для всех успешно арендовавших адреса клиентов) и создает на их основе статические записи. Исходные динамические записи при этом могут быть удалены.
- После преобразования устройства, для которых были созданы статические записи, больше не будут обновлять свои записи через DHCP. Если их IP-адрес изменится вручную, необходимо будет обновить и статическую запись на коммутаторе.

2.7.18.26 (config-if)# ip arp inspection check-vlan

Включение проверки VLAN для ARP Inspection на интерфейсе

Синтаксис:

```
(config-if)# ip arp inspection check-vlan
```

Объяснение: Включение функции проверки VLAN.

Рекомендации:

- Команда ip arp inspection check-vlan, выполняемая в режиме конфигурации интерфейса, включает дополнительную проверку для функции **Dynamic ARP Inspection (DAI)** на данном порту.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Когда эта опция включена, коммутатор проверяет, принадлежит ли VLAN, указанная в ARP-пакете, к списку VLAN, для которых глобально включен DAI (ip arp inspection vlan <vlan_list>). Если VLAN не входит в этот список, ARP-пакет может быть отброшен или обработан иначе (зависит от реализации).
- **Зачем это нужно:**
    - ✓ **Дополнительный уровень безопасности:** Гарантирует, что ARP-пакеты обрабатываются только для тех VLAN, которые администратор явно решил защищать.
    - ✓ **Изоляция трафика:** Предотвращает случайное применение правил DAI к трафику из VLAN, где защита не требуется или может нарушить работу.
- Эта проверка обычно применяется на ненадежных (untrusted) портах, куда подключаются конечные пользователи. На доверенных (trusted) портах (например, uplink) она может быть отключена, так как там проходят ARP-пакеты из разных VLAN, и проверка может быть излишней.

Удаление конфигурации:

```
(config-if)# no ip arp inspection check-vlan
```

Отключает проверку VLAN на данном интерфейсе. ARP-пакеты из любых VLAN будут обрабатываться (или не обрабатываться) DAI в соответствии с другими настройками.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.27 (config-if)# ip arp inspection logging

Настройка логирования ARP Inspection на конкретном интерфейсе

Синтаксис:

```
(config-if)# ip arp inspection logging { deny | permit | all }
```

Объяснение: Включение функции логирования на конкретном интерфейсе.

Параметры:

- { deny | permit | all }: Укажите один из типов логирования.
  - ✓ deny: Логировать заблокированные (отклоненные) записи.
  - ✓ permit: Логировать разрешенные записи.
  - ✓ all: Логировать все записи.

Рекомендации:

- Команда ip arp inspection logging, выполняемая в режиме конфигурации интерфейса, позволяет включить выборочное логирование событий Dynamic ARP Inspection (DAI) для данного конкретного порта, переопределяя (или дополняя) глобальные настройки логирования для VLAN.
- **Зачем нужно логирование на порту:**
  - ✓ **Детальная диагностика:** Позволяет сфокусироваться на трафике конкретного проблемного порта, не засоряя журнал событиями со всех остальных портов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Мониторинг подозрительной активности:** Если на определенном порту ожидаются или были замечены атаки, можно включить логирование только для него.
- ✓ **Тестирование:** Включить логирование всех пакетов (all) на тестовом порту для отладки, не влияя на производительность и объем логов на рабочих портах.

- **Выбор уровня логирования:**
  - ✓ deny **(рекомендуется для обычной работы):** Логирует только ARP-пакеты, которые были заблокированы на этом порту. Это основной способ обнаружения попыток атак.
  - ✓ permit**:** Логирует успешно пропущенные ARP-пакеты. Может быть полезно для отладки, но в рабочей сети создаст избыточный трафик логов.
  - ✓ all**:** Логирует все ARP-пакеты на порту. Используйте только для кратковременной глубокой диагностики.
- Если на порту не задана эта команда, логирование для него будет определяться глобальными настройками для VLAN (ip arp inspection vlan <...> logging).

Удаление конфигурации:

```
(config-if)# no ip arp inspection logging
```

Удаляет настройку логирования на интерфейсе, возвращаясь к использованию глобальных настроек VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.28 (config-if)# ip arp inspection trust

Настройка доверенного состояния порта для ARP Inspection

Синтаксис:

```
(config-if)# ip arp inspection trust
```

Объяснение: Включение доверенного состояния (trust state) на выбранных интерфейсах.

Рекомендации:

- Команда ip arp inspection trust является ключевой для настройки работы Dynamic ARP Inspection (DAI) на порту. Она определяет, будет ли порт считаться доверенным (trusted) или ненадежным (untrusted).
- **Принцип работы DAI:**
    - ✓ **Ненадежные порты (Untrusted - по умолчанию):** На этих портах (обычно порты доступа, подключенные к конечным устройствам) весь ARP-трафик проверяется. Коммутатор сверяет каждый ARP-пакет с базой данных привязок (из DHCP Snooping) и блокирует несоответствующие пакеты.
    - ✓ **Доверенные порты (Trusted):** На этих портах (обычно порты, ведущие к другим коммутаторам, маршрутизаторам или DHCP-серверам) проверка ARP-пакетов отключена. Весь ARP-трафик с таких портов автоматически пропускается. Это необходимо, чтобы не блокировать легитимный ARP-трафик между сетевыми устройствами.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    - ✓ **Безопасность:** Все порты доступа должны быть ненадежными, чтобы DAI мог защитить их от ARP-спуфинга.
    - ✓ **Работоспособность сети:** Порты, соединяющие коммутаторы между собой (uplink), должны быть доверенными, чтобы не нарушать нормальную работу протоколов маршрутизации и коммутации.
- По умолчанию все порты могут находиться в состоянии **untrusted** (ненадежном). Администратор обязан вручную настроить порты, подключенные к доверенным устройствам, как trust.

Удаление конфигурации:

```
(config-if)# no ip arp inspection trust
```

Возвращает порт в состояние по умолчанию — ненадежное (untrusted).

2.7.18.29 (config-if)# ip dhcp snooping trust

Настройка доверенного порта для DHCP Snooping

Синтаксис:

```
(config-if)# ip dhcp snooping trust
```

Объяснение: Установить данный интерфейс как доверенный (trusted) порт для DHCP Snooping.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда ip dhcp snooping trust является ключевой для настройки работы DHCP Snooping на порту. Она определяет, будет ли порт считаться доверенным (trusted) или ненадежным (untrusted).
- **Принцип работы DHCP Snooping:**
    - ✓ **Ненадежные порты (Untrusted - по умолчанию):** На этих портах (обычно порты доступа, подключенные к конечным устройствам) DHCP-ответы (OFFER, ACK, NAK) от серверов блокируются. Разрешены только DHCP-запросы (DISCOVER, REQUEST) от клиентов. Это предотвращает атаки с подменой DHCP-сервера (Rogue DHCP Server).
    - ✓ **Доверенные порты (Trusted):** На этих портах (обычно порты, ведущие к DHCP-серверам, или uplink к другому коммутатору, за которым есть сервер) весь DHCP-трафик разрешен. Коммутатор доверяет пакетам, приходящим с этих портов.
- **Зачем это нужно:**
    - ✓ **Безопасность:** Все порты доступа должны быть ненадежными, чтобы DHCP Snooping мог блокировать ответы от подставных DHCP-серверов, которые могут попытаться подключиться к сети.
    - ✓ **Работоспособность сети:** Порты, на которых находятся легитимные DHCP-серверы, или порты, соединяющие коммутаторы между собой (через которые проходят ответы от сервера), должны быть доверенными, чтобы не нарушить нормальное получение адресов клиентами.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- По умолчанию все порты находятся в состоянии **untrusted** (ненадежном). Администратор обязан вручную настроить порты, подключенные к DHCP-серверам или к магистрали, ведущей к ним, как trust.

Удаление конфигурации:

```
(config-if)# no ip dhcp snooping trust
```

Возвращает порт в состояние по умолчанию — ненадежное (untrusted).

Просмотр:

```
> show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
# show ip dhcp snooping [ interface ( <port_type> [ <in_port_list> ] ) ]
```

2.7.18.30 (config-if)# ip igmp snooping filter

Применение фильтра многоадресного трафика к порту

Синтаксис:

```
(config-if)# ip igmp snooping filter <profile_name>
```

Объяснение: Используйте эту команду для фильтрации определенного многоадресного (multicast) трафика на уровне порта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <profile_name>: Укажите имя настроенного профиля многоадресных групп, доступ к которым запрещен на порту. Когда определенная многоадресная группа выбрана на порту, IGMP-сообщения о присоединении (join reports), полученные на этом порту, отбрасываются.

Рекомендации:

- Команда ip igmp snooping filter применяет заранее созданный профиль фильтрации многоадресного трафика (multicast filter profile) к конкретному порту. Сам профиль, содержащий список разрешенных или запрещенных групп, создается отдельной командой (например, ip igmp profile).
- Это позволяет администратору реализовать политики контроля доступа к многоадресным потокам на уровне портов. Например, можно запретить пользователям на определенном порту подписываться на "видеотрансляцию для руководства" или разрешить доступ только к определенным multicast-каналам (IP-телевидение).
- Эта функция является важным инструментом управления multicast-трафиком и повышения безопасности.

Удаление конфигурации:

```
(config-if)# no ip igmp snooping filter
```

Удаляет привязку профиля фильтрации с порта. Фильтрация multicast-трафика на этом порту прекращается.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
> show ip igmp snooping [vlan <v_vlan_list> ] [ group-database [ interface ( <
port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface (
<port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```

Информация о примененных фильтрах может отображаться в детальном выводе по IGMP Snooping или по конкретным интерфейсам.

2.7.18.31 (config-if)# ip igmp snooping immediate-leave

Включение функции немедленного выхода (Fast Leave) на порту

Синтаксис:

```
(config-if)# ip igmp snooping immediate-leave
```

Объяснение: Включение функции быстрого выхода (fast leave) на конкретном порту. Когда получен пакет Leave (о выходе из группы), коммутатор немедленно удаляет порт из многоадресной службы, не отправляя на этот интерфейс IGMP-запрос, специфичный для группы (Group-Specific Query).

Рекомендации:

- Команда ip igmp snooping immediate-leave активирует на порту функцию немедленного выхода (Immediate Leave), также известную как **Fast Leave**.
- **Зачем это нужно:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. **Быстрое освобождение ресурсов:** Ускоряет процесс прекращения передачи ненужного многоадресного трафика на порт, экономя полосу пропускания.
2. **Снижение задержек при переключении каналов:** Важно для приложений, чувствительных к задержкам, таких как IP-телевидение (IPTV). Когда пользователь переключает канал, Immediate Leave позволяет быстро прекратить прием старого потока и начать прием нового.

- Внимание! Immediate Leave следует включать только на портах, к которым подключено максимум одно устройство-подписчик (например, один IP-телевизор или один ПК). Если к порту подключено несколько устройств (через другой коммутатор или хаб), использование Immediate Leave приведет к тому, что при выходе одного из них все остальные также потеряют доступ к группе.

Удаление конфигурации:

```
(config-if)# no ip igmp snooping immediate-leave
```

Отключает функцию немедленного выхода на порту, возвращаясь к стандартному процессу с отправкой Group-Specific Query.

Просмотр:

```
> show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```

Статус Immediate Leave может отображаться в детальном выводе по IGMP Snooping или по конкретным интерфейсам.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.32 (config-if)# ip igmp snooping max-groups

Ограничение количества многоадресных групп на порту

Синтаксис:

```
(config-if)# ip igmp snooping max-groups <throttling>
```

Объяснение: Укажите максимальное количество многоадресных (multicast) групп, к которым порт может присоединиться одновременно.

Параметры:

- <throttling>: Это поле ограничивает максимальное количество многоадресных групп, к которым порт может присоединиться одновременно. Когда на порту достигнуто максимальное количество, любые новые IGMP-запросы на присоединение (join reports) будут отброшены. По умолчанию выбрано неограниченное количество (unlimited). Допустимый диапазон значений от 1 до 10 (в данной реализации).

Рекомендации:

- Команда ip igmp snooping max-groups вводит ограничение (порог, throttling) на количество многоадресных групп, в которых может одновременно состоять данный порт.
- **Зачем это нужно:**
    - ✓ **Защита от истощения ресурсов (DoS-атака):** Предотвращает ситуацию, когда один порт пытается подписаться на огромное количество multicast-потоков, что может исчерпать аппаратные ресурсы (TCAM) коммутатора, предназначенные для хранения multicast-записей, и повлиять на работу других портов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Контроль доступа:** Позволяет административно ограничить количество multicast-каналов, которые может просматривать пользователь на данном порту (например, в сети IPTV ограничить число одновременно просматриваемых каналов).

- **Принцип работы:** Коммутатор ведет подсчет активных multicast-групп для каждого порта. Когда порт достигает лимита (<throttling>), все последующие IGMP-запросы на присоединение к новым группам игнорируются/отбрасываются. Уже существующие подписки продолжают работать.
- **Значение по умолчанию:** "unlimited" (не ограничено). Рекомендуется устанавливать разумные пределы, особенно на пользовательских портах доступа. Указанный в параметрах диапазон 1-10 может быть мал для некоторых приложений; возможно, в реальных системах он шире.

Удаление конфигурации:

```
(config-if)# no ip igmp snooping max-groups
```

Снимает ограничение на количество групп для порта (возврат к значению "unlimited").

Просмотр:

```
> show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ip igmp snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```

Информация о текущем количестве групп и лимите может отображаться в детальном выводе по интерфейсу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.33 (config-if)# ip igmp snooping mrouter

Настройка порта как статического Multicast Router Port

Синтаксис:

```
(config-if)# ip igmp snooping mrouter
```

Объяснение: Установить этот интерфейс как порт маршрутизатора (Router port). Если IGMP Snooping не может обнаружить IGMP-запросчик (querier), вы можете вручную назначить порт, который подключен к известному IGMP-запросчику (т.е., многоадресному маршрутизатору/коммутатору). Этот интерфейс затем присоединится ко всем текущим многоадресным группам, поддерживаемым подключенным маршрутизатором/коммутатором, чтобы гарантировать, что многоадресный трафик передается на все соответствующие интерфейсы внутри коммутатора.

Рекомендации:

- Команда *ip igmp snooping mrouter* используется для статического назначения порта как "порта маршрутизатора" (Multicast Router Port). В обычных условиях коммутатор динамически определяет, какие порты ведут к маршрутизаторам многоадресной рассылки (мультикаст-маршрутизаторам или запросчикам), прослушивая IGMP-запросы (Queries).
- **Когда это нужно:**
    - ✓ **Отсутствие динамического обнаружения:** Если в сети нет активного IGMP-запросчика (например, в изолированной сети или при использовании статических multicast-маршрутов), коммутатор не сможет определить

SEC.RU | Короткий путь к информации Скачано с sec.ru

порты, на которые нужно пересылать весь многоадресный трафик (для всех групп).

- ✓ **Гарантированная доставка:** Ручное назначение гарантирует, что порт, ведущий к маршрутизатору, будет получать копию всего многоадресного трафика, независимо от того, есть ли у него подписчики на этом или других коммутаторах.

- Когда порт помечен как mrouter, он ведет себя как динамически обнаруженный Router Port. Это означает, что весь многоадресный трафик для всех активных групп будет пересылаться на этот порт. Это необходимо для того, чтобы маршрутизатор мог пересылать трафик между VLAN или в другие сети.

Удаление конфигурации:

```
(config-if)# no ip igmp snooping mrouter
```

Удаляет статическое назначение порта как Router Port.

Просмотр:

```
> show ip igmp snooping mrouter [ detail ]
# show ip igmp snooping mrouter [ detail ]
```

Отображает список портов, которые в данный момент выполняют роль Router Port (как динамически обнаруженные, так и статически настроенные).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.34 (config-if)# ip verify source

Включение IP Source Guard на интерфейсе

Синтаксис:

```
(config-if)# ip verify source
```

Объяснение: Включение защиты источника IP (IP Source Guard) на этом интерфейсе.

Рекомендации:

- Команда ip verify source, выполняемая в режиме конфигурации интерфейса, активирует функцию IP Source Guard на конкретном порту. Глобальное включение IP Source Guard (ip verify source на глобальном уровне) необходимо, но недостаточно — функцию нужно явно включить на нужных портах.
- **Что делает IP Source Guard на порту:** Включает фильтрацию входящего IP-трафика на этом порту на основе базы данных привязок (binding table), созданной DHCP Snooping и статическими записями. Только пакеты с исходным IP-адресом, соответствующим разрешенной привязке для данного порта и VLAN, будут пропущены.
- **Зачем это нужно на уровне порта:** Позволяет применять защиту от подмены IP-адреса (IP spoofing) выборочно — например, только на портах доступа, где подключаются конечные пользователи. На магистральных (uplink) портах эта функция обычно не нужна.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Существует два основных режима работы на порту (зависит от дополнительных параметров или версии ПО):
    - ✓ **Проверка только IP-адреса (**ip verify source**):** Фильтрация только по IP-адресу источника.
    - ✓ **Проверка IP и MAC-адреса (**ip verify source port-security**):** Более строгая фильтрация по паре (IP-адрес, MAC-адрес).
- Для корректной работы IP Source Guard на порту, на этом порту также должен быть включен **DHCP Snooping** (и порт должен быть ненадежным) или должны быть настроены статические привязки.

Удаление конфигурации:

```
(config-if)# no ip verify source
```

Отключает IP Source Guard на указанном интерфейсе. Фильтрация IP-трафика на этом порту прекращается.

Просмотр:

```
> show ip verify source [ interface ( <port_type> [ <in_port_type_list> ] ) ]
# show ip verify source [ interface ( <port_type> [ <in_port_type_list> ] ) ]
```

Отображает статус IP Source Guard на портах и применяемые фильтры.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.35 (config-if)# ip verify source limit

Ограничение количества динамических клиентов для IP Source Guard на порту

Синтаксис:

```
(config-if)# ip verify source limit <0-2>
```

Объяснение: Укажите максимальное количество динамических клиентов, которые могут быть изучены на порту. Доступные значения: 0, 1, 2. Если режим порта включен и максимальное количество динамических клиентов равно 0, коммутатор будет пересылать только те IP-пакеты, которые соответствуют статическим записям для данного порта.

Параметры:

- <0-2>: Укажите максимальное количество динамических клиентов, которые могут быть изучены на порту.

Рекомендации:

- Команда ip verify source limit задает лимит на количество динамических клиентов (т.е., клиентов, получивших IP-адрес по DHCP), записи о которых могут быть созданы в базе данных IP Source Guard для данного порта.
- **Зачем это нужно:**
    - ✓ **Контроль и предотвращение истощения:** Ограничивает количество устройств, которые могут одновременно получать доступ к сети

SEC.RU | Короткий путь к информации Скачано с sec.ru

через один порт. Это может быть полезно для предотвращения атак или для соблюдения политики безопасности (например, на порту доступа должен быть только один компьютер).

- ✓ **Совместная работа со статическими записями:** Позволяет гибко управлять сочетанием статических и динамических привязок на порту.

- **Значения параметра:**
  - ✓ 0**:** На порту не допускаются динамические клиенты. Будут пропускаться только пакеты от устройств, для которых созданы статические записи (ip source binding interface). Это самый строгий режим.
  - ✓ 1**:** На порту может быть не более одного динамического клиента. Стандартное ограничение для порта доступа с одним устройством.
  - ✓ 2**:** На порту может быть не более двух динамических клиентов. Может использоваться, если к порту через небольшой неуправляемый коммутатор подключены два устройства.
- Это ограничение применяется только к динамическим клиентам (из DHCP Snooping). Статические записи в этот лимит, как правило, не входят.

Удаление конфигураци:

```
(config-if)# no ip verify source limit
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Снимает ограничение на количество динамических клиентов для порта (возврат к поведению по умолчанию, которое может быть неограниченным или зависеть от глобальных настроек).

Просмотр:

```
> show ip verify source [ interface ( <port_type> [ <in_port_type_list> ] ) ]
# show ip verify source [ interface ( <port_type> [ <in_port_type_list> ] ) ]
```

В выводе может отображаться информация о лимите и текущем количестве клиентов.

2.7.18.36 (config-if-vlan)# ip address

Настройка IPv4-адреса для интерфейса VLAN (SVI)

Синтаксис:

```
(config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [ fallback <fall
back_address> <fallback_netmask> [ timeout <fallback_timeout> ] ] } }
```

Объяснение: Настройка IPv4-адреса для данного интерфейса VLAN.

Параметры:

- <address> <netmask>: Укажите IPv4-адрес и маску подсети (статическая адресация).
- dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]: Использовать DHCP-сервер для автоматического назначения IP-адреса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ fallback <fallback_address> <fallback_netmask>: Укажите резервный IP-адрес и маску подсети, которые будут использоваться, если DHCP-сервер недоступен.
- ✓ timeout <fallback_timeout>: Укажите время ожидания (таймаут) ответа от DHCP-сервера, после которого будет применен резервный адрес.

Рекомендации:

- Команда ip address является основной для назначения IP-адреса интерфейсу VLAN уровня 3 (SVI). Этот адрес используется для управления коммутатором и, при включенной маршрутизации (ip routing), служит шлюзом по умолчанию для устройств в этой VLAN.
- **Два основных способа настройки:**
  - ✓ **Статический (Static):** ip address 192.168.1.100 255.255.255.0. Администратор вручную задает IP и маску. Это наиболее распространенный способ для постоянных адресов управления.
  - ✓ **Динамический (DHCP):** ip address dhcp. Адрес запрашивается у DHCP-сервера (если поддерживается) Удобно для временных сетей или когда управление адресами централизовано.
- **Функция Fallback (Резервный адрес):** Это мощная опция для обеспечения отказоустойчивости. Если интерфейс настроен на получение адреса по DHCP, но DHCP-сервер не отвечает в течение заданного timeout, интерфейс автоматически настраивается на указанный статический fallback адрес. Это

SEC.RU | Короткий путь к информации Скачано с sec.ru

гарантирует, что устройство всегда будет иметь IP-адрес для управления, даже при проблемах с DHCP-сервером.

- Для удаления IP-адреса с интерфейса используется команда no ip address.

Удаление конфигурации:

```
(config-if-vlan)# no ip address
```

Удаляет IP-адрес с интерфейса VLAN.

Просмотр:

```
> show ip interface brief
# show ip interface brief
```

Отображает краткую информацию по всем интерфейсам уровня 3 (включая VLAN), их IP-адреса и статус.

2.7.18.37 (config-if-vlan)# ip igmp snooping

Включение IGMP Snooping на конкретном VLAN

Синтаксис:

```
(config-if-vlan)# ip igmp snooping
```

Объяснение: Включение IGMP Snooping на данном конкретном VLAN.

Рекомендации:

- Команда ip igmp snooping, выполняемая в режиме конфигурации интерфейса VLAN ((config-if-vlan)#), позволяет включить IGMP

SEC.RU | Короткий путь к информации Скачано с sec.ru

Snooping для данного конкретного VLAN. Это дает более тонкий контроль, чем глобальное включение для всех VLAN.

- **Взаимосвязь с глобальной настройкой:** В некоторых реализациях для работы IGMP Snooping необходимо выполнить оба шага:
    1. Глобально включить IGMP Snooping (ip igmp snooping).
    2. Включить его на нужных VLAN (ip igmp snooping vlan <vlan_list> или через данную интерфейсную команду).
- Для корректной работы IGMP Snooping в VLAN также необходимо наличие **IGMP Querier** (запросчика) в этом VLAN. Обычно это multicast-маршрутизатор, но коммутатор сам может выполнять эту роль, если настроен как Querier.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping
```

Отключает IGMP Snooping для данного VLAN.

Просмотр:

```
> show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
# show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp-msg <type> ]
```

Для просмотра статуса IGMP Snooping обычно используются специализированные команды show ip igmp snooping*, а не общая статистика IP.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.38 (config-if-vlan)# ip igmp snooping compatibility

Настройка версии совместимости IGMP Snooping для VLAN

Синтаксис:

```
(config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }
```

Объяснение: Настройка версии IGMP Snooping, используемой для данного конкретного VLAN.

Параметры:

- { auto | v1 | v2 | v3 }: Укажите один из вариантов IGMP Snooping.
  - ✓ auto: Совместимость с версиями 1, 2 и 3 (автоматическое определение).
  - ✓ v1: Совместимость с IGMP версии 1.
  - ✓ v2: Совместимость с IGMP версии 2.
  - ✓ v3: Совместимость с IGMP версии 3.

Рекомендации:

- Команда ip igmp snooping compatibility определяет, с какой версией протокола IGMP (Internet Group Management Protocol) должен работать IGMP Snooping в данном VLAN. Это важно для корректного взаимодействия с multicast-маршрутизаторами и хостами, которые могут использовать разные версии протокола.
- **Версии IGMP:**
  - ✓ **IGMPv1:** Самая ранняя версия. Имеет ограниченные возможности (нет сообщений о выходе из группы Leave).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **IGMPv2:** Наиболее распространенная версия. Добавляет сообщения Leave и оптимизирует процесс выхода.
- ✓ **IGMPv3:** Самая современная версия. Добавляет поддержку Source-Specific Multicast (SSM), позволяя клиентам указывать, от какого источника они хотят получать трафик. Это повышает безопасность и эффективность.

- **Выбор режима:**
  - ✓ auto **(рекомендуется):** Коммутатор автоматически определяет версию IGMP, используемую в VLAN, на основе получаемых запросов (Queries) и сообщений. Это наиболее гибкий и безопасный вариант для сетей со смешанным оборудованием.
  - ✓ **Принудительная установка версии (**v1**,** v2**,** v3**):** Может потребоваться, если в сети используется только одна версия протокола и нужно гарантировать совместимость или, наоборот, заблокировать использование более новых версий по соображениям безопасности. Например, принудительное использование v2 отключит поддержку SSM.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping compatibility
```

Сбрасывает настройку версии к значению по умолчанию (обычно auto*).*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.39 (config-if-vlan)# ip igmp snooping last-member-query-interval

Настройка интервала последнего запроса к участникам (Last Member Query Interval) для IGMP Snooping

Синтаксис:

```
(config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>
```

Объяснение: LMQI (Last Member Query Interval) — это интервал последнего запроса к участникам. Он используется для настройки максимального времени ожидания IGMP/MLD-отчетов о членстве на порту получателя перед удалением порта из членства в многоадресной группе. Допустимый диапазон: 0–31744 десятых долей секунды.

Параметры:

- <ipmc_lmqi: 0-31744>: Укажите значение LMQI (в десятых долях секунды).

Рекомендации:

- Команда ip igmp snooping last-member-query-interval настраивает таймер LMQI (Last Member Query Interval) для данного VLAN. Этот таймер является ключевым для процесса выхода из многоадресной группы (leave process).
- **Как это работает:**
    1. Когда на порт приходит IGMP-сообщение Leave (о выходе из группы), коммутатор не удаляет порт сразу, так как на нем могут быть другие подписчики той же группы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Вместо этого он отправляет на этот порт Group-Specific Query(s) (запросы, специфичные для группы), чтобы проверить, есть ли еще заинтересованные клиенты.
3. **LMQI** определяет интервал времени, в течение которого коммутатор ожидает ответа (Report) на эти запросы.
4. Если за время, равное LMQI * [Last Member Query Count] (обычно 2 запроса), ответ не получен, порт удаляется из списка получателей группы.

- Влияние на производительность:
    1. **Слишком большое значение:** Замедляет процесс прекращения передачи ненужного multicast-трафика на порт, где больше нет подписчиков. Может негативно сказаться на переключении каналов в IPTV.
    2. **Слишком маленькое значение:** Может привести к преждевременному удалению порта из группы, если ответ клиента слегка задержался, вызывая временные потери multicast-трафика.
- **Единица измерения:** Значение задается в десятых долях секунды. Например, значение `10` соответствует 1 секунде (10 * 0.1с). Значение по умолчанию часто составляет 10 (1 секунда).
- Эта настройка применяется к конкретному VLAN и переопределяет глобальные значения.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping last-member-query-interval
```

Сбрасывает значение LMQI для данного VLAN к глобальному значению по умолчанию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.40 (config-if-vlan)# ip igmp snooping priority

Настройка приоритета для управляющих IGMP/MLD-кадров

Синтаксис:

```
(config-if-vlan)# ip igmp snooping priority <cos_priority>
```

Объяснение: Укажите приоритет для передачи управляющих кадров IGMP/MLD. По умолчанию приоритет установлен в 0. Допустимые значения приоритета: 0–7.

Параметры:

- <cos_priority: 0-7>: Укажите значение COS (Class of Service) для данного конкретного VLAN. Допустимый диапазон от 0 до 7.

Рекомендации:

- Команда ip igmp snooping priority назначает приоритет CoS (Class of Service) для управляющих кадров протоколов IGMP (IPv4) и MLD (IPv6), передаваемых в данном VLAN.
- **Зачем это нужно:**
    - ✓ **Гарантия доставки управляющего трафика:** Управляющие кадры (запросы Queries, отчеты Reports, сообщения Leave) критически важны для корректной работы multicast. Если сеть перегружена, они могут быть отброшены, что приведет к сбоям в доставке multicast-трафика. Назначение более высокого приоритета (например, 5, 6 или 7) гарантирует, что эти кадры будут обрабатываться в первую очередь.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Качество обслуживания (QoS):** Позволяет интегрировать управление multicast-подписками в общую политику QoS сети.

- **Значение по умолчанию:** 0 (наименьший приоритет). Для критичных сетей (IPTV, видеоконференции) рекомендуется повышать этот приоритет.
- **CoS (802.1p):** Это 3-битовое поле в теге VLAN (802.1Q), которое определяет приоритет кадра. Значения 0–7, где 7 — наивысший приоритет (обычно для сетевого управления), 5 — для голоса и видео, 0 — best effort.
- Эта настройка влияет только на кадры, генерируемые самим коммутатором в рамках IGMP/MLD Snooping. Она не меняет приоритет пользовательского multicast-трафика.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping priority
```

Сбрасывает приоритет управляющих кадров к значению по умолчанию (0).

2.7.18.41 (config-if-vlan)# ip igmp snooping querier address

Настройка IP-адреса запросчика (Querier) для IGMP Snooping

Синтаксис:

```
(config-if-vlan)# ip igmp snooping querier address <v_ipv4_ucast>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Укажите IP-адрес запросчика (querier) IGMP Snooping.

Параметры:

- <v_ipv4_ucast>: Укажите одноадресный (unicast) IP-адрес запросчика IGMP Snooping.

Рекомендации:

- Команда *ip igmp snooping querier address* задает **I**P-адрес источника, который будет использоваться коммутатором при отправке IGMP-запросов (General Queries), если он выполняет роль IGMP Querier (запросчика) в данном VLAN.
- Роль IGMP Querier**:** В каждом VLAN, где включен IGMP Snooping, должен быть один запросчик (querier). Обычно эту роль выполняет multicast-маршрутизатор. Если в VLAN нет маршрутизатора, коммутатор может сам выполнять эту функцию (если она включена командой ip igmp snooping querier).
- Зачем нужен этот адрес:
    1. **Идентификация:** Все IGMP-запросы (Queries) будут содержать этот IP-адрес в качестве адреса источника.
    2. **Выбор Querier:** Если в VLAN есть несколько устройств, способных быть запросчиками (например, другой коммутатор), они используют этот адрес в процессе выбора активного Querier (обычно побеждает устройство с наименьшим IP-адресом). Поэтому важно назначить этому адресу значение, которое будет корректно в рамках сети и процесса выборов.
- Обычно в качестве адреса запросчика используется IP-адрес самого интерфейса VLAN (SVI). Если этот адрес не задан явно,

SEC.RU | Короткий путь к информации Скачано с sec.ru

коммутатор может использовать IP-адрес интерфейса по умолчанию или адрес из другого источника.

- Эта настройка имеет смысл только в том случае, если коммутатор выполняет роль IGMP Querier.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping querier address
```

Удаляет явно заданный IP-адрес запросчика, возвращаясь к использованию адреса по умолчанию (обычно IP-адрес интерфейса).

2.7.18.42 (config-if-vlan)# ip igmp snooping querier election

Участие в выборах IGMP Querier

Синтаксис:

```
(config-if-vlan)# ip igmp snooping querier election
```

Объяснение: Включение функции участия в выборах запросчика (querier election) для IGMP Snooping.

Рекомендации:

- Команда *ip igmp snooping querier election* определяет, будет ли коммутатор участвовать в процессе выборов IGMP Querier (запросчика) в данном VLAN, если он настроен как Querier (команда ip igmp snooping querier).
- В VLAN может присутствовать несколько устройств, способных выполнять роль IGMP Querier (например, multicast-

SEC.RU | Короткий путь к информации Скачано с sec.ru

маршрутизатор и сам коммутатор). Чтобы избежать конфликтов, между ними проводится процедура выборов:

1. Все устройства, настроенные как потенциальные Querier, начинают отправлять IGMP-запросы (General Queries).
2. Устройство, получившее запрос с более низким IP-адресом источника, чем его собственный, уступает роль и перестает быть активным Querier (становится non-querier).
3. Устройство с наименьшим IP-адресом выигрывает выборы и становится активным запросчиком.

- Если функция `querier election` включена**:**

    1. Коммутатор будет полноценно участвовать в выборе, сравнивая свой IP-адрес с IP-адресами других запросчиков. Он станет активным Querier, только если его адрес окажется наименьшим. В противном случае он перейдет в состояние non-querier.

- Если функция `querier election` отключена **(**`no ip igmp snooping querier election`**):**

    1. Коммутатор будет всегда пытаться быть активным Querier, независимо от наличия других запросчиков с меньшим IP-адресом. Это может привести к конфликтам и нестабильной работе multicast в сети. Обычно эта функция оставляется включенной.

- Эта команда имеет смысл только при включенной функции `ip igmp snooping querier`.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping querier election
```

Отключает участие в выборах Querier (коммутатор всегда будет пытаться быть активным запросчиком).

2.7.18.43 (config-if-vlan)# ip igmp snooping query-interval

Настройка интервала отправки IGMP-запросов

Синтаксис:

```
(config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>
```

Объяснение: Укажите значение интервала IPMC-запросов (Query interval).

Параметры:

- <ipmc_qi: 1-31744>: Укажите значение интервала IPMC-запросов. Допустимые значения: от 1 до 31744 (в секундах).

Рекомендации:

- Команда ip igmp snooping query-interval задает периодичность (интервал), с которой IGMP Querier (запросчик) отправляет общие (General) IGMP-запросы в данном VLAN. Эти запросы используются для того, чтобы выяснить, какие многоадресные группы все еще актуальны (есть ли подписчики).
- Зачем это нужно:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Актуализация информации:** Регулярные запросы позволяют коммутатору обновлять свои таблицы о членстве в multicast-группах. Клиенты, заинтересованные в группах, отвечают на эти запросы, подтверждая свое членство. Если клиент не отвечает несколько интервалов, его запись может быть удалена (по истечении таймера).
- **Влияние на сеть:** Слишком частые запросы (маленький интервал) увеличивают служебный трафик в сети. Слишком редкие запросы (большой интервал) могут замедлить реакцию на изменения в членстве групп (например, на выход клиента из группы).

- **Единица измерения:** Интервал задается в **секундах**.
- **Взаимосвязь с другими таймерами:** От этого интервала зависят другие таймеры, такие как query-response-interval и last-member-query-interval.
- Эта настройка применяется к конкретному VLAN и имеет смысл только в том случае, если коммутатор выполняет роль IGMP Querier (или потенциально может ей стать).

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping query-interval
```

Сбрасывает значение интервала запросов для данного VLAN к глобальному значению по умолчанию (обычно 125 секунд).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.44 (config-if-vlan)# ip igmp snooping query-max-response-time

Настройка максимального времени ответа на IGMP-запросы

Синтаксис:

```
(config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>
```

Объяснение: Укажите значение времени ответа на IPMC-запросы (Query Response Time).

Параметры:

- <ipmc_qri>: Укажите значение времени ответа на IPMC-запросы. Допустимые значения: от 1 до 31744

Рекомендации:

- Команда ip igmp snooping query-max-response-time задает максимальное время, в течение которого клиенты (хосты) могут ответить на IGMP-запрос (General Query) от Querier.
- **Как это работает:**
    1. IGMP Querier отправляет общий запрос (General Query) в VLAN. В этом запросе указывается значение Max Response Time.
    2. Получив запрос, каждый хост, заинтересованный в какой-либо многоадресной группе, должен ответить IGMP-отчетом (Report) в течение этого времени.
    3. Хосты выбирают случайное время в пределах этого интервала для отправки своего ответа, чтобы избежать

SEC.RU | Короткий путь к информации Скачано с sec.ru

одновременной отправки большого количества отчетов ("взрывной" трафик).

- **Влияние на сеть:**
    1. **Маленькое значение:** Ускоряет процесс сбора информации о подписчиках, но может привести к всплеску трафика, если хосты выберут близкое время ответа.
    2. **Большое значение:** Увеличивает задержку в обнаружении новых подписчиков и делает процесс менее чувствительным.
- Эта настройка применяется к конкретному VLAN и имеет смысл только при включенном IGMP Snooping и наличии активного Querier.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping query-max-response-time
```

Сбрасывает значение максимального времени ответа для данного VLAN к значению по умолчанию.

2.7.18.45 (config-if-vlan)# ip igmp snooping robustness-variable

Настройка переменной устойчивости (Robustness Variable) для IGMP Snooping

Синтаксис:

```
(config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Переменная устойчивости (Robustness Variable, RV) позволяет настроить ожидаемую потерю пакетов в подсети. Если подсеть подвержена потере пакетов, это значение можно увеличить. Значение RV не должно быть нулевым и не должно равняться единице. Значение должно быть 2 или больше. По умолчанию установлено 2.

Параметры:

- <ipmc_rv: 1-255>: Укажите значение переменной устойчивости IPMC. Допустимые значения: от 1 до 255.

Рекомендации:

- Команда ip igmp snooping robustness-variable настраивает **п**еременную устойчивости (Robustness Variable) для данного VLAN. Этот параметр влияет на то, сколько раз будут повторяться некоторые IGMP-сообщения и как долго будут храниться записи о членстве в группах.
- **Как это работает:** Переменная устойчивости используется для расчета нескольких важных таймеров и счетчиков:
    - ✓ **Количество повторных запросов:** Определяет, сколько Group-Specific Queries будет отправлено при получении Leave-сообщения (обычно равно RV). Это повышает надежность процесса выхода.
    - ✓ **Время жизни записи (Group Membership Interval):** Рассчитывается как (Robustness Variable * Query Interval) + Query Response Time. Более высокое RV увеличивает это время, делая записи более "живучими" при временных потерях пакетов.
- **Рекомендации по выбору:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Значение по умолчанию (2):** Подходит для большинства надежных проводных сетей.
- ✓ **Увеличение (3-5):** Рекомендуется для сетей с высоким уровнем потерь пакетов (например, беспроводные сети, спутниковые каналы, перегруженные сегменты). Это повышает устойчивость к потерям управляющих пакетов, но также увеличивает время реакции на изменения (например, на выход из группы).
- ✓ **Значение 1:** Не рекомендуется, так как делает протокол очень чувствительным к единичным потерям пакетов.

- Эта настройка применяется к конкретному VLAN.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping robustness-variable
```

Сбрасывает значение переменной устойчивости для данного VLAN к значению по умолчанию (2).

2.7.18.46 (config-if-vlan)# ip igmp snooping unsolicited-report-interval

Настройка интервала передачи незапрошенных IGMP-отчетов

Синтаксис:

```
(config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>
```

Объяснение: Интервал незапрошенных отчетов (Unsolicited Report Interval) — это время, в течение которого вышестоящий (upstream) интерфейс должен передавать незапрошенные IGMP-отчеты, когда

SEC.RU | Короткий путь к информации Скачано с sec.ru

включено подавление отчетов (report suppression) или прокси-отчетность (proxy reporting). Допустимый диапазон для URI: 0–31744 секунд.

Параметры:

- <ipmc_uri: 0-31744>: Укажите значение интервала незапрошенных отчетов. Допустимые значения: от 0 до 31744 секунд.

Рекомендации:

- Команда ip igmp snooping unsolicited-report-interval настраивает таймер URI (Unsolicited Report Interval) для данного VLAN. Эта функция актуальна, когда на коммутаторе включены механизмы подавления отчетов (Report Suppression) или прокси-отчетности (Proxy Reporting).
- **Для чего используется:**
    - ✓ **Подавление отчетов (Report Suppression):** В IGMPv2 и v3, когда несколько клиентов в одном VLAN подписаны на одну группу, только первый из них отправляет отчет (Report) в ответ на запрос Querier. Остальные подавляют свои отчеты, что уменьшает служебный трафик. Коммутатор, выполняющий функции прокси, должен периодически отправлять "незапрошенные" отчеты вышестоящему маршрутизатору, чтобы подтвердить, что группа все еще активна в этом VLAN.
    - ✓ **Прокси-отчетность (Proxy Reporting):** Коммутатор выступает в роли прокси для всех клиентов в VLAN и сам отправляет отчеты маршрутизатору.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **URI** определяет, как часто коммутатор будет отправлять эти подтверждающие (незапрошенные) IGMP-отчеты о членстве в группах вышестоящему маршрутизатору (upstream Querier), даже если от клиентов в данный момент не поступает новых запросов.
- Поддержание состояния: Гарантирует, что вышестоящий маршрутизатор не удалит группу из-за отсутствия активности, даже если все клиенты в данный момент молчат.
- Уменьшение задержек: Позволяет быстрее восстановить multicast-трафик после кратковременных сбоев.
- Значение 0**:** Отключает периодическую отправку незапрошенных отчетов.
- Эта настройка применяется к конкретному VLAN.

Удаление конфигурации:

```
(config-if-vlan)# no ip igmp snooping unsolicited-report-interval
```

Сбрасывает значение интервала незапрошенных отчетов для данного VLAN к значению по умолчанию.

2.7.18.47 (config-if-vlan)# ipv6 address

Настройка IPv6-адреса для интерфейса VLAN

Синтаксис:

```
(config-if-vlan)# ipv6 address <subnet>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Настройка IPv6-адреса для данного интерфейса VLAN.

Параметры:

- <subnet>: Укажите IPv6-адрес в формате X:X:X:X::X/<0-128> (например, 2001:db8:1::1/64).

Рекомендации:

- Команда ipv6 address является основной для назначения глобального IPv6-адреса или адреса интерфейсу VLAN уровня 3 (SVI). Этот адрес используется для управления коммутатором по IPv6 и, при включенной маршрутизации, служит шлюзом по умолчанию для устройств в этой VLAN.
- **Формат адреса:** Адрес указывается в стандартной нотации IPv6 с двоеточиями, с указанием длины префикса через слеш (CIDR). Например: 2001:db8:10::1/64.
- Для работы маршрутизации IPv6 между VLAN необходимо также глобально включить маршрутизацию IPv6 командой ip routing (которая включает и IPv4, и IPv6) или отдельной командой ipv6 routing (в зависимости от реализации). Если поддерживается коммутатором.
- Помимо статических адресов, задаваемых этой командой, интерфейс VLAN также может автоматически получить link-local адрес (начинающийся с fe80::). Этот адрес используется для связи с соседними устройствами в том же сегменте.
- Для удаления всех IPv6-адресов с интерфейса используется команда no ipv6 address. Для удаления конкретного адреса можно указать его подсеть.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 address [ <ipv6_subnet> ]
```

Без параметра удаляет все IPv6-адреса с интерфейса. С указанием подсети удаляет только конкретный адрес.

Просмотр:

```
> show ip interface brief
> show ipv6 interface [ vlan <v_vlan_list> { brief | statistics } ]
# show ip interface brief
# show ipv6 interface [ vlan <v_vlan_list> { brief | statistics } ]
```

2.7.18.48 (config-if-vlan)# ipv6 mld snooping

Включение MLD Snooping на конкретном VLAN

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping
```

Объяснение: Включение MLD (Multicast Listener Discovery) Snooping на данном конкретном VLAN.

Рекомендации:

- Команда ipv6 mld snooping является **I**Pv6-аналогом команды ip igmp snooping для IPv4. Она включает функцию MLD Snooping для указанного интерфейса VLAN.
- MLD (Multicast Listener Discovery) — это протокол, используемый в IPv6 для управления членством в многоадресных группах

SEC.RU | Короткий путь к информации Скачано с sec.ru

(аналог IGMP в IPv4). MLD Snooping позволяет коммутатору уровня 2 "прослушивать" обмен MLD-сообщениями между маршрутизаторами и хостами, чтобы эффективно пересылать многоадресный (multicast) IPv6-трафик только на те порты, где есть подписчики, вместо рассылки во все порты VLAN.

- **Зачем это нужно:**
  - ✓ **Оптимизация трафика:** Предотвращает ненужную рассылку IPv6 multicast-трафика по всем портам, экономя пропускную способность и снижая нагрузку на конечные устройства.
  - ✓ **Повышение производительности:** Аналогично IGMP Snooping, но для IPv6-сетей.
- **Взаимосвязь с глобальной настройкой:** Обычно для работы MLD Snooping необходимо выполнить оба шага:
  1. Глобально включить MLD Snooping (команда типа `ipv6 mld snooping` на глобальном уровне).
  2. Включить его на нужных VLAN с помощью данной интерфейсной команды (или через `ipv6 mld snooping vlan <vlan_list>`).
- Для корректной работы MLD Snooping в VLAN должен присутствовать MLD Querier (запросчик), обычно это IPv6 multicast-маршрутизатор. В его отсутствие коммутатор может выполнять эту роль, если настроен соответствующим образом.

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping
```

Отключает MLD Snooping для данного VLAN.

Просмотр:

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
text
> show ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp -msg <type> ]
# show ipv6 statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ] [ icmp -msg <type> ]
```

Используется для детального просмотра состояния MLD Snooping

2.7.18.49 (config-if-vlan)# ipv6 mld snooping compatibility

Настройка версии совместимости MLD Snooping для VLAN

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping compatibility { auto | v1 | v2 }
```

Объяснение: Настройка версии MLD Snooping, используемой для данного конкретного VLAN.

Параметры:

- { auto | v1 | v2 }: Укажите один из вариантов MLD Snooping.
  - ✓ auto: Совместимость с версиями 1 и 2 (автоматическое определение).
  - ✓ v1: Совместимость с MLD версии 1.
  - ✓ v2: Совместимость с MLD версии 2.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда ipv6 mld snooping compatibility является IPv6-аналогом команды ip igmp snooping compatibility и определяет, с какой версией протокола MLD (Multicast Listener Discovery) должен работать MLD Snooping в данном VLAN. Это важно для корректного взаимодействия с IPv6 multicast-маршрутизаторами и хостами.
- Версии MLD (аналоги IGMP для IPv6):
    - ✓ **MLDv1 (версия 1):** Соответствует IGMPv2. Позволяет хостам сообщать о своем желании получать трафик от любой группы.
    - ✓ **MLDv2 (версия 2):** Соответствует IGMPv3. Добавляет поддержку Source-Specific Multicast (SSM), позволяя клиентам указывать, от какого конкретного IPv6-адреса источника они хотят получать трафик. Это повышает безопасность и эффективность.
- **Выбор режима:**
    - ✓ auto **(рекомендуется):** Коммутатор автоматически определяет версию MLD, используемую в VLAN, на основе получаемых запросов (Queries) и сообщений. Это наиболее гибкий вариант для сетей со смешанным оборудованием.
    - ✓ **Принудительная установка версии (**v1**,** v2**):** Может потребоваться, если в сети используется только одна версия протокола и нужно гарантировать совместимость или заблокировать использование более новых версий (например, для упрощения или по соображениям безопасности). Принудительное использование v1 отключит поддержку SSM.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping compatibility
```

Сбрасывает настройку версии к значению по умолчанию (обычно auto*).*

2.7.18.50 (config-if-vlan)# ipv6 mld snooping last-member-query-interval

Настройка интервала последнего запроса к участникам для MLD Snooping

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping last-member-query-interval <ipmc_lmqi>
```

Объяснение: LMQI (Last Member Query Interval) — это интервал последнего запроса к участникам. Он используется для настройки максимального времени ожидания IGMP/MLD-отчетов о членстве на порту получателя перед удалением порта из членства в многоадресной группе. Допустимый диапазон: 0–31744 десятых долей секунды.

Параметры:

- <ipmc_lmqi: 0-31744>: Укажите значение LMQI (в десятых долях секунды).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `ipv6 mld snooping last-member-query-interval` является IPv6-аналогом команды `ip igmp snooping last-member-query-interval`. Она настраивает таймер LMQI (Last Member Query Interval) для данного VLAN в контексте MLD (Multicast Listener Discovery) Snooping.
- Влияние на производительность (аналогично IGMP):
    1. **Слишком большое значение:** Замедляет процесс прекращения передачи ненужного IPv6 multicast-трафика на порт, где больше нет подписчиков.
    2. **Слишком маленькое значение:** Может привести к преждевременному удалению порта из группы, если ответ клиента слегка задержался, вызывая временные потери multicast-трафика.
- Единица измерения: Значение задается в десятых долях секунды. Например, значение `10` соответствует 1 секунде (10 * 0.1с). Значение по умолчанию часто составляет 10 (1 секунда).
- Эта настройка применяется к конкретному VLAN и переопределяет глобальные значения.

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping last-member-query-interval
```

Сбрасывает значение LMQI для данного VLAN к глобальному значению по умолчанию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.51 (config-if-vlan)# ipv6 mld snooping priority

Настройка приоритета для управляющих MLD-кадров

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping priority <cos_priority>
```

Объяснение: Укажите приоритет для передачи управляющих кадров IGMP/MLD. По умолчанию приоритет установлен в 0. Допустимые значения приоритета: 0–7.

Параметры:

- <cos_priority: 0-7>: Укажите значение COS (Class of Service) для данного конкретного VLAN. Допустимый диапазон от 0 до 7.

Рекомендации:

- Команда ipv6 mld snooping priority является IPv6-аналогом команды ip igmp snooping priority. Она назначает приоритет CoS (Class of Service) для управляющих кадров протокола MLD (Multicast Listener Discovery), передаваемых в данном VLAN.
- **Зачем это нужно:**
    - ✓ **Гарантия доставки управляющего трафика:** Управляющие кадры MLD (запросы Queries, отчеты Reports, сообщения Done) критически важны для корректной работы IPv6 multicast. Если сеть перегружена, они могут быть отброшены, что приведет к сбоям в доставке multicast-трафика. Назначение более

SEC.RU | Короткий путь к информации Скачано с sec.ru

высокого приоритета (например, 5, 6 или 7) гарантирует, что эти кадры будут обрабатываться в первую очередь.

- ✓ **Качество обслуживания (QoS):** Позволяет интегрировать управление IPv6 multicast-подписками в общую политику QoS сети.

- Значение по умолчанию: 0 (наименьший приоритет). Для критичных IPv6 multicast-приложений рекомендуется повышать этот приоритет.
- **CoS (802.1p):** Это 3-битовое поле в теге VLAN (802.1Q), которое определяет приоритет кадра. Значения 0–7, где 7 — наивысший приоритет (обычно для сетевого управления), 5 — для голоса и видео, 0 — best effort.
- Эта настройка влияет только на кадры MLD, генерируемые самим коммутатором в рамках MLD Snooping. Она не меняет приоритет пользовательского IPv6 multicast-трафика.

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping priority
```

Сбрасывает приоритет управляющих MLD-кадров к значению по умолчанию (0).

2.7.18.52 (config-if-vlan)# ipv6 mld snooping query-interval

Настройка интервала отправки MLD-запросов

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Укажите значение интервала MLD-запросов (Query interval).

Параметры:

- <ipmc_qi: 1-31744>: Укажите значение интервала IPMC-запросов. Допустимые значения: от 1 до 31744 (в секундах).

Рекомендации:

- Команда ipv6 mld snooping query-interval является IPv6-аналогом команды ip igmp snooping query-interval. Она задает периодичность (интервал), с которой MLD Querier отправляет общие (General) MLD-запросы в данном VLAN.
- Регулярные запросы позволяют коммутатору обновлять свои таблицы о членстве в IPv6 multicast-группах.
- **Влияние на сеть:** Слишком частые запросы (маленький интервал) увеличивают служебный трафик. Слишком редкие запросы (большой интервал) могут замедлить реакцию на изменения.
- Интервал задается в **секундах**.
- Эта настройка имеет смысл только в том случае, если коммутатор выполняет роль MLD Querier.

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping query-interval
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.18.53 (config-if-vlan)# ipv6 mld snooping query-max-response-time

Настройка максимального времени ответа на MLD-запросы

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>
```

Объяснение: Укажите значение времени ответа на MLD-запросы (Query Response Time).

Параметры:

- <ipmc_qri>: Укажите значение времени ответа на MLD-запросы. Допустимые значения: от 1 до 31744.

Рекомендации:

- Команда ipv6 mld snooping query-max-response-time является IPv6-аналогом команды ip igmp snooping query-max-response-time. Она задает максимальное время, в течение которого IPv6-хосты (клиенты) могут ответить на MLD-запрос (General Query) от Querier в данном VLAN.
- **Влияние на сеть:**
    1. **Маленькое значение:** Ускоряет процесс сбора информации о подписчиках, но может привести к всплеску трафика, если хосты выберут близкое время ответа.
    2. **Большое значение:** Увеличивает задержку в обнаружении новых подписчиков и делает процесс менее чувствительным.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Эта настройка применяется к конкретному VLAN и имеет смысл только при включенном MLD Snooping и наличии активного MLD Querier.

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping query-max-response-time
```

Сбрасывает значение максимального времени ответа для данного VLAN к значению по умолчанию.

2.7.18.54 (config-if-vlan)# ipv6 mld snooping robustness-variable

Настройка переменной устойчивости для MLD Snooping

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>
```

Объяснение: Переменная устойчивости (Robustness Variable, RV) позволяет настроить ожидаемую потерю пакетов в подсети. Если подсеть подвержена потере пакетов, это значение можно увеличить. Значение RV не должно быть нулевым и не должно равняться единице. Значение должно быть 2 или больше. По умолчанию установлено 2.

Параметры:

- <ipmc_rv: 1-255>: Укажите значение переменной устойчивости IPMC. Допустимые значения: от 1 до 255.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `ipv6 mld snooping robustness-variable` является IPv6-аналогом команды `ip igmp snooping robustness-variable`. Она настраивает переменную устойчивости (Robustness Variable) для данного VLAN в контексте MLD (Multicast Listener Discovery) Snooping.
- **Как это работает:** Переменная устойчивости используется для расчета нескольких важных таймеров и счетчиков в MLD:
    - ✓ **Количество повторных запросов:** Определяет, сколько Multicast Address Specific Queries будет отправлено при получении MLD-сообщения Done (аналог Leave в IPv4). Обычно это число равно RV.
    - ✓ **Время жизни записи (Multicast Listener Interval):** Рассчитывается как `(Robustness Variable * Query Interval) + Query Response Time`. Более высокое RV увеличивает это время, делая записи более "живучими" при временных потерях пакетов.
- **Рекомендации по выбору:**
    - ✓ **Значение по умолчанию (2):** Подходит для большинства надежных проводных сетей.
    - ✓ **Увеличение (3-5):** Рекомендуется для сетей с высоким уровнем потерь пакетов (например, беспроводные сети, спутниковые каналы, перегруженные сегменты). Это повышает устойчивость к потерям управляющих пакетов MLD, но также увеличивает время реакции на изменения (например, на выход из группы).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Значение 1:** Не рекомендуется (как указано в описании), так как делает протокол очень чувствительным к единичным потерям пакетов.

- Эта настройка применяется к конкретному VLAN.

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping robustness-variable
```

Сбрасывает значение переменной устойчивости для данного VLAN к значению по умолчанию (2).

2.7.18.55 (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval

Настройка интервала передачи незапрошенных MLD-отчетов

Синтаксис:

```
(config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>
```

Объяснение: Интервал незапрошенных отчетов (Unsolicited Report Interval) — это время, в течение которого вышестоящий (upstream) интерфейс должен передавать незапрошенные MLD-отчеты, когда включено подавление отчетов (report suppression) или прокси-отчетность (proxy reporting). Допустимый диапазон для URI: 0–31744 секунд.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <ipmc_uri: 0-31744>: Укажите значение интервала незапрошенных отчетов. Допустимые значения: от 0 до 31744 секунд.

Рекомендации:

- Команда ipv6 mld snooping unsolicited-report-interval является IPv6-аналогом команды ip igmp snooping unsolicited-report-interval. Она настраивает таймер **URI (Unsolicited Report Interval)** для данного VLAN в контексте MLD Snooping. Эта функция актуальна, когда на коммутаторе включены механизмы **подавления отчетов (Report Suppression)** или **прокси-отчетности (Proxy Reporting)** для IPv6 multicast.
- **Контекст использования (аналогично IGMP):**
    - ✓ **Подавление отчетов (Report Suppression):** В MLDv1 и v2, когда несколько клиентов в одном VLAN подписаны на одну группу, коммутатор, выполняющий функции прокси, должен периодически отправлять "незапрошенные" отчеты вышестоящему маршрутизатору, чтобы подтвердить, что группа все еще активна в этом VLAN.
    - ✓ **Прокси-отчетность (Proxy Reporting):** Коммутатор выступает в роли прокси для всех клиентов в VLAN и сам отправляет отчеты маршрутизатору.
- **URI** определяет, как часто коммутатор будет отправлять эти подтверждающие (незапрошенные) MLD-отчеты о членстве в

SEC.RU | Короткий путь к информации Скачано с sec.ru

группах вышестоящему маршрутизатору (upstream Querier), даже если от клиентов в данный момент не поступает новых запросов.

- **Зачем это нужно:**
  - ✓ **Поддержание состояния:** Гарантирует, что вышестоящий маршрутизатор не удалит группу из-за отсутствия активности, даже если все клиенты в данный момент молчат.
  - ✓ **Уменьшение задержек:** Позволяет быстрее восстановить IPv6 multicast-трафик после кратковременных сбоев.
- Значение 0**:** Отключает периодическую отправку незапрошенных отчетов.
- Эта настройка применяется к конкретному VLAN.

Удаление конфигурации:

```
(config-if-vlan)# no ipv6 mld snooping unsolicited-report-interval
```

Сбрасывает значение интервала незапрошенных отчетов для данного VLAN к значению по умолчанию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.19 Настройка профилей IP-многоадресной рассылки (IPMC) (config)# ipmc

2.7.19.1 (config)# ipmc profile

Глобальное включение функции профилей IPMC

Синтаксис:

```
(config)# ipmc profile
```

Объяснение: Глобальное включение функции профилей IP-многоадресной рассылки (IP Multicast, IPMC).

Рекомендации:

- Команда ipmc profile глобально активирует возможность создания и использования профилей IP-многоадресной рассылки (IPMC) на коммутаторе.
- **IPMC профили –** это механизм, позволяющий администратору создавать именованные списки многоадресных (multicast) групп (как IPv4, так и IPv6). Эти профили затем могут применяться к портам для фильтрации (разрешения или запрета) доступа к определенным multicast-потокам. Это более гибкий и управляемый способ, чем настройка фильтрации по каждой группе отдельно.
- **Зачем это нужно:**
    - ✓ **Централизованное управление:** Создается один профиль (например, IPTV_CHANNELS), в который включаются все необходимые multicast-группы. Затем этот профиль применяется ко множеству портов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Контроль доступа:** Позволяет реализовать политики доступа к multicast-трафику. Например, можно создать профиль VIP_VIDEO и применить его только к портам руководства, а профиль BASIC_IPTV — к обычным пользовательским портам.
- ✓ **Упрощение конфигурации:** Вместо длинных списков ACL для multicast на каждом порту, используется один профиль.

Удаление конфигурации:

```
(config)# no ipmc profile
```

Глобально отключает функцию профилей IPMC. Все созданные профили и их привязки перестанут действовать.

Просмотр:

```
# show ipmc profile
```

Отображает список созданных IPMC-профилей и их содержимое.

2.7.19.2 (config)# ipmc profile <profile_name>

Создание и вход в режим конфигурации IPMC-профиля

Синтаксис:

```
(config)# ipmc profile <profile_name>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <profile_name: word16>: Укажите желаемое имя профиля (до 16 символов). После нажатия Enter команда переключится в режим (config-ipmc-profile)#.

Объяснение: Создание IPMC-профиля.

Рекомендации:

- Команда *ipmc profile <profile_name>* используется для создания нового именованного профиля IP-многоадресной рассылки (IPMC) и одновременного перехода в режим его конфигурации (config-ipmc-profile)#.
- **Процесс создания профиля:**
    1. Сначала глобально включается функция IPMC профилей (ipmc profile).
    2. Затем с помощью данной команды создается профиль с уникальным именем.
    3. После этого вы оказываетесь в режиме (config-ipmc-profile)#, где с помощью специальных команд (например, deny, permit) определяете, какие многоадресные группы (адреса или диапазоны) будут входить в этот профиль.
- **Назначение профиля:** Профиль служит контейнером для списка разрешенных или запрещенных multicast-групп. Сам по себе он не фильтрует трафик, пока не будет применен к порту с помощью команды типа ip igmp snooping filter <profile_name>.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Имя профиля должно быть уникальным и описательным, чтобы было понятно его назначение (например, ALLOW_IPTV, BLOCK_VIDEO).

Удаление конфигурации:

```
(config)# no ipmc profile <profile_name>
```

Удаляет указанный IPMC-профиль. Профиль должен быть предварительно отвязан от всех портов, иначе команда может не выполниться или привести к ошибкам.

Просмотр:

```
# show ipmc profile [ <profile_name> ] [ detail ]
```

Показывает список профилей,параметром <profile_name> *показывает содержимое конкретного профиля. С ключевым словом* detail *может показывать более подробную информацию.*

2.7.19.3 (config)# ipmc range

Создание именованного диапазона многоадресных IP-адресов

Синтаксис:

```
(config)# ipmc range <entry_name> { <v_ipv4_mcast> [ <v_ipv4_mcast_1> ] | <v_ipv6_mcast> [ <v_ipv6_mcast_1> ] }
```

Объяснение: Укажите диапазон многоадресных (multicast) IP-адресов. Доступный диапазон IP-адресов: от 224.0.0.0 до 239.255.255.255.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <entry_name>: Имя, используемое для указания диапазона адресов.
- { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }: Укажите диапазон многоадресных IP-адресов. Для IPv4 доступный диапазон: от 224.0.0.0 до 239.255.255.255.

Рекомендации:

- Команда ipmc range позволяет создать именованный диапазон (entry) многоадресных IP-адресов (как для IPv4, так и для IPv6). Этот именованный диапазон затем может быть использован при создании правил внутри IPMC-профилей (в режиме (config-ipmc-profile)#), что делает конфигурацию более читаемой и удобной для повторного использования.
- **Форматы указания диапазона:**
    - ✓ **Одиночный адрес:** Указывается только один адрес (<v_ipv4_mcast>).
    - ✓ **Диапазон адресов:** Указываются начальный и конечный адреса (<v_ipv4_mcast> и <v_ipv4_mcast_1>). Например, 224.1.1.1 224.1.1.10.
- **Зачем это нужно:**
    - ✓ **Упрощение управления:** Вместо того чтобы в каждом профиле перечислять длинные списки групп, можно создать один именованный диапазон (например, IPTV_BASIC) и ссылаться на него.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Повторное использование:** Один и тот же диапазон можно использовать в нескольких разных профилях.

- Эти именованные диапазоны являются глобальными объектами и не привязаны к конкретному профилю.

Удаление конфигурации:

```
(config)# no ipmc range <entry_name>
```

Удаляет ранее созданный именованный диапазон.

Просмотр:

```
# show ipmc profile [ <profile_name> ] [ detail ]
```

Команда show ipmc profile *также может отображать информацию о созданных именованных диапазонах.*

2.7.19.4 (config-ipmc-profile)# default range

Установка правила по умолчанию для IPMC-профиля

Синтаксис:

```
(config-ipmc-profile)# default range <entry_name>
```

Параметры:

- <entry_name: word16>: Укажите имя записи (до 16 символов) для данного IPMC-профиля.

Объяснение: Установка правила по умолчанию для конкретного IPMC-профиля.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда default range, выполняемая в режиме конфигурации IPMC-профиля (config-ipmc-profile)#, позволяет задать действие по умолчанию для данного профиля, используя ранее созданный именованный диапазон (ipmc range).
- В контексте IPMC-профилей, правило по умолчанию определяет, что делать с трафиком для групп, не попадающих под другие, более конкретные правила (permit/deny), заданные в профиле.
- Если в профиле не задано ни одного правила permit или deny, действие по умолчанию применяется ко всему multicast-трафику. Если есть и другие правила, то default range действует как "все остальное".
- Обычно default range используется в сочетании с одним из ключевых слов (permit или deny), которые задаются отдельно в этом же режиме. Например, можно создать профиль, где разрешен (permit) только диапазон IPTV_CHANNELS, а все остальное запрещено по умолчанию (или наоборот). Сама команда default range, вероятно, просто привязывает именованный диапазон как цель для действия по умолчанию, а само действие (permit/deny) задается другой командой (например, permit range). В предоставленном синтаксисе не указано само действие, поэтому можно предположить, что default range само по себе может подразумевать либо разрешение, либо запрет, либо это часть более сложной конструкции.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-ipmc-profile)# no range <entry_name>
```

Удаляет привязку именованного диапазона (вероятно, в качестве правила по умолчанию) из профиля.

Просмотр:

```
# show ipmc profile
# show ipmc profile [ <profile_name> ] [ detail ]
```

2.7.19.5 (config-ipmc-profile)# description

Добавление описания к IPMC-профилю

Синтаксис:

```
(config-ipmc-profile)# description <profile_desc>
```

Параметры:

- <profile_desc: line 64>: Дополнительное описание для указанного профиля (до 64 символов).

Объяснение: Укажите описательную информацию для указанного профиля.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда description позволяет добавить текстовое описание (комментарий) к текущему IPMC-профилю в режиме его конфигурации (config-ipmc-profile)#.
- **Зачем это нужно:**
    - ✓ **Документирование:** Описание помогает другим администраторам (или вам самому через несколько месяцев) понять назначение профиля, не вникая в детали его правил. Например, вместо загадочного имени PROF1 можно добавить описание Permit IPTV channels for floor 3.
    - ✓ **Управление конфигурацией:** Упрощает поддержку и аудит конфигурации.
- Описание не влияет на работу профиля и фильтрацию трафика, оно служит исключительно для информационных целей.
- Рекомендуется всегда добавлять осмысленные описания к создаваемым профилям, особенно если их много.

Удаление конфигурации:

```
(config-ipmc-profile)# no description
```

Удаляет описание профиля.

Просмотр:

```
# show ipmc profile
# show ipmc profile [ <profile_name> ] [ detail ]
```

*Описание профиля отображается при просмотре информации о профиле, особенно в детальном режиме (*detail*).*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.19.6 (config-ipmc-profile)# range

Добавление правила фильтрации на основе именованного диапазона в IPMC-профиль

Синтаксис:

```
(config-ipmc-profile)# range <entry_name> { permit | deny } [ log ] [ next <next_entry> ]
```

Параметры:

- <entry_name>: Укажите имя записи (именованного диапазона, созданного командой ipmc range).
- { permit | deny }: Укажите действие, выполняемое при получении кадра Join/Report (запроса на присоединение), адрес группы которого соответствует диапазону адресов данного правила.
    - ✓ permit: Адрес группы, попадающий в диапазон, указанный в правиле, будет принят (изучен).
    - ✓ deny: Адрес группы, попадающий в диапазон, указанный в правиле, будет отброшен.
- [log]: Вести журнал (логировать) при совпадении.
- [next <next_entry>]: Укажите следующую запись, используемую в профиле.

Объяснение: Установка действия для записи (правила) в конкретном IPMC-профиле.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда range в режиме конфигурации профиля (config-ipmc-profile)# является основной для создания правил фильтрации. Она связывает ранее созданный именованный диапазон (ipmc range) с конкретным действием (permit или deny).
- **Параметр** log**:** Включает запись в системный журнал (syslog) каждого случая срабатывания данного правила. Полезно для отладки или мониторинга подозрительной активности.
- **Параметр** next**:** Позволяет явно указать порядок обработки правил в профиле. Правила проверяются последовательно. С помощью next можно, например, вставить новое правило перед существующим. Если next не указан, правило добавляется в конец списка.
- Профиль может содержать множество правил. Важен их порядок: обычно более конкретные правила ставятся выше, более общие — ниже.

Удаление конфигурации:

```
(config-ipmc-profile)# no range <entry_name>
```

Удаляет указанное правило из профиля.

Просмотр:

```
# show ipmc profile
# show ipmc profile [ <profile_name> ] [ detail ]
```

В детальном выводе показываются все правила профиля с их действиями и порядком.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.20 Настройка MLD-прокси для IPv6 (config)# ipv6 mld host-proxy

2.7.20.1 (config)# ipv6 mld host-proxy

Глобальное включение функции MLD-прокси

Синтаксис:

```
(config)# ipv6 mld host-proxy
```

Объяснение: Включение IPv6 MLD-прокси. Когда MLD-прокси включен, коммутатор обменивается MLD-сообщениями с маршрутизатором на своем вышестоящем (upstream) интерфейсе и выполняет роль хоста в части задач MLD на вышестоящем интерфейсе следующим образом:

- При получении запроса (Queried) отправляет отчеты многоадресного прослушивания (multicast listener reports) в группу.
- Когда хост присоединяется к многоадресной группе, к которой не принадлежит ни один другой хост, он отправляет незапрошенные отчеты многоадресного прослушивания (unsolicited multicast listener reports) в эту группу.
- Когда последний хост в определенной многоадресной группе покидает ее, он отправляет незапрошенный отчет о завершении многоадресного прослушивания (unsolicited multicast listener done report) на адрес всех маршрутизаторов (FF02::2) для MLDv1.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда ipv6 mld host-proxy глобально активирует функцию MLD-прокси (MLD Proxy) на коммутаторе. Это IPv6-аналог функции ip igmp host-proxy для IPv4.
- **MLD-прокси –** Это функция, при которой коммутатор выступает в роли представителя (прокси) для всех IPv6-хостов, подключенных к его портам, в диалоге с вышестоящим MLD-маршрутизатором (querier). Вместо того чтобы пересылать все MLD-сообщения от каждого хоста, коммутатор агрегирует их и отправляет маршрутизатору только обобщенную информацию о том, какие группы активны в данном сегменте сети.
- **Зачем это нужно:**
    1. **Снижение служебного трафика:** Значительно уменьшает количество MLD-пакетов, циркулирующих в сети, особенно в сегментах с большим количеством хостов.
    2. **Экономия ресурсов:** Снижает нагрузку на вышестоящий маршрутизатор, которому не нужно обрабатывать MLD-сообщения от каждого отдельного хоста.
- Эта функция тесно связана с MLD Snooping и обычно используется вместе с ним.

Удаление конфигурации:

```
(config)# no ipv6 mld host-proxy
```

Глобально отключает функцию MLD-прокси.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```

Статус MLD-прокси может отображаться в детальном выводе команд show ipv6 mld snooping*.*

2.7.20.2 (config)# ipv6 mld host-proxy leave-proxy

Включение функции MLD Leave Proxy

Синтаксис:

```
(config)# ipv6 mld host-proxy leave-proxy
```

Объяснение: Включение IPv6 MLD Leave Proxy. Чтобы предотвратить перегрузку многоадресного маршрутизатора сообщениями о выходе (leave messages), MLD snooping подавляет сообщения о выходе, если они не получены от последнего порта-участника в группе. Когда коммутатор выступает в роли запросчика (querier), функция leave proxy не будет работать.

Рекомендации:

- Команда ipv6 mld host-proxy leave-proxy является IPv6-аналогом команды ip igmp host-proxy leave-proxy. Она включает функцию проксирования выхода (Leave Proxy) для MLD в дополнение к базовой функции MLD-прокси.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Leave Proxy –** Эта функция оптимизирует обработку сообщений о выходе из многоадресной группы (MLD Done messages). Без неё, когда любой хост на любом порту покидает группу, коммутатор должен был бы переслать это сообщение вышестоящему маршрутизатору, создавая ненужную нагрузку.
- **Зачем это нужно:**
    1. **Снижение нагрузки на маршрутизатор:** Маршрутизатору не нужно обрабатывать множество сообщений о выходе от отдельных хостов, он узнает только о том, что группа полностью исчезла из сегмента сети.
    2. **Уменьшение служебного трафика:** Меньше MLD-пакетов циркулирует в сети.
- Функция не работает, если коммутатор сам является MLD Querier (запросчиком). Она предназначена для сценария, где вышестоящий маршрутизатор выполняет роль Querier, а коммутатор — только прокси.

Удаление конфигурации:

```
(config)# no ipv6 mld host-proxy leave-proxy
```

Отключает функцию MLD Leave Proxy.

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.20.3 (config)# ipv6 mld snooping

Глобальное включение функции MLD Snooping

Синтаксис:

```
(config)# ipv6 mld snooping
```

Объяснение: Глобальное включение функции MLD Snooping. При включении это устройство будет отслеживать сетевой трафик и определять, какие хосты должны получать многоадресный (multicast) трафик. Коммутатор может пассивно отслеживать (snoop) MLD-пакеты Listener Query и Report, передаваемые между IP-маршрутизаторами многоадресной рассылки и подписчиками IP-многоадресных служб, для идентификации членов многоадресной группы. Коммутатор просто отслеживает проходящие через него MLD пакеты, извлекает информацию о регистрации групп и соответствующим образом настраивает фильтры многоадресной рассылки.

Рекомендации:

- Команда ipv6 mld snooping является глобальным аналогом для IPv6 команды ip igmp snooping для IPv4. Она включает **MLD Snooping** на коммутаторе.
- MLD (Multicast Listener Discovery) — это протокол, используемый в IPv6 для управления членством в многоадресных группах (аналог IGMP в IPv4). MLD Snooping позволяет коммутатору уровня 2 "прослушивать" обмен MLD-сообщениями между маршрутизаторами и хостами, чтобы эффективно пересылать многоадресный (multicast) IPv6-трафик только на те порты, где есть подписчики, вместо рассылки во все порты VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    - ✓ **Оптимизация трафика:** Предотвращает ненужную рассылку IPv6 multicast-трафика по всем портам, экономя пропускную способность и снижая нагрузку на конечные устройства.
    - ✓ **Повышение производительности:** Снижает нагрузку на устройства, которые не должны обрабатывать ненужный им трафик.
- **Взаимосвязь с настройками по VLAN:** После глобального включения, MLD Snooping необходимо также включить на конкретных VLAN (командой `ipv6 mld snooping vlan <vlan_list>` или в интерфейсе VLAN), где планируется его использование.
- Для работы MLD Snooping в VLAN должен присутствовать MLD Querier (запросчик), обычно это IPv6 multicast-маршрутизатор. В его отсутствие коммутатор может выполнять эту роль, если настроен соответствующим образом (например, с помощью `ipv6 mld snooping querier`).

Удаление конфигурации:

```
(config)# no ipv6 mld snooping
```

Глобально отключает MLD Snooping. IPv6 многоадресный трафик будет рассылаться во все порты VLAN (широковещательно).

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.20.4 (config)# ipv6 mld snooping vlan

Включение MLD Snooping в указанных VLAN

Синтаксис:

```
(config)# ipv6 mld snooping vlan <v_vlan_list>
```

Параметры:

- <v_vlan_list>: Укажите идентификатор VLAN для MLD.

Объяснение: Включение MLD Snooping в указанных VLAN.

Рекомендации:

- Команда ipv6 mld snooping vlan активирует MLD Snooping не глобально на всех VLAN, а только в указанном списке VLAN. Это IPv6-аналог команды ip igmp snooping vlan.
- **Зачем нужно указывать VLAN:**
    - ✓ **Выборочная оптимизация:** MLD Snooping имеет смысл только в тех VLAN, где есть IPv6 multicast-трафик (например, IPTV, видеоконференции). Включение его в VLAN без такого трафика будет бесполезной тратой ресурсов.
    - ✓ **Изоляция:** В некоторых VLAN может требоваться, чтобы IPv6 multicast-трафик распространялся широковещательно (например, в тестовых средах). В таких VLAN MLD Snooping можно отключить.
- **Последовательность настройки:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Сначала MLD Snooping включается глобально (ipv6 mld snooping).
2. Затем с помощью этой команды указываются VLAN, в которых он должен работать.

- Если VLAN не указан в списке, MLD Snooping в нем будет отключен (или будет использоваться поведение по умолчанию, зависящее от реализации).

Удаление конфигурации:

```
(config)# no ipv6 mld snooping vlan [ <v_vlan_list> ]
```

Отключает MLD Snooping в указанных VLAN. Если список не указан, может отключить во всех VLAN, где он был включен этой командой.

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
> show ipv6 mld snooping mrouter [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping mrouter [ detail ]
```

Команды show ipv6 mld snooping *показывают статус по VLAN. Команда* show ipv6 mld snooping mrouter *показывает порты, выполняющие роль MLD Router Port.*

Очистка статистики:

```
# clear ipv6 mld snooping [ vlan <v_vlan_list> ] statistics
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.20.5 (config)# ipv6 mld ssm-range

Настройка диапазона адресов для Source-Specific Multicast (SSM) в IPv6

Синтаксис:

```
(config)# ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>
```

Параметры:

- <v_ipv6_mcast>: Укажите допустимый IPv6-адрес многоадресной рассылки.
- <ipv6_prefix_length>: Укажите длину префикса в диапазоне от 8 до 128.

Объяснение: Укажите диапазон SSM (Source-Specific Multicast). Эта настройка позволяет хостам и маршрутизаторам, поддерживающим SSM, использовать модель обслуживания SSM для групп в указанном диапазоне адресов.

Рекомендации:

- Команда ipv6 mld ssm-range является IPv6-аналогом команды ip igmp ssm-range. Она определяет диапазон многоадресных (multicast) IPv6-адресов, для которых будет применяться модель **Source-Specific Multicast (SSM)**.
- **SSM в IPv6**
    - ✓ В стандартной ASM (Any-Source Multicast) клиент подписывается на группу и получает трафик от любого источника, передающего в эту группу.
    - ✓ В модели SSM клиент подписывается на конкретный источник и группу одновременно

SEC.RU | Короткий путь к информации Скачано с sec.ru

(например, (2001:db8::10, ff3e::1)). Это повышает безопасность и упрощает управление, так как исключает возможность получения трафика от нежелательных источников.

- **Стандартный диапазон SSM для IPv6:** Согласно IANA, для SSM в IPv6 выделен диапазон адресов **FF3x::/32** (где x — любые флаги). Однако данная команда позволяет администратору переопределить или сузить этот диапазон, если это требуется.
- Для MLD-запросов, попадающих в указанный диапазон, коммутатор и подключенные к нему маршрутизаторы будут ожидать и обрабатывать сообщения в формате MLDv2 (который поддерживает указание источника). Более старая версия MLDv1 не будет корректно работать в этом диапазоне.
- Эта команда обычно требуется только в том случае, если необходимо использовать нестандартный диапазон адресов для SSM. По умолчанию устройства могут поддерживать стандартный диапазон без дополнительной настройки.

Удаление конфигурации:

```
(config)# no ipv6 mld ssm-range
```

Удаляет настройку нестандартного диапазона SSM, возвращаясь к поведению по умолчанию.

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.20.6 (config)# ipv6 mld unknown-flooding

Настройка обработки неизвестного IPv6 многоадресного трафика

Синтаксис:

```
(config)# ipv6 mld unknown-flooding
```

Объяснение: Включение режима пересылки для незарегистрированного (к которому не присоединились) IP-многоадресного трафика.

Рекомендации:

- Команда ipv6 mld unknown-flooding является IPv6-аналогом команды ip igmp unknown-flooding. Она определяет, как коммутатор должен обрабатывать IPv6 многоадресный (multicast) трафик, для которого в таблице MLD Snooping нет ни одного подписчика (незарегистрированный трафик).
- **Два режима работы:**
  - ✓ **Режим (flooding) - команда включена (**ipv6 mld unknown-flooding**):** Если для многоадресной группы нет подписчиков, коммутатор будет рассылать этот трафик во все порты VLAN. Это поведение похоже на широковещательную рассылку (broadcast).
  - ✓ **Режим (dropping) - команда отключена (**no ipv6 mld unknown-flooding**):** Если для многоадресной группы нет подписчиков, коммутатор будет отбрасывать этот трафик. Он не будет отправлен ни на один порт.
- **Зачем это нужно и что выбрать:**
  - ✓ ipv6 mld unknown-flooding **:** Выбирается для обеспечения совместимости с устаревшими приложениями или протоколами, которые могут полагаться на

SEC.RU | Короткий путь к информации Скачано с sec.ru

широковещательную природу многоадресной рассылки. Однако это создает избыточный трафик в сети и может снижать производительность, особенно если много неизвестного multicast-трафика.

- ✓ no ipv6 mld unknown-flooding (рекомендуется для современных сетей)**:** Является более эффективным и безопасным режимом. Он предотвращает ненужное распространение IPv6 многоадресного трафика, к которому никто не проявил интереса, экономя пропускную способность и ресурсы устройств. Этот режим является стандартным для MLD Snooping.

- В большинстве современных сетей, где MLD Snooping настроен корректно, рекомендуется отключать эту функцию (no ipv6 mld unknown-flooding).

Удаление конфигурации:

```
(config)# no ipv6 mld unknown-flooding
```

Отключает режим затопления (включает режим отбрасывания) для неизвестного IPv6 многоадресного трафика.

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
> show ipv6 mld snooping mrouter [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping mrouter [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.20.7 (config)# ipv6 route

Настройка статического IPv6-маршрута

Синтаксис:

```
(config)# ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }
```

Параметры:

- <v_ipv6_subnet>: Укажите IPv6-адрес сети назначения в формате X:X:X:X::X/<0-128> (например, 2001:db8:1::/64).
- { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }: Укажите один из вариантов. Это может быть либо одноадресный (unicast) IPv6-адрес следующего перехода (next-hop), либо интерфейс и IPv6-адрес.
    - ✓ <v_ipv6_ucast>: IPv6-адрес следующего перехода (шлюза).
    - ✓ interface vlan <v_vlan_id> <v_ipv6_addr>: Можно указать исходящий интерфейс (VLAN) и IPv6-адрес следующего перехода (некоторые реализации позволяют указывать только интерфейс для маршрутов к непосредственно подключенным сетям).

Объяснение: Настройка статического IPv6-маршрута.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `ipv6 route` является IPv6-аналогом команды `ip route` для IPv4. Она создает статический маршрут в таблице маршрутизации IPv6 коммутатора уровня 3 (L3).
- Наиболее важное применение — маршрут по умолчанию (default route) для IPv6:
    - ✓ Если сеть назначения не совпадает ни с одним из более конкретных маршрутов и не является непосредственно подключенной сетью, используется маршрут по умолчанию.
    - ✓ Синтаксис для маршрута по умолчанию: `ipv6 route ::/0 <IPv6_адрес_шлюза>`. Префикс `::/0` означает "любой IPv6-адрес".
- Два способа указания next-hop**:**
    - ✓ **Через адрес шлюза:** Наиболее распространенный способ. Указывается IP-адрес следующего маршрутизатора, который должен быть доступен через один из интерфейсов VLAN коммутатора.
    - ✓ **Через интерфейс (и адрес):** Может использоваться для указания маршрутов к непосредственно подключенным сетям или в некоторых специальных случаях.
- Для работы статической маршрутизации IPv6 необходимо, чтобы на коммутаторе была глобально включена маршрутизация (`ip routing`, которая включает и IPv4, и IPv6, или отдельная команда `ipv6 routing`). Если поддерживается коммутатором.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }
```

Удаляет указанный статический IPv6-маршрут.

Просмотр:

```
# show ipv6 route [ interface vlan <v_vlan_list> ]
```

2.7.20.8 (config-if)# ipv6 mld snooping filter

Применение профиля фильтрации MLD к порту

Синтаксис:

```
(config-if)# ipv6 mld snooping filter <profile_name>
```

Объяснение: Используйте эту команду для фильтрации определенного многоадресного (multicast) трафика на уровне порта.

Параметры:

- <profile_name>: Укажите имя настроенного профиля (IPMC-профиля), содержащего список многоадресных групп, доступ к которым запрещен на порту. Когда определенная многоадресная группа выбрана на порту, MLD-сообщения о присоединении (join reports), полученные на этом порту, отбрасываются.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда ipv6 mld snooping filter является IPv6-аналогом команды ip igmp snooping filter. Она применяет заранее созданный IPMC-профиль (который содержит правила permit/deny для диапазонов IPv6 multicast-адресов) к конкретному порту.
- **Зачем это нужно:** Позволяет администратору реализовать политики контроля доступа к IPv6 многоадресным потокам на уровне портов. Например, можно запретить пользователям на определенном порту подписываться на определенные IPv6 multicast-каналы.
- **Принцип работы:**
    1. Создается IPMC-профиль (например, BLOCK_IPV6_VIDEO), в котором с помощью правил range ... deny перечислены запрещенные IPv6 многоадресные группы (например, ff3e::1/128).
    2. На порту доступа применяется команда ipv6 mld snooping filter BLOCK_IPV6_VIDEO.
    3. Когда на этот порт приходит MLD-запрос (Report) на подписку на группу из списка запрещенных, коммутатор отбрасывает (drop) этот запрос, и клиент не получает трафик.
    4. Запросы на группы, не входящие в запрещенный список, обрабатываются обычным образом.
- Эта функция является важным инструментом управления IPv6 multicast-трафиком и повышения безопасности.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no ipv6 mld snooping filter
```

Удаляет привязку профиля фильтрации с порта. Фильтрация IPv6 multicast-трафика на этом порту прекращается.

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```

Информация о примененных фильтрах может отображаться в детальном выводе по MLD Snooping или по конкретным интерфейсам.

2.7.20.9 (config-if)# ipv6 mld snooping immediate-leave

Включение функции немедленного выхода (Fast Leave) для MLD на порту

Синтаксис:

```
(config-if)# ipv6 mld snooping immediate-leave
```

Объяснение: Включение функции быстрого выхода (fast leave) на конкретном порту. Когда получен пакет Leave (о выходе из группы), коммутатор немедленно удаляет порт из многоадресной службы, не отправляя на этот интерфейс MLD-запрос, специфичный для группы

SEC.RU | Короткий путь к информации Скачано с sec.ru

(Group-Specific Query). (В описании опечатка: указано IGMP вместо MLD, но по смыслу это MLD для IPv6.)

Рекомендации:

- Команда ipv6 mld snooping immediate-leave является IPv6-аналогом команды ip igmp snooping immediate-leave. Она активирует на порту функцию немедленного выхода (Immediate Leave / Fast Leave) для протокола MLD (Multicast Listener Discovery).
- Стандартный процесс выхода из IPv6 multicast-группы (без Immediate Leave):
    1. Клиент отправляет MLD-сообщение Done (аналог Leave в IPv4), сообщая, что больше не хочет получать трафик определенной многоадресной группы.
    2. Коммутатор, получив Done, не может сразу удалить порт, так как на нем могут быть другие клиенты, все еще заинтересованные в этой группе.
    3. Поэтому коммутатор отправляет на этот порт Multicast Address Specific Query (запрос, специфичный для группы), чтобы проверить, есть ли еще подписчики.
    4. Если в течение определенного времени (Last Member Query Interval) не приходит ответа, порт удаляется из списка получателей группы.
- Процесс с включенным Immediate Leave:
    1. Клиент отправляет MLD-сообщение Done.
    2. Коммутатор немедленно удаляет порт из списка получателей группы, не отправляя дополнительный запрос.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    1. **Быстрое освобождение ресурсов:** Ускоряет процесс прекращения передачи ненужного IPv6 multicast-трафика на порт, экономя полосу пропускания.
    2. **Снижение задержек при переключении каналов:** Критически важно для приложений, чувствительных к задержкам, таких как IPv6-телевидение (IPTv6).
- Immediate Leave следует включать только на портах, к которым подключено максимум одно устройство-подписчик (например, один IP-телевизор). Если к порту подключено несколько устройств, использование Immediate Leave приведет к тому, что при выходе одного из них все остальные также потеряют доступ к группе.

Удаление конфигурации:

```
(config-if)# no ipv6 mld snooping immediate-leave
```

Отключает функцию немедленного выхода на порту, возвращаясь к стандартному процессу с отправкой Group-Specific Query.

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.20.10 (config-if)# ipv6 mld snooping max-groups

Ограничение количества IPv6 многоадресных групп на порту

Синтаксис:

```
(config-if)# ipv6 mld snooping max-groups <throttling>
```

Объяснение: Укажите максимальное количество MLD групп, к которым порт может присоединиться одновременно.

Параметры:

- <throttling>: Это поле ограничивает максимальное количество многоадресных групп, к которым порт может присоединиться одновременно. Когда на порту достигнуто максимальное количество, любые новые MLD-запросы на присоединение (join reports) будут отброшены. По умолчанию выбрано неограниченное количество (unlimited). Допустимый диапазон значений от 1 до 10 (в данной реализации).

Рекомендации:

- Команда ipv6 mld snooping max-groups является IPv6-аналогом команды ip igmp snooping max-groups. Она вводит ограничение (порог, throttling) на количество IPv6 многоадресных групп, в которых может одновременно состоять данный порт.
- **Зачем это нужно:**
    - ✓ **Защита от истощения ресурсов (DoS-атака):** Предотвращает ситуацию, когда один порт пытается подписаться на огромное количество IPv6

SEC.RU | Короткий путь к информации Скачано с sec.ru

multicast-потоков, что может исчерпать аппаратные ресурсы (TCAM) коммутатора, предназначенные для хранения multicast-записей, и повлиять на работу других портов.

- ✓ **Контроль доступа:** Позволяет административно ограничить количество IPv6 multicast-каналов, которые может просматривать пользователь на данном порту.

- **Принцип работы:** Коммутатор ведет подсчет активных IPv6 multicast-групп для каждого порта. Когда порт достигает лимита (<throttling>), все последующие MLD-запросы на присоединение к новым группам игнорируются/отбрасываются. Уже существующие подписки продолжают работать.
- Значение по умолчанию: не ограничено. Рекомендуется устанавливать разумные пределы, особенно на пользовательских портах доступа. Указанный в параметрах диапазон 1-10 может быть мал для некоторых приложений

Удаление конфигурации:

```
(config-if)# no ipv6 mld snooping max-groups
```

Снимает ограничение на количество групп для порта (возврат к значению "unlimited").

Просмотр:

```
> show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
# show ipv6 mld snooping [ vlan <v_vlan_list> ] [ group-database [ interface ( <port_type> [ <v_port_type_list> ] ) ] [ sfm-information ] ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.21 Настройка LACP (Link Aggregation Control Protocol) (config)# lacp

2.7.21.1 (config)# lacp system-priority

Настройка системного приоритета LACP

Синтаксис:

```
(config)# lacp system-priority <v_1_to_65535>
```

Параметры:

- <v_1_to_65535>: Приоритет системы. Допустимый диапазон значений: от 1 до 65535.

Объяснение: Настройка системного приоритета для функции LACP. Меньшее число означает более высокий приоритет. Это значение приоритета определяет, какие порты будут активными, а какие — в резервной роли.

Рекомендации:

- Команда *lacp system-priority* задает глобальный приоритет системы (System Priority) для протокола LACP. Этот приоритет используется в процессе выбора, какие порты войдут в агрегированный канал (LAG) и какой из коммутаторов будет управлять агрегацией.
- При формировании LACP-канала между двумя устройствами, они обмениваются своими системными идентификаторами (System ID), которые состоят из системного приоритета (System Priority) и MAC-адреса системы (System MAC). Устройство

SEC.RU | Короткий путь к информации Скачано с sec.ru

с меньшим (более высоким) системным приоритетом становится "лидирующим" в процессе принятия решений о состоянии портов (активный/резервный).

- **Влияние на порты:** Внутри самого коммутатора этот приоритет также влияет на выбор активных и резервных портов в пределах одной системы (хотя основную роль здесь играет приоритет порта).
- **Значение по умолчанию:** Обычно равно 32768. Изменять его имеет смысл, когда нужно гарантировать, что конкретный коммутатор в паре будет иметь более высокий приоритет (например, более мощное ядро сети).

Удаление конфигурации:

```
(config)# no lacp system-priority <v_1_to_65535>
```

Сбрасывает системный приоритет к значению по умолчанию (обычно 32768).

Просмотр:

```
# show lacp { internal | statistics | system-id | neighbour }
```

Команда show lacp system-id *отображает текущий системный приоритет и системный MAC-адрес.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.21.2 (config-if)# lacp

Включение LACP на интерфейсе

Синтаксис:

```
(config-if)# lacp
```

Объяснение: Включение LACP на данном интерфейсе.

Рекомендации:

- Команда lacp, выполняемая в режиме конфигурации интерфейса ((config-if)#), активирует протокол LACP (Link Aggregation Control Protocol) на конкретном порту. Это позволяет порту участвовать в динамическом формировании агрегированного канала (LAG).
- **Что происходит после включения:**
    1. Порт начинает обмениваться LACP-пакетами (LACPDU) с соседним устройством.
    2. Если на другом конце также включен LACP и порты объединены в одну группу, они могут автоматически сформировать агрегированный канал.
    3. LACP автоматически управляет состоянием портов: добавляет их в канал, удаляет при сбоях, балансирует нагрузку.
- Для создания LACP-канала необходимо:
    1. Включить LACP на всех портах, которые должны войти в канал (на обоих устройствах).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Объединить эти порты в одну логическую группу (LAG) с помощью соответствующей команды.
3. Убедиться, что настройки портов (скорость, дуплекс, VLAN) совместимы.

Удаление конфигурации:

```
(config-if)# no lacp
```

Отключает LACP на интерфейсе. Порт перестает участвовать в LACP-переговорах и будет удален из любых динамических агрегированных каналов.

Просмотр:

```
# show lacp { internal | statistics | system-id | neighbour }
```

Эти команды показывают статус LACP на портах: internal *— внутренние параметры,* neighbour *— информацию о соседних устройствах,* statistics *— статистику LACPDU.*

Очистка:

```
# clear lacp statistics
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.21.3 (config-if)# lacp key

Настройка ключа LACP для интерфейса

Синтаксис:

```
(config-if)# lacp key { <v_1_to_65535> | auto }
```

Объяснение: Настройка ключа LACP для данного интерфейса.

Параметры:

- { <v_1_to_65535> | auto }: Укажите ключ LACP для этого интерфейса.
    - ✓ auto: Устанавливает ключ автоматически, в зависимости от скорости физического линка.
    - ✓ <v_1_to_65535>: Если вы хотите задать ключ вручную, введите значение от 1 до 65535. Порты в одной агрегированной группе должны иметь одинаковый ключ LACP порта. Чтобы позволить порту присоединиться к агрегированной группе, ключ порта должен быть установлен в то же значение.

Рекомендации:

- Команда lacp key задает **ключ (Key)** для порта в контексте LACP. Ключ — это числовой идентификатор, который объединяет порты в одну логическую группу (LAG) на данном коммутаторе.
- **Как это работает:**
    1. Все порты, которые должны войти в один и тот же LACP-канал, должны иметь одинаковый ключ.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. LACP использует этот ключ, чтобы определить, какие порты могут быть агрегированы вместе. Пакеты LACPDU, отправляемые соседу, содержат этот ключ, чтобы соседнее устройство также понимало принадлежность портов к группе.
3. Ключ, наряду с приоритетами, используется для определения того, какие порты будут активны, а какие — в резерве (standby) в пределах одной системы.

- **Режим** auto**:** Удобен для автоматического создания групп на основе скорости портов. Например, все гигабитные порты могут автоматически получить один ключ, а все 10-гигабитные — другой. Однако для точного контроля обычно используется ручное задание ключа.
- **Ручное задание ключа (рекомендуется):** Администратор сам назначает одинаковый ключ (например, 100) для всех портов, которые должны образовать канал. Это дает полный контроль над составом группы.

Удаление конфигурации:

```
(config-if)# no lacp key { <v_1_to_65535> | auto }
```

Удаляет настройку ключа. Порт может вернуться к значению по умолчанию или перестать быть частью LACP-группы.

Просмотр:

```
# show lacp { internal | statistics | system-id | neighbour }
```

Команда show lacp internal *отображает ключи, назначенные портам.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.21.4 (config-if)# lacp port-priority

Настройка приоритета порта LACP

Синтаксис:

```
(config-if)# lacp port-priority <v_1_to_65535>
```

Объяснение: Настройка ключа LACP для этого интерфейса. (Опечатка в оригинале: должно быть "Настройка приоритета порта LACP для этого интерфейса".)

Параметры:

- <v_1_to_65535>: Укажите приоритет порта LACP для этого интерфейса. Меньшее число означает более высокий приоритет. Это значение приоритета определяет, какие порты будут активными, а какие — в резервной роли.

Рекомендации:

- Команда lacp port-priority задает приоритет конкретного порта в рамках LACP. Этот приоритет используется для принятия решения о том, какие порты будут активными, а какие перейдут в режим ожидания (standby), если количество портов в агрегированной группе превышает максимально допустимое.
- **Как это работает:**
    1. В агрегированном LACP-канале может быть ограничение на максимальное количество активных портов (например, 8).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Если в группе больше портов, чем разрешено, LACP выбирает, какие из них будут активны, на основе **приоритета порта**.
3. Порты с **меньшим (более высоким) приоритетом** становятся активными. Порты с большим (более низким) приоритетом переходят в состояние ожидания (standby) и активируются только в случае выхода из строя одного из активных портов.

- **Взаимодействие с системным приоритетом:** Сначала сравниваются системные приоритеты коммутаторов, затем, внутри одной системы, для выбора активных портов используется приоритет порта.
- **Значение по умолчанию:** Обычно равно 32768. Изменять его имеет смысл, чтобы гарантировать, что определенные порты (например, более высокоскоростные или подключенные к более важным линкам) будут активны в первую очередь.

Удаление конфигурации:

```
(config-if)# no lacp port-priority <v_1_to_65535>
```

Сбрасывает приоритет порта к значению по умолчанию (обычно 32768).

Просмотр:

```
# show lacp { internal | statistics | system-id | neighbour }
```

Команда show lacp internal *отображает приоритеты портов.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.21.5 (config-if)# lacp role

Настройка роли LACP для интерфейса

Синтаксис:

```
(config-if)# lacp role { active | passive }
```

Объяснение: Настройка роли LACP для этого интерфейса.

Параметры:

- { active | passive }: Укажите роль "Active" или "Passive" в зависимости от возможности устройства вести переговоры и отправлять управляющие пакеты LACP.
    - ✓ active **(Активная):** Порты, назначенные как "Active", способны обрабатывать и отправлять управляющие кадры LACP. Это позволяет устройствам, поддерживающим LACP, вести переговоры об агрегированном канале, чтобы группа могла динамически изменяться по мере необходимости.
    - ✓ passive **(Пассивная):** Порты в пассивном режиме отвечают на LACP-пакеты, но не инициируют соединение

Рекомендации:

- Команда lacp role определяет, будет ли порт активно инициировать установление LACP-соединения или только пассивно отвечать на запросы от соседа.
- **Как это работает:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ active **(Активный):** Порт периодически отправляет LACP-пакеты (LACPDU) для инициирования и поддержания агрегированного канала. Он может начать переговоры в любой момент.
- ✓ passive **(Пассивный):** Порт не отправляет LACP-пакеты по своей инициативе. Он только отвечает на LACP-пакеты, полученные от соседнего устройства, настроенного в режиме active. Если оба конца настроены как passive, LACP-канал не сформируется.

- Чтобы добавить или удалить порты из группы, по крайней мере одно из участвующих устройств должно быть настроено на роль active. Второе устройство может быть active или passive.
- **Типичные сценарии:**
  - ✓ **Рекомендуется:** Настраивать оба конца как active. Это наиболее надежный и быстрый способ установления связи.
  - ✓ **Сценарий с** passive**:** Может использоваться на стороне, которая не должна инициировать соединение (например, на старом оборудовании или в особых конфигурациях), но обычно предпочтительнее active.

Удаление конфигурации:

```
(config-if)# no lacp role { active | passive }
```

Сбрасывает роль LACP порта к значению по умолчанию (обычно passive *или зависит от реализации).*

Просмотр:

```
# show lacp { internal | statistics | system-id | neighbour }
```

Команда отображает роль и состояние LACP на портах.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.21.6 (config-if)# lacp timeout

Настройка тайм-аута LACP

Синтаксис:

```
(config-if)# lacp timeout { fast | slow }
```

Объяснение: Настройка режима тайм-аута.

Параметры:

- { fast | slow }: Тайм-аут управляет периодом между передачами BPDU (LACPDU). Режим fast будет передавать LACP-пакеты каждую секунду, в то время как режим slow будет ждать 30 секунд перед отправкой следующего LACP-пакета.

Рекомендации:

- Команда lacp timeout задает интервал, с которым порт отправляет LACP-пакеты (LACPDU) и, соответственно, как быстро он обнаружит потерю связи с партнером.
- **Два режима:**
  - ✓ fast **(быстрый):** LACP-пакеты отправляются каждую 1 секунду. Если в течение 3 интервалов (т.е. 3 секунд) не получен ответ от партнера, порт считается вышедшим из строя, и LACP инициирует переключение на резервный порт (если он есть). Обеспечивает очень быстрое обнаружение сбоев (менее 3 секунд).
  - ✓ slow **(медленный):** LACP-пакеты отправляются каждые 30 секунд. Для обнаружения сбоя потребуется 3

SEC.RU | Короткий путь к информации Скачано с sec.ru

интервала (90 секунд). Используется для снижения служебного трафика, но ценой более медленной реакции на отказы.

- **Выбор режима:**
  - ✓ fast (рекомендуется): Для большинства сетей, где важна быстрая сходимость при отказах (например, в ядре сети, для критически важных линков).
  - ✓ slow**:** Может использоваться на менее критичных линках или в сетях, где служебный трафик LACP необходимо минимизировать.
- Важно, чтобы режим тайм-аута был согласован (или, по крайней мере, совместим) с настройками на соседнем устройстве, хотя LACP может работать и с разными значениями, но это может привести к неоптимальной работе.

Удаление конфигурации:

```
(config-if)# no lacp timeout { fast | slow }
```

Сбрасывает режим тайм-аута к значению по умолчанию

Просмотр:

```
# show lacp { internal | statistics | system-id | neighbour }
```

Команда show lacp internal *отображает настроенный и используемый тайм-аут для портов.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.22 Настройка линий (терминалов) (config)# line

2.7.22.1 (config)# line

Вход в режим конфигурации линии

Синтаксис:

```
(config)# line { <0~16> | console 0 | vty <0~15> }
```

Объяснение: Вход в режим конфигурации конкретной линии (терминала). При нажатии Enter командная строка изменится на (config-line)#.

Параметры:

- { <0~16> | console 0 | vty <0~15> }: Укажите один из вариантов.
  - ✓ <0~16>: Список номеров линий (может использоваться для прямого указания).
  - ✓ console 0: Линия консольного подключения (физический консольный порт).
  - ✓ vty <0~15>: Линии VTY (Virtual Terminal lines) — это виртуальные терминальные линии устройства, используемые исключительно для управления входящими Telnet/SSH-соединениями. Они являются виртуальными в том смысле, что являются функцией программного обеспечения — с ними не связано никакое аппаратное обеспечение.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда line используется для перехода в режим конфигурации линий (линий терминала)**.** В этом режиме ((config-line)#) настраиваются параметры, общие для определенного типа доступа: консольного (console) или удаленного по Telnet/SSH (vty).
- **Типы линий:**
  - ✓ console 0**:** Относится к физическому консольному порту. Настройки, примененные здесь, влияют на сессии, установленные через этот порт.
  - ✓ vty 0 15 **(**или vty <0~15>**) :** Относится к виртуальным терминальным линиям. Обычно их несколько (например, от 0 до 15), что позволяет нескольким администраторам одновременно подключаться к коммутатору по сети. Настройки, примененные здесь, влияют на все Telnet/SSH-сессии.
- **Что настраивается в режиме** (config-line)#**:**
  - ✓ Пароль для входа (password).
  - ✓ Тайм-аут бездействия (exec-timeout).
  - ✓ Размер истории команд (history size).
  - ✓ Протоколы, разрешенные для входа (transport input).
  - ✓ Уровень привилегий при входе (privilege level).
  - ✓ И другие параметры сессии.

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```

Отображает статус и настройки линий. Ключевое слово alive *показывает только активные сессии.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.22.2 (config-line)# do

Выполнение команд привилегированного режима из режима конфигурации линии

Синтаксис:

```
(config-line)# do <command>
```

Объяснение: Выполнение команд режима EXEC.

Параметры:

- <command>: Введите команду режима EXEC.

Рекомендации:

- Команда do, доступная в любом режиме конфигурации (включая (config-line)#), позволяет выполнять команды привилегированного режима EXEC (Exec mode, #), не выходя из текущего режима настройки.
- Часто при настройке возникает необходимость быстро проверить текущее состояние (например, посмотреть таблицу MAC-адресов, проверить статус интерфейса, посмотреть версию ПО) или сохранить конфигурацию. Вместо того чтобы выходить из режима конфигурации с помощью exit или end, а затем снова входить в него, можно просто набрать do show ....
- **Примеры использования:**
    - ✓ (config-line)# do show running-config interface Gi1/1 — просмотреть конфигурацию интерфейса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ (config-line)# do show ip interface brief — проверить IP-адреса.
- ✓ (config-line)# do copy running-config startup-config — сохранить конфигурацию.

- Команда do работает во всех режимах конфигурации: (config)#, (config-if)#, (config-line)#, (config-vlan)# и т.д.

2.7.22.3 (config-line)# exec-banner

Включение отображения баннера EXEC

Синтаксис:

(config-line)# exec-banner

Объяснение: Включение отображения баннера EXEC.

Рекомендации:

- Команда exec-banner в режиме конфигурации линии ((config-line)#) управляет отображением баннера EXEC (баннера, настроенного командой banner exec) для данной линии (консольной или VTY).
- **баннер EXEC –** Это сообщение, которое отображается пользователю после успешной аутентификации, но до появления приглашения командной строки (> или #). Обычно содержит информацию о правилах использования системы, предупреждения или приветствия.
- Как это работает:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Если баннер EXEC был настроен глобально (banner exec ...), то с помощью команды exec-banner на линии можно разрешить его отображение для данной линии. По умолчанию эта функция может быть включена.
- ✓ Команда no exec-banner отключает отображение баннера EXEC для данной конкретной линии, даже если он настроен глобально. Это может быть полезно, например, для консольной линии, чтобы ускорить вход, или для определенных VTY-линий, используемых скриптами.

- Эта команда действует независимо от баннера входа (login banner), который отображается до аутентификации и управляется командой login-banner.

Удаление конфигурации:

```
(config-line)# no exec-banner
```

Отключает отображение баннера EXEC для данной линии.

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```

Статус отображения баннера может отображаться в выводе команды show line*.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.22.4 (config-line)# exec-timeout

Настройка тайм-аута бездействия для линии

Синтаксис:

```
(config-line)# exec-timeout <min> [ <sec> ]
```

Параметры:

- <min>: Укажите тайм-аут в минутах. Допустимый диапазон от 0 до 1440.
- [<sec>]: Укажите тайм-аут в секундах (необязательно). Допустимый диапазон от 0 до 3600.

Объяснение: Настройка тайм-аута бездействия для линии.

Рекомендации:

- Команда exec-timeout задает время бездействия (idle timeout) для терминальной сессии на данной линии (консольной или VTY). Если в течение указанного времени пользователь не вводит никаких команд, сессия автоматически завершается.
- В отличие от terminal exec-timeout**:** Эта команда устанавливает глобальное значение тайм-аута для всех сессий, подключающихся через данную линию. Оно сохраняется в конфигурации и действует постоянно. Команда terminal exec-timeout меняет тайм-аут только для текущей сессии.
- **Значения:**
    - ✓ exec-timeout 0 0 – Тайм-аут отключен. Сессия никогда не будет разорвана по причине бездействия (не

SEC.RU | Короткий путь к информации Скачано с sec.ru

рекомендуется по соображениям безопасности, кроме консоли в защищенном помещении).

- ✓ `exec-timeout 5 0` – 5 минут бездействия.
- ✓ `exec-timeout 0 30` – 30 секунд бездействия.

- **Зачем это нужно:**
  - ✓ **Безопасность:** Предотвращает несанкционированный доступ, если администратор забыл завершить сессию.
  - ✓ **Освобождение ресурсов:** Закрывает неиспользуемые сессии, освобождая VTY-линии для новых подключений.
- Рекомендуется устанавливать разумные тайм-ауты (например, 5-10 минут) для VTY-линий. Для консольной линии в защищенном помещении часто оставляют `0 0`.

Удаление конфигурации:

```
(config-line)# no exec-timeout
```

Сбрасывает тайм-аут для линии к значению по умолчанию (зависит от устройства, часто 10 минут или 0).

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.22.5 (config-line)# help

Отображение справки

Синтаксис:

```
(config-line)# help
```

Объяснение: Показать пояснение по справке (Help).

Рекомендации:

- Команда help в режиме конфигурации линии (config-line)# аналогична команде help в других режимах. Она выводит краткое текстовое описание того, как пользоваться встроенной системой контекстной справки, активируемой символом ?.
- Напоминает пользователю, что для получения списка доступных команд в текущем режиме или для уточнения синтаксиса конкретной команды нужно использовать знак вопроса ?.
- Сама команда help не предоставляет список команд, доступных в режиме (config-line)#. Для этого нужно использовать ?.
- Сообщение, выводимое командой help, обычно статично и не зависит от текущего режима.

2.7.22.6 (config-line)# history size

Настройка размера истории команд для линии

Синтаксис:

```
(config-line)# history size <history_size>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Управление количеством отображаемых команд в истории.

Параметры:

- <history_size>: Допустимый диапазон от 0 до 32. Значение 0 означает "отключено".

Рекомендации:

- Команда history size задает глобальный размер буфера истории команд для всех сессий, подключающихся через данную линию (консольную или VTY). История команд позволяет пользователю просматривать и повторно вызывать ранее введенные команды с помощью клавиш Стрелка вверх и Стрелка вниз.
- В отличие от terminal history size**:** Эта команда устанавливает глобальное значение размера истории для линии, которое сохраняется в конфигурации. Команда terminal history size меняет размер истории только для текущей сессии.
- **Значения:**
  - ✓ history size 0 – История команд отключена. Навигация по предыдущим командам невозможна.
  - ✓ history size 20 – Будет сохраняться до 20 последних команд.
- **Зачем это нужно:**
  - ✓ **Удобство:** Позволяет быстро повторять длинные или сложные команды без повторного набора.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Диагностика:** Можно просмотреть, какие команды выполнялись ранее в сессии.

- Увеличение размера истории полезно для длительных сеансов настройки. Слишком маленький размер может быть неудобен.

Удаление конфигурации:

```
(config-line)# no history size
```

Сбрасывает размер истории для линии к значению по умолчанию (зависит от устройства, часто 10).

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```

2.7.22.7 (config-line)# length

Настройка длины экрана (количества строк) для линии

Синтаксис:

```
(config-line)# length <length>
```

Объяснение: Настройка количества строк, отображаемых на экране.

Параметры:

- <length>: Укажите количество строк, отображаемых на экране. Допустимый диапазон от 3 до 512. Укажите 0 для отключения постраничного вывода (без пауз).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда length задает глобальное значение длины экрана (постраничного вывода) для всех сессий, подключающихся через данную линию.
- В отличие от terminal length**:** Эта команда устанавливает глобальное значение для линии, сохраняемое в конфигурации. Команда terminal length меняет длину только для текущей сессии.
- **Значения:**
    - ✓ 0 – Отключает постраничный вывод. Вся информация выводится непрерывно, без пауз. Удобно при копировании вывода или работе через скрипты.
    - ✓ 24 (или другое значение, например, 30) – Устанавливает паузу после указанного количества строк.
- Позволяет настроить удобный размер экрана для разных типов подключений. Например, для консоли можно оставить значение по умолчанию, а для VTY-сессий, используемых скриптами, установить 0, чтобы вывод не зависал в ожидании нажатия пробела.
- Эта настройка действует на все сессии, подключаемые к данной линии, но пользователь может переопределить её для своей текущей сессии командой terminal length.

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.22.8 (config-line)# location

Настройка описательного местоположения линии

Синтаксис:

```
(config-line)# location <location>
```

Объяснение: Настройка описательного местоположения данного устройства (линии).

Параметры:

- <location>: Описание местоположения для терминала. Допустимое количество символов — 32.

Рекомендации:

- Команда location позволяет добавить текстовое описание (комментарий), указывающее физическое или логическое местоположение данной линии (консольной или VTY).
- **Зачем это нужно:**
  - ✓ Помогает администраторам понять, где физически находится устройство или для каких целей предназначена данная линия. Например, "Console port in server room rack 3" или "VTY lines for management network".
  - ✓ Упрощает управление и аудит конфигурации.
- Описание не влияет на работу линии, оно служит исключительно для информационных целей и может отображаться в некоторых командах show.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Эта команда применяется к конкретной линии (например, line console 0 или line vty 0 15). Описание, заданное для диапазона VTY-линий, будет относиться ко всем линиям в этом диапазоне.

Удаление конфигурации:

```
(config-line)# no location
```

Удаляет описание местоположения для данной линии.

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```

Описание местоположения может отображаться в выводе команды show line*.*

2.7.22.9 (config-line)# motd-banner

Включение отображения баннера "Сообщение дня" (MOTD)

Синтаксис:

```
(config-line)# motd-banner
```

Объяснение: Включение отображения баннера MOTD (сообщение дня).

Рекомендации:

- Команда motd-banner в режиме конфигурации линии ((config-line)#) управляет отображением баннера MOTD (Message of the Day) для данной линии (консольной или VTY).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **MOTD –** Это сообщение, которое отображается пользователю сразу после подключения к устройству, но до запроса имени пользователя и пароля. Обычно содержит общие уведомления, предупреждения о несанкционированном доступе или информацию о предстоящих работах.
- **Как это работает:**
    - ✓ Если баннер MOTD был настроен глобально (banner motd ...), то с помощью команды motd-banner на линии можно разрешить его отображение для данной линии. По умолчанию эта функция может быть включена.
    - ✓ Команда no motd-banner отключает отображение баннера MOTD для данной конкретной линии, даже если он настроен глобально. Это может быть полезно для определенных VTY-линий, используемых скриптами, чтобы ускорить подключение.
- Эта команда действует независимо от баннера входа (login banner) и баннера EXEC.

Удаление конфигурации:

```
(config-line)# no motd-banner
```

Отключает отображение баннера MOTD для данной линии.

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```

Статус отображения баннера MOTD может отображаться в выводе команды show line*.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.22.10 (config-line)# privilege level

Настройка уровня привилегий для терминальной линии

Синтаксис:

```
(config-line)# privilege level <privileged_level>
```

Объяснение: Настройка уровня привилегий для терминальной линии.

Параметры:

- <privileged_level>: Уровень привилегий для терминальной линии. Допустимый диапазон от 0 до 15.

Рекомендации:

- Команда privilege level задает уровень привилегий по умолчанию, с которым пользователь будет попадать в CLI после успешной аутентификации на данной линии (консольной или VTY).
- **Уровни привилегий:**
    - ✓ **Уровень 1:** Пользовательский режим (>). Команды только для просмотра и базовой диагностики (по умолчанию для многих линий).
    - ✓ **Уровни 2-14:** Промежуточные уровни, которые могут быть настроены администратором для предоставления ограниченного доступа к определенным командам.
    - ✓ **Уровень 15:** Привилегированный режим (#). Полный доступ ко всем командам (включая конфигурационные).
- **Как это работает:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Если на линии настроен privilege level 15, пользователь после ввода логина/пароля сразу попадет в привилегированный режим EXEC (с приглашением #), и ему не нужно будет вводить команду enable.
- ✓ Если настроен privilege level 1, пользователь попадет в пользовательский режим (>) и для выполнения команд конфигурации ему нужно будет ввести enable и пароль.

- **Зачем это нужно:**
  - ✓ **Удобство:** Для консольной линии в защищенном помещении часто устанавливают уровень 15, чтобы сразу иметь полный доступ.
  - ✓ **Безопасность:** Для VTY-линий (удаленный доступ) обычно оставляют уровень 1, требуя дополнительной аутентификации enable для повышения привилегий.
- **Взаимодействие с AAA:** Если используется AAA-аутентификация (RADIUS/TACACS+), сервер может назначать уровень привилегий динамически, переопределяя локальную настройку линии.

Удаление конфигурации:

```
(config-line)# no privilege level
```

Сбрасывает уровень привилегий для линии к значению по умолчанию (обычно 1).

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.22.11 (config-line)# width

Настройка ширины терминальной линии

Синтаксис:

(config-line)# width <width>

Объяснение: Настройка ширины терминальной линии.

Параметры:

- <width>: Укажите ширину терминальной линии. Допустимый диапазон от 40 до 512. Укажите 0 для неограниченной ширины.

Рекомендации:

- Команда width задает глобальное значение ширины экрана (количества символов в строке) для всех сессий, подключающихся через данную линию. Она определяет, в какой момент длинные строки вывода (например, таблицы из show interface status) будут переноситься на следующую строку.
- В отличие от terminal width**:** Эта команда устанавливает глобальное значение для линии, сохраняемое в конфигурации. Команда terminal width меняет ширину только для текущей сессии.
- **Значения:**
    - ✓ 0 – Неограниченная ширина. Вывод никогда не переносится, позволяя отображать очень широкие таблицы в одну строку. Удобно для сохранения форматирования при копировании.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ 80 – Стандартная ширина, соответствующая традиционным терминалам.
- ✓ 132 – Ширина, подходящая для широкоформатных дисплеев.

- Позволяет настроить удобную ширину экрана для разных типов подключений. Например, для консоли можно оставить значение по умолчанию, а для VTY-сессий, используемых для копирования конфигурации, установить 0.
- Эта настройка действует на все сессии, подключаемые к данной линии, но пользователь может переопределить её для своей текущей сессии командой terminal width.

Удаление конфигурации:

```
(config-line)# no width
```

Сбрасывает ширину для линии к значению по умолчанию (зависит от устройства и настроек клиента, обычно 80).

Просмотр:

```
> show line [ alive ]
# show line [ alive ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.23 Настройка LLDP (Link Layer Discovery Protocol) (config)# lldp

2.7.23.1 (config)# lldp holdtime

Настройка времени удержания (Holdtime) LLDP

Синтаксис:

```
(config)# lldp holdtime <val>
```

Объяснение: Эта настройка определяет, как долго LLDP-кадры считаются действительными, и используется для вычисления TTL (Time To Live). Значение по умолчанию — 4.

Параметры:

- <val>: Укажите значение времени удержания. Допустимое значение от 2 до 10.

Рекомендации:

- Команда lldp holdtime задает время удержания (Holdtime) для протокола LLDP. Это множитель, который используется для расчета TTL (Time To Live) в LLDP-пакетах.
- **Как это работает:**
    - ✓ Время жизни (TTL) информации в LLDP вычисляется по формуле: TTL = (Holdtime) * (LLDP Transmission Interval). Интервал передачи (lldp tx-interval) также настраивается отдельно.
    - ✓ Полученное значение TTL (в секундах) указывается в LLDP-пакетах. Соседнее устройство, получившее

SEC.RU | Короткий путь к информации Скачано с sec.ru

информацию, считает её действительной в течение этого времени. Если за время TTL не придет новое обновление от того же устройства, информация о нем удаляется из таблицы соседей.

- ✓ **Пример:** Если Holdtime = 4, а интервал передачи = 30 секунд, то TTL = 120 секунд. Если устройство не получит новое LLDP-сообщение в течение 120 секунд, оно удалит запись о соседе.

- **Влияние на сеть:**
  - ✓ **Большое значение Holdtime:** Увеличивает время жизни информации о соседях, делая её более устойчивой к временным потерям LLDP-пакетов, но замедляет обнаружение того факта, что устройство исчезло (например, было выключено).
  - ✓ **Маленькое значение Holdtime:** Ускоряет обнаружение исчезновения соседа, но требует более частого обновления информации.
- **Значение по умолчанию:** 4. Рекомендуется изменять только при необходимости тонкой настройки работы протокола.

Удаление конфигурации:

```
(config)# no lldp holdtime
```

Сбрасывает время удержания к значению по умолчанию (4).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.23.2 (config)# lldp reinit

Настройка задержки перед повторной инициализацией LLDP

Синтаксис:

```
(config)# lldp reinit <val>
```

Объяснение: Настройка задержки между отправкой кадра завершения (shutdown frame) и новой инициализацией LLDP.

Параметры:

- <val>: Укажите значение от 1 до 10 (в секундах).

Рекомендации:

- Команда lldp reinit задает время задержки (reinitialization delay) перед тем, как протокол LLDP будет перезапущен на порту после его отключения (административного shutdown) или после изменения конфигурации LLDP.
- **Как это работает:**
    1. Когда LLDP на порту отключается (например, командой no lldp receive или no lldp transmit), он может отправить специальный LLDP-кадр с TTL=0, информируя соседей о том, что он больше не активен.
    2. Если после этого LLDP снова включается (или конфигурация меняется), коммутатор ждет в течение времени, заданного lldp reinit, прежде чем начать отправку новых LLDP-пакетов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Эта задержка предотвращает возможные конфликты или "флуд" при частых переключениях состояния LLDP на порту.

- **Влияние на сеть:**
    1. Защищает соседние устройства от быстрой смены состояний (flapping) LLDP.
    2. Увеличивает время, необходимое для повторного обнаружения соседа после перезапуска LLDP.
- **Значение по умолчанию:** Обычно 1 или 2 секунды. Изменять его имеет смысл в очень нестабильных средах, где LLDP часто перезапускается.

Удаление конфигурации:

```
(config)# no lldp reinit
```

Сбрасывает задержку повторной инициализации к значению по умолчанию.

2.7.23.3 (config)# lldp timer

Настройка интервала отправки LLDP-кадров

Синтаксис:

```
(config)# lldp timer <val>
```

Объяснение: Настройка интервала между отправкой LLDP-кадров соседям для обновления информации об обнаружении. Значение по умолчанию – 30 секунд.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <val>: Укажите значение от 5 до 32768 (в секундах).

Рекомендации:

- Команда lldp timer задает интервал (Tx Interval), с которым устройство отправляет LLDP-кадры (объявления) на все порты, где включена передача LLDP.
- **Как это работает:**
    1. Устройство периодически, каждые <val> секунд, рассылает LLDP-пакеты, содержащие информацию о себе (идентификация, возможности, порт и т.д.).
    2. Соседние устройства, получив этот пакет, обновляют свою базу данных LLDP-соседей.
- **Влияние на сеть:**
    1. **Маленький интервал (например, 5-10 сек):** Обеспечивает более быстрое обнаружение изменений в сети (например, появление нового устройства), но увеличивает служебный трафик LLDP.
    2. **Большой интервал (например, 120-300 сек):** Снижает служебный трафик, но замедляет обнаружение новых устройств и обновление информации об исчезнувших.
- **Взаимосвязь с Holdtime:** Значение TTL в LLDP-пакетах вычисляется как timer * holdtime. Поэтому при увеличении timer или holdtime увеличивается время жизни информации о соседе.
- **Значение по умолчанию:** 30 секунд – хороший баланс для большинства сетей.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no lldp timer
```

Сбрасывает интервал отправки к значению по умолчанию (30 секунд).

2.7.23.4 (config)# lldp transmission-delay

Настройка задержки передачи при изменении конфигурации LLDP

Синтаксис:

```
(config)# lldp transmission-delay <val>
```

Параметры:

- <val>: Укажите значение от 1 до 8192 (в секундах).

Объяснение: Настройка задержки между отправкой LLDP-кадров, содержащих измененную конфигурацию. Задержка передачи (Tx Delay) не может быть больше 1/4 от значения интервала передачи (Tx Interval).

Рекомендации:

- Команда lldp transmission-delay задает минимальный интервал времени между отправкой последовательных LLDP-кадров, которые содержат изменения в конфигурации устройства. Это предотвращает отправку множества обновлений за короткий промежуток времени при быстрых изменениях.
- **Как это работает:**
    1. Если в конфигурации устройства произошло изменение, влияющее на LLDP-объявления (например, изменилось

SEC.RU | Короткий путь к информации Скачано с sec.ru

описание порта), LLDP не отправляет новое объявление немедленно.

2. Вместо этого он ждет в течение времени, заданного transmission-delay, прежде чем отправить обновленную информацию.
3. Если за это время произойдет еще несколько изменений, они будут объединены и отправлены в одном кадре по истечении задержки.

- **Влияние на сеть:**

1. **Снижение нагрузки:** Предотвращает "лавину" LLDP-кадров при множественных быстрых изменениях конфигурации.
2. **Ограничение:** значение transmission-delay не может превышать 1/4 **от** lldp timer (интервала передачи). Это гарантирует, что задержка не нарушит регулярный цикл отправки.

- **Значение по умолчанию:** Обычно равно 1 или 2 секундам.

Удаление конфигурации:

```
(config)# no lldp transmission-delay
```

Сбрасывает задержку передачи к значению по умолчанию.

2.7.23.5 (config)# lldp med datum

Настройка геодезической системы координат (Map Datum) для LLDP-MED

SEC.RU | Короткий путь к информации Скачано с sec.ru

Синтаксис:

```
(config)# lldp med datum { wgs84 | nad83-navd88 | nad83-mllw }
```

Объяснение: Геодезическая система координат (Map Datum) используется для координат, заданных в вышеуказанных опциях.

Параметры:

- { wgs84 | nad83-navd88 | nad83-mllw }: Укажите один из вариантов.
    - ✓ **WGS84:** (Geographical 3D) - Всемирная геодезическая система 1984 года, код системы координат (CRS Code) 4327, название начального меридиана: Гринвич.
    - ✓ **NAD83/NAVD88:** Североамериканская геодезическая система координат 1983 года, код CRS 4269, название начального меридиана: Гринвич; соответствующая вертикальная система координат — Североамериканская вертикальная система координат 1988 года (NAVD88). Эта пара систем координат используется при указании местоположений на суше, не рядом с приливными водами (для которых используется система NAD83/MLLW).
    - ✓ **NAD83/MLLW:** Североамериканская геодезическая система координат 1983 года, код CRS 4269, название начального меридиана: Гринвич; соответствующая вертикальная система координат — средний нижний уровень малой воды (Mean Lower Low Water, MLLW). Эта пара систем координат используется при указании местоположений на воде/море/океане.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `lldp med datum` является частью расширения LLDP-MED (LLDP for Media Endpoint Devices). LLDP-MED позволяет сетевым устройствам, особенно связанным с голосом и видео (IP-телефоны, видеокамеры), обмениваться дополнительной информацией, включая информацию о местоположении.
- Эта команда задает геодезическую систему координат (Map Datum), которая используется для интерпретации координат, передаваемых в LLDP-MED-сообщениях о местоположении (Location Identification TLV). Разные географические регионы и приложения используют разные системы координат для определения местоположения.
- Если ваша сеть использует службы определения местоположения на основе LLDP-MED (например, для автоматического определения местоположения телефона для служб экстренного вызова, таких как E911), необходимо правильно настроить систему координат в соответствии с вашим регионом и типом местности (суша/вода).
- **Выбор параметра:**
    - ✓ `wgs84`**:** Это глобальная система координат, используемая в GPS. Подходит для большинства случаев, если не требуется более точная локальная привязка.
    - ✓ `nad83-navd88`**:** Используется в Северной Америке для местоположений на суше.
    - ✓ `nad83-mllw`**:** Используется в Северной Америке для местоположений на воде (например, для портовых сооружений, кораблей).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no lldp med datum
```

Удаляет настройку системы координат, возвращаясь к значению по умолчанию (зависит от устройства).

2.7.23.6 (config)# lldp med fast

Настройка количества повторений быстрого запуска LLDP-MED (Fast Start)

Синтаксис:

```
(config)# lldp med fast <v_1_to_10>
```

Объяснение: Быстрый запуск (Rapid startup) и обнаружение местоположения для служб экстренного вызова (Emergency Call Service Location Identification) конечных точек (endpoints) являются критически важными аспектами VoIP-систем в целом. Кроме того, лучше рекламировать только те фрагменты информации, которые непосредственно относятся к конкретным типам конечных точек (например, рекламировать политику голосовой сети только разрешенным устройствам с поддержкой голоса), как для экономии ограниченного пространства LLDPU, так и для уменьшения проблем безопасности и целостности системы, которые могут возникнуть при ненадлежащем знании политики сети. С учетом этого, LLDP-MED определяет взаимодействие быстрого запуска LLDP-MED (LLDP-MED Fast Start) между протоколом и прикладными уровнями поверх протокола для достижения этих связанных свойств. С помощью счетчика повторений быстрого запуска (Fast start repeat count) можно

SEC.RU | Короткий путь к информации Скачано с sec.ru

указать количество раз, которое повторяется передача при быстром запуске. Рекомендуемое значение – 4, что означает, что будет передано 4 LLDP-кадра с интервалом в 1 секунду при получении LLDP-кадра с новой информацией. Следует отметить, что LLDP-MED и механизм быстрого запуска LLDP-MED предназначены только для работы на линках между сетевыми устройствами подключения LLDP-MED (Network Connectivity Devices) и конечными устройствами (Endpoint Devices) и, как таковые, не применяются к линкам между элементами инфраструктуры ЛВС, включая соединения между сетевыми устройствами подключения, или к другим типам линков.

Параметры:

- `<v_1_to_10>`: Укажите допустимое значение от 1 до 10.

Рекомендации:

- Команда `lldp med fast` настраивает параметр Fast Start Repeat Count для LLDP-MED.
- **Fast Start –** Это механизм, который позволяет конечному устройству (например, IP-телефону) быстро получить необходимую информацию от коммутатора сразу после подключения. Вместо того чтобы ждать стандартного интервала LLDP (например, 30 секунд), коммутатор отправляет серию из нескольких LLDP-MED-кадров с интервалом в 1 секунду.
- **Как это работает:**
    1. Когда конечное устройство подключается к порту и включает LLDP, коммутатор обнаруживает это.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Коммутатор инициирует "быстрый старт" и отправляет `n` LLDP-кадров (где `n` задается этой командой) с интервалом 1 секунда.
3. После отправки этих кадров коммутатор возвращается к обычному интервалу LLDP (`lldp timer`).

- **Зачем это нужно:**
    1. Быстрое получение критической информации: Особенно важно для VoIP-телефонов, которым нужна информация о VLAN для голоса, политиках QoS и, что критически важно, для получения информации о местоположении для служб экстренного вызова (E911). Быстрый старт позволяет телефону получить эту информацию за несколько секунд, а не за минуты.
    2. Экономия ресурсов и безопасность: Позволяет передавать только релевантную информацию (например, голосовую политику) только тем устройствам, которые в ней нуждаются.
- **Рекомендуемое значение:** 4 . Это обеспечивает баланс между скоростью и служебным трафиком.
- **Область применения:** Fast Start работает только на линках между коммутатором и конечным устройством, а не между сетевыми устройствами (коммутатор-коммутатор).

Удаление конфигурации:

```
(config)# no lldp med fast
```

Сбрасывает количество повторений быстрого запуска к значению по умолчанию (4).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.23.7 (config)# lldp med location-tlv altitude

Настройка высоты (Altitude) для TLV местоположения LLDP-MED

Синтаксис:

```
(config)# lldp med location-tlv altitude { meters | floors } <v_word11>
```

Объяснение: Высота (Altitude) должна быть нормализована в диапазоне от -32767 до 32767 с максимум 4 цифрами. Можно выбрать между двумя типами высоты: "этажи" (floors) или "метры" (meters). "meters" означает метры высоты, определенные указанной вертикальной системой координат (vertical datum); "floors" означает высоту в форме, более уместной в зданиях, где расстояния между этажами различаются.

Параметры:

- `{ meters | floors }`: Укажите один из вариантов.
- `<v_word11>`: Укажите значение для выбранного параметра.

Рекомендации:

- Команда `lldp med location-tlv altitude` является частью настройки **TLV местоположения (Location TLV)** для протокола **LLDP-MED**. Этот TLV используется для передачи информации о физическом местоположении устройства (например, IP-телефона) для служб экстренного вызова (E911).
- Назначение: Позволяет администратору задать **высоту (Altitude)**, которая будет передаваться в LLDP-MED-объявлениях на подключенные конечные устройства. Это

SEC.RU | Короткий путь к информации Скачано с sec.ru

критически важно для корректного определения местоположения вызывающего абонента в многоэтажных зданиях.

- **Два формата высоты:**
  - ✓ meters **(метры):** Задает высоту в метрах относительно указанной вертикальной системы координат (например, WGS84, NAD83). Подходит для местоположений, где важна точная высота над уровнем моря.
  - ✓ floors **(этажи):** Задает высоту в виде номера этажа (или условного обозначения). Это более удобный формат для зданий, где расстояние между этажами может различаться. Например, floors 10 означает 10-й этаж.
- **Ограничения:** Значение должно быть в диапазоне от -32767 до 32767 и содержать не более 4 цифр.

Удаление конфигурации:

```
(config)# no lldp med location-tlv altitude
```

Удаляет настройку высоты для TLV местоположения.

2.7.23.8 (config)# lldp med location-tlv civic-addr

Настройка гражданского адреса (Civic Address) для TLV местоположения LLDP-MED

Синтаксис:

```
(config)# lldp med location-tlv civic-addr { country | state | county | city | distri
ct | block | street | leading-street-direction | trailing-street-suffix | street-suffix |
house-no | house-no-suffix | landmark | additional-info | name | zip-code | buil
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

ding | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_string250>

Объяснение: Настройка информации гражданского адреса.

Параметры:

- Укажите один из вариантов для настройки адреса:
  - ✓ **country**: Двухбуквенный код страны по стандарту ISO 3166 заглавными буквами ASCII. Пример: DK, DE, US.
  - ✓ **state**: Административные единицы (штат, кантон, регион, провинция, префектура).
  - ✓ **county**: Округ, приход, район.
  - ✓ **city**: Город, муниципалитет.
  - ✓ **district**: Район города, округ, квартал.
  - ✓ **block**: Микрорайон, квартал.
  - ✓ **street**: Улица.
  - ✓ **leading-street-direction**: Направление перед названием улицы. Пример: N.
  - ✓ **trailing-street-suffix**: Суффикс после названия улицы. Пример: SW.
  - ✓ **street-suffix**: Тип улицы (Ave, Platz).
  - ✓ **house-no**: Номер дома.
  - ✓ **house-no-suffix**: Суффикс номера дома. Пример: A, 1/2.
  - ✓ **landmark**: Ориентир или адрес по достопримечательности. Пример: Columbia University.
  - ✓ **additional-info**: Дополнительная информация. Пример: South Wing.
  - ✓ **name**: Имя. Пример: Flemming Jahn.
  - ✓ **zip-code**: Почтовый индекс. Пример: 2791.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **building**: Здание (строение). Пример: Low Library.
- ✓ **apartment**: Квартира, офис. Пример: Apt 42.
- ✓ **floor**: Этаж. Пример: 4.
- ✓ **room-number**: Номер комнаты. Пример: 450F.
- ✓ **place-type**: Тип помещения. Пример: Office.
- ✓ **postal-community-name**: Название почтового сообщества. Пример: Leonia.
- ✓ **p-o-box**: Абонентский ящик. Пример: 12345.
- ✓ **additional-code**: Дополнительный код. Пример: 1320300003.

- <v_string250>: Укажите значение для выбранного параметра (до 250 символов).

Рекомендации:

- Команда lldp med location-tlv civic-addr является ключевой для настройки **гражданского адреса (Civic Address)** в составе TLV местоположения LLDP-MED. Этот TLV используется для передачи подробной информации о физическом местоположении устройства (например, IP-телефона) для служб экстренного вызова (E911).
- В отличие от географических координат (широта/долгота): Гражданский адрес использует понятный человеку формат: страна, город, улица, дом и т.д. Это более практично для определения местоположения внутри зданий и для служб спасения.
- **Как использовать:** Обычно настраивается несколько полей (например, country, city, street, house-no, floor), чтобы сформировать полный адрес. Каждое поле настраивается отдельной командой.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Важность для VoIP:** Критически важно для корректной работы служб экстренного вызова. При вызове по номеру 911 (или 112) из IP-телефона, коммутатор передает телефону настроенный гражданский адрес через LLDP-MED, и этот адрес затем передается диспетчеру службы спасения.

Удаление конфигурации (Negation):

```
(config)# no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }
```

Удаляет указанный параметр гражданского адреса.

2.7.23.9 (config)# lldp med location-tlv elin-addr

Настройка экстренного идентификатора местоположения (ELIN)

Синтаксис:

```
(config)# lldp med location-tlv elin-addr <v_word25>
```

Объяснение: Настройка значения для информации об экстренном местоположении (Emergency Location Information).

Параметры:

- <v_word25>: Значение для экстренного идентификатора местоположения (ELIN).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `lldp med location-tlv elin-addr` настраивает **ELIN (Emergency Location Identification Number)** — экстренный идентификатор местоположения, который передается в TLV местоположения LLDP-MED.
- **Что такое ELIN?** Это номер телефона (или идентификатор), который система экстренной связи (например, E911) использует для определения физического местоположения вызывающего абонента. В отличие от гражданского адреса (civic address), ELIN — это номер, который маршрутизирует вызов в центр обработки вызовов (PSAP — Public Safety Answering Point) и позволяет диспетчеру получить точную информацию о местоположении.
- **Как это работает:**
    1. Администратор настраивает на коммутаторе ELIN для определенного порта (или глобально, в зависимости от реализации).
    2. При подключении IP-телефона коммутатор передает ему ELIN через LLDP-MED.
    3. Когда пользователь набирает номер экстренной службы (911, 112), телефон отправляет вызов, который содержит этот ELIN.
    4. Система экстренной связи (например, ALI — Automatic Location Identification) использует ELIN для определения точного адреса и направления вызова в соответствующий центр обработки вызовов.
- **В отличие от гражданского адреса:** Гражданский адрес — это текстовое описание местоположения (улица, дом, офис). ELIN

SEC.RU | Короткий путь к информации Скачано с sec.ru

— это телефонный номер, который используется для автоматической маршрутизации вызова и извлечения информации о местоположении из базы данных.

- Обычно ELIN настраивается на портах, к которым подключены телефоны, или глобально для здания/этажа. Значение ELIN должно быть уникальным для каждого физического местоположения (например, для каждого этажа или даже комнаты) в пределах области обслуживания PSAP.

Удаление конфигурации:

```
(config)# no lldp med location-tlv elin-addr
```

Удаляет настройку ELIN.

2.7.23.10 (config)# lldp med location-tlv latitude

Настройка широты (Latitude) для TLV местоположения LLDP-MED

Синтаксис:

```
(config)# lldp med location-tlv latitude { north | south } <v_word8>
```

Объяснение: Настройка значения широты. Значение широты должно быть между 0 и 90.

Параметры:

- { north | south }: Укажите один из вариантов — северная (north) или южная (south) широта.
- <v_word8>: Укажите значение широты для выбранного варианта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда lldp med location-tlv latitude является частью настройки географических координат в TLV местоположения LLDP-MED. Вместе с долготой (longitude) и высотой (altitude) она определяет точное географическое положение устройства (например, IP-телефона) для служб экстренного вызова (E911).
- **Формат:** Широта задается в градусах (0–90) с указанием полушария: северное (north) или южное (south). Значение может включать десятичные доли для повышения точности.
- **Для чего используется:** Когда IP-телефон подключен к сети, коммутатор может передать ему через LLDP-MED его географические координаты. Эти координаты затем используются службами экстренного вызова для определения местоположения вызывающего абонента, если гражданский адрес недоступен или требуется более точная привязка.
- **В отличие от гражданского адреса:** Географические координаты (широта/долгота) являются более универсальным способом указания местоположения, особенно для объектов вне помещений (кампусы, промышленные зоны), где традиционная адресация может быть неоднозначной.
- Для полного описания местоположения необходимо также настроить **долготу** (longitude) и, при необходимости, **высоту** (altitude) и **геодезическую систему координат** (datum).

Удаление конфигурации:

```
(config)# no lldp med location-tlv latitude
```

Удаляет настройку широты.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.23.11 (config)# lldp med location-tlv longitude

Настройка долготы (Longitude) для TLV местоположения LLDP-MED

Синтаксис:

```
(config)# lldp med location-tlv longitude { west | east } <v_word9>
```

Объяснение: Настройка значения долготы. Значение долготы должно быть между 0 и 180.

Параметры:

- { west | east }: Укажите один из вариантов — западная (west) или восточная (east) долгота.
- <v_word9>: Укажите значение долготы для выбранного варианта.

Рекомендации:

- Команда lldp med location-tlv longitude является частью настройки географических координат в TLV местоположения LLDP-MED. Вместе с широтой (latitude) и высотой (altitude) она определяет точное географическое положение устройства (например, IP-телефона) для служб экстренного вызова (E911).
- **Формат:** Долгота задается в градусах (0–180) с указанием направления: западное (west) или восточное (east). Значение может включать десятичные доли для повышения точности.
- **Для чего используется:** Когда IP-телефон подключен к сети, коммутатор может передать ему через LLDP-MED его географические координаты. Эти координаты затем

SEC.RU | Короткий путь к информации Скачано с sec.ru

используются службами экстренного вызова для определения местоположения вызывающего абонента, если гражданский адрес недоступен или требуется более точная привязка (например, в больших кампусах, на открытых пространствах).

- **В сочетании с широтой:** Для полного описания географического местоположения необходимы обе координаты — широта и долгота. Широта указывает положение относительно экватора (север/юг), долгота — относительно Гринвичского меридиана (восток/запад).

Удаление конфигурации:

```
(config)# no lldp med location-tlv longitude
```

Удаляет настройку долготы.

2.7.23.12 (config)# lldp med media-vlan-policy

Настройка политики VLAN для медиа-трафика LLDP-MED

Синтаксис:

```
(config)# lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [ l2-priority <v_0_to_7> ] [ dscp <v_0_to_63> ]
```

Объяснение: Настройка политики LLDP-MED для определенного сервиса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <policy_index>: Укажите идентификатор политики. Допустимый диапазон: от 0 до 31.
- { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling }: Укажите один из сервисов для данного идентификатора политики.
    - ✓ **voice**: Голосовой трафик.
    - ✓ **voice-signaling**: Сигнальный трафик голоса (SIP, H.323 и т.д.).
    - ✓ **guest-voice**: Гостевой голосовой трафик.
    - ✓ **guest-voice-signaling**: Сигнальный трафик гостевого голоса.
    - ✓ **softphone-voice**: Голосовой трафик программных телефонов.
    - ✓ **video-conferencing**: Трафик видеоконференций.
    - ✓ **streaming-video**: Трафик потокового видео.
    - ✓ **video-signaling**: Сигнальный трафик видео.
- { tagged <v_vlan_id> | untagged }: Укажите, будет ли этот сервис использовать тегированный (tagged) или нетегированный (untagged) трафик. Если указано tagged, необходимо указать идентификатор VLAN.
- [l2-priority <v_0_to_7>]: Укажите значение приоритета уровня 2 (CoS, 802.1p). Допустимый диапазон: от 0 до 7.
- [dscp <v_0_to_63>]: Укажите значение DSCP (Differentiated Services Code Point) для уровня 3. Допустимый диапазон: от 0 до 63.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `lldp med media-vlan-policy` является ключевой для настройки медиа-политик (Media Policies) в рамках LLDP-MED. Эти политики используются для автоматической конфигурации конечных устройств (например, IP-телефонов) при подключении к сети.
- **Как это работает:**
    1. Администратор настраивает на коммутаторе одну или несколько политик, определяющих, в какую VLAN должен попадать трафик определенного типа (голос, видео), какой приоритет (CoS/DSCP) ему назначать.
    2. При подключении IP-телефона (или другого MED-устройства) коммутатор передает эти политики через LLDP-MED.
    3. Телефон автоматически настраивается: начинает использовать указанную VLAN для голосового трафика, устанавливает правильные приоритеты для QoS.
- **Зачем это нужно:**
    - ✓ **Автоматизация:** Упрощает развертывание VoIP и видеосетей — не нужно вручную настраивать каждый телефон.
    - ✓ **Качество обслуживания (QoS):** Обеспечивает единую и корректную маркировку приоритетов для голосового и видеотрафика.
    - ✓ **Безопасность:** Голосовой трафик может быть изолирован в отдельную VLAN.
    - ✓ **Значения приоритетов (рекомендации):**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **l2-priority (CoS):** Для голоса рекомендуется 5 или 6, для видео — 4 или 5.
- ✓ **dscp:** Для голоса рекомендуется EF (46) или AF41 (34), для видео — AF41 (34) или AF42 (36).

Удаление конфигурации:

```
(config)# no lldp med media-vlan-policy <policies_list>
```

Удаляет указанные политики (одну или несколько).

Просмотр:

```
> show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]
```

2.7.23.13 (config-if)# lldp cdp-aware

Включение поддержки CDP на интерфейсе

Синтаксис:

```
(config-if)# lldp cdp-aware
```

Объяснение: Настраивает, будет ли интерфейс поддерживать CDP (информация об обнаружении CDP добавляется в таблицу соседей LLDP).

Рекомендации:

- Команда lldp cdp-aware, выполняемая в режиме конфигурации интерфейса, включает **поддержку протокола CDP (Cisco**

SEC.RU | Короткий путь к информации Скачано с sec.ru

Discovery Protocol) на данном порту. CDP — это проприетарный протокол Cisco, используемый для обнаружения соседних устройств.

- В сетях, где присутствует как оборудование Cisco (которое использует CDP), так и оборудование других вендоров (которое использует LLDP), команда `lldp cdp-aware` позволяет коммутатору извлекать информацию из CDP-пакетов от соседних устройств Cisco и представлять её в таблице LLDP-соседей. Это позволяет унифицировать управление и мониторинг сети через единый протокол LLDP.
- **Как это работает:**
    1. На порту, где включена эта функция, коммутатор продолжает передавать LLDP-пакеты (если LLDP включен).
    2. Одновременно он прослушивает (snoops) входящие CDP-пакеты от соседних устройств.
    3. Информация, извлеченная из CDP-пакетов (например, идентификатор устройства, тип, версия ПО), добавляется в таблицу LLDP-соседей, где она отображается наряду с информацией, полученной через LLDP.
- Эта команда не включает передачу CDP-пакетов. Коммутатор не отправляет собственные CDP-объявления, он только "понимает" и обрабатывает входящие. Если требуется двустороннее взаимодействие с CDP-устройством, на этом порту также должно быть включено LLDP (команда `lldp` или аналогичная).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no lldp cdp-aware
```

Отключает поддержку CDP на интерфейсе. Информация из CDP-пакетов больше не будет добавляться в таблицу LLDP-соседей.

Просмотр:

```
> show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

В выводе команды show lldp neighbors *для порта с включенным* cdp-aware *будут отображаться устройства, обнаруженные как через LLDP, так и через CDP.*

2.7.23.14 (config-if)# lldp med media-vlan policy-list

Применение политики MED Media-VLAN к интерфейсу

Синтаксис:

```
(config-if)# lldp med media-vlan policy-list <v_range_list>
```

Объяснение: Применение политики MED Media-VLAN протокола LLDP на данном интерфейсе.

Параметры:

- <v_range_list>: Назначьте политику (или список политик) данному интерфейсу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `lldp med media-vlan policy-list` в режиме конфигурации интерфейса применяет одну или несколько LLDP-MED медиа-политик (media policies) к конкретному порту. Сами политики предварительно создаются глобальной командой `lldp med media-vlan-policy`.
- **Как это работает:**
    1. Администратор создает глобальные политики (например, политику для голоса, политику для видео) с помощью команды `lldp med media-vlan-policy`.
    2. Затем на порту, к которому подключаются конечные устройства (IP-телефоны, видеокамеры), с помощью данной команды указывается, какие из этих политик должны передаваться на этот порт.
    3. Когда устройство подключается и инициирует LLDP-MED-обмен, коммутатор передает ему только те политики, которые привязаны к данному порту.
- **Зачем это нужно:**
    1. **Гибкость:** Разные порты могут иметь разные политики. Например, порт в конференц-зале может получать политику для видеоконференций, а порт в обычном офисе — только политику для голоса.
    2. **Безопасность и экономия ресурсов:** Не передается лишняя информация, которая не нужна устройству на данном порту.
- **Параметр** `<v_range_list>`**:** Позволяет указать одну политику (например, `1`), несколько политик через запятую (`1,2,3`) или диапазон (`1-5`).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no lldp med media-vlan policy-list <v_range_list>
```

Удаляет привязку указанных политик к интерфейсу.

Просмотр:

```
> show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]
```

Показывает список настроенных политик. Для проверки привязки к интерфейсу может потребоваться просмотр running-config.

2.7.23.15 (config-if)# lldp med transmit-tlv

Настройка передачи TLV для LLDP-MED на интерфейсе

Синтаксис:

```
(config-if)# lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]
```

Объяснение: Настройка типов TLV (Type-Length-Value) LLDP-MED для конкретного интерфейса.

Параметры:

- [capabilities]: Включить передачу необязательного TLV возможностей (Capabilities TLV). Этот TLV сообщает о поддерживаемых устройством возможностях LLDP-MED (например, является ли устройство сетевым устройством подключения, конечной точкой и т.д.).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [location]: Включить передачу необязательного TLV местоположения (Location TLV). Этот TLV содержит информацию о физическом местоположении устройства (географические координаты, гражданский адрес, ELIN).
- [network-policy]: Включить передачу необязательного TLV сетевой политики (Network Policy TLV). Этот TLV определяет политики VLAN и QoS для различных типов медиа-трафика (голос, видео).

Рекомендации:

- Команда lldp med transmit-tlv в режиме конфигурации интерфейса управляет тем, какие дополнительные (необязательные) TLV LLDP-MED будут передаваться через данный порт.
- **LLDP-MED TLV (Type-Length-Value):** В дополнение к базовым LLDP-объявлениям, LLDP-MED определяет ряд специализированных TLV, которые передают важную информацию для медиа-устройств (IP-телефонов, видеокамер).
    - ✓ **Capabilities TLV:** Базовый TLV, который всегда должен передаваться, чтобы объявить о поддержке LLDP-MED. Он сообщает о роли устройства и поддерживаемых MED-TLV.
    - ✓ **Location TLV:** Передает информацию о местоположении (для служб экстренного вызова E911).
    - ✓ **Network Policy TLV:** Передает политики VLAN и QoS для голоса/видео.
- **Зачем это нужно:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Выборочная передача:** Не на всех портах может требоваться передача всей информации. Например, на порту, где нет телефонов, можно отключить передачу network-policy и location.
- ✓ **Снижение нагрузки:** Уменьшает размер LLDP-пакетов и служебный трафик.
- ✓ **Безопасность:** Не передает чувствительную информацию о местоположении на порты, где она не нужна.

- **Рекомендации для портов с IP-телефонами:**
  - ✓ Обычно включают все три типа: capabilities (обязателен для MED), network-policy (для автонастройки телефона) и, при необходимости, location (для E911).

Удаление конфигурации:

```
(config-if)# no lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ]
```

Отключает передачу указанных TLV на интерфейсе.

Просмотр:

```
> show lldp med media-vlan-policy [ <v_0_to_31> ]
# show lldp med media-vlan-policy [ <v_0_to_31> ]
```

Для просмотра статуса передачи TLV на интерфейсе может потребоваться команда show lldp interface.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.23.16 (config-if)# lldp receive

Включение приема LLDP-пакетов на интерфейсе

Синтаксис:

```
(config-if)# lldp receive
```

Объяснение: Коммутатор будет анализировать информацию LLDP, полученную от соседей.

Рекомендации:

- Команда lldp receive в режиме конфигурации интерфейса включает прием и обработку LLDP-пакетов на данном порту. Когда эта функция включена, коммутатор анализирует входящие LLDP-объявления от соседних устройств и обновляет свою таблицу LLDP-соседей.
- **Взаимодействие с передачей:**
    - ✓ lldp receive управляет только **входящим** трафиком LLDP.
    - ✓ Отдельная команда lldp transmit (если существует) управляет **исходящим** трафиком LLDP.
    - ✓ В некоторых реализациях одна команда lldp может включать и прием, и передачу одновременно. Данная команда позволяет более тонко настраивать поведение порта.
- **Когда может потребоваться отключить прием:**
    - ✓ **Безопасность:** На портах, подключенных к ненадежным внешним сетям, можно отключить прием LLDP, чтобы

SEC.RU | Короткий путь к информации Скачано с sec.ru

предотвратить утечку информации о топологии сети злоумышленникам, которые могут подключать свое устройство и собирать LLDP-объявления.

- ✓ **Снижение нагрузки:** В некоторых случаях, когда LLDP не используется, можно отключить его прием для экономии ресурсов.

- **По умолчанию:** На большинстве портов прием LLDP может быть включен по умолчанию. Явное включение/отключение позволяет управлять поведением.

Удаление конфигурации:

```
(config-if)# no lldp receive
```

Отключает прием и обработку LLDP-пакетов на интерфейсе. Коммутатор будет игнорировать LLDP-объявления от соседей на этом порту.

Просмотр:

```
> show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Команда show lldp statistics *показывает количество принятых и переданных LLDP-пакетов на портах, что позволяет проверить работу приема.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.23.17 (config-if)# lldp tlv-select

Выбор TLV для передачи в LLDP-объявлениях на интерфейсе

Синтаксис:

(config-if)# lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name }

Объяснение: Настройка атрибутов TLV LLDP-MED для конкретного интерфейса.

Параметры:

- { management-address | port-description | system-capabilities | system-description | system-name }: Укажите атрибут TLV LLDP. LLDP использует несколько атрибутов для обнаружения соседних устройств. Эти атрибуты содержат описания типа, длины и значения и называются TLV. Подробная информация, такая как описание порта, системное имя, системное описание, системные возможности и управляющий адрес, может быть отправлена с данного устройства.

Рекомендации:

- Команда lldp tlv-select в режиме конфигурации интерфейса позволяет выборочно включать или отключать передачу определенных базовых LLDP TLV на конкретном порту.
- **Базовые LLDP TLV (описаны в IEEE 802.1AB):**
  - ✓ system-name (Имя системы): Имя устройства (hostname).
  - ✓ system-description (Описание системы): Описание устройства (обычно модель и версия ПО).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ system-capabilities (Возможности системы): Роль устройства (коммутатор, маршрутизатор, мост и т.д.).
- ✓ port-description (Описание порта): Текстовое описание порта (например, "Uplink to Core").
- ✓ management-address (Управляющий адрес): IP-адрес для управления устройством.

- **Зачем это нужно:**
  - ✓ **Безопасность:** На портах, подключенных к ненадежным внешним сетям, можно отключить передачу чувствительной информации, такой как system-description (версия ПО) или management-address.
  - ✓ **Снижение нагрузки:** Уменьшает размер LLDP-пакетов и служебный трафик.
  - ✓ **Конфиденциальность:** Предотвращает утечку информации о топологии сети и используемом оборудовании.
- **Отличие от LLDP-MED TLV:** Данная команда управляет базовыми (стандартными) LLDP TLV, в то время как команда lldp med transmit-tlv управляет специализированными LLDP-MED TLV (capabilities, location, network-policy).

Удаление конфигурации:

```
(config-if)# no lldp tlv-select { management-address | port-description |
system-capabilities | system-description | system-name }
```

Отключает передачу указанного TLV на интерфейсе.

Просмотр:

```
> show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show lldp neighbors [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Вывод команды show lldp neighbors *отображает информацию, полученную от соседей, включая те TLV, которые были переданы.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.23.18 (config-if)# lldp transmit

Включение передачи LLDP-пакетов на интерфейсе

Синтаксис:

```
(config-if)# lldp transmit
```

Объяснение: Настройка режима передачи LLDP (только Tx) для конкретного интерфейса.

Рекомендации:

- Команда lldp transmit в режиме конфигурации интерфейса **включает передачу LLDP-пакетов** на данном порту. Когда эта функция включена, коммутатор отправляет LLDP-объявления соседним устройствам.
- **Взаимодействие с приемом:**
  - ✓ lldp transmit управляет только **исходящим** трафиком LLDP.
  - ✓ Отдельная команда lldp receive управляет **входящим** трафиком LLDP.
  - ✓ В некоторых реализациях одна команда lldp может включать и передачу, и прием одновременно. Данная команда позволяет более тонко настраивать поведение порта.
- **Когда может потребоваться отключить передачу:**
  - ✓ **Безопасность:** На портах, подключенных к ненадежным внешним сетям, можно отключить передачу LLDP, чтобы не раскрывать злоумышленникам информацию о

SEC.RU | Короткий путь к информации Скачано с sec.ru

топологии сети, имени устройства, версии ПО и управляющих адресах.

- ✓ **Снижение нагрузки:** В некоторых случаях, когда LLDP не требуется, можно отключить его передачу для экономии ресурсов и снижения служебного трафика.

- **Режим «только Tx» (Transmit Only):** эта команда может использоваться для настройки порта в режим, когда LLDP-пакеты только передаются, но не принимаются (если прием отключен отдельно). Однако в данном синтаксисе команда `lldp transmit` сама по себе включает передачу, а прием управляется отдельной командой `lldp receive`.
- **По умолчанию:** На большинстве портов передача LLDP может быть включена по умолчанию. Явное включение/отключение позволяет управлять поведением.

Удаление конфигурации:

```
(config-if)# no lldp transmit
```

Отключает передачу LLDP-пакетов на интерфейсе. Коммутатор не будет отправлять LLDP-объявления на этот порт.

Просмотр:

```
# show lldp statistics [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Команда `show lldp statistics` *показывает количество переданных LLDP-пакетов на портах, что позволяет проверить работу передачи.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.24 Настройка журналирования (logging) (config)# logging

2.7.24.1 (config)# logging on

Глобальное включение отправки системных сообщений (syslog)

Синтаксис:

```
(config)# logging on
```

Объяснение:

Эта команда устанавливает режим работы сервера (отправки сообщений). Когда режим работы включен (on), системные сообщения (syslog) будут отправляться на syslog-сервер (по указанному адресу). Протокол syslog основан на UDP-связи и принимается на UDP-порту 514. Syslog-сервер не отправляет подтверждений обратно отправителю, поскольку UDP является протоколом без установления соединения и не предусматривает подтверждений. Syslog-пакет будет отправлен всегда, даже если syslog-сервер не существует. Когда режим работы отключен, syslog-пакеты не отправляются.

Рекомендации:

- Команда logging on **глобально включает** функцию отправки системных сообщений (syslog) на внешний syslog-сервер. Это необходимо для централизованного сбора логов с сетевых устройств.
- **Как это работает:**
    1. Коммутатор генерирует системные сообщения (логи) о различных событиях: изменения конфигурации, ошибки интерфейсов, нарушения безопасности и т.д.
    2. Когда logging on включен, коммутатор отправляет эти сообщения на один или несколько настроенных syslog-серверов (с помощью команды logging host).

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Сообщения отправляются по протоколу UDP на порт 514 (стандартный порт syslog). UDP не гарантирует доставку, поэтому сообщения могут быть потеряны при перегрузке сети.

- Как указано в описании, syslog-пакеты отправляются **даже если сервер не существует**. Это создает дополнительный трафик, поэтому перед включением рекомендуется убедиться, что сервер настроен и доступен.
- **Порядок настройки:**
  1. Сначала включается глобальная отправка: `logging on`.
  2. Затем настраиваются адреса syslog-серверов: `logging host <ip-address>`.
  3. При необходимости настраивается уровень серьезности отправляемых сообщений: `logging trap <level>`.

Удаление конфигурации:

```
(config)# no logging on
```

Отключает глобальную отправку syslog-сообщений. Сообщения не будут отправляться на внешние серверы.

Просмотр:

```
# show logging
```

Отображает текущие настройки syslog, включая состояние (включено/отключено), настроенные серверы и уровень логирования.

Очистка:

```
# clear logging [ info ] [ warning ] [ error ] [ switch <switch_list> ]
```

Очищает внутренний буфер системных сообщений.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.24.2 (config)# logging host

Настройка адреса syslog-сервера

Синтаксис:

```
(config)# logging host { <v_ipv4_ucast> | <v_word45> }
```

Параметры:

- { <hostname> | <ipv4_ucast> }: Укажите один из вариантов. hostname — это доменное имя сервера логов; ipv4_ucast — это IPv4-адрес сервера логов.

Объяснение: Настройка адреса сервера журналирования (syslog).

Рекомендации:

- Команда logging host задает IP-адрес или доменное имя внешнего syslog-сервера, на который коммутатор будет отправлять системные сообщения. Для работы этой команды необходимо предварительно включить глобальную отправку syslog командой logging on.
- **Форматы указания:**
  - ✓ **IPv4-адрес:** logging host 192.168.1.100 — наиболее распространенный способ.
  - ✓ **Доменное имя:** logging host syslog.company.com — если используется DNS, необходимо также настроить DNS-серверы (ip name-server) и включить разрешение имен.
- **Поддержка нескольких серверов:** Можно настроить несколько syslog-серверов, повторяя команду logging host для каждого

SEC.RU | Короткий путь к информации Скачано с sec.ru

адреса. Сообщения будут отправляться на все настроенные серверы (одновременно). Это повышает надежность сбора логов.

- **Порт:** По умолчанию сообщения отправляются на UDP-порт **514**. Если сервер использует другой порт, его можно указать с помощью команды `logging host <ip> port <port>` (в зависимости от реализации).
- **Протокол:** Syslog использует протокол UDP, который не гарантирует доставку. Если требуется надежная доставка, могут использоваться другие механизмы (например, локальное хранение логов на самом устройстве).

Удаление конфигурации:

```
(config)# no logging host
```

Удаляет настройку syslog-сервера. Если указать конкретный адрес, удаляется только он; без параметра удаляются все настроенные серверы.

Просмотр (Show):

```
# show logging
# show logging <logging_id: 1-4294967295>
# show logging [info] [warning] [error]
```

Команда `show logging` *отображает текущие настройки syslog, включая список настроенных серверов.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.24.3 (config)# logging level

Настройка уровня серьезности сообщений, отправляемых на syslog-сервер

Синтаксис:

```
(config)# logging level { info | warning | error }
```

Объяснение: Настройка того, какие типы сообщений будут отправляться на syslog-сервер.

Параметры:

- { info | warning | error }: Укажите один из вариантов сообщений лога.
    - ✓ info: Отправлять информационные сообщения, предупреждения и ошибки.
    - ✓ warning: Отправлять предупреждения и ошибки.
    - ✓ error: Отправлять только ошибки.

Рекомендации:

- Команда logging level задает **уровень важности (severity) сообщений**, которые будут отправляться на внешний syslog-сервер. Это позволяет фильтровать сообщения и отправлять только те, которые действительно важны, снижая нагрузку на сеть и сервер.
- **Иерархия уровней (от наиболее подробного к наименее подробному):**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ info **(информационный):** Самый подробный уровень. Включает все сообщения: информационные (например, о старте системы, изменениях конфигурации), предупреждения (например, о превышении порога) и ошибки. Рекомендуется для полного аудита, но может генерировать большой объем трафика.
- ✓ warning **(предупреждения):** Включает только предупреждения и ошибки. Информационные сообщения не отправляются. Хороший баланс между детализацией и объемом логов.
- ✓ error **(ошибки):** Самый строгий уровень. Отправляются только сообщения об ошибках (например, потеря линка, сбой протокола, аппаратные проблемы). Подходит для оперативного мониторинга критических событий.

- **Рекомендации по выбору:**
  - ✓ Для **постоянного мониторинга** обычно используют уровень warning или error, чтобы не перегружать сервер информационными сообщениями.
  - ✓ Для **диагностики и отладки** временно устанавливают уровень info, чтобы получить максимальную детализацию.
  - ✓ Для **соответствия стандартам безопасности** может требоваться отправка всех сообщений (включая информационные) на центральный сервер.

Просмотр:

```
# show logging
# show logging <logging_id: 1-4294967295>
# show logging [info] [warning] [error]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.25 Настройка защиты от петель (loop-protect) (config)# loop-protect

2.7.25.1 (config)# loop-protect

Глобальное включение защиты от петель

Синтаксис:

```
(config)# loop-protect
```

Объяснение: Включение функции защиты от петель (loop protection).

Рекомендации:

- Команда loop-protect **глобально активирует** функцию защиты от петель на коммутаторе. Эта функция предназначена для предотвращения образования сетевых петель (loops) уровня 2 на портах, где не используется протокол Spanning Tree Protocol (STP) или где STP может не сработать (например, на портах, подключенных к неуправляемым коммутаторам или конечным устройствам).
- **Как это работает:**
    1. На портах, где включена защита от петель (обычно на портах доступа), коммутатор периодически отправляет специальные **loop-protect-пакеты**.
    2. Если порт получает обратно тот же пакет, который он отправил (что возможно только при наличии петли), это означает обнаружение петли.
    3. При обнаружении петли коммутатор может **заблокировать порт** (временно или постоянно) и/или отправить системное сообщение (syslog).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    1. **Дополнительная защита:** В сетях, где STP отключен (например, по соображениям производительности или совместимости), loop-protect обеспечивает защиту от случайных петель.
    2. **Защита конечных портов:** На портах, подключенных к неуправляемым коммутаторам или хабам (которые не поддерживают STP), loop-protect может предотвратить распространение петель в управляемую сеть.
    3. **Быстрое обнаружение:** В отличие от STP, который может занимать десятки секунд для обнаружения и устранения петли, loop-protect может работать быстрее.
- **Взаимодействие со STP:** Эта функция обычно используется в дополнение к STP или на портах, где STP отключен. На портах с включенным STP может не требоваться.
- После глобального включения защиты от петель, её необходимо **включить на конкретных портах** (командой loop-protect в режиме интерфейса) для активации.

Удаление конфигурации:

```
(config)# no loop-protect
```

Глобально отключает функцию защиты от петель на коммутаторе.

Просмотр:

```
# show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
```

Отображает статус защиты от петель глобально и на конкретных портах.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.25.2 (config)# loop-protect shutdown-time

Настройка времени блокировки порта при обнаружении петли

Синтаксис:

```
(config)# loop-protect shutdown-time <t>
```

Параметры:

- <t: 0-604800>: Укажите значение времени блокировки. Допустимые значения от 0 до 604800 секунд (7 дней). Значение 0 означает, что порт остается заблокированным до следующей перезагрузки устройства.

Объяснение: Настройка периода, в течение которого порт будет оставаться отключенным (заблокированным).

Рекомендации:

- Команда loop-protect shutdown-time задает **время (в секундах)**, на которое порт будет автоматически отключен (переведен в состояние errdisable/shutdown) после обнаружения петли. По истечении этого времени порт автоматически возвращается в рабочее состояние и снова начинает проверять наличие петли.
- **Как это работает:**
    1. Функция защиты от петель обнаруживает петлю на порту.
    2. Порт переводится в состояние блокировки (shutdown) для предотвращения циркуляции трафика и дальнейшего ухудшения работы сети.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Через время, заданное shutdown-time, порт автоматически восстанавливается (активируется) и начинает мониторинг заново.
4. Если петля все еще существует, процесс повторяется.

- **Выбор значения:**
  1. 0 — порт блокируется до следующей перезагрузки устройства. Это требует ручного вмешательства администратора для восстановления порта (например, с помощью no shutdown или перезагрузки).
  2. Короткое время (например, 30–180 секунд) — порт восстанавливается быстро, что полезно в средах с временными нарушениями, но может привести к повторным блокировкам, если проблема не устранена.
  3. Длинное время (например, 3600 секунд и более) — дает администратору время на устранение проблемы до автоматического восстановления порта.
- **Рекомендуется** устанавливать разумное значение (например, 180–600 секунд) для автоматического восстановления портов после устранения проблемы, но не настолько короткое, чтобы порт постоянно переключался туда-обратно.

Удаление конфигурации:

```
(config)# no loop-protect shutdown-time
```

Сбрасывает время блокировки к значению по умолчанию (зависит от реализации).

Просмотр:

```
# show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.25.3 (config)# loop-protect transmit-time

Настройка интервала передачи тестовых пакетов защиты от петель

Синтаксис:

```
(config)# loop-protect transmit-time <t>
```

Параметры:

- <t: 1-10>: Укажите значение интервала передачи. Допустимые значения от 1 до 10 секунд.

Объяснение: Настройка интервала между отправкой каждого тестового пакета (PDU) защиты от петель на каждом порту.

Рекомендации:

- Команда loop-protect transmit-time задает **интервал времени (в секундах)**, с которым коммутатор отправляет специальные тестовые пакеты (loop-protect PDUs) на порты, где включена защита от петель. Эти пакеты используются для обнаружения петель в сети.
- **Как это работает:**
    1. Коммутатор периодически отправляет уникальный тестовый пакет на порт.
    2. Если порт получает обратно тот же самый пакет (что указывает на наличие петли в сети), срабатывает защита.
    3. Интервал transmit-time определяет, как часто отправляются эти тестовые пакеты.
- **Влияние на сеть:**
    1. **Короткий интервал (например, 1-2 секунды):** Обеспечивает более быстрое обнаружение

SEC.RU | Короткий путь к информации Скачано с sec.ru

петель, но увеличивает служебный трафик на порту. Рекомендуется для критических участков сети, где важна скорость реакции.

2. **Длинный интервал (например, 5-10 секунд):** Снижает служебный трафик, но увеличивает время обнаружения петли. Подходит для менее критичных портов или сетей с низкой плотностью трафика.

- **Значение по умолчанию:** Обычно 2-5 секунд. Рекомендуется выбирать баланс между скоростью обнаружения и служебной нагрузкой.

Удаление конфигурации:

```
(config)# no loop-protect transmit-time
```

Сбрасывает интервал передачи к значению по умолчанию.

Просмотр:

```
# show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
```

2.7.25.4 (config-if)# loop-protect

Включение защиты от петель на интерфейсе

Синтаксис:

```
(config-if)# loop-protect
```

Объяснение: Включение функции защиты от петель (loop protection) на данном интерфейсе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `loop-protect` в режиме конфигурации интерфейса **активирует защиту от петель на конкретном порту**. Для работы этой функции необходимо предварительно глобально включить защиту от петель командой `loop-protect` в глобальном режиме конфигурации.
- **На каких портах включать:**
    - ✓ **Порты доступа (access ports):** Рекомендуется включать на портах, подключенных к конечным пользователям, где возможно случайное создание петли (например, подключение неуправляемого коммутатора или соединение двух портов кабелем).
    - ✓ **Порты, где STP отключен:** На портах, где протокол Spanning Tree (STP) не используется или отключен, защита от петель является важной мерой безопасности.
    - ✓ **Порты, подключенные к неуправляемым коммутаторам:** Эти устройства не участвуют в STP, поэтому защита от петель на порту коммутатора предотвращает распространение петель в управляемую сеть.
- **Где не рекомендуется включать:**
    - ✓ **Магистральные порты (uplink) между управляемыми коммутаторами:** На этих портах уже работает STP, и защита от петель может быть избыточной или даже мешать нормальной работе протокола.
- **Принцип работы на порту:** Коммутатор периодически отправляет специальные тестовые пакеты на порт. Если порт получает обратно тот же пакет (что указывает на петлю), порт

SEC.RU | Короткий путь к информации Скачано с sec.ru

автоматически блокируется (shutdown) на время, заданное командой loop-protect shutdown-time.

Удаление конфигурации:

```
(config-if)# no loop-protect
```

Отключает защиту от петель на данном интерфейсе.

Просмотр:

```
# show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
```

Отображает статус защиты от петель на всех портах или на указанном интерфейсе.

2.7.25.5 (config-if)# loop-protect action

Настройка действия при обнаружении петли на порту

Синтаксис:

```
(config-if)# loop-protect action { [ shutdown ] [ log ] }
```

Объяснение: Настройка действия, выполняемого при обнаружении петель на порту.

Параметры:

- { [shutdown] [log] }: Когда на порту обнаружена петля, защита от петель немедленно выполняет соответствующие действия. Действия включают: "Отключить порт" (Shutdown Port),

SEC.RU | Короткий путь к информации Скачано с sec.ru

"Отключить порт и зарегистрировать событие" (Shutdown Port and Log) или "Только зарегистрировать событие" (Log Only).

Рекомендации:

- Команда `loop-protect action` позволяет настроить, как именно коммутатор будет реагировать на обнаружение петли на конкретном порту. Это дает гибкость в управлении поведением защиты в зависимости от важности порта и требований сети.
- **Варианты действий:**
  - ✓ `shutdown` **(только отключение):** При обнаружении петли порт переводится в состояние блокировки (shutdown/errdisable). Само событие не записывается в журнал (syslog) — только может быть видно в выводе команд `show loop-protect`. Подходит для портов, где важна автоматическая защита, но логирование не требуется.
  - ✓ `shutdown log` **(отключение и логирование):** Порт блокируется **и** в системный журнал (syslog) отправляется сообщение о событии. **Рекомендуемый вариант для большинства портов**, так как позволяет администратору узнать о проблеме и принять меры.
  - ✓ `log` **(только логирование):** Порт **не блокируется**, но событие записывается в журнал. Это "мягкий" режим, который позволяет отслеживать потенциальные проблемы без нарушения работы сети. Полезен для мониторинга или на портах, где блокировка недопустима.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Без параметров (или комбинация без shutdown):** Если действие не настроено явно, может использоваться поведение по умолчанию (часто shutdown log или log в зависимости от реализации).

- **Как задать параметры:** Параметры shutdown и log можно комбинировать:
  - ✓ loop-protect action shutdown — только отключение.
  - ✓ loop-protect action log — только логирование.
  - ✓ loop-protect action shutdown log — отключение и логирование.

Удаление конфигурации:

```
(config-if)# no loop-protect action
```

Сбрасывает настройку действия к значению по умолчанию (зависит от реализации).

Просмотр:

```
# show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
```

2.7.25.6 (config-if)# loop-protect tx-mode

Включение активной генерации тестовых пакетов защиты от петель на порту

Синтаксис:

```
(config-if)# loop-protect tx-mode
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Включение активной генерации тестовых пакетов (PDU) защиты от петель на порту.

Рекомендации:

- Команда loop-protect tx-mode в режиме конфигурации интерфейса **включает активную отправку тестовых пакетов** (loop-protect PDUs) на данном порту. Эти пакеты используются для обнаружения петель в сети.
- **Два режима работы порта:**
    - ✓ **Режим "передача включена" (**loop-protect tx-mode**):** Порт **активно отправляет** тестовые пакеты для обнаружения петель. Это стандартный и наиболее распространенный режим для портов, на которых включена защита от петель. Коммутатор периодически генерирует и отправляет уникальные тестовые пакеты.
    - ✓ **Режим "передача отключена" (**no loop-protect tx-mode**):** Порт **не отправляет** тестовые пакеты, но может **прослушивать** (слушать) входящие тестовые пакеты. Если порт получает тестовый пакет, который был отправлен с другого порта того же коммутатора, это также может указывать на петлю.
- **Зачем может потребоваться отключить передачу:**
    - ✓ **Снижение нагрузки:** На портах с очень высокой загрузкой можно отключить отправку тестовых пакетов, чтобы снизить служебный трафик.
    - ✓ **Специфические топологии:** В некоторых сетевых конфигурациях может быть достаточно только

SEC.RU | Короткий путь к информации Скачано с sec.ru

прослушивания входящих пакетов для обнаружения петель.

- ✓ **Порты, где передача нежелательна:** Например, на порту, подключенном к устройству, которое может некорректно реагировать на loop-protect PDUs.

- **Рекомендация:** На большинстве портов с включенной защитой от петель оставлять loop-protect tx-mode включенным (активным) для наиболее эффективного обнаружения.

Удаление конфигурации:

```
(config-if)# no loop-protect tx-mode
```

Отключает активную генерацию тестовых пакетов на порту. Порт не будет отправлять loop-protect PDUs.

Просмотр:

```
# show loop-protect [ interface ( <port_type> [ <plist> ] ) ]
```

2.7.26 Настройка таблицы MAC-адресов (mac) (config)# mac

2.7.26.1 (config)# mac address-table aging-time

Настройка времени устаревания (aging time) динамических MAC-адресов

Синтаксис:

```
(config)# mac address-table aging-time <v_0_10_to_1000000>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <v_0_10_to_1000000>: Укажите значение времени устаревания для таблицы MAC-адресов. Допустимые значения: от 10 до 1000000 секунд. Используйте 0 для отключения функции устаревания.

Объяснение: Настройка времени устаревания (aging time) для изученных MAC-адресов в таблице MAC-адресов.

Рекомендации:

- Команда mac address-table aging-time задает **время жизни динамических записей в таблице MAC-адресов**. Динамические записи — это MAC-адреса, которые коммутатор узнает, наблюдая за входящим трафиком.
- **Как это работает:**
    1. Коммутатор изучает MAC-адреса устройств, видя трафик, поступающий на порты.
    2. Каждая динамическая запись имеет таймер устаревания (aging timer).
    3. Каждый раз, когда коммутатор видит трафик с этого MAC-адреса, таймер сбрасывается.
    4. Если в течение времени, заданного aging-time, трафик с этого MAC-адреса не появляется, запись удаляется из таблицы.
- **Влияние на сеть:**
    1. **Слишком короткое время (например, 10-60 секунд):** Записи быстро удаляются, что может привести

SEC.RU | Короткий путь к информации Скачано с sec.ru

к излишнему flooding (широковещательной рассылке) трафика на неизвестные MAC-адреса, так как коммутатору приходится заново изучать адреса. Может увеличить нагрузку на сеть.

2. **Слишком длинное время (например, 86400 секунд и более):** Таблица может содержать устаревшие записи (например, если устройство было перемещено или отключено), что может вызывать неправильную пересылку трафика и "загрязнение" таблицы.
3. **Значение 0 (отключено):** Динамические записи никогда не удаляются. Таблица может переполниться, и коммутатор может начать отказывать в изучении новых адресов.

- Стандартное значение времени устаревания обычно составляет **300 секунд (5 минут)**. Это баланс между эффективностью коммутации и актуальностью таблицы.

Удаление конфигурации:

```
(config)# no mac address-table aging-time
(config)# no mac address-table aging-time <v_0_10_to_1000000>
```

Сбрасывает время устаревания к значению по умолчанию (обычно 300 секунд).

Просмотр:

```
> show mac address-table [ conf | static | aging-time | { { learning | count } [ in
terface ( <port_type> [ <v_port_type_list> ] ) ] } | { address <v_mac_addr> [ vl
an <v_vlan_id> ] } | vlan <v_vlan_id> | interface ( <port_type> [ <v_port_type
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
_list_1> ] ) ]
# show mac address-table [ conf | static | aging-time | { { learning | count } [ in
terface ( <port_type> [ <v_port_type_list> ] ) ] } | { address <v_mac_addr> [ vl
an <v_vlan_id> ] } | vlan <v_vlan_id> | interface ( <port_type> [ <v_port_type
_list_1> ] ) ]
# show mac address-table aging-time
```

2.7.26.2 (config)# mac address-table static

Настройка статической записи в таблице MAC-адресов

Синтаксис:

```
(config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> interface
( <port_type> [ <v_port_type_list> ] )
```

Параметры:

- <v_mac_addr>: Укажите MAC-адрес в формате xx:xx:xx:xx:xx:xx.
- vlan <v_vlan_id>: Укажите идентификатор VLAN для данной записи.
- interface (<port_type> [<v_port_type_list>]): Укажите тип интерфейса и номер порта.

Объяснение: Настройка статической таблицы отображения MAC-адресов.

Рекомендации:

- Команда mac address-table static создает **статическую запись** в таблице MAC-адресов, которая принудительно связывает

SEC.RU | Короткий путь к информации Скачано с sec.ru

указанный MAC-адрес с определенным портом (или диапазоном портов) в указанной VLAN.

- **В отличие от динамических записей:**
  - ✓ Статические записи **не устаревают** (не удаляются по таймеру aging-time).
  - ✓ Они **не перезаписываются** динамически изученными адресами.
  - ✓ Сохраняются в конфигурации и восстанавливаются после перезагрузки.
- **Зачем это нужно:**
  - ✓ **Безопасность:** Предотвращает атаки с подменой MAC-адреса (MAC spoofing), фиксируя MAC-адрес критически важного устройства (сервер, шлюз) на определенном порту.
  - ✓ **Фиксация местоположения:** Гарантирует, что трафик для определенного устройства всегда направляется на правильный порт, даже если устройство временно отключено.
  - ✓ **Обход изучения:** Используется для устройств, которые не генерируют трафик, но должны быть достижимы (например, принтеры в режиме ожидания).
- При создании статической записи для одного MAC-адреса можно указать несколько портов (например, для транковых линков), но обычно статическая запись привязывается к одному порту для предотвращения петель.

Удаление конфигурации (Negation):

```
(config)# no mac address-table static <v_mac_addr> vlan <v_vlan_id> interface ( <port_type> [ <v_port_type_list> ] )
```

Удаляет указанную статическую запись из таблицы MAC-адресов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
> show mac address-table [ conf | static | aging-time | { { learning | count } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } | { address <v_mac_addr> [ vlan <v_vlan_id> ] } | vlan <v_vlan_id> | interface ( <port_type> [ <v_port_type_list_1> ] ) ]
# show mac address-table [ conf | static | aging-time | { { learning | count } [ interface ( <port_type> [ <v_port_type_list> ] ) ] } | { address <v_mac_addr> [ vlan <v_vlan_id> ] } | vlan <v_vlan_id> | interface ( <port_type> [ <v_port_type_list_1> ] ) ]
```

Очистка:

```
# clear mac address-table
```

Очищает все динамические записи в таблице MAC-адресов (статические записи сохраняются).

2.7.26.3 (config-if)# mac address-table learning

Настройка режима изучения MAC-адресов на интерфейсе

Синтаксис:

```
(config-if)# mac address-table learning [ secure ]
```

Параметры:

- [secure]: Только статические MAC-записи, перечисленные в Таблице статических MAC-адресов (Static MAC Table), будут изучены. Все остальные будут отброшены.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Установка данного интерфейса в защищенный (secure) режим.

Рекомендации:

- Команда mac address-table learning в режиме конфигурации интерфейса управляет тем, как порт изучает MAC-адреса.
- **Два режима работы:**
  - ✓ mac address-table learning (без параметра secure**):** Включает обычное динамическое изучение MAC-адресов на порту (режим по умолчанию). Порт изучает MAC-адреса из входящего трафика и добавляет их в таблицу MAC-адресов.
  - ✓ mac address-table learning secure (с параметром secure**):** Включает **защищенный (secure) режим** изучения. В этом режиме порт изучает (добавляет в таблицу) только те MAC-адреса, которые явно указаны в статической таблице MAC-адресов (mac address-table static). Все остальные MAC-адреса, появляющиеся на порту, будут отброшены.
- **Зачем нужен защищенный режим:**
  - ✓ **Максимальная безопасность:** Гарантирует, что на порту могут подключаться только заранее определенные устройства (серверы, принтеры), чьи MAC-адреса внесены в статическую таблицу. Любое другое устройство будет заблокировано.
  - ✓ **Предотвращение атак:** Защищает от атак с подменой MAC-адреса (MAC flooding) и несанкционированного подключения.
- **Внимание!** Перед включением защищенного режима на порту, через который осуществляется управление коммутатором

SEC.RU | Короткий путь к информации Скачано с sec.ru

(например, порт, используемый для Telnet/SSH-доступа или консольный порт), необходимо предварительно добавить MAC-адрес управляющего устройства в статическую таблицу MAC-адресов. В противном случае **управление коммутатором будет потеряно**, и восстановить доступ можно будет только через другой незащищенный порт или через последовательный интерфейс (консоль).

Удаление конфигурации:

```
(config-if)# no mac address-table learning [ secure ]
```

Отключает защищенный режим, возвращая порт к обычному динамическому изучению MAC-адресов.

Просмотр:

```
> show mac address-table [ conf | static | aging-time | { { learning | count } [
interface ( <port_type> [ <v_port_type_list> ] ) ] } | { address <v_mac_addr> [
vlan <v_vlan_id> ] } | vlan <v_vlan_id> | interface ( <port_type> [
<v_port_type_list_1> ] ) ]
# show mac address-table [ conf | static | aging-time | { { learning | count } [
interface ( <port_type> [ <v_port_type_list> ] ) ] } | { address <v_mac_addr> [
vlan <v_vlan_id> ] } | vlan <v_vlan_id> | interface ( <port_type> [
<v_port_type_list_1> ] ) ]
```

Для проверки режима изучения на порту используйте show mac address-table learning interface <port>.

Очистка:

```
# clear mac address-table
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.27 (config-if)# media-type

Настройка типа носителя (медиа) для интерфейса

Синтаксис:

```
(config-if)# media-type { rj45 | sfp | dual }
```

Объяснение: Настройка типа носителя (медиа), поддерживаемого для данного конкретного интерфейса.

Параметры:

- { rj45 | sfp | dual }: Варианты: RJ-45, SFP или dual (поддерживаются оба — RJ-45 и SFP).

Рекомендации:

- Команда media-type используется на комбинированных портах (combo ports), которые имеют **два физических интерфейса на одном порту** — обычно это медный порт RJ-45 и оптический порт SFP (Small Form-factor Pluggable). Эти порты разделяют один логический интерфейс, и одновременно активным может быть только один тип носителя.
- **Варианты:**
  - ✓ rj45: Активен медный порт RJ-45 (витая пара). SFP-порт отключен.
  - ✓ sfp: Активен оптический SFP-порт (модуль SFP). RJ-45 порт отключен.
  - ✓ dual: Оба порта могут быть активны (если поддерживается аппаратно, но как правило, на

SEC.RU | Короткий путь к информации Скачано с sec.ru

комбинированных портах это не так; чаще этот параметр означает автоматическое определение или возможность использования любого).

- **Зачем это нужно:**
  - ✓ Комбинированные порты позволяют гибко выбирать тип подключения (медь или оптика) без необходимости занимать два отдельных порта на коммутаторе. Администратор выбирает нужный тип в зависимости от расстояния и условий прокладки кабеля.
- **Внимание!** Если SFP-модуль установлен, а порт настроен на rj45, оптический интерфейс не будет работать, и наоборот. Убедитесь, что настройка соответствует физически подключенному кабелю/модулю.
- Если порт не является комбинированным (имеет только один физический интерфейс), эта команда может не применяться или не иметь эффекта.

Удаление конфигурации:

```
(config-if)# no media-type
```

Сбрасывает настройку типа носителя к значению по умолчанию (зависит от модели).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.28 (config-if)# mtu

Настройка максимального блока передачи (MTU) для интерфейса

Синтаксис:

```
(config-if)# mtu <max_length>
```

Объяснение: Настройка максимального блока передачи (Maximum Transmission Unit, MTU) для данного конкретного интерфейса.

Параметры:

- <max_length: 1518-9600>: Укажите значение MTU. Диапазон от 1518 до 9600 байт.

Рекомендации:

- Команда mtu задает **максимальный размер кадра (frame)**, который может быть передан или принят на данном порту без фрагментации.
- **Стандартное значение (1518 байт):** Соответствует стандартному Ethernet-кадру (1500 байт полезной нагрузки + 18 байт заголовков Ethernet: MAC-адреса назначения/источника, EtherType и FCS). Это значение используется в большинстве сетей.
- **Jumbo Frames (значения выше 1518):** Позволяют передавать кадры большего размера (до 9600 байт и более, в зависимости от оборудования). Использование jumbo frames может повысить эффективность передачи больших объемов данных за счет уменьшения накладных расходов (меньшее количество кадров, меньшее количество заголовков, снижение нагрузки на CPU).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Когда использовать jumbo frames:**
    - ✓ В **дата-центрах** и **сетях хранения данных** для передачи больших блоков данных между серверами и хранилищами.
    - ✓ На **магистральных линках (uplink)** между коммутаторами для повышения пропускной способности и эффективности.
    - ✓ Для передачи multicast трафика в некоторых случаях (видео по ethernet и т.д.)
- **Внимание!** Все устройства в одном широковещательном домене (VLAN) должны иметь одинаковое значение MTU. Если на одном устройстве установлен jumbo frame (например, 9000), а на другом — стандартный (1500), кадры большего размера будут отбрасываться или фрагментироваться, что приведет к проблемам с соединением.
- **Влияние на конфигурацию VLAN:** MTU на порту транка должен быть достаточным для передачи кадров с тегами VLAN (добавляется 4 байта для 802.1Q). Если на порту включены тегированные VLAN, MTU должен учитывать этот дополнительный размер.

Удаление конфигурации:

```
(config-if)# no mtu
```

Сбрасывает MTU к значению по умолчанию (обычно 1518 байт).

Просмотр:

```
# show interface ( <port_type> [ <v_port_type_list> ] ) status
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29 Настройка MEP (Maintenance End Point) (config)# mep

2.7.29.1 (config)# mep <inst>

Создание экземпляра MEP (Maintenance End Point)

Синтаксис:

(config)# mep <inst> [mip] { up | down } domain { port | evc | vlan } [vid <vid>] flow <flow> level <level> interface <port_type> <port>

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- [mip]: Режим MIP (Maintenance Entity Intermediate Point) — промежуточная точка обслуживания.
- { up | down }: Укажите направление трафика (входящий или исходящий) для мониторинга на порту резиденции.
- domain { port | evc | vlan }: Укажите опцию домена.
    - ✓ **port**: Это MEP в домене порта. "Экземпляр потока" (Flow Instance) — это порт. (В настоящее время доступен для использования порт.)
    - ✓ **evc**: Это MEP в домене EVC. "Экземпляр потока" — это EVC. EVC должен быть создан.
    - ✓ **vlan**: Это MEP в домене VLAN. "Экземпляр потока" — это VLAN. VLAN должна быть создана.
- [vid <vid>]: AC-тег или S-тег (в зависимости от типа VLAN порта) добавляется с этим VID. Ввод 0 означает, что тег не будет добавлен.
- flow <flow>: MEP, связанный с этим потоком.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- level <level>: Уровень MEP (MEG Level).
- interface <port_type> <port>: Укажите номер порта, который вы хотите мониторить.

Объяснение: Создание экземпляра MEP.

Рекомендации:

- Команда mep создает экземпляр конечной точки обслуживания (MEP — Maintenance End Point), который используется в рамках стандартов **IEEE 802.1ag** (CFM — Connectivity Fault Management) и **ITU-T Y.1731**. Эти протоколы предназначены для диагностики, мониторинга и измерения производительности в Ethernet-сетях уровня операторской связи (Carrier Ethernet).
- MEP — это логическая конечная точка в рамках домена обслуживания (Maintenance Domain). MEP могут генерировать и принимать служебные сообщения для проверки связности, измерения задержек, потерь и других параметров. MIP (Maintenance Intermediate Point) — это промежуточная точка, которая может отвечать на некоторые запросы, но не инициирует их.
- **Ключевые параметры:**
  - ✓ up / down: Определяет направление мониторинга. up — мониторинг трафика, идущего к процессору коммутатора (внутренний); down — мониторинг трафика, выходящего на линк (внешний).
  - ✓ domain: Определяет уровень, на котором работает MEP. port — на уровне физического порта; vlan — на уровне VLAN; evc — на уровне EVC (Ethernet Virtual Connection), используется в сетях операторов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ level: Уровень MEG (Maintenance Entity Group) от 0 до 7. Чем выше уровень, тем шире область обслуживания. Например, уровень 7 может использоваться для клиентской сети, уровень 3 — для операторской инфраструктуры.

- Эти настройки требуют глубокого понимания стандартов CFM/Y.1731 и обычно используются в сложных сетях провайдеров.

Удаление конфигурации:

```
(config)# no mep <inst>
```

Удаляет указанный экземпляр MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Отображает информацию о MEP, соседях, результатах измерений и тестов.

2.7.29.2 (config)# mep <inst> ais

Настройка AIS (Alarm Indication Signal) для экземпляра MEP

Синтаксис:

```
(config)# mep <inst> ais [ fr1s | fr1m ] [ protect ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Настройка AIS для экземпляра MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- ais [fr1s | fr1m]: AIS расшифровывается как Alarm Indication Signal (сигнал индикации тревоги). fr1s означает частоту кадров 1 кадр в секунду. fr1m означает частоту кадров 1 кадр в минуту.
- [protect]: AIS может использоваться для защиты. В момент изменения состояния передаются три AIS PDU максимально быстро.

Рекомендации:

- Команда mep <inst> ais настраивает функцию **AIS (Alarm Indication Signal)** для указанного экземпляра MEP. AIS является частью стандартов **ITU-T Y.1731** и **IEEE 802.1ag (CFM)** и используется для подавления вторичных аварийных сигналов в сетях операторской связи.
- **Что такое AIS?** Это сигнал, который генерируется MEP (или MIP) при обнаружении сбоя (потери связности) на вышестоящем уровне обслуживания. AIS передается "вниз" по иерархии обслуживания, чтобы уведомить нижестоящие уровни о наличии проблемы, не генерируя при этом множество избыточных аварийных сигналов. Это позволяет "подавить" вторичные аварийные сигналы и избежать их лавинообразного распространения.
- **Параметры:**
    - ✓ fr1s **(1 кадр в секунду):** Высокая частота отправки AIS-кадров. Используется для быстрого уведомления о сбое

SEC.RU | Короткий путь к информации Скачано с sec.ru

в сетях с жесткими требованиями к времени восстановления.

- ✓ fr1m **(1 кадр в минуту):** Низкая частота отправки AIS-кадров. Используется в менее критичных сегментах или для снижения служебного трафика.

- protect**:** Включает режим защиты. При изменении состояния (например, при переходе из нормального состояния в состояние сбоя) три AIS PDU передаются немедленно (как можно быстрее), чтобы ускорить оповещение о проблеме.

Удаление конфигурации:

```
(config)# no mep <inst> ais
```

Отключает функцию AIS для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

2.7.29.3 (config)# mep <inst> aps

Настройка APS (Automatic Protection Switching) для экземпляра MEP

Синтаксис:

```
(config)# mep <inst> aps <prio> [ multi | uni ] { laps | { raps [ octet <octet> ] } }
```

Объяснение: Настройка APS для экземпляра MEP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- aps <prio>: Приоритет, который будет вставлен в биты PCP в теге (если есть).
- [multi | uni]: Укажите один из вариантов.
    - ✓ multi: OAM PDU передается с многоадресным MAC-адресом. Должен использоваться multi в случае RAPS (Ring Automatic Protection Switching Protocol — протокол автоматического переключения защиты в кольце).
    - ✓ uni: OAM PDU передается с одноадресным MAC-адресом. MAC-адрес берется из базы данных MAC-адресов MEP-соседа. Этот вариант возможен только в случае LAPS (Linear Automatic Protection Switching Protocol — протокол автоматического переключения защиты в линейной топологии).
- { laps | { raps [octet <octet>] } }: Укажите один из вариантов.
    - ✓ laps: APS PDU передается как L-APS (для ELPS — Ethernet Linear Protection Switching).
    - ✓ raps: APS PDU передается как R-APS (для ERPS — Ethernet Ring Protection Switching).
    - ✓ octet: Это последний октет (байт) передаваемого и ожидаемого многоадресного MAC-адреса RAPS. В стандарте G.8031 (03/2010) многоадресный MAC-адрес RAPS определен как 01-19-A7-00-00-XX. В текущем стандарте значение для этого последнего октета равно '01', а использование других значений оставлено для дальнейшего изучения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `mep <inst> aps` настраивает **APS (Automatic Protection Switching)** для указанного экземпляра MEP. APS является частью стандартов защиты Ethernet на уровне операторской связи (Carrier Ethernet) — **G.8031 (линейная защита)** и **G.8032 (кольцевая защита)**.
- APS обеспечивает автоматическое переключение на резервный путь (защиту) при обнаружении сбоя на основном пути, обычно с целью восстановления связи менее чем за 50 мс.
- **Два основных типа APS:**
    - ✓ **LAPS (Linear APS):** Используется в линейных топологиях (точка-точка). В этом случае APS PDU передаются на **одноадресный (unicast)** MAC-адрес соседнего MEP.
    - ✓ **RAPS (Ring APS):** Используется в кольцевых топологиях (ERPS). В этом случае APS PDU передаются на **многоадресный (multicast)** MAC-адрес, определяемый стандартом.
- **Параметры:**
    - ✓ `prio`: Задает приоритет (PCP — Priority Code Point) в теге VLAN для APS PDU. Обычно для служебного трафика устанавливается высокий приоритет.
    - ✓ `octet`: Для RAPS позволяет настроить последний байт многоадресного MAC-адреса. Обычно используется значение `01`.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no mep <inst> aps
```

Удаляет настройку APS для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

2.7.29.4 (config)# mep <inst> cc

Настройка проверки непрерывности (Continuity Check) для экземпляра MEP

Синтаксис:

```
(config)# mep <inst> cc <prio> [ fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h ]
```

Объяснение: Настройка проверки непрерывности (Continuity Check) для экземпляра MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- cc: Проверка непрерывности (Continuity Check).
- <prio: 0-7>: Приоритет, который будет вставлен в биты PCP в теге (если есть).
- [fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h]: Частота кадров: 300 кадров/сек, 100 кадров/сек, 10 кадров/сек, 1 кадр/сек, 6 кадров/мин, 1 кадр/мин, 6 кадров/час.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда mep <inst> cc настраивает функцию **CC (Continuity Check)** для указанного экземпляра MEP. CC является частью стандартов **IEEE 802.1ag** (CFM – Connectivity Fault Management) и **ITU-T Y.1731**.
- **CC** Это механизм для непрерывного мониторинга связности между MEP в рамках домена обслуживания (Maintenance Domain). MEP периодически отправляют CC-сообщения (CCM — Continuity Check Messages) друг другу. Если в течение определенного времени (обычно в 3.5 раза больше интервала передачи) CC-сообщение не получено, это интерпретируется как потеря связности (сбой).
- **Частоты передачи (Frame Rates):**
    - ✓ **Высокие частоты (fr300s, fr100s, fr10s, fr1s):** Обеспечивают быстрое обнаружение сбоев (миллисекунды-секунды). Используются на критически важных линках, где требуется быстрая реакция (например, для триггера APS).
    - ✓ **Средние частоты (fr6m, fr1m):** Обеспечивают баланс между скоростью обнаружения и служебным трафиком. Часто используются в стандартных конфигурациях.
    - ✓ **Низкая частота (fr6h):** Используется для долгосрочного мониторинга с минимальным служебным трафиком.
- **Параметр** prio**:** Задает приоритет (PCP — Priority Code Point) для CC-сообщений в теге VLAN. Рекомендуется устанавливать высокий приоритет (5-7), чтобы гарантировать доставку служебных сообщений даже при перегрузке сети.

Удаление конфигурации:

```
(config)# no mep <inst> cc
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Отключает проверку непрерывности для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

2.7.29.5 (config)# mep <inst> client domain

Настройка домена клиентского уровня для экземпляра MEP

Синтаксис:

```
(config)# mep <inst> client domain { evc | vlan }
```

Объяснение: Настройка домена клиентского уровня для экземпляра MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- { evc | vlan }: Домен клиентского уровня. Доступны варианты: домен EVC и домен VLAN.

Рекомендации:

- Команда mep <inst> client domain определяет **домен клиентского уровня (client layer domain)** для указанного экземпляра MEP. Это важная концепция в иерархических моделях обслуживания Ethernet, используемых в стандартах **IEEE 802.1ag (CFM)** и **ITU-T Y.1731**.
- **Иерархия доменов (Client-Server Relationship):** В сетях операторской связи часто используется иерархическая

SEC.RU | Короткий путь к информации Скачано с sec.ru

структура, где один уровень обслуживания (серверный) предоставляет транспорт для вышестоящего уровня (клиентского). Например:

- ✓ **Домен VLAN (сервер):** Транспортный уровень, предоставляющий VLAN-соединения.
- ✓ **Домен EVC (клиент):** Клиентский уровень, который использует VLAN для передачи своих сервисов (EVC — Ethernet Virtual Connection).

- **Зачем это нужно:** Установление связи между доменами позволяет:
  - ✓ **Подавление аварийных сигналов:** Если происходит сбой на серверном уровне (например, VLAN), MEP на этом уровне может сгенерировать AIS (Alarm Indication Signal), который будет передан в клиентский домен (EVC), чтобы уведомить его о проблеме и предотвратить генерацию избыточных аварийных сигналов.
  - ✓ **Согласованное управление:** Позволяет связать мониторинг и защиту между разными уровнями обслуживания.
- **Параметры:**
  - ✓ vlan: Указывает, что клиентский домен использует VLAN.
  - ✓ evc: Указывает, что клиентский домен использует EVC (Ethernet Virtual Connection).

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.6 (config)# mep <inst> client flow

Настройка приоритета для передачи AIS и LCK в клиентском потоке

Синтаксис:

(config)# mep <inst> client flow <cflow> level <level> [ais-prio [<aisprio> | ais-highest]] [lck-prio [<lckprio> | lck-highest]]

Объяснение: Настройка приоритета, используемого при передаче AIS в каждом клиентском потоке.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- client flow <cflow: unit>: Номер потока клиентского уровня.
- level <level: 0-7>: Значение уровня MEG (Maintenance Entity Group).
- [ais-prio [<aisprio:0-7> | ais-highest]]: Настройка приоритета для инъекции AIS. Укажите значение от 0 до 7 или наивысший возможный приоритет.
- [lck-prio [<lckprio:0-7> | lck-highest]]: Настройка приоритета для инъекции LCK. Укажите значение от 0 до 7 или наивысший возможный приоритет.

Рекомендации:

- Команда mep <inst> client flow настраивает параметры для **клиентского потока (client flow)**, связанного с данным экземпляром MEP. Эта команда используется в иерархических конфигурациях обслуживания, где один MEP (серверный) обслуживает несколько клиентских потоков (например, EVC или VLAN).
- **Параметр** level**:** Задает уровень MEG (Maintenance Entity Group) для клиентского потока. Уровни MEG (0-7) используются для

SEC.RU | Короткий путь к информации Скачано с sec.ru

иерархического разделения доменов обслуживания. Более низкие уровни обычно соответствуют более высоким уровням иерархии (ближе к клиенту).

- **AIS (Alarm Indication Signal) и LCK (Locked Signal):**
  - ✓ **AIS:** Сигнал, указывающий на наличие проблемы на вышестоящем уровне обслуживания. Используется для подавления вторичных аварийных сигналов.
  - ✓ **LCK (Locked Signal):** Сигнал, указывающий, что обслуживание заблокировано (например, для планового технического обслуживания) и недоступно.
- **Приоритеты AIS и LCK:**
  - ✓ ais-prio **/** lck-prio**:** Задает конкретный приоритет (0-7) для этих служебных сообщений. Высокий приоритет (например, 7) гарантирует, что они будут обработаны раньше пользовательского трафика.
  - ✓ ais-highest **/** lck-highest**:** Автоматически устанавливает наивысший возможный приоритет для этих сообщений.
- Эта команда позволяет тонко настроить поведение при передаче служебных сообщений в клиентские потоки, что важно для корректной работы механизмов защиты и подавления аварийных сигналов в сложных иерархических сетях.

Удаление конфигурации:

```
(config)# no mep <inst> client-flow { <cflow> | all }
```

*Удаляет настройки для указанного клиентского потока или для всех потоков (*all*).*

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.7 (config)# mep <inst> dm

Настройка измерения задержки (Delay Measurement, DM) для MEP

Синтаксис:

```
(config)# mep <inst> dm <prio> [ multi | { uni mep-id <mepid> } ] [ single | dual ] [ rdtrp | flow ] interval <interval> last-n <lastn>
```

Объяснение: Настройка измерения задержки (Delay Measurement) для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- dm <prio: 0-7>: Настройка значения приоритета для измерения задержки (DM). Приоритет в случае тегированного OAM. В домене EVC это COS-ID.
- [multi | { uni mep-id <mepid> }]: Укажите многоадресный (multicast) или одноадресный (unicast) идентификатор MEP.
- [single | dual]: Одностороннее (One-Way) или двустороннее (Two-Way) измерение задержки, реализуемое с помощью 1DM или DMM/DMR соответственно.
- [rdtrp | flow]: Укажите одно значение.
    - ✓ **rdtrp**: Задержка кадра рассчитывается по временным меткам отправки и получения инициатора. Задержка кадра = RxTimeb - TxTimeStampf.
    - ✓ **flow**: Задержка кадра рассчитывается по временным меткам отправки и получения инициатора и удаленной стороны. Задержка кадра = (RxTimeb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- interval <interval>: Интервал между передачами PDU в 10 мс. Минимальное значение — 10.
- last-n <lastn>: Последние N задержек, используемых для расчета среднего значения за последние N. Минимальное значение — 10.

Рекомендации:

- Команда mep <inst> dm настраивает функцию **измерения задержки (Delay Measurement, DM)** для указанного экземпляра MEP. DM является частью стандартов **ITU-T Y.1731** и используется для измерения производительности Ethernet-сетей.
- **Типы измерения задержки:**
  - ✓ **Одностороннее (One-Way,** single**):** Измеряется с помощью сообщений 1DM (One-Way Delay Measurement). Требует синхронизации времени между двумя MEP (обычно с помощью PTP или NTP). Результат = время получения - время отправки.
  - ✓ **Двустороннее (Two-Way,** dual**):** Измеряется с помощью сообщений DMM (Delay Measurement Message) и DMR (Delay Measurement Reply). Не требует синхронизации времени. Результат = (время получения ответа - время отправки запроса) - (время обработки на удаленной стороне).
- **Расчет задержки (**rdtrp **vs** flow**):**
  - ✓ rdtrp **(Round Trip):** Измеряет полное время туда и обратно (RTT — Round Trip Time). Это наиболее распространенный метод для двустороннего измерения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ flow **(Frame Delay):** Измеряет одностороннюю задержку кадра с вычетом времени обработки на удаленной стороне.

- **Параметры:**
  - ✓ prio**:** Приоритет служебных сообщений DM. Рекомендуется высокий приоритет (5-7).
  - ✓ multi **/** uni**:** Определяет, отправляются ли DM-сообщения на многоадресный или конкретный одноадресный MEP-сосед.
  - ✓ interval**:** Частота отправки DM-сообщений (в 10-миллисекундных интервалах). Например, interval 100 = 1 секунда.
  - ✓ last-n**:** Количество последних измерений, используемых для расчета средних значений.

Удаление конфигурации:

```
(config)# no mep <inst> dm
```

Отключает измерение задержки для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.8 (config)# mep <inst> dm ns

Настройка измерения задержки в наносекундах для MEP

Синтаксис:

```
(config)# mep <inst> dm ns
```

Объяснение: Настройка измерения задержки (Delay Measurement) в наносекундах для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

Рекомендации:

- Команда mep <inst> dm ns включает режим измерения задержки (Delay Measurement, DM) с наносекундной точностью для указанного экземпляра MEP. Это расширение стандартных функций DM, определенных в ITU-T Y.1731.
- В высокопроизводительных сетях, таких как дата-центры, финансовые сети и сети операторов связи, может потребоваться измерение задержки с очень высокой точностью (наносекунды) для:
    - ✓ Мониторинга производительности критически важных приложений (торговые платформы, высокочастотный трейдинг).
    - ✓ Соответствия строгим требованиям SLA (Service Level Agreement) по задержке.
    - ✓ Диагностики микрозадержек и джиттера.
- **Как это работает:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Стандартные DM-сообщения (1DM, DMM/DMR) используют временные метки с точностью до микросекунд (или более низкой).
- ✓ При включении режима dm ns, временные метки в DM-сообщениях формируются с **наносекундной точностью**, что позволяет измерять задержки с гораздо более высокой детализацией.

- **Важные требования:**
  - ✓ Для корректной работы наносекундного DM необходима **высокоточная синхронизация времени** между MEP, обычно с использованием **PTP (Precision Time Protocol, IEEE 1588)**.
  - ✓ Оба MEP (инициатор и получатель) должны поддерживать и быть настроены на наносекундный режим DM.
- Эта команда обычно используется вместе с базовыми настройками DM (mep <inst> dm), задающими приоритет, тип (одно-/двусторонний) и интервал.

Удаление конфигурации:

```
(config)# no mep <inst> dm ns
```

Отключает режим измерения задержки в наносекундах, возвращаясь к стандартной (микросекундной) точности.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.9 (config)# mep <inst> dm overflow-reset

Автоматический сброс результатов измерения задержки при переполнении счетчика

Синтаксис:

```
(config)# mep <inst> dm overflow-reset
```

Объяснение: Сброс всех результатов измерения задержки (Delay Measurement) при переполнении счетчика общей задержки.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

Рекомендации:

- Команда mep <inst> dm overflow-reset включает функцию **автоматического сброса статистики измерения задержки (DM)**, когда внутренние счетчики, используемые для накопления данных (например, суммарная задержка или количество измерений), достигают максимального значения (переполнение).
- **Зачем это нужно:**
    - ✓ В процессе длительного мониторинга производительности (DM) счетчики, накапливающие суммарную задержку, количество измерений и другие параметры, могут достичь своего максимального значения (переполниться).
    - ✓ При переполнении без автоматического сброса статистика может стать некорректной (например,

SEC.RU | Короткий путь к информации Скачано с sec.ru

суммарная задержка может "обнулиться" неожиданно, а средние значения — исказиться).

- ✓ Включение этой функции гарантирует, что при достижении предельного значения счетчики будут **автоматически сброшены**, и сбор статистики продолжится корректно с нуля.

- **Альтернатива:** Если функция не включена (no mep <inst> dm overflow-reset), администратору может потребоваться периодически вручную очищать статистику DM (командой clear mep <inst> dm) для предотвращения проблем с переполнением.
- **Рекомендуется** включать эту функцию для долгосрочного непрерывного мониторинга производительности, чтобы избежать необходимости ручного сброса статистики.

Удаление конфигурации:

```
(config)# no mep <inst> dm overflow-reset
```

Отключает автоматический сброс статистики DM при переполнении. Администратор должен будет вручную очищать статистику при необходимости.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Статус функции overflow-reset может отображаться в детальном выводе DM.

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.10 (config)# mep <inst> dm proprietary

Использование проприетарного (собственного) измерения задержки

Синтаксис:

```
(config)# mep <inst> dm proprietary
```

Объяснение: Использовать проприетарное измерение задержки (Proprietary Delay Measurement).

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

Рекомендации:

- Команда mep <inst> dm proprietary переводит функцию **измерения задержки (Delay Measurement, DM)** для указанного экземпляра MEP в **проприетарный (собственный) режим**, специфичный для данного производителя оборудования.
- **Зачем это нужно:**
    - ✓ **Расширенные возможности:** Проприетарные реализации DM могут предлагать дополнительные функции, не предусмотренные стандартами ITU-T Y.1731 или IEEE 802.1ag. Например, более высокую частоту измерений, расширенную статистику, интеграцию с другими проприетарными протоколами.
    - ✓ **Совместимость:** В сетях, построенных на оборудовании одного вендора, использование проприетарного DM

SEC.RU | Короткий путь к информации Скачано с sec.ru

может обеспечить более полную функциональность и оптимизацию по сравнению со стандартными методами.

- ✓ **Специфические требования:** Некоторые приложения могут требовать особых алгоритмов измерения задержки, которые реализованы только в проприетарном решении.

- **Внимание!** При использовании проприетарного DM **оба MEP (инициатор и получатель) должны быть от одного производителя и поддерживать одинаковый проприетарный режим**. В противном случае измерение задержки работать не будет.
- Если проприетарный режим не требуется или требуется совместимость с оборудованием других вендоров, следует использовать стандартный DM (команда `mep <inst> dm` без параметра `proprietary` или с явным указанием `no mep <inst> dm proprietary`).

Удаление конфигурации:

```
(config)# no mep <inst> dm proprietary
```

Отключает проприетарный режим, возвращаясь к стандартному (стандартизированному) измерению задержки.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.11 (config)# mep <inst> dm synchronized

Настройка синхронизации времени для измерения задержки

Синтаксис:

```
(config)# mep <inst> dm synchronized
```

Объяснение: Настройка синхронизации времени для измерения задержки (Delay Measurement).

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

Рекомендации:

- Команда mep <inst> dm synchronized включает режим **синхронизированного измерения задержки (Synchronized Delay Measurement)** для указанного экземпляра MEP. Этот режим требует, чтобы временные базы на обоих концах измерения (инициатор и удаленный MEP) были **синхронизированы** с высокой точностью.
- **Зачем это нужно:**
    - ✓ **Одностороннее измерение задержки (One-Way Delay):** Для измерения односторонней задержки (от инициатора к удаленному MEP) без отправки ответных сообщений необходима синхронизация времени между устройствами. Только так можно вычислить задержку как RxTime - TxTime.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Высокоточные измерения:** При использовании синхронизации по PTP (Precision Time Protocol, IEEE 1588) можно достичь наносекундной точности измерений, что критически важно для приложений, чувствительных к задержкам.

- **Как это работает:**
  - ✓ При включении синхронизированного DM, MEP использует локальную временную метку (полученную от синхронизированного источника времени, такого как PTP) при отправке DM-сообщений.
  - ✓ Удаленный MEP также использует свою синхронизированную временную метку при получении.
  - ✓ Разница между метками позволяет вычислить одностороннюю задержку (при условии, что временные базы синхронизированы).
- **Важные требования:**
  - ✓ Для работы синхронизированного DM необходима **высокоточная синхронизация времени** между MEP, обычно с использованием **PTP (IEEE 1588)**.
  - ✓ Без синхронизации времени результаты измерений будут некорректными.
- Эта команда часто используется вместе с `mep <inst> dm ns` (наносекундная точность) для максимальной детализации измерений.

Удаление конфигурации:

```
(config)# no mep <inst> dm synchronized
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Отключает режим синхронизированного измерения задержки. Измерения будут выполняться в асинхронном режиме (обычно двусторонние измерения, не требующие синхронизации).

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```

2.7.29.12 (config)# mep <inst> lb

Настройка функции Loopback для MEP

Синтаксис:

```
(config)# mep <inst> lb <prio> [ dei ] [ multi | { uni { { mep-id <mepid> } | { mac <mac> } } } ] count <count> size <size> interval <interval>
```

Объяснение: Настройка функции Loopback для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- lb <prio: 0-7>: Настройка приоритета Loopback. Приоритет, который будет вставлен в биты PCP в теге (если есть).
- [dei]: Значение DEI (Drop Eligible Indicator), которое будет вставлено в биты PCP в теге (если есть).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [multi | { uni { { mep-id <mepid> } | { mac <mac> } } }]: Укажите, будет ли LBM PDU передаваться как одноадресный (unicast) или многоадресный (multicast). Одноадресный MAC-адрес будет настроен через "Peer MEP" или "Unicast Peer MAC". К MIP возможен только одноадресный Loopback.
- count <count>: Количество отправляемых LBM PDU.
- size <size>: Количество байт в Data Pattern TLV LBM PDU.
- interval <interval>: Интервал между отправками LBM PDU (в миллисекундах?).

Рекомендации:

- Команда mep <inst> lb настраивает функцию **Loopback (LB)** для указанного экземпляра MEP. Loopback является частью стандартов **IEEE 802.1ag (CFM)** и **ITU-T Y.1731** и используется для диагностики связности.
- **Loopback** Это механизм, аналогичный команде ping в IP-сетях, но работающий на уровне Ethernet (канальный уровень). MEP отправляет специальный кадр — **LBM (Loopback Message)** — на целевой MEP или MIP. Целевая точка должна ответить кадром **LBR (Loopback Reply)**, подтверждая связность.
- **Типы Loopback:**
    - ✓ **Multicast (многоадресный):** LBM отправляется на групповой адрес, обычно используется для проверки связности со всеми MEP в домене. Не все реализации поддерживают.
    - ✓ **Unicast (одноадресный):** LBM отправляется на конкретный MEP (по ID) или на конкретный MAC-адрес

SEC.RU | Короткий путь к информации Скачано с sec.ru

(например, для проверки связности с MIP).
Единственный способ для проверки связности с MIP.

- **Параметры:**
  - ✓ prio**:** Приоритет служебных сообщений LB. Рекомендуется высокий приоритет (5-7).
  - ✓ dei**:** Указывает, могут ли эти сообщения быть отброшены при перегрузке (если включен DEI). Обычно для служебных сообщений DEI не устанавливается.
  - ✓ count**:** Количество отправляемых LBM. По умолчанию может быть 5.
  - ✓ size**:** Размер полезной нагрузки LBM. Позволяет тестировать прохождение кадров разного размера (например, для проверки MTU).
  - ✓ interval**:** Интервал между отправками LBM (в миллисекундах).

Удаление конфигурации:

```
(config)# no mep <inst> lb
```

Отключает функцию Loopback для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.13 (config)# mep <inst> lck

Настройка частоты передачи заблокированных кадров (Locked Frame) для MEP

Синтаксис:

```
(config)# mep <inst> lck [ fr1s | fr1m ]
```

Объяснение: Настройка частоты передачи заблокированных кадров (Locked Frame Rate) для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- [fr1s | fr1m]: Частота кадров: 1 кадр в секунду (fr1s) или 1 кадр в минуту (fr1m).

Рекомендации:

- Команда mep <inst> lck настраивает функцию **LCK (Locked Signal)** для указанного экземпляра MEP. LCK является частью стандартов **ITU-T Y.1731** и используется для индикации состояния "заблокировано" в сетях операторской связи.
- **Locked Signal** Это сигнал, который передается MEP (или MIP) вниз по иерархии обслуживания, чтобы уведомить нижестоящие уровни о том, что вышестоящий уровень **временно недоступен по административным причинам** (например, плановое техническое обслуживание, тестирование, блокировка). Это позволяет подавить генерацию ложных аварийных сигналов на нижестоящих уровнях во время плановых работ.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- В отличие от AIS (Alarm Indication Signal): AIS указывает на *аварийный* сбой (потерю связности), в то время как LCK указывает на *плановое* отключение (административную блокировку). Оба сигнала используются для подавления вторичных аварийных сигналов, но по разным причинам.
- **Частота передачи (Frame Rate):**
    - ✓ `fr1s` **(1 кадр в секунду):** Высокая частота. Используется, когда требуется быстрое оповещение о состоянии блокировки, особенно если блокировка может быть кратковременной.
    - ✓ `fr1m` **(1 кадр в минуту):** Низкая частота. Используется для длительных плановых работ, чтобы снизить служебный трафик.
- Когда MEP начинает передавать LCK, нижестоящие MEP, получающие этот сигнал, должны подавить генерацию своих собственных аварийных сигналов (например, AIS или RDI), так как знают, что проблема не в их сегменте, а вызвана плановой блокировкой выше.

Удаление конфигурации:

```
(config)# no mep <inst> lck
```

Отключает функцию LCK для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.14 (config)# mep <inst> level

Настройка уровня MEG для MEP

Синтаксис:

(config)# mep <inst> level <level>

Объяснение: Настройка уровня MEG (Maintenance Entity Group) для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- <level: 0-7>: Значение уровня MEG.

Рекомендации:

- Команда mep <inst> level задает **уровень MEG (Maintenance Entity Group)** для указанного экземпляра MEP. Уровень MEG является ключевым понятием в стандартах **IEEE 802.1ag (CFM)** и **ITU-T Y.1731** и определяет место данного MEP в иерархии обслуживания.
- **Иерархия уровней (MEG Levels):**
    - ✓ Уровни MEG варьируются от 0 до 7.
    - ✓ Чем выше уровень, тем шире домен обслуживания. Например:
        - Уровень 7 может использоваться для клиентской сети (самый широкий домен, ближе к пользователю).

SEC.RU | Короткий путь к информации Скачано с sec.ru

    - Уровень 3-5 — для операторской инфраструктуры.
    - Уровень 0 — для самого узкого, "нижнего" уровня (например, для физического оборудования).
- **Зачем это нужно:**
    - ✓ **Иерархическое управление:** Позволяет разделять функции мониторинга и диагностики между разными уровнями сети (клиентский, операторский, транспортный).
    - ✓ **Подавление аварийных сигналов (AIS/LCK):** MEP на более высоком уровне может генерировать AIS, который будет передан на более низкие уровни, чтобы уведомить их о проблеме и предотвратить генерацию ложных аварийных сигналов.
    - ✓ **Изоляция доменов:** CFM/Y.1731 сообщения (CCM, LBM, LBR и т.д.) не пересекают границы уровней. MEP на уровне 5 не будет обрабатывать сообщения с уровнем 4 или 6, что обеспечивает четкое разделение зон ответственности.
- **Внимание!** Все MEP, находящиеся в одной группе обслуживания (MEG), должны иметь **одинаковый уровень MEG**. Это гарантирует, что они могут обмениваться служебными сообщениями друг с другом.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.15 (config)# mep <inst> lm

Настройка измерения потерь (Loss Measurement) для MEP

Синтаксис:

```
(config)# mep <inst> lm <prio> [ multi | uni ] [ single | dual ] [ fr10s | fr1s | fr6m | fr1m | fr6h ] [ flr <flr> ]
```

Объяснение: Настройка измерения потерь (Loss Measurement) для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- lm <prio: 0-7>: Настройка приоритета измерения потерь в случае тегированного OAM. В домене EVC это COS-ID.
- [multi | uni]: OAM PDU передается с многоадресным (multicast) или одноадресным (unicast) MAC-адресом. Одноадресный MAC-адрес берется из базы данных MEP-соседа. В случае LM существует только один MEP-сосед.
- [single | dual]: Двустороннее (dual-ended) LM основано на CCM PDU. Одностороннее (single-ended) LM основано на LMM/LMR PDU.
- [fr10s | fr1s | fr6m | fr1m | fr6h]: Укажите частоту кадров.
    - ✓ fr10s: 10 кадров в секунду.
    - ✓ fr1s: 1 кадр в секунду.
    - ✓ fr6m: 6 кадров в минуту.
    - ✓ fr1m: 1 кадр в минуту.
    - ✓ fr6h: 6 кадров в час.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [flr <flr: unit>]: Значение интервала коэффициента потерь кадров (Frame Loss Ratio).

Рекомендации:

- Команда mep <inst> lm настраивает функцию **измерения потерь (Loss Measurement, LM)** для указанного экземпляра MEP. LM является частью стандартов **ITU-T Y.1731** и используется для измерения потерь кадров (frame loss) в Ethernet-сетях, что критически важно для мониторинга SLA (Service Level Agreement).
- **Типы измерения потерь:**
    - ✓ **Двустороннее (Dual-ended,** dual**):** Основано на обмене CCM (Continuity Check Messages). Оба MEP (инициатор и получатель) передают CCM, и каждый вычисляет потери на основе счетчиков, полученных от соседа. Обеспечивает измерение потерь в обоих направлениях.
    - ✓ **Одностороннее (Single-ended,** single**):** Основано на обмене LMM (Loss Measurement Message) и LMR (Loss Measurement Reply). Инициатор отправляет LMM, получатель отвечает LMR, и инициатор вычисляет потери в направлении "туда и обратно" (round-trip). Может также использоваться для вычисления потерь в одном направлении при наличии синхронизации времени.
- **Частота передачи (Frame Rate):** Определяет, как часто отправляются LM-сообщения. Более высокая частота (fr10s, fr1s) дает более детальную картину потерь, но увеличивает служебный трафик. Более низкая частота (fr6m, fr1m, fr6h) используется для долгосрочного мониторинга.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **FLR (Frame Loss Ratio):** Коэффициент потерь кадров, используемый для определения порогов аварийных сигналов. Если потери превышают заданное значение, может быть сгенерировано уведомление.

Удаление конфигурации:

```
(config)# no mep <inst> lm
```

Отключает измерение потерь для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```

2.7.29.16 (config)# mep <inst> lt

Настройка трассировки линка (Link Trace) для MEP

Синтаксис:

```
(config)# mep <inst> lt <prio> { { mep-id <mepid> } | { mac <mac> } } ttl <ttl>
```

Объяснение: Настройка трассировки линка (Link Trace) для MEP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- lt <prio: 0-7>: Настройка приоритета трассировки линка в случае тегированного OAM. В домене EVC это COS-ID.
- { { mep-id <mepid> } | { mac <mac> } }: Укажите идентификатор MEP-соседа (Peer MEP-ID) для одноадресного MAC-адреса цели трассировки линка или сам одноадресный MAC-адрес цели трассировки.
- ttl <ttl>: Значение времени жизни (Time to Live).

Рекомендации:

- Команда mep <inst> lt настраивает функцию **трассировки линка (Link Trace, LT)** для указанного экземпляра MEP. LT является частью стандартов **IEEE 802.1ag (CFM)** и **ITU-T Y.1731** и используется для диагностики пути в Ethernet-сетях.
- **Что такое Link Trace?** Это механизм, аналогичный команде traceroute в IP-сетях. MEP отправляет специальный кадр — **LTM (Link Trace Message)** — на целевой MEP или MIP. Каждый MIP (промежуточная точка обслуживания) на пути и целевой MEP отвечают кадром **LTR (Link Trace Reply)**. В результате формируется карта пути с указанием всех промежуточных узлов.
- **Как это работает:**
    1. Инициатор (MEP) отправляет LTM с указанием целевого MEP или MIP и значением TTL (Time to Live).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Каждый MIP на пути уменьшает TTL и, если TTL достигает нуля, отвечает LTR, содержащим информацию о себе.
3. Целевой MEP (когда TTL достигает его) отвечает LTR, подтверждая достижение цели.

- **Параметры:**
  1. prio**:** Приоритет служебных сообщений LT. Рекомендуется высокий приоритет (5-7).
  2. mep-id **или** mac**:** Цель трассировки. Можно указать идентификатор MEP-соседа (если он известен) или конкретный MAC-адрес (например, для трассировки до MIP).
  3. ttl**:** Максимальное количество переходов (hops), которое может пройти LTM. Значение должно быть достаточно большим, чтобы достичь цели, но не слишком большим, чтобы не генерировать избыточный трафик.
- **Результат трассировки:** Выводит список всех узлов (MIP и целевой MEP) на пути от инициатора к цели, включая их идентификаторы и время отклика.

Удаление конфигурации:

```
(config)# no mep <inst> lt
```

Отключает функцию трассировки линка для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.17 (config)# mep <inst> meg-id

Настройка формата идентификатора MEG (MEG-ID)

Синтаксис:

```
(config)# mep <inst> meg-id <megid> { itu | itu-cc | { ieee [ name <name> ] } }
```

Объяснение: Настройка формата идентификатора MEG (MEG-ID).

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- meg-id <megid>: Укажите строку идентификатора MEG. Это либо ITU MEG-ID, либо IEEE Short MA, в зависимости от выбранного формата MEG-ID. Максимальная длина: ITU — 13 символов, ITU-CC — 15 символов, IEEE — 16 символов.
- { itu | itu-cc | { ieee [name <name>] } }: Укажите формат MEG-ID.
    - ✓ itu: MEG-ID имеет формат ITU (ICC - UMC). Максимальная длина meg-id — 13 символов.
    - ✓ itu-cc: MEG-ID имеет формат ITU с кодом страны (CC - ICC - UMC). Максимальная длина meg-id — 15 символов.
    - ✓ ieee: MEG-ID (Short MA Name) имеет формат строки символов IEEE. Максимальная длина meg-id — 16 символов.
    - ✓ name <name>: Это поле актуально только для формата IEEE.

Рекомендации:

- Команда mep <inst> meg-id задает **идентификатор группы обслуживания (MEG-ID)** для указанного экземпляра MEP. MEG-

SEC.RU | Короткий путь к информации Скачано с sec.ru

ID уникально идентифицирует группу обслуживания (Maintenance Entity Group) в рамках домена CFM/Y.1731.

- **Форматы MEG-ID:**
  - ✓ **ITU (**itu**):** Формат, определенный в ITU-T Y.1731. Состоит из двух частей: ICC (ITU Carrier Code) и UMC (Unique Maintenance Code). Пример: ABC123 (где ABC — ICC, 123 — UMC). Максимум 13 символов.
  - ✓ **ITU с кодом страны (**itu-cc**):** Расширенный ITU-формат, включающий код страны (CC). Пример: US-ABC-123. Максимум 15 символов.
  - ✓ **IEEE (**ieee**):** Формат, определенный в IEEE 802.1ag. Использует "Short MA Name" в виде строки символов. Максимум 16 символов. Дополнительный параметр name может использоваться для указания дополнительной информации.
- MEG-ID является частью служебных сообщений CFM/Y.1731 (CCM, LBM, LTM и т.д.). MEP принимают и обрабатывают только сообщения, которые имеют **одинаковый MEG-ID и одинаковый уровень (MEG Level)**. Это гарантирует, что сообщения не пересекают границы между разными группами обслуживания.
- **Внимание!** Все MEP в одной группе обслуживания (MEG) должны иметь **один и тот же MEG-ID в одном и том же формате**. В противном случае они не будут распознавать друг друга.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.18 (config)# mep <inst> peer-mep-id

Настройка идентификатора MEP-соседа

Синтаксис:

```
(config)# mep <inst> peer-mep-id <mepid> [ mac <mac> ]
```

Объяснение: Настройка идентификатора MEP-соседа (peer MEP-ID).

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- peer-mep-id <mepid>: Настройте значение идентификатора MEP-соседа.
- [mac <mac>]: MAC-адрес соседа.

Рекомендации:

- Команда mep <inst> peer-mep-id определяет **идентификатор MEP-соседа (peer MEP)** для указанного экземпляра MEP. В рамках одной группы обслуживания (MEG) может существовать несколько MEP. Для корректного обмена служебными сообщениями (CC, LM, DM, LB, LT) каждый MEP должен знать идентификаторы своих соседей.
- **Зачем это нужно:**
    - ✓ **Одноадресные (unicast) сервисы:** Для функций, требующих одноадресной передачи (например, LM, DM, LB), необходимо знать конкретный MEP-сосед, с которым происходит взаимодействие.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Валидация:** MEP проверяет входящие CCM (Continuity Check Messages) на наличие идентификатора отправителя. Если идентификатор не совпадает с настроенным peer MEP-ID, сообщение может быть проигнорировано.
- ✓ **Автоматическое обнаружение MAC-адреса:** Параметр mac <mac> может использоваться для явного указания MAC-адреса соседа. Если MAC-адрес не указан, он может быть изучен автоматически через CCM или другие механизмы.

Удаление конфигурации:

```
(config)# no mep <inst> peer-mep-id { <mepid> | all }
```

*Удаляет настройку для указанного MEP-соседа или для всех соседей (*all*).*

2.7.29.19 (config)# mep <inst> performance-monitoring

Включение мониторинга производительности для MEP

Синтаксис:

```
(config)# mep <inst> performance-monitoring
```

Объяснение: Включение мониторинга производительности для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда mep <inst> performance-monitoring **включает функцию мониторинга производительности** для указанного экземпляра MEP. Эта функция позволяет собирать статистические данные о качестве работы канала связи.
- **Что включает мониторинг производительности:**
    - ✓ **Потери кадров (Frame Loss):** Сбор статистики по потерям на основе данных LM (Loss Measurement).
    - ✓ **Задержка (Delay) и вариация задержки (Delay Variation):** Сбор статистики по задержкам на основе данных DM (Delay Measurement).
    - ✓ **Доступность (Availability):** Мониторинг времени, когда канал считается доступным или недоступным (на основе порогов потерь).
    - ✓ **Коэффициенты (Ratios):** Расчет FLR (Frame Loss Ratio) и других метрик.
- **Зачем это нужно:**
    - ✓ **Соблюдение SLA (Service Level Agreement):** Позволяет оператору или администратору контролировать, соответствуют ли параметры канала (потери, задержка) заявленным соглашениям.
    - ✓ **Долгосрочный анализ:** Накопление исторических данных о производительности для выявления тенденций и профилактики проблем.
- **Взаимодействие с LM/DM:** Для работы мониторинга производительности должны быть предварительно настроены функции LM (Loss Measurement) и/или DM (Delay Measurement).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no mep <inst> performance-monitoring
```

Отключает мониторинг производительности для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

2.7.29.20 (config)# mep <inst> tst

Настройка тестового сигнала (Test Signal) для MEP

Синтаксис:

```
(config)# mep <inst> tst <prio> [ dei ] mep-id <mepid> [ sequence ] [ all-zero | all-one | one-zero ] rate <rate> size <size>
```

Объяснение: Включение тестового сигнала для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- tst <prio: 0-7>: Настройка приоритета тестового сигнала в случае тегированного OAM. В домене EVC это COS-ID.
- [dei]: Индикатор возможности отбрасывания (Drop Eligible Indicator) в случае тегированного OAM.
- mep-id <mepid>: Настройка значения идентификатора MEP-соседа (Peer MEP-ID) для одноадресного TST. MAC-адрес берется из базы данных MAC-адресов MEP-соседа.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [sequence]: Включить порядковый номер (sequence number) в TST PDU.
- [all-zero | all-one | one-zero]: Укажите один из вариантов тестового паттерна.
    - ✓ all-zero: Тестовый паттерн установлен в "все нули".
    - ✓ all-one: Тестовый паттерн установлен в "все единицы".
    - ✓ one-zero: Тестовый паттерн установлен в "10101010".
- rate <rate>: Значение скорости передачи (количество кадров в секунду).
- size <size>: Значение размера кадра.

Рекомендации:

- Команда mep <inst> tst настраивает функцию **тестового сигнала (Test Signal, TST)** для указанного экземпляра MEP. TST является частью стандартов **ITU-T Y.1731** и используется для **проверки целостности канала связи (bit error rate testing)** на уровне Ethernet.
- **Что такое TST?** Это механизм, позволяющий генерировать тестовый трафик между двумя MEP для проверки качества канала. TST отправляет кадры с известным тестовым паттерном (например, все нули, все единицы или чередующиеся 10101010) и может проверять полученный трафик на наличие ошибок (битовых искажений).
- **Параметры:**
    - ✓ prio**:** Приоритет тестового трафика. Рекомендуется использовать высокий приоритет (5-7), чтобы тестовый трафик не отбрасывался при перегрузках.
    - ✓ dei**:** Указывает, могут ли тестовые кадры быть отброшены при перегрузке. Обычно не устанавливается для тестового трафика.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ mep-id**:** Целевой MEP-сосед, с которым производится тестирование.
- ✓ sequence**:** Включает порядковые номера в TST-кадрах, что позволяет обнаруживать потери и нарушение порядка пакетов.
- ✓ **Тестовый паттерн (**all-zero**,** all-one**,** one-zero**):** Определяет битовую последовательность полезной нагрузки. Использование разных паттернов позволяет выявлять различные типы ошибок (например, чувствительные к частоте битов).
- ✓ rate**:** Скорость отправки тестовых кадров (в кадрах в секунду).
- ✓ size**:** Размер тестового кадра (в байтах).

Удаление конфигурации:

```
(config)# no mep <inst> tst
```

Отключает тестовый сигнал для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.21 (config)# mep <inst> tst rx

Включение приема тестового сигнала (Test Signal RX) для MEP

Синтаксис:

```
(config)# mep <inst> tst rx
```

Объяснение: Включение приема тестового сигнала (RX transmission) для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

Рекомендации:

- Команда mep <inst> tst rx **включает прием и анализ тестового сигнала** на указанном экземпляре MEP. Это парная функция к команде mep <inst> tst (которая обычно настраивает передачу TST).
- **Как это работает:**
    1. Один MEP настраивается на **передачу** тестового сигнала (с помощью mep <inst> tst).
    2. Другой MEP (или тот же, при двустороннем тестировании) должен быть настроен на **прием** тестового сигнала с помощью mep <inst> tst rx.
    3. Принимающий MEP анализирует входящие TST-кадры, проверяет тестовый паттерн (битовую последовательность), порядковые номера (если включены) и накопленную статистику (потери, ошибки).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    1. **Двустороннее тестирование:** В некоторых сценариях тестирования (например, для измерения битовых ошибок на канале) требуется, чтобы принимающая сторона была явно включена для сбора статистики, даже если она не инициирует тест.
    2. **Мониторинг:** MEP может быть настроен на постоянный прием тестового сигнала от соседа для непрерывного мониторинга качества канала.
- Для корректного тестирования оба MEP (или один MEP на прием, другой на передачу) должны иметь согласованные параметры (паттерн, размер кадра, частота), даже если один из них только принимает, а другой только передает.

Удаление конфигурации:

```
(config)# no mep <inst> tst rx
```

Отключает прием и анализ тестового сигнала для указанного экземпляра MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.22 (config)# mep <inst> tst tx

Включение передачи тестового сигнала (Test Signal TX) для MEP

Синтаксис:

```
(config)# mep <inst> tst tx
```

Объяснение: Включение передачи тестового сигнала (TX transmission) для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

Рекомендации:

- Команда mep <inst> tst tx **включает передачу тестового сигнала** от указанного экземпляра MEP. Это парная функция к команде mep <inst> tst rx (прием тестового сигнала). Вместе они образуют полноценный механизм тестирования канала на битовые ошибки.
- **Как это работает:**
    1. MEP, на котором включена tst tx, начинает отправлять TST-кадры на целевой MEP-сосед (заданный параметром mep-id в базовой настройке TST).
    2. Целевой MEP должен быть настроен на прием (tst rx) для анализа этих кадров.
    3. Принимающий MEP собирает статистику о полученных кадрах: количество, порядковые номера (если включены), проверку тестового паттерна (all-zero, all-one, one-zero), выявление битовых ошибок.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Отличие от базовой команды** mep <inst> tst**:** Базовая команда mep <inst> tst настраивает все параметры тестового сигнала (приоритет, паттерн, скорость, размер кадра, цель) и, вероятно, включает как передачу, так и прием в зависимости от контекста. Команды tst tx и tst rx позволяют разделить функции: один MEP только передает, другой только принимает. Это полезно при:
    1. **Одностороннем тестировании:** Когда нужно измерить качество канала только в одном направлении.
    2. **Выделенных ролях:** В сложных конфигурациях, где один MEP является "генератором" тестового трафика, а другие MEP — "анализаторами".
- **Взаимодействие с базовой настройкой TST:** Для работы tst tx необходимо, чтобы базовая конфигурация TST (mep <inst> tst ...) уже была задана (или настройки передатчика были заданы отдельно). Эта команда только активирует/деактивирует передачу, не изменяя параметры.

Удаление конфигурации:

```
(config)# no mep <inst> tst tx
```

Отключает передачу тестового сигнала для указанного экземпляра MEP. MEP перестает отправлять TST-кадры.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

Очистка:

```
# clear mep <inst> { lm | dm | tst }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.29.23 (config)# mep <inst> vid

Настройка VID для MEP

Синтаксис:

```
(config)# mep <inst> vid <vid>
```

Объяснение: Настройка VID для MEP.

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.
- <vid>: Значение VID для MEP.

Рекомендации:

- Команда mep <inst> vid задает **идентификатор VLAN (VID)**, в котором функционирует указанный экземпляр MEP. Это один из ключевых параметров при создании MEP в **домене VLAN** (когда domain vlan).
- **Зачем это нужно:**
    - ✓ **Привязка к VLAN:** MEP, работающий в домене VLAN, ассоциируется с определенной VLAN. Все служебные сообщения (CCM, LBM, LTM, TST и т.д.), отправляемые этим MEP, будут передаваться в тегированных кадрах с указанным VID.
    - ✓ **Идентификация домена:** VID помогает определить, к какому широковещательному домену (VLAN) относится данный MEP. Это важно для корректной маршрутизации OAM-сообщений.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Эта команда имеет смысл только для MEP, созданных в домене VLAN (domain vlan). Для MEP в домене порта (domain port) или EVC (domain evc) этот параметр может не применяться или использоваться иначе.
- **Взаимосвязь с другими параметрами:** VID должен соответствовать VLAN, уже существующей на коммутаторе. Кроме того, для MEP, работающих в домене VLAN, также может настраиваться тегирование (например, vid <vid> в команде создания MEP mep <inst> ... vid <vid>).

Удаление конфигурации:

```
(config)# no mep <inst> vid
```

Удаляет настройку VID для указанного экземпляра MEP. Если MEP находится в домене VLAN, это может привести к неработоспособности MEP.

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```

2.7.29.24 (config)# mep <inst> voe

Настройка MEP на основе VOE (Virtual OAM Endpoint)

Синтаксис:

```
(config)# mep <inst> voe
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: MEP основан на VOE (Virtual OAM Endpoint).

Параметры:

- <inst>: Укажите номер идентификатора экземпляра.

Рекомендации:

- Команда mep <inst> voe указывает, что данный экземпляр MEP является **VOE-базированным (Virtual OAM Endpoint)**. VOE — это концепция, используемая в некоторых реализациях для создания **виртуальных (логических) конечных точек обслуживания**, которые могут работать независимо от физических портов.
- **VOE**
    - ✓ **Virtual OAM Endpoint (VOE)** — это виртуальная конечная точка OAM, которая может быть привязана к виртуальному интерфейсу (например, EVC, L2VPN, VPLS), а не к физическому порту.
    - ✓ VOE позволяют выполнять функции CFM/Y.1731 (CC, LM, DM, LB, LT, TST) в виртуализированных средах, таких как MPLS, VPLS, L2VPN или в сетях с использованием EVC (Ethernet Virtual Connections).
- **Зачем это нужно:**
    - ✓ **Поддержка виртуальных сервисов:** В сетях операторов связи многие сервисы предоставляются через виртуальные соединения (EVC, VPLS). VOE позволяет мониторить и диагностировать эти виртуальные соединения на уровне Ethernet OAM, даже

SEC.RU | Короткий путь к информации Скачано с sec.ru

если они проходят через несколько физических интерфейсов.

- ✓ **Гибкость:** VOE могут быть созданы независимо от физической инфраструктуры, что упрощает управление OAM в сложных сетях.
- ✓ **Мультиплексирование:** Несколько VOE могут существовать на одном физическом порту, каждый из которых соответствует своему виртуальному сервису.

- **Внимание!** Если MEP настроен как VOE-базированный (voe), он не привязан к конкретному физическому порту в традиционном смысле. Его поведение определяется виртуальным контекстом (например, EVC, VPLS). Если VOE не требуется (MEP работает на физическом порту), команда не используется или отключается.

Удаление конфигурации:

```
(config)# no mep <inst> voe
```

Отключает режим VOE для указанного экземпляра MEP. MEP становится базированным на физическом порту (или стандартным).

Просмотр:

```
# show mep [ <inst> ] [ peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck ] [ detail ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.30 Настройка мониторинга трафика (config)# monitor

2.7.30.1 (config)# monitor destination interface

Настройка порта назначения для зеркалирования трафика

Синтаксис:

```
(config)# monitor destination interface <port_type> <in_port_type>
```

Объяснение: Настройка порта для зеркалироваться (копирования) трафика на него.

Параметры:

- <port_type>: Укажите тип интерфейса.
- <in_port_type>: Укажите номер порта.

Рекомендации:

- Команда monitor destination interface определяет порт назначения (destination port) для функции зеркалирования трафика (port mirroring). На этот порт будут отправляться копии пакетов, проходящих через порты-источники (source ports).
- Порт назначения также часто называют "мониторинговым портом" (monitoring port) или "анализирующим портом" (analyzer port). К этому порту обычно подключается устройство для анализа трафика (например, сетевой анализатор, IDS/IPS система, Wireshark).
- Ключевые требования к порту назначения:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Порт назначения не должен использоваться для обычного сетевого трафика. Все пакеты, отправленные на этот порт коммутатором, являются копиями трафика с портов-источников.
- ✓ Трафик, поступающий на порт назначения извне (например, с подключенного анализатора), обычно игнорируется или не влияет на работу зеркалирования.
- ✓ Рекомендуется использовать порт с высокой пропускной способностью, чтобы он мог обрабатывать суммарный трафик с нескольких портов-источников без перегрузок.
- ✓ В некоторых реализациях порт назначения может быть только один для всей системы.

- После настройки порта назначения необходимо настроить порты-источники (source ports), трафик с которых будет копироваться (команда monitor session source interface или аналогичная).

Удаление конфигурации:

```
(config)# no monitor destination
```

Удаляет настройку порта назначения для зеркалирования трафика.

2.7.30.2 (config)# monitor source

Настройка портов-источников для зеркалирования трафика

Синтаксис:

```
(config)# monitor source { [ interface ( <port_type> ) [ <v_port_type_list> ] ] }
| { cpu [ <cpu_switch_range> ] } { both | rx | tx }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Настройка того, какой трафик (RX или TX) с портов-источников должен зеркалироваться на порт назначения.

Параметры:

- { [interface (<port_type>) [<v_port_type_list>]] }: Укажите один из вариантов. Символ * означает все интерфейсы.
- { both | rx | tx }: Укажите, какое направление трафика должно зеркалироваться на порт назначения.
    - ✓ both: Зеркалировать как входящий (received), так и исходящий (transmitted) трафик.
    - ✓ rx: Зеркалировать только входящий трафик.
    - ✓ tx: Зеркалировать только исходящий трафик.

Рекомендации:

- Команда monitor source определяет **порты-источники (source ports)** для функции зеркалирования трафика, а также направление трафика (входящий, исходящий или оба), которое должно копироваться на порт назначения.
- **Как это работает:**
    1. Предварительно настраивается порт назначения (команда monitor destination interface).
    2. С помощью monitor source указываются порты, трафик с которых необходимо копировать.
    3. Коммутатор дублирует указанный трафик с портов-источников и отправляет его копии на порт назначения.
- **Выбор направления:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. both **(рекомендуется для полного анализа):** Копирует весь трафик (входящий и исходящий) с порта-источника. Используется для детального анализа, но создает наибольшую нагрузку.
2. rx**:** Копирует только входящий трафик. Полезно, если нужно анализировать только то, что приходит на порт.
3. tx**:** Копирует только исходящий трафик. Полезно, если нужно анализировать только то, что отправляется с порта.

- **Указание портов-источников:**
    1. Можно указать один порт: interface GigabitEthernet 1/1
    2. Диапазон портов: interface GigabitEthernet 1/1-5
    3. Список портов: interface GigabitEthernet 1/1,3,5
    4. Все порты: * (если поддерживается)
- **Зеркалирование CPU:** Параметр cpu [<cpu_switch_range>] позволяет зеркалировать трафик, который поступает на CPU коммутатора (например, управляющий трафик, SNMP, Telnet/SSH). Это полезно для диагностики проблем с управлением.

Удаление конфигурации:

```
(config)# no monitor source { { interface ( <port_type> [ <v_port_type_list> ] ) } | { cpu [ <cpu_switch_range> ] } }
```

Удаляет настройку зеркалирования для указанных портов-источников или CPU.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.31 Настройка NTP (Network Time Protocol) (config)# ntp

2.7.31.1 (config)# ntp

Глобальное включение NTP

Синтаксис:

```
(config)# ntp
```

Объяснение: Включение функции NTP (Network Time Protocol).

Рекомендации:

- Команда ntp **глобально активирует** протокол NTP (Network Time Protocol) на коммутаторе. NTP используется для синхронизации системного времени устройства с внешними серверами точного времени, что критически важно для:
    - ✓ **Корректного времени в логах (syslog):** Позволяет точно сопоставлять события во времени.
    - ✓ **Аутентификации:** Некоторые протоколы безопасности (например, Kerberos) и сертификаты зависят от точного времени.
    - ✓ **Планирования задач:** Для корректного выполнения задач по расписанию (например, green-ethernet led interval).
    - ✓ **Анализа инцидентов:** Точное время на всех устройствах упрощает расследование сетевых инцидентов.
- **После глобального включения** необходимо настроить:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Адреса NTP-серверов (команда ntp server <ip-address>).
- ✓ При необходимости — аутентификацию NTP, интервалы обновления и другие параметры.

- **Внимание!** Для работы NTP коммутатор должен иметь IP-связность с настроенными NTP-серверами. Если NTP-сервер находится в другой подсети, должен быть настроен маршрут по умолчанию или статический маршрут.

Удаление конфигурации:

```
(config)# no ntp
```

Глобально отключает функцию NTP на коммутаторе.

Просмотр:

```
# show ntp status
```

Отображает статус NTP: включен/выключен, текущий источник синхронизации, смещение времени, задержку и другую информацию.

2.7.31.2 (config)# ntp server

Настройка адреса NTP-сервера

Синтаксис:

Объяснение: Настройка списка адресов NTP-серверов.

Параметры:

- <index_var: 1-5>: Укажите порядковый номер NTP-сервера. Допустимый диапазон от 1 до 5. NTP-серверы опрашиваются в

SEC.RU | Короткий путь к информации Скачано с sec.ru

числовом порядке. Если "Сервер 1" недоступен, NTP-клиент попытается связаться с "Сервером 2".

- { <ipv4_var> | <ipv6_var> | <name_var> }: Укажите один из трех вариантов.
    - ✓ <ipv4_var>: IPv4-адрес.
    - ✓ <ipv6_var>: IPv6-адрес в 128-битной записи, представленной восемью полями до четырех шестнадцатеричных цифр с двоеточием (:) в качестве разделителя. Например, fe80::215:c5ff:fe03:4dc7. Символ :: — это специальный синтаксис, который можно использовать как сокращенное обозначение для нескольких 16-битных групп из непрерывных нулей, но он может появляться только один раз.
    - ✓ <name_var>: Доменное имя NTP-сервера.

Рекомендации:

- Команда ntp server задает **список NTP-серверов**, к которым коммутатор будет обращаться для синхронизации времени.
- **Приоритет и отказоустойчивость:** Серверы опрашиваются в порядке возрастания индекса (от 1 до 5). Если первый сервер недоступен, коммутатор автоматически переключается на следующий. Это обеспечивает надежность синхронизации.
- **Поддержка IPv6:** Команда поддерживает как IPv4, так и IPv6 адреса NTP-серверов, что позволяет использовать ее в современных сетях с двойным стеком протоколов.
- **Доменные имена:** можно использовать доменные имена вместо IP-адресов (например, pool.ntp.org). В этом случае

SEC.RU | Короткий путь к информации Скачано с sec.ru

коммутатор должен иметь настроенные DNS-серверы (ip name-server) для разрешения имени.

- **Рекомендуемое количество серверов:** для повышения надежности рекомендуется настраивать не менее двух NTP-серверов (например, ntp server 1 ... и ntp server 2 ...).

Удаление конфигурации:

```
(config)# no ntp server <index_var>
```

Удаляет настройку NTP-сервера с указанным индексом.

Просмотр:

```
# show ntp status
```

Отображает текущее состояние NTP, включая информацию о том, с каким сервером выполняется синхронизация.

2.7.32 Настройка PoE (Power over Ethernet) (config)# poe

Для моделей с поддержкой PoE

2.7.32.1 (config)# poe management mode

Настройка режима управления питанием PoE

Синтаксис:

```
(config)# poe management mode { allocation-consumption | allocation-reserved-power }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Команды для управления Power over Ethernet (PoE) используются для настройки максимальной мощности PoE, предоставляемой порту, максимального бюджета мощности для коммутатора (мощности, доступной для всех портов RJ-45), режима работы PoE порта, приоритета выделения питания и максимальной мощности, выделяемой на каждый порт. Если потребность в мощности от устройств, подключенных к коммутатору, превышает бюджет мощности, коммутатор использует настройки приоритета порта для ограничения подаваемого питания.

Параметры:

- `allocation-consumption`: При использовании этого режима порты отключаются в следующих ситуациях:
    - ✓ Когда фактическое потребление мощности всеми портами превышает мощность, которую может обеспечить источник питания.
    - ✓ Когда фактическое потребление мощности для данного порта превышает зарезервированную мощность для этого порта.
    - ✓ Порты отключаются в соответствии с их приоритетом. Если два порта имеют одинаковый приоритет, отключается порт с большим номером.
- `allocation-reserved-power`: При выборе этого режима порты отключаются, когда общая зарезервированная мощность превышает мощность, которую может обеспечить источник питания. В этом режиме, если питаемое устройство (PD — Powered Device) продолжает запрашивать больше мощности,

SEC.RU | Короткий путь к информации Скачано с sec.ru

чем доступно от источника питания, питание на порт не включается.

Режимы распределения (allocation modes): Эти режимы используются для настройки того, как подключенные PD могут резервировать мощность:

- **allocation**: Количество мощности, зарезервированной для каждого порта, указывается в поле "Максимальная мощность [Вт]".

Внимние: Если порты используют больше мощности, чем зарезервировано для них, они будут отключены.

Рекомендации:

- Команда `poe management mode` определяет **способы управления питанием PoE** на коммутаторе. Это критически важно, когда общая мощность, запрашиваемая подключенными устройствами (например, IP-телефонами, камерами, точками доступа), может превысить доступный бюджет питания.
- **Режим** `allocation-consumption` **(резервирование по потреблению):**
    - ✓ Мощность резервируется на основе **фактического потребления** устройства (real-time). Если потребление превышает резерв, порт может быть отключен.
    - ✓ Более гибкий, но может привести к неожиданным отключениям, если устройство потребляет больше ожидаемого.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Режим** allocation-reserved-power **(резервирование по выделенной мощности):**
    - ✓ Мощность резервируется на основе **максимальной выделенной мощности**, указанной в конфигурации порта (или запрошенной PD при обнаружении).
    - ✓ Если суммарная зарезервированная мощность превышает бюджет, новые устройства не получают питание, а работающие не отключаются (если не пытаются увеличить потребление сверх резерва).
    - ✓ Более предсказуемый и стабильный режим.
- **Приоритет портов:** В обоих режимах при недостатке питания порты отключаются в порядке приоритета. Высокий приоритет (например, для голосовых шлюзов) обеспечивает сохранение питания для критически важных устройств.

Удаление конфигурации:

```
(config)# no poe management mode
```

Сбрасывает режим управления питанием к значению по умолчанию.

Просмотр:

```
> show poe [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show poe [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Отображает статус PoE, текущий режим управления, потребление и бюджет питания.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.32.2 (config)# poe supply

Настройка максимальной мощности PoE, доступной на устройстве

Синтаксис:

```
(config)# poe supply <v_1_to_600>
```

Параметры:

- <v_1_to_600>: Укажите максимальную мощность (в ваттах), которую устройство может обеспечить.

Объяснение: Настройка максимальной мощности, которую устройство может отдать (для PoE).

Рекомендации:

- Команда poe supply задает **общий бюджет мощности PoE** (в ваттах), доступный для всех портов коммутатора. Это значение определяет, сколько суммарной мощности могут потреблять все подключенные устройства (PD — Powered Devices).
- **Зачем это нужно:**
    - ✓ Коммутатор может иметь несколько источников питания (блоков питания) или поддерживать разные конфигурации. Эта команда позволяет администратору указать фактическую максимальную мощность, которую может обеспечить установленная конфигурация питания.
    - ✓ Это значение используется механизмом управления PoE для принятия решений о включении/отключении портов при превышении бюджета.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Как это работает:**

    1. Коммутатор отслеживает суммарную потребляемую мощность всех PoE-портов.
    2. Если суммарное потребление (или суммарная зарезервированная мощность в зависимости от режима) приближается к значению, заданному poe supply, новые PoE-устройства могут не получить питание, а существующие могут быть отключены в порядке приоритета.
- **Внимание:** Значение poe supply не должно превышать реальные возможности источника питания (блока питания) коммутатора. Установка завышенного значения может привести к тому, что коммутатор попытается отдать больше мощности, чем может физически обеспечить, что вызовет перегрузку блока питания и возможное отключение устройства.
- **Рекомендуется** проверить спецификации коммутатора и установленных блоков питания, чтобы определить корректное значение.

Удаление конфигурации:

```
(config)# no poe supply
```

Сбрасывает значение максимальной мощности к значению по умолчанию (определяется аппаратно).

Просмотр:

```
> show poe [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show poe [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.33 Настройка безопасности портов (Port Security) (config)# port-security

2.7.33.1 (config)# port-security

Глобальное включение функции безопасности портов

Синтаксис:

```
(config)# port-security
```

Объяснение: Глобальное включение функции безопасности портов (port security).

Рекомендации:

- Команда port-security **глобально активирует** функцию безопасности портов на коммутаторе. Эта функция предназначена для ограничения доступа к портам на основе MAC-адресов подключенных устройств.
- **Что такое Port Security?** Это механизм защиты уровня 2, который позволяет администратору:
    - ✓ Ограничить **количество MAC-адресов**, которые могут быть изучены на порту (например, только один MAC-адрес на порту доступа).
    - ✓ Определить, какие MAC-адреса разрешены на порту (статически или динамически).
    - ✓ Задать **действие при нарушении** (violation action): отключить порт (shutdown), отбросить трафик (restrict) или только зарегистрировать нарушение (protect).
- **Как это работает:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Коммутатор отслеживает MAC-адреса, появляющиеся на портах с включенной port-security.
2. Если количество изученных MAC-адресов превышает установленный лимит, или на порту появляется MAC-адрес, не входящий в список разрешенных, срабатывает действие при нарушении.
3. Типичное применение: на порту доступа (например, для подключения одного компьютера) устанавливается лимит 1 MAC-адрес, и при появлении второго MAC-адреса порт блокируется, предотвращая подключение неуправляемого коммутатора или устройства-нарушителя.

- **После глобального включения** необходимо:
  1. Включить port-security на конкретных портах (port-security в режиме интерфейса).
  2. Настроить лимит MAC-адресов, разрешенные MAC-адреса (опционально) и действие при нарушении.

Удаление конфигурации:

```
(config)# no port-security
```

Глобально отключает функцию безопасности портов на коммутаторе.

Просмотр:

```
> show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Отображает статус port-security глобально и на конкретных портах, включая лимиты MAC-адресов, изученные адреса и информацию о нарушениях.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.33.2 (config)# port-security aging

Глобальное включение функции устаревания (aging) для безопасных MAC-адресов

Синтаксис:

```
(config)# port-security aging
```

Объяснение: Включение функции устаревания (aging) для безопасности портов. Если функция включена, защищенные (secured) MAC-адреса подлежат устареванию, как описано в команде "Aging time". При включенном устаревании таймер запускается после того, как конечный хост становится защищенным. Когда таймер истекает, коммутатор начинает поиск кадров от конечного хоста, и, если такие кадры не обнаружены в течение следующего периода устаревания, предполагается, что конечный хост отключен, и соответствующие ресурсы на коммутаторе освобождаются.

Рекомендации:

- Команда port-security aging **глобально активирует** функцию автоматического устаревания (aging) для динамически изученных безопасных MAC-адресов.
- **Зачем это нужно:**
    - ✓ Без устаревания динамически изученные безопасные MAC-адреса остаются в таблице port-security бесконечно, даже если устройство отключилось. Это может привести к тому, что лимит MAC-адресов на порту будет исчерпан, и новое устройство не сможет подключиться.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Устаревание позволяет автоматически удалять записи о MAC-адресах устройств, которые отключились или неактивны в течение заданного времени, освобождая ресурсы для новых устройств.

- **Как это работает:**

  1. Когда устройство подключается к порту с включенной port-security, его MAC-адрес добавляется в таблицу как безопасный (secured).
  2. Запускается таймер устаревания.
  3. Если в течение заданного времени (настраивается командой `port-security aging time`) от этого MAC-адреса не поступает трафик, запись удаляется.
  4. При удалении записи ресурсы порта освобождаются, и новое устройство может занять "слот" в лимите MAC-адресов.

- Функция устаревания может применяться только к **динамически изученным** безопасным MAC-адресам. **Статические** безопасные MAC-адреса (настроенные вручную) не подлежат устареванию.
- **Взаимодействие с aging time:** Для работы необходимо также настроить время устаревания командой `port-security aging time <value>`.

Удаление конфигурации:

```
(config)# no port-security aging
```

Отключает функцию устаревания безопасных MAC-адресов. Динамически изученные записи остаются в таблице бесконечно, пока порт не будет перезагружен или запись не будет удалена вручную.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
> show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

Отображает статус устаревания и текущие безопасные MAC-адреса на портах.

2.7.33.3 (config)# port-security aging time

Настройка времени устаревания для безопасных MAC-адресов

Синтаксис:

```
(config)# port-security aging time <v_10_to_10000000>
```

Параметры:

- <v_10_to_10000000>: Укажите значение времени устаревания. Допустимый диапазон от 10 до 10 000 000 секунд.

Объяснение: Настройка желаемого значения времени устаревания. Если функция "Aging" включена, защищенные (secured) MAC-адреса подлежат устареванию, как описано в этой команде. При включенном устаревании таймер запускается после того, как конечный хост становится защищенным. Когда таймер истекает, коммутатор начинает поиск кадров от конечного хоста, и, если такие кадры не обнаружены в течение следующего периода устаревания, предполагается, что конечный хост отключен, и соответствующие ресурсы на коммутаторе освобождаются.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `port-security aging time` задает **время жизни (в секундах)** для динамически изученных безопасных MAC-адресов. Эта команда работает только в том случае, если глобально включена функция устаревания (`port-security aging`).
- **Как это работает:**
    1. Когда устройство подключается к порту с включенной port-security, его MAC-адрес добавляется в таблицу как безопасный (secured), и запускается таймер устаревания.
    2. Каждый раз, когда от этого MAC-адреса поступает трафик, таймер сбрасывается (запись "омолаживается").
    3. Если в течение времени, заданного `aging time`, от MAC-адреса не поступает ни одного кадра, запись считается устаревшей и удаляется.
    4. После удаления записи ресурсы порта (например, "слот" в лимите MAC-адресов) освобождаются для подключения нового устройства.
- **Выбор значения:**
    1. **Короткое время (например, 60-300 секунд):** Быстрое освобождение ресурсов, но может привести к удалению записи, если устройство временно неактивно (например, в спящем режиме).
    2. **Большое время (например, 86400 секунд = 1 сутки):** Записи остаются в таблице надолго, что может быть проблемой, если устройства часто меняются.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. **Рекомендуемое значение:** Часто используется 300-600 секунд (5-10 минут) для офисных сред, где устройства могут быть временно отключены.

- Эта настройка применяется только к **динамически изученным** безопасным MAC-адресам. Статические безопасные MAC-адреса (настроенные вручную) не подлежат устареванию.

Удаление конфигурации:

```
(config)# no port-security aging time
```

Сбрасывает время устаревания к значению по умолчанию.

Просмотр:

```
> show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

2.7.33.4 (config-if)# port-security

Включение безопасности порта на выбранных интерфейсах

Синтаксис:

```
(config-if)# port-security
```

Объяснение: Включение функции безопасности порта (port security) на выбранных портах.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда port-security в режиме конфигурации интерфейса **активирует функцию безопасности порта на конкретном порту (или диапазоне портов)**. Для работы этой функции необходимо предварительно глобально включить port-security командой port-security в глобальном режиме конфигурации.
- **На каких портах включать:**
    - ✓ **Порты доступа (access ports):** Рекомендуется включать на всех портах, к которым подключаются конечные пользователи (компьютеры, принтеры, IP-телефоны). Это предотвращает подключение неуправляемых коммутаторов, хабаров или несанкционированных устройств.
    - ✓ **Порты, где необходимо ограничить количество подключаемых устройств:** Например, на порту, к которому должен быть подключен только один компьютер.
- **Где не рекомендуется включать:**
    - ✓ **Магистральные порты (uplink):** На портах, ведущих к другим коммутаторам или маршрутизаторам, port-security может нарушить нормальную работу, так как на таких портах может быть много MAC-адресов.
- **После включения port-security на порту** рекомендуется настроить:
    - ✓ **Максимальное количество MAC-адресов** (port-security maximum <value>) — по умолчанию часто 1.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Действие при нарушении** (port-security violation {protect | restrict | shutdown}).
- ✓ **Разрешенные MAC-адреса** (опционально) — можно добавить статические записи.

Удаление конфигурации:

```
(config-if)# no port-security
```

Отключает безопасность порта на данном интерфейсе.

Просмотр:

```
> show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security switch [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

2.7.33.5 (config-if)# port-security maximum

Настройка максимального количества MAC-адресов на порту

Синтаксис:

```
(config-if)# port-security maximum [ <v_1_to_1024> ]
```

Параметры:

- [<v_1_to_1024>]: Укажите значение от 1 до 1024.

Объяснение: Максимальное количество MAC-адресов, которые могут быть защищены на этом порту. Количество не может превышать 1024. Если лимит превышен, выполняется соответствующее действие (action).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда port-security maximum задает **максимальное количество MAC-адресов**, которые могут быть изучены (и защищены) на данном порту. Это один из ключевых параметров для ограничения доступа.
- **Значения:**
    - ✓ **1 (используется чаще всего):** Используется на портах доступа, к которым должно подключаться только одно устройство (например, компьютер, принтер, IP-телефон). Это предотвращает подключение дополнительных устройств через неуправляемый коммутатор или хаб.
    - ✓ **Больше 1 (например, 5-10):** Может использоваться на портах, к которым через неуправляемый коммутатор подключено несколько устройств (например, несколько компьютеров в переговорной комнате), или на портах, где разрешено подключение нескольких устройств (например, IP-телефон + компьютер, где компьютер проходит через телефон).
    - ✓ **1024 (максимум):** Фактически отключает ограничение (но сохраняет другие функции port-security).
- **Как это работает:**

    1. Порт изучает MAC-адреса устройств, подключенных к нему.
    2. Как только количество изученных MAC-адресов достигает значения, заданного maximum, порт перестает изучать новые адреса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Если на порту появляется новый MAC-адрес сверх лимита, срабатывает действие, заданное командой port-security violation (например, порт отключается).

- В это ограничение входят как **динамически изученные**, так и **статически настроенные** безопасные MAC-адреса. Общее количество защищенных MAC-адресов на порту не может превышать значение maximum.

Удаление конфигурации:

```
(config-if)# no port-security maximum
```

Сбрасывает лимит MAC-адресов к значению по умолчанию (зависит от устройства, часто 1 или неограниченно)

Просмотр:

```
> show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

2.7.33.6 (config-if)# port-security violation

Настройка действия при нарушении безопасности порта

Синтаксис:

```
(config-if)# port-security violation { protect | trap | trap-shutdown | shutdown }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- { protect | trap | trap-shutdown | shutdown }: Укажите одно из действий, выполняемых при превышении лимита.
    - ✓ protect: Не допускать доступа более указанного лимита MAC-адресов на порту. Дальнейшие действия не предпринимаются. Пакеты от "лишних" MAC-адресов отбрасываются, но порт остается активным.
    - ✓ trap: Если на порту обнаружен (Limit + 1) MAC-адрес, отправить SNMP-ловушку (trap). Если устаревание (Aging) отключено, будет отправлена только одна SNMP-ловушка, но если устаревание включено, новые SNMP-ловушки будут отправляться каждый раз при превышении лимита.
    - ✓ trap-shutdown: Если на порту обнаружен (Limit + 1) MAC-адрес, будут выполнены оба действия: "Trap" (отправка SNMP-ловушки) и "Shutdown" (отключение порта), описанные выше.
    - ✓ shutdown: Если на порту обнаружен (Limit + 1) MAC-адрес, отключить порт. Это означает, что все защищенные MAC-адреса будут удалены с порта, и новые адреса не будут изучаться. Даже если кабель физически отключен и снова подключен на порту, порт останется отключенным. Существует три способа повторно открыть порт:
        1. Перезагрузить коммутатор.
        2. Отключить и снова включить контроль лимита (Limit Control) на порту или на коммутаторе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Нажать кнопку "Reopen" (в веб-интерфейсе) или использовать команду `no port-security shutdown` в CLI.

Рекомендации:

- Команда `port-security violation` определяет, **как коммутатор реагирует на нарушение безопасности порта** (превышение лимита MAC-адресов или появление неразрешенного MAC-адреса).
- **Выбор действия:**
  - ✓ `shutdown` **(рекомендуется для большинства портов доступа):** Наиболее строгое действие. При попытке подключения лишнего устройства порт отключается, что полностью предотвращает нарушение. Требует административного вмешательства для восстановления.
  - ✓ `protect` **(менее строгое):** Порт остается активным, но "лишние" устройства не получают доступ. Полезно, когда нельзя прерывать работу, но нужно контролировать нарушения (например, в сочетании с мониторингом).
  - ✓ `trap`**:** Только уведомление (SNMP). Порт продолжает работу, но администратор получает оповещение о нарушении. Подходит для мониторинга без автоматического вмешательства.
  - ✓ `trap-shutdown`**:** Комбинирует уведомление и отключение порта. Полезно, когда нужно и оповестить администратора, и немедленно пресечь нарушение.
- **Восстановление порта после shutdown:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Самый простой способ — использовать команду no port-security shutdown [interface <port>] в привилегированном режиме EXEC.

Удаление конфигурации:

```
(config-if)# no port-security violation
```

Сбрасывает действие при нарушении к значению по умолчанию (обычно shutdown*).*

Просмотр:

```
> show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
# show port-security port [ interface ( <port_type> [ <v_port_type_list> ] ) ]
```

2.7.34 Настройка уровней привилегий для команд (config)# privilege

Настройка уровня привилегий для команд, доступных в режиме конфигурации

Синтаксис

```
(config)# privilege { exec | configure | config-vlan | line | interface | if-vlan | ip mc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <privilege> <cmd>
```

Объяснение: Эта команда используется для изменения уровня привилегий команд, доступных в режиме конфигурации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile }: Укажите группу команд, которую вы хотите настроить.
- level <privilege>: Укажите уровень привилегий. Допустимый диапазон от 0 до 15.
- <cmd>: Начальные допустимые слова и литералы команды для изменения, до 128 символов.

Рекомендации:

- Команда privilege позволяет администратору **назначать или изменять уровень привилегий, необходимый для выполнения определенных команд**. Это основа реализации **Role-Based Access Control (RBAC)** в CLI.
- **Как это работает:**
    1. Каждая команда в CLI имеет уровень привилегий (по умолчанию, уровень 15 для конфигурационных команд, уровень 1 для большинства команд просмотра).
    2. С помощью команды privilege можно **понизить уровень** для определенных команд, чтобы они стали доступны пользователям с более низким уровнем привилегий (например, уровень 5).
    3. Также можно **повысить уровень** для команд, которые должны быть недоступны обычным пользователям.
    4. После настройки, если пользователь вошел в систему с определенным уровнем привилегий (например, уровень 5), он сможет выполнять только команды, уровень которых не превышает его уровня.
- **Группы команд:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. exec: Команды привилегированного режима EXEC (#).
2. configure: Команды глобального режима конфигурации ((config)#).
3. config-vlan: Команды режима конфигурации VLAN ((config-vlan)#).
4. line: Команды режима конфигурации линии ((config-line)#).
5. interface: Команды режима конфигурации интерфейса ((config-if)#).
6. if-vlan: Команды режима конфигурации интерфейса VLAN ((config-if-vlan)#).
7. ipmc-profile: Команды режима конфигурации IPMC-профиля ((config-ipmc-profile)#).
8. snmps-host, stp-aggr, dhcp-pool, rfc2544-profile: Другие группы команд.

Удаление конфигурации:

```
(config)# no privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <0-15> <cmd>
```

Удаляет настройку уровня привилегий для указанной команды.

Просмотр:

```
> show privilege
# show privilege
```

Отображает текущий уровень привилегий пользователя.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35 Настройка QoS (Quality of Service) (config)# qos

2.7.35.1 (config)# qos map cos-dscp

Настройка отображения COS в DSCP

Синтаксис:

(config)# qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Объяснение: Настройка отображения COS в DSCP.

Параметры:

- cos-dscp <cos>: Отображение COS в DSCP. Укажите уровень Class of Service. Допустимый диапазон от 0 до 7. CoS класс 0 имеет наименьший приоритет, а 7 — наивысший.
- dpl <dpl>: Укажите уровень приоритета отбрасывания (Drop Precedence Level). Допустимый диапазон от 0 до 7.
- dscp { <dscp_num> | { be | af11 | ... | ef | va } }: Укажите значение DSCP или один из предопределенных именованных классов.
    - ✓ <dscp_num: 0-63>: Числовое значение DSCP от 0 до 63.
    - ✓ be: PHB по умолчанию (DSCP 0) для трафика "best effort".
    - ✓ af11...af43: Assured Forwarding PHB (AF). Соответствуют значениям DSCP: AF11=10, AF12=12, AF13=14, AF21=18, AF22=20, AF23=22, AF31=26, AF32=28, AF33=30, AF41=34, AF42=36, AF43=38.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ cs1...cs7: Class Selector PHB. Соответствуют значениям: CS1=8, CS2=16, CS3=24, CS4=32, CS5=40, CS6=48, CS7=56.
- ✓ ef: Expedited Forwarding PHB (DSCP 46).
- ✓ va: Voice Admit PHB (DSCP 44).

Рекомендации:

- Команда qos map cos-dscp определяет, как значение **CoS (Class of Service, 802.1p)** из тега VLAN преобразуется в значение **DSCP (Differentiated Services Code Point)** в IP-заголовке. Это ключевая функция для обеспечения сквозного качества обслуживания (QoS) при переходе трафика из сети уровня 2 в сеть уровня 3.
- **Зачем это нужно:**
  - ✓ CoS используется в сетях уровня 2 (в тегах VLAN 802.1Q).
  - ✓ DSCP используется в IP-сетях уровня 3.
  - ✓ При передаче трафика через маршрутизатор или между разными сегментами сети, значения CoS должны быть преобразованы в соответствующие значения DSCP, чтобы политики QoS применялись согласованно на всем пути.
- **Параметр DPL (Drop Precedence Level):** Указывает приоритет отбрасывания в рамках одного класса трафика. Используется для реализации механизма WRED (Weighted Random Early Detection).
- **Предопределенные классы DSCP:**
  - ✓ **BE (Best Effort):** Обычный трафик, без гарантий.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **AF (Assured Forwarding):** Обеспечивает гарантированную доставку с различными уровнями приоритета отбрасывания.
- ✓ **EF (Expedited Forwarding):** Минимальная задержка и джиттер, используется для голосового трафика.
- ✓ **VA (Voice Admit):** Для голосового трафика с контролем допуска.
- ✓ **CS (Class Selector):** Обеспечивает обратную совместимость с IP Precedence.

Удаление конфигурации:

```
(config)# no qos map cos-dscp <cos> dpl <dpl>
```

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.2 (config)# qos map dscp-classify

Настройка классификации DSCP на входящем трафике (DSCP Ingress Classification)

Синтаксис:

```
(config)# qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение Настройка классификации DSCP на входящем трафике.

Параметры:

- dscp-classify { <dscp_num> | { be | af11 | ... | ef | va } }: Укажите одно из значений DSCP.
    - ✓ <dscp_num: 0-63>: Числовое значение DSCP от 0 до 63.
    - ✓ be: PHB по умолчанию (DSCP 0) для трафика "best effort".
    - ✓ af11...af43: Assured Forwarding PHB. Соответствуют значениям DSCP: AF11=10, AF12=12, AF13=14, AF21=18, AF22=20, AF23=22, AF31=26, AF32=28, AF33=30, AF41=34, AF42=36, AF43=38.
    - ✓ cs1...cs7: Class Selector PHB. Соответствуют значениям: CS1=8, CS2=16, CS3=24, CS4=32, CS5=40, CS6=48, CS7=56.
    - ✓ ef: Expedited Forwarding PHB (DSCP 46).
    - ✓ va: Voice Admit PHB (DSCP 44).

Рекомендации:

- Команда qos map dscp-classify определяет, как входящий IP-трафик будет **классифицироваться** на основе значения DSCP в заголовке IP-пакета. Это позволяет применять политики QoS (приоритезацию, ограничение скорости, маркировку) к трафику в зависимости от его DSCP-метки.
- **Как это работает:**
    1. При поступлении IP-пакета на коммутатор, значение DSCP из его заголовка считывается.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. С помощью таблицы dscp-classify это значение отображается во **внутренний класс трафика (CoS или очередь)** коммутатора.
3. В зависимости от полученного класса, к пакету применяются соответствующие политики QoS.

- **Зачем это нужно:**

1. **Уважение меток вышестоящих устройств:** Если трафик уже помечен DSCP на границе сети (например, маршрутизатором или файрволом), коммутатор должен корректно интерпретировать эти метки для обеспечения сквозного качества обслуживания.
2. **Гибкость классификации:** Позволяет настроить, какие DSCP-значения соответствуют какому классу обслуживания внутри коммутатора.

Удаление конфигурации:

```
(config)# no qos map dscp-classify { <dscp_num> | { be | af11 | ... | ef | va } }
```

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.3 (config)# qos map dscp-cos

Настройка отображения DSCP в CoS для входящего трафика

Синтаксис:

```
(config)# qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>
```

Объяснение: Настройка классификации входящего трафика QoS на основе DSCP.

Параметры:

- dscp-cos { <dscp_num> | { be | af11 | ... | ef | va } }: Укажите одно из значений DSCP.
    - ✓ <dscp_num: 0-63>: Числовое значение DSCP от 0 до 63.
    - ✓ be: Default PHB (DSCP 0) для трафика "best effort".
    - ✓ af11...af43: Assured Forwarding PHB. Соответствуют значениям DSCP: AF11=10, AF12=12, AF13=14, AF21=18, AF22=20, AF23=22, AF31=26, AF32=28, AF33=30, AF41=34, AF42=36, AF43=38.
    - ✓ cs1...cs7: Class Selector PHB. Соответствуют значениям: CS1=8, CS2=16, CS3=24, CS4=32, CS5=40, CS6=48, CS7=56.
    - ✓ ef: Expedited Forwarding PHB (DSCP 46).
    - ✓ va: Voice Admit PHB (DSCP 44).
- cos <cos>: Укажите уровень Class of Service. Допустимый диапазон от 0 до 7. CoS класс 0 имеет наименьший приоритет, а 7 — наивысший.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- dpl <dpl>: Укажите уровень приоритета отбрасывания (Drop Precedence Level). Допустимый диапазон от 0 до 7.

Рекомендации:

- Команда qos map dscp-cos определяет, как значение **DSCP (Differentiated Services Code Point)** из IP-заголовка входящего пакета преобразуется в значение **CoS (Class of Service)** и **DPL (Drop Precedence Level)** для внутренней обработки на коммутаторе.
- **В отличие от** dscp-classify**:** Команда dscp-classify просто классифицирует трафик на основе DSCP. Команда dscp-cos выполняет **явное отображение** (mapping) из DSCP в CoS и DPL, что дает более детальный контроль.
- **Зачем это нужно:**
    - ✓ **Сквозное QoS:** Позволяет преобразовывать метки DSCP (уровень 3) в приоритеты CoS (уровень 2) для дальнейшей обработки внутри коммутатора (например, для определения очереди).
    - ✓ **Совместимость:** Обеспечивает согласованную обработку трафика, помеченного различными схемами маркировки (DSCP или CoS).
- **Параметр DPL (Drop Precedence Level):** Используется совместно с WRED (Weighted Random Early Detection) для выборочного отбрасывания пакетов в зависимости от их приоритета отбрасывания.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no qos map dscp-cos { <dscp_num> | { be | af11 | ... | ef | va } }
```

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.4 (config)# qos map dscp-egress-translation

Настройка таблицы отображения DSCP на исходящем трафике (DSCP Egress Translation)

Синтаксис:

```
(config)# qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }
```

Объяснение: Настройка таблицы отображения DSCP на исходящем трафике.

Параметры:

- dscp-egress-translation { <dscp_num> | { be | af11 | ... | ef | va } }: Укажите исходное значение DSCP (которое будет переписано).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- to { <dscp_num_tr> | { be | af11 | ... | ef | va } }: Укажите целевое значение DSCP (новое значение, которое будет записано в заголовок исходящего пакета).
    - ✓ <dscp_num: 0-63>: Числовое значение DSCP от 0 до 63.
    - ✓ be: Default PHB (DSCP 0) для трафика "best effort".
    - ✓ af11...af43: Assured Forwarding PHB. Соответствуют значениям DSCP: AF11=10, AF12=12, AF13=14, AF21=18, AF22=20, AF23=22, AF31=26, AF32=28, AF33=30, AF41=34, AF42=36, AF43=38.
    - ✓ cs1...cs7: Class Selector PHB. Соответствуют значениям: CS1=8, CS2=16, CS3=24, CS4=32, CS5=40, CS6=48, CS7=56.
    - ✓ ef: Expedited Forwarding PHB (DSCP 46).
    - ✓ va: Voice Admit PHB (DSCP 44).

Рекомендации:

- Команда qos map dscp-egress-translation определяет **таблицу перезаписи (translation) значений DSCP** для исходящих IP-пакетов. Это позволяет изменить метку DSCP при выходе пакета из коммутатора.
- **Зачем это нужно:**
    - ✓ **Политики безопасности:** Некоторые сети требуют, чтобы при выходе из доверенного сегмента значения DSCP были переписаны на определенные значения (например, сброшены до 0) для предотвращения утечки информации о приоритетах.
    - ✓ **Согласование политик:** При передаче трафика между разными административными доменами или

SEC.RU | Короткий путь к информации Скачано с sec.ru

операторами может потребоваться переписать DSCP в соответствии с политиками принимающей стороны.

- ✓ **Упрощение:** В некоторых случаях может потребоваться преобразование сложных DSCP-меток в более простые значения для упрощения обработки в downstream-устройствах.

- **Как это работает:**
  1. Пакет обрабатывается внутри коммутатора с учетом его внутренних приоритетов (CoS, DPL).
  2. Перед отправкой пакета, коммутатор проверяет текущее значение DSCP в его заголовке.
  3. Если в таблице dscp-egress-translation есть правило для этого значения, DSCP перезаписывается на указанное целевое значение.
- В отличие от dscp-ingress-translation**:** dscp-ingress-translation перезаписывает DSCP при входе пакета в коммутатор. dscp-egress-translation перезаписывает DSCP при выходе.

Удаление конфигурации:

```
(config)# no qos map dscp-egress-translation { <dscp_num> | { be | af11 | ... | ef | va } }
```

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.5 (config)# qos map dscp-ingress-translation

Настройка таблицы отображения DSCP на входящем трафике (DSCP Ingress Translation)

Синтаксис:

(config)# qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Объяснение: Настройка таблицы отображения DSCP на входящем трафике.

Параметры:

- dscp-ingress-translation { <dscp_num> | { be | af11 | ... | ef | va } }: Укажите исходное значение DSCP (которое будет переписано при входе).
- to { <dscp_num_tr> | { be | af11 | ... | ef | va } }: Укажите целевое значение DSCP (новое значение, которое будет записано в заголовок входящего пакета).
    - ✓ <dscp_num: 0-63>: Числовое значение DSCP от 0 до 63.
    - ✓ be: Default PHB (DSCP 0) для трафика "best effort".
    - ✓ af11...af43: Assured Forwarding PHB. Соответствуют значениям DSCP: AF11=10, AF12=12, AF13=14, AF21=18, AF22=20, AF23=22, AF31=26, AF32=28, AF33=30, AF41=34, AF42=36, AF43=38.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ cs1...cs7: Class Selector PHB. Соответствуют значениям: CS1=8, CS2=16, CS3=24, CS4=32, CS5=40, CS6=48, CS7=56.
- ✓ ef: Expedited Forwarding PHB (DSCP 46).
- ✓ va: Voice Admit PHB (DSCP 44).

Рекомендации:

- Команда qos map dscp-ingress-translation определяет **таблицу перезаписи (translation) значений DSCP** для входящих IP-пакетов. Это позволяет изменить метку DSCP сразу при поступлении пакета на коммутатор.
- **Зачем это нужно:**
  - ✓ **Нормализация меток:** Если в сеть поступают пакеты с нестандартными или неподдерживаемыми значениями DSCP, можно переписать их в значения, которые понимает и обрабатывает ваша политика QoS.
  - ✓ **Безопасность:** Можно сбрасывать подозрительные или несанкционированные DSCP-метки в значение по умолчанию (BE) для предотвращения обхода политик QoS.
  - ✓ **Согласование политик:** При приеме трафика от другого административного домена может потребоваться переписать DSCP в соответствии с внутренними политиками организации.
- **Как это работает:**

  1. Пакет поступает на порт коммутатора.
  2. Коммутатор считывает значение DSCP из заголовка IP-пакета.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Если в таблице dscp-ingress-translation есть правило для этого значения, DSCP перезаписывается на указанное целевое значение.
4. Дальнейшая обработка пакета (классификация, маршрутизация, очереди) использует уже переписанное значение DSCP.

- **Отличие от** dscp-egress-translation**:** dscp-ingress-translation применяется до обработки пакета коммутатором. dscp-egress-translation применяется после обработки, перед отправкой пакета.

Удаление конфигурации:

```
(config)# no qos map dscp-ingress-translation { <dscp_num> | { be | af11 | ... | ef | va } }
```

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.6 (config)# qos qce refresh

Обновление записей QCE (QoS Control Entries)

Синтаксис:

```
(config)# qos qce refresh
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Обновление записей QCE (QoS Control Entries).

Рекомендации:

- Команда `qos qce refresh` инициирует **принудительное обновление (перезагрузку) всех записей QoS Control Entries (QCE)** на коммутаторе. QCE — это правила, которые определяют, как трафик классифицируется и маркируется на основе различных критериев (порт, VLAN, MAC-адрес, IP-адрес, DSCP, CoS и т.д.).
- **Зачем это нужно:**
    - ✓ **Применение изменений:** После изменения конфигурации QCE (добавления, удаления или изменения правил QoS) может потребоваться принудительное обновление, чтобы изменения вступили в силу немедленно.
    - ✓ **Синхронизация:** В некоторых реализациях QCE хранятся в аппаратной таблице (TCAM — Ternary Content Addressable Memory).
      Команда `refresh` перезагружает эти аппаратные записи из текущей конфигурации, гарантируя, что аппаратное обеспечение и программная конфигурация синхронизированы.
    - ✓ **Устранение проблем:** Если наблюдаются аномалии в работе QoS (например, трафик не маркируется ожидаемым образом), выполнение `refresh` может устранить временные рассогласования между программной и аппаратной частями.
- **Когда использовать:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ После массового добавления или изменения QCE правил.
- ✓ После загрузки новой конфигурации.
- ✓ При диагностике проблем с QoS.

- Эта команда не изменяет саму конфигурацию QoS, а только применяет существующие правила в аппаратную часть коммутатора. В большинстве случаев изменения QCE применяются автоматически, но данная команда может быть полезна для принудительного применения в сложных сценариях.

2.7.35.7 (config)# qos qce update

Обновление записи QoS Control Entry (QCE)

Синтаксис:

(config)# qos qce [update] <qce_id> [{ next <qce_id_next> } | last] [interface (<port_type> [<port_list>])] [smac { <smac> | <smac_24> | any }] [dmac { <dmac> | unicast | multicast | broadcast | any }] [tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <ot_vid> | any }] [pcp { <ot_pcp> | any }] [dei { <ot_dei> | any }] }] [inner-tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <it_vid> | any }] [pcp { <it_pcp> | any }] [dei { <it_dei> | any }] }] [frame-type { any | { etype [{ <etype_type> | any }] } | { llc [dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }] } | { snap [{ <snap_data> | any }] } | { ipv4 [proto { <pr4> | tcp | udp | any }] [sip { <sip4> | any }] [dip { <dip4> | any }] [dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [fragment { yes |

SEC.RU | Короткий путь к информации Скачано с sec.ru

no | any }] [sport { <sp4> | any }] [dport { <dp4> | any }] } | { ipv6 [proto { <pr6> | tcp | udp | any }] [sip { <sip6> | any }] [dip { <dip6> | any }] [dscp { <dscp6> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [sport { <sp6> | any }] [dport { <dp6> | any }] } }] [action { [cos { <action_cos> | default }] [dpl { <action_dpl> | default }] [pcp-dei { <action_pcp> <action_dei> | default }] [dscp { <action_dscp_dscp> | { be | af11 | ... | ef | va } | default }] [policy { <action_policy> | default }] }]

Объяснение: Обновление записи QCE.

Параметры:

- [update]: Обновление QCE (необязательный ключ).
- <qce_id>: Укажите идентификатор QCE.
- [{ next <qce_id_next> } | last]: Поместить эту QCE после указанной или в конец.
- [interface (<port_type> [<port_list>])]: Укажите тип порта и номер порта, к которым применяется это обновленное правило QCE.
- [smac { <smac> | <smac_24> | any }]: Настройка исходного MAC-адреса для сопоставления.
- [dmac { <dmac> | unicast | multicast | broadcast | any }]: Настройка MAC-адреса назначения для сопоставления.
- [tag { ... }]: Настройка внешнего тега (outer tag) для сопоставления (тип, VID, PCP, DEI).
- [inner-tag { ... }]: Настройка внутреннего тега (inner tag) для сопоставления (для Q-in-Q).
- [frame-type { any | etype | llc | snap | ipv4 | ipv6 }]: Тип кадра для сопоставления.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [action { ... }]: Действие, выполняемое при совпадении с правилом (установка CoS, DPL, PCP/DEI, DSCP, политики).

Рекомендации:

- Команда qos qce update позволяет создавать или изменять записи QoS Control Entry (QCE) – правила классификации и маркировки трафика на уровне портов.
- **QCE** Это правила, которые определяют, как коммутатор должен классифицировать входящий трафик на основе множества критериев (порт, MAC-адреса, VLAN-теги, IP-адреса, протоколы, DSCP и т.д.) и какие действия применять (установка CoS, DPL, DSCP, PCP/DEI, назначение очереди).
- **Порядок обработки QCE:** Правила обрабатываются в порядке возрастания ID. Можно вставить новое правило перед существующим (next <qce_id>) или добавить в конец (last).
- **Широкие возможности фильтрации:**
    - ✓ **MAC-адреса:** исходный (SMAC) и назначения (DMAC), включая типы (unicast, multicast, broadcast).
    - ✓ **VLAN-теги:** внешний и внутренний теги для Q-in-Q (тип, VID, PCP, DEI).
    - ✓ **Типы кадров:** Ethernet II (etype), LLC, SNAP, IPv4, IPv6.
    - ✓ **IPv4/IPv6:** протокол (TCP, UDP, любой), IP-адреса источника/назначения, DSCP, фрагментация, TCP/UDP порты.
- **Действия (action):** При совпадении можно:
    - ✓ Установить CoS (cos) и DPL (dpl) для определения очереди и приоритета отбрасывания.
    - ✓ Установить PCP и DEI (pcp-dei) в теге VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Переписать DSCP (dscp).
- ✓ Применить политику QoS (policy).

Удаление конфигурации:

```
(config)# no qos qce <qce_id_range>
```

Удаляет указанные QCE-записи.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.8 (config)# qos storm

Настройка защиты от штормов (Storm Control) для QoS

Синтаксис:

```
(config)# qos storm { unicast | multicast | broadcast } { { <rate> [ kfps ] } | { 1024 kfps } }
```

Объяснение: Настройка защиты от широковещательных штормов (broadcast storm control) для QoS.

Параметры:

- { unicast | multicast | broadcast }: Укажите тип шторма, который вы хотите настроить.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ unicast: Одноадресный трафик.
- ✓ multicast: Многоадресный трафик.
- ✓ broadcast: Широковещательный трафик.

- { { <rate> [kfps] } | { 1024 kfps } }: Задайте ограничение скорости шторма в килокадрах в секунду (kfps — kilo frames per second). Можно указать пользовательское значение или установить значение 1024 kfps.

Рекомендации:

- Команда qos storm настраивает функцию **storm control** для различных типов трафика (широковещательный, многоадресный, одноадресный). Эта функция ограничивает количество кадров определенного типа, проходящих через порт, предотвращая перегрузку сети при атаках или неисправностях.
- **Зачем это нужно:**
  - ✓ **Широковещательные штормы (broadcast storm):** Возникают при наличии петель в сети или при атаках (например, MAC flooding). Могут полностью парализовать работу сети.
  - ✓ **Многоадресные штормы (multicast storm):** Могут возникать при неправильной настройке multicast-протоколов.
  - ✓ **Одноадресные штормы (unicast storm):** Могут быть вызваны атаками или сбоями в работе устройств.
- **Единица измерения:** Скорость задается в **килокадрах в секунду (kfps)**. Например, 100 kfps означает 100 000 кадров в секунду. Значение 1024 kfps часто используется как "выключено" или "без ограничений" (так как это максимальное значение).
- **Принцип работы:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Коммутатор отслеживает количество кадров каждого типа, проходящих через порт.
2. Если количество кадров превышает заданный порог (<rate>), коммутатор начинает отбрасывать (drop) избыточные кадры до тех пор, пока нагрузка не снизится.
3. Это позволяет защитить CPU коммутатора и другие порты от перегрузки.

- **Рекомендации по настройке:**

1. Для портов доступа обычно устанавливают ограничения на broadcast и multicast трафик (например, 100-500 kfps).
2. Для магистральных портов (uplink) ограничения могут быть выше или отсутствовать.
3. Значение 1024 kfps часто используется для отключения ограничения (так как это максимальное значение, которое не будет достигнуто в обычных условиях).

Удаление конфигурации:

```
(config)# no qos storm { unicast | multicast | broadcast }
```

Удаляет настройку защиты от штормов для указанного типа трафика.

Просмотр:

```
# show qos storm
```

Отображает текущие настройки защиты от штормов для различных типов трафика.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.9 (config-if)# qos cos

Настройка значения CoS на выбранном интерфейсе

Синтаксис:

```
(config-if)# qos cos <cos>
```

Параметры:

- <cos>: Укажите значение CoS (Class of Service) от 0 до 7.

Объяснение: Настройка значения CoS на данном выбранном интерфейсе.

Рекомендации:

- Команда qos cos в режиме конфигурации интерфейса задает **значение CoS (Class of Service, 802.1p) по умолчанию** для всего трафика, проходящего через данный порт, если трафик не классифицирован иначе (например, QCE правилами).
- **CoS** Это 3-битовое поле в теге VLAN (802.1Q), которое используется для маркировки приоритета кадра уровня 2. Значения от 0 до 7, где 7 — наивысший приоритет.
- **Как это работает:**
    1. Если на порту настроено qos cos <value>, то все входящие кадры, которые не имеют тега VLAN (untagged), получают этот CoS при добавлении тега.
    2. Для кадров, уже имеющих тег VLAN (tagged), значение CoS может быть сохранено или переопределено в зависимости от конфигурации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Это значение затем используется для определения очереди (queue) и дальнейшей обработки QoS внутри коммутатора.

- **Типичные сценарии:**
  1. На портах доступа, где подключены конечные устройства (компьютеры, принтеры), часто устанавливается `qos cos 0` (best effort) или другое значение по умолчанию.
  2. Если к порту подключено устройство, генерирующее критически важный трафик (например, IP-камера), можно установить более высокий CoS (например, `qos cos 5`) для маркировки всего его трафика.
- Эта команда не отменяет и не заменяет более специфичные правила QCE (QoS Control Entries), которые могут классифицировать трафик на основе более детальных критериев (IP-адреса, порты, протоколы).

Удаление конфигурации:

```
(config-if)# no qos cos
```

Сбрасывает значение CoS на интерфейсе к значению по умолчанию (обычно 0).

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.10 (config-if)# qos dei

Настройка значения DEI на выбранном интерфейсе

Синтаксис:

```
(config-if)# qos dei <dei>
```

Параметры:

- <dei>: Укажите значение DEI (Drop Eligible Indicator) для нетегированных (untagged) кадров.

Объяснение: Настройка значения DEI (Drop Eligible Indicator) на данном выбранном интерфейсе.

Рекомендации:

- Команда qos dei в режиме конфигурации интерфейса задает **значение DEI (Drop Eligible Indicator) по умолчанию** для нетегированных (untagged) кадров, поступающих на порт. DEI — это 1-битовое поле в теге VLAN (802.1Q), которое указывает, может ли кадр быть отброшен при перегрузке (1 — может быть отброшен, 0 — не может).
- **DEI** используется для обозначения приоритета отбрасывания. В сочетании с CoS (PCP) позволяет реализовать более гибкие политики QoS. Например, в рамках одного класса трафика (CoS) можно выделить подклассы с разным приоритетом отбрасывания.
- **Как это работает:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Для нетегированных кадров (untagged frames), поступающих на порт, коммутатор добавляет тег VLAN. В этом теге бит DEI устанавливается в значение, заданное командой `qos dei`.
2. Для кадров, уже имеющих тег VLAN (tagged frames), значение DEI сохраняется (если не переопределено другими правилами QoS).
3. Внутри коммутатора значение DEI используется механизмами управления очередями (например, WRED — Weighted Random Early Detection) для принятия решения о том, отбрасывать ли кадр при перегрузке.

- **Значения:**
    1. **0 (не подлежит отбрасыванию):** Кадр имеет более высокий приоритет и будет отброшен только в крайнем случае.
    2. **1 (подлежит отбрасыванию):** Кадр имеет более низкий приоритет и будет отброшен в первую очередь при перегрузке.
- **Типичные сценарии:**
    1. На портах доступа обычно устанавливают `qos dei 0`, чтобы не маркировать трафик как "отбрасываемый" по умолчанию.
    2. В сетях (SLA) можно маркировать менее важный трафик (например, best effort) значением DEI 1, чтобы защитить более критичный трафик.

Удаление конфигурации:

```
(config-if)# no qos dei
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Сбрасывает значение DEI на интерфейсе к значению по умолчанию (обычно 0).

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.11 (config-if)# qos dpl

Настройка значения DPL на выбранном интерфейсе

Синтаксис:

```
(config-if)# qos dpl <dpl>
```

Параметры:

- <dpl>: Укажите уровень приоритета отбрасывания (Drop Precedence Level) по умолчанию.

Объяснение: Настройка значения DPL на данном выбранном интерфейсе.

Рекомендации:

- Команда qos dpl в режиме конфигурации интерфейса задает **уровень приоритета отбрасывания (Drop Precedence Level, DPL) по умолчанию** для трафика, проходящего через данный порт.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- DPL – это параметр, используемый внутри коммутатора для определения, какие пакеты должны быть отброшены в первую очередь при перегрузке. В сочетании с CoS (или DSCP) DPL позволяет реализовать дифференцированное отбрасывание пакетов в рамках одного класса обслуживания.
- **Как это работает:**
    1. DPL назначается пакету на основе правил классификации (например, из QCE или отображений DSCP-to-CoS).
    2. Если пакет не попадает ни под одно правило классификации, используется значение DPL по умолчанию, заданное командой `qos dpl`.
    3. При перегрузке очереди механизмы управления очередями (например, WRED — Weighted Random Early Detection) используют DPL для принятия решения: пакеты с более высоким DPL отбрасываются с большей вероятностью.
- DPL обычно находится в диапазоне от 0 до 7. **Меньшее значение означает более низкий приоритет отбрасывания** (пакет менее вероятно будет отброшен). Большее значение означает более высокий приоритет отбрасывания (пакет будет отброшен с большей вероятностью).
- **Типичные сценарии:**
    1. Для критического трафика (голос, видео) устанавливается DPL 0.
    2. Для обычного трафика (best effort) — DPL 1 или выше.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Для трафика, который может быть легко передан повторно (например, фоновые передачи данных), можно установить более высокий DPL.

Удаление конфигурации:

```
(config-if)# no qos dpl
```

Сбрасывает значение DPL на интерфейсе к значению по умолчанию (обычно 0).

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.12 (config-if)# qos dscp-classify

Настройка метода классификации на основе DSCP на интерфейсе

Синтаксис:

```
(config-if)# qos dscp-classify { zero | selected | any }
```

Параметры:

- { zero | selected | any }: Укажите метод классификации.
  - ✓ zero: Классифицировать, если входящий DSCP равен 0.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ selected: Классифицировать только выбранные DSCP, для которых классификация включена в таблице преобразования DSCP.
- ✓ any: Классифицировать все DSCP.

Объяснение: Настройка метода классификации на основе DSCP на интерфейсе.

Рекомендации:

- Команда qos dscp-classify в режиме конфигурации интерфейса определяет, **какие входящие IP-пакеты с какими значениями DSCP будут подвергаться классификации QoS** на данном порту.
- Это позволяет контролировать, насколько агрессивно коммутатор обрабатывает DSCP-метки для классификации трафика. Это может быть полезно для:
  - ✓ **Безопасности:** Игнорировать все DSCP-метки (zero) или доверять только определенным (selected), чтобы предотвратить попытки обхода политик QoS с помощью поддельных DSCP-меток.
  - ✓ **Производительности:** Ограничить количество DSCP-значений, которые необходимо обрабатывать, если в сети используются только некоторые из них.
- **Варианты:**
  - ✓ any **(по умолчанию):** Все входящие DSCP-метки учитываются при классификации. Трафик классифицируется на основе глобальной таблицы dscp-

SEC.RU | Короткий путь к информации Скачано с sec.ru

classify. Это наиболее гибкий, но и наиболее ресурсоемкий вариант.

- ✓ selected**:** Классифицируются только те DSCP-значения, для которых явно включена классификация (вероятно, через таблицу dscp-classify или другие механизмы). Позволяет точно контролировать, какие метки обрабатываются.
- ✓ zero**:** Только пакеты с DSCP = 0 классифицируются. Все остальные DSCP-значения игнорируются при классификации (т.е. трафик с ненулевыми DSCP может обрабатываться как best effort). Это может использоваться в средах, где не доверяют внешним DSCP-меткам.

- Эта команда работает в связке с глобальными настройками qos map dscp-classify. Если на порту установлено selected, то классификация применяется только к DSCP-значениям, присутствующим в глобальной таблице классификации.

Удаление конфигурации:

```
(config-if)# no qos dscp-classify
```

Сбрасывает метод классификации к значению по умолчанию (обычно any*).*

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.13 (config-if)# qos dscp-remark

Настройка перезаписи значений DSCP на исходящем трафике порта

Синтаксис

```
(config-if)# qos dscp-remark { rewrite | remap | remap-dp }
```

Параметры:

- { rewrite | remap | remap-dp }: Укажите один из вариантов.
  - ✓ rewrite: Переписать поле DSCP классифицированным значением DSCP.
  - ✓ remap: Кадр с DSCP от анализатора (входящего) переотображается и маркируется переотображенным значением DSCP. В зависимости от уровня DP (Drop Precedence) кадра, переотображенное значение DSCP берется либо из таблицы преобразования DSCP, либо из поля Egress Remap DP0 или DP1.
  - ✓ remap-dp: Кадр с DSCP от анализатора переотображается и маркируется переотображенным значением DSCP. Переотображенное значение DSCP всегда берется из таблицы преобразования DSCP, из поля Egress Remap DP0.

Объяснение: Настройка перезаписи значений DSCP на исходящем трафике порта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда qos dscp-remark определяет, как коммутатор обрабатывает значение DSCP (Differentiated Services Code Point) в IP-заголовке исходящих пакетов на данном порту. Это позволяет контролировать, какие DSCP-метки покидают коммутатор, обеспечивая согласованность политик QoS на границах сети.
- **Варианты:**
    - ✓ rewrite **(перезапись):** Поле DSCP перезаписывается значением, которое было присвоено пакету в процессе классификации внутри коммутатора (например, на основе правил QCE, отображений CoS-to-DSCP и т.д.). Это наиболее распространенный режим для доверенных границ сети.
    - ✓ remap **(переотображение с учетом DP):** DSCP переотображается с использованием таблицы преобразования DSCP (DSCP Translation Table), но выбор значения зависит от уровня приоритета отбрасывания (DP — Drop Precedence) пакета. Пакеты с разным DP могут получить разные исходящие DSCP. Это позволяет, например, внутри одного класса трафика маркировать пакеты с разной вероятностью отбрасывания разными DSCP-значениями.
    - ✓ remap-dp **(переотображение без учета DP):** DSCP переотображается с использованием таблицы преобразования DSCP, всегда из поля Egress Remap DP0 (игнорируя фактический DP пакета). Это более простой вариант переотображения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    - ✓ **Нормализация меток:** При передаче трафика в другой домен (например, к другому оператору) может потребоваться переписать DSCP в соответствии с политиками принимающей стороны.
    - ✓ **Безопасность:** Можно сбрасывать DSCP в значение по умолчанию при выходе из доверенного сегмента, чтобы предотвратить утечку информации о приоритетах.
    - ✓ **Согласованность QoS:** Обеспечивает, чтобы внутренние политики QoS корректно отражались на исходящих метках.

Удаление конфигурации:

```
(config-if)# no qos dscp-remark
```

Отключает перезапись DSCP на порту, возвращаясь к поведению по умолчанию (обычно оставляет DSCP без изменений).

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.14 (config-if)# qos dscp-translate

Включение преобразования DSCP на входящем трафике интерфейса

Синтаксис:

```
(config-if)# qos dscp-translate
```

Объяснение: Настройка преобразования DSCP на входящем трафике QoS для конкретного интерфейса.

Рекомендации:

- Команда qos dscp-translate в режиме конфигурации интерфейса **включает функцию преобразования (translation) DSCP для входящих IP-пакетов** на данном порту. Эта функция позволяет перезаписывать (переводить) значения DSCP в соответствии с таблицей dscp-ingress-translation (которая настраивается глобально).
- **Как это работает:**
    1. IP-пакет поступает на порт, где включена dscp-translate.
    2. Коммутатор считывает текущее значение DSCP из заголовка пакета.
    3. Если в таблице dscp-ingress-translation есть правило для этого значения, DSCP перезаписывается на соответствующее целевое значение.
    4. После преобразования пакет обрабатывается с новым значением DSCP (классификация, маршрутизация, очереди).
- **Зачем это нужно:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. **Нормализация меток:** Преобразование нестандартных или неподдерживаемых DSCP-значений в стандартные, принятые в вашей сети.
2. **Безопасность:** Сброс подозрительных DSCP-меток (например, высокоприоритетных от недоверенных источников) в значение по умолчанию (BE).
3. **Согласование политик:** При приеме трафика от другого административного домена или устаревшего оборудования может потребоваться преобразование DSCP в соответствии с внутренними политиками.

- Эта команда включает преобразование, но **сами правила преобразования** (какое значение во что переводить) задаются глобальной командой `qos map dscp-ingress-translation`. Если эта команда не настроена, включение `dscp-translate` на порту не будет иметь эффекта.
- **Отличие от** `dscp-classify`**:** `dscp-classify` определяет, *какие* DSCP-значения учитываются при классификации. `dscp-translate` *изменяет* сами DSCP-значения перед классификацией.

Удаление конфигурации:

```
(config-if)# no qos dscp-translate
```

Отключает преобразование DSCP на входящем трафике порта. DSCP-значения не будут изменяться.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.15 (config-if)# qos map cos-tag cos

Настройка отображения (QoS Class, DP Level) в (PCP, DEI) для интерфейса

Синтаксис:

```
(config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>
```

Параметры:

- cos <cos: 0-7>: Укажите значение QoS-класса.
- dpl <dpl: 0-1>: Укажите значение DPL (Drop Precedence Level) — 0 или 1.
- pcp <pcp: 0-7>: Укажите значение PCP (Priority Code Point).
- dei <dei: 0-1>: Укажите значение DEI (Drop Eligible Indicator) — 0 или 1.

Объяснение: Настройка отображения (QoS класс, уровень DP) в (PCP, DEI) для QoS на конкретном интерфейсе.

Рекомендации:

- Команда qos map cos-tag cos определяет, как внутренняя метка QoS (класс CoS и уровень приоритета отбрасывания DPL) преобразуется в **исходящий тег VLAN (PCP и DEI)** на данном порту.
- **Как это работает:**
    1. Внутри коммутатора каждый пакет имеет внутреннюю метку, состоящую из CoS (0-7) и DPL (0-1). Эта метка назначается на основе классификации (QCE, отображения DSCP-to-CoS и т.д.).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. При отправке пакета на порт, где настроено отображение, коммутатор использует эту команду для определения, какие значения PCP и DEI записать в тег VLAN (если пакет тегированный) или добавить (если пакет нетегированный).
3. Если для конкретной пары (CoS, DPL) не задано явное отображение, может использоваться отображение по умолчанию.

- **Зачем это нужно:**
    1. **Гибкость:** Позволяет настраивать, как внутренние приоритеты QoS преобразуются в приоритеты уровня 2 (PCP/DEI) на разных портах. Например, на магистральном порту можно использовать одно отображение, а на порту доступа — другое.
    2. **Совместимость:** Обеспечивает корректную маркировку трафика для downstream-устройств, которые могут ожидать определенные значения PCP/DEI.
    3. **Политики:** Можно, например, отображать два разных внутренних уровня (CoS=5, DPL=0) и (CoS=5, DPL=1) в разные значения PCP, чтобы отражать приоритет отбрасывания в теге VLAN.
- Отображение cos-tag обычно имеет более высокий приоритет, чем отображение по умолчанию (если таковое существует). Если на порту не настроено отображение, используется глобальное отображение или поведение по умолчанию.

Удаление конфигурации:

```
(config-if)# no qos map cos-tag cos <cos> dpl <dpl>
```

Удаляет отображение для указанной пары (CoS, DPL).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.16 (config-if)# qos map tag-cos pcp

Настройка отображения (PCP, DEI) в (QoS Class, DP Level) для интерфейса

Синтаксис:

```
(config-if)# qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>
```

Параметры:

- pcp <pcp: 0-7>: Укажите значение PCP (Priority Code Point).
- dei <dei: 0-1>: Укажите значение DEI (Drop Eligible Indicator) — 0 или 1.
- cos <cos: 0-7>: Укажите значение QoS-класса.
- dpl <dpl: 0-1>: Укажите значение DPL (Drop Precedence Level) — 0 или 1.

Объяснение: Настройка отображения (PCP, DEI) в (QoS класс, уровень DP) для QoS на конкретном интерфейсе.

Рекомендации:

- Команда qos map tag-cos pcp является **парной к команде** qos map cos-tag и определяет, как значения **входящего тега VLAN**

SEC.RU | Короткий путь к информации Скачано с sec.ru

(PCP и DEI) преобразуются во **внутреннюю метку QoS (CoS и DPL)** на данном порту.

- **Как это работает:**
    1. При поступлении тегированного кадра (с тегом VLAN 802.1Q) на порт, коммутатор считывает значения PCP (приоритет) и DEI (индикатор возможности отбрасывания) из тега.
    2. Если на порту настроено отображение `tag-cos`, коммутатор использует эту команду для определения, какая внутренняя метка QoS (CoS и DPL) будет присвоена пакету.
    3. Если для конкретной пары (PCP, DEI) не задано явное отображение, может использоваться отображение по умолчанию.
- **Зачем это нужно:**
    1. Позволяет контролировать, насколько коммутатор доверяет значениям PCP/DEI, поступающим на порт. Например, на порту, подключенном к доверенному устройству, можно настроить прямое отображение PCP в CoS. На порту, подключенном к ненадежному пользователю, можно все PCP отображать в низкий CoS.
    2. Позволяет настраивать отображение по-разному на разных портах в зависимости от роли порта (доступ, магистраль, подключение к внешнему оператору).
    3. Предотвращает попытки обхода политик QoS путем подмены PCP-меток на ненадежных портах.
- Отличие от `cos-tag`**:** `cos-tag` отображает внутреннюю метку в исходящий тег (внутрь → наружу). `tag-cos` отображает входящий тег во внутреннюю метку (снаружи → внутрь).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no qos map tag-cos pcp <pcp> dei <dei>
```

Удаляет отображение для указанной пары (PCP, DEI).

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.17 (config-if)# qos pcp

Настройка значения PCP на выбранном интерфейсе

Синтаксис:

```
(config-if)# qos pcp <pcp>
```

Параметры:

- pcp <pcp: 0-7>: Укажите значение PCP (Priority Code Point).

Объяснение: Настройка значения PCP для конкретного интерфейса.

Рекомендации:

- Команда qos pcp в режиме конфигурации интерфейса задает **значение PCP (Priority Code Point) по умолчанию** для

SEC.RU | Короткий путь к информации Скачано с sec.ru

нетегированных (untagged) кадров, поступающих на порт. PCP — это 3-битовое поле в теге VLAN (802.1Q), которое используется для маркировки приоритета кадра уровня 2.

- **Как это работает:**
    1. Для нетегированных кадров (без тега VLAN), поступающих на порт, коммутатор добавляет тег VLAN. В этом теге биты PCP устанавливаются в значение, заданное командой `qos pcp`.
    2. Для кадров, уже имеющих тег VLAN (tagged frames), значение PCP сохраняется (если не переопределено другими правилами QoS, например, QCE).
    3. Это значение затем используется для определения внутренней метки QoS (CoS) и дальнейшей обработки внутри коммутатора.
- **Значения:**
    1. **0** — наименьший приоритет (best effort).
    2. **7** — наивысший приоритет (обычно для сетевого управления).
    3. **5** — часто используется для голосового трафика (VoIP).
    4. **4** — для видеотрафика.

Удаление конфигурации:

```
(config-if)# no qos pcp
```

Сбрасывает значение PCP на интерфейсе к значению по умолчанию (обычно 0).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.18 (config-if)# qos policer

Настройка ограничителя скорости на интерфейсе

Синтаксис:

```
(config-if)# qos policer <rate> [ fps ] [ flowcontrol ]
```

Параметры:

- <rate>: Укажите скорость для *ограничителя скорости*. По умолчанию используется 500 кбит/с. Допустимый диапазон для кбит/с и кадров/с (fps) составляет от 100 до 1 000 000. Допустимый диапазон для Мбит/с и ккадров/с (kfps) составляет от 1 до 3300 Мбит/с.
- [fps]: Скорость задается в кадрах в секунду (fps). По умолчанию используется кбит/с (kbps).
- [flowcontrol]: Включить управление потоком (Flow Control). Если управление потоком включено и порт находится в режиме управления потоком, то вместо отбрасывания кадров отправляются pause-кадры.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда qos policer в режиме конфигурации интерфейса настраивает **ограничитель скорости** для входящего трафика на данном порту. Функция ограничивает скорость входящего трафика, отбрасывая (или отправляя pause-кадры) пакеты, превышающие заданный лимит.
- **Единицы измерения:**
    - ✓ **По умолчанию (без** fps**):** Скорость задается в **килобитах в секунду (kbps)** или **мегабитах в секунду (Mbps)**. Например, 1000 означает 1000 кбит/с = 1 Мбит/с.
    - ✓ **С параметром** fps**:** Скорость задается в **кадрах в секунду (fps)** или **килокадрах в секунду (kfps)**. Например, 100 fps означает 100 кадров в секунду.
- **Действие при превышении лимита:**
    - ✓ **По умолчанию:** Пакеты, превышающие лимит, **отбрасываются (drop)**.
    - ✓ **С параметром** flowcontrol**:** Если на порту также включено управление потоком (flow control), то вместо отбрасывания пакетов отправляются **pause-кадры** на устройство-источник, временно приостанавливая передачу. Это более щадящий способ, но требует поддержки управления потоком на подключенном устройстве.
- **Типичные сценарии:**
    - ✓ **Ограничение скорости для пользователей:** На портах доступа можно установить лимит, например, 10 Мбит/с, чтобы пользователь не мог использовать больше.
    - ✓ **Защита от перегрузок:** Ограничение скорости для определенных типов трафика (например, broadcast).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no qos policer
```

Отключает ограничитель скорости на интерфейсе.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.19 (config-if)# qos queue-policer queue

Настройка ограничетеля для входящей очереди на интерфейсе

Синтаксис:

```
(config-if)# qos queue-policer queue <queue> <rate>
```

Параметры:

- <queue: 0-7>: Укажите номер очереди (или диапазон) для полицейского.
- <rate: 100-3300000>: Укажите скорость ограничителя в килобитах в секунду (kbps).

Объяснение: Настройка скорости ограничителя (Ingress Queue Policers Rate) для QoS на конкретном интерфейсе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `qos queue-policer queue` настраивает **ограничитель скорости для конкретной входящей очереди (или диапазона очередей)** на данном порту. Это позволяет ограничивать скорость трафика, попадающего в определенную очередь, на этапе входа (ingress).
- **Как это работает:**
    1. Трафик классифицируется и направляется в одну из очередей (0-7) на основе правил QoS (QCE, отображения DSCP-to-CoS и т.д.).
    2. Для каждой очереди можно установить отдельный лимит скорости (`<rate>`).
    3. Если скорость трафика в очереди превышает заданный лимит, избыточные пакеты отбрасываются (или могут быть обработаны иначе, в зависимости от реализации).
- **Зачем это нужно:**
    1. **Защита от перегрузки очереди:** Ограничивает максимальную скорость трафика, который может быть передан в определенную очередь, предотвращая заполнение очереди и негативное влияние на другие трафики.
    2. **Дифференцированное ограничение:** Позволяет установить разные лимиты для разных классов трафика. Например, для голосового трафика (очередь 5) можно установить высокий лимит или вообще не ограничивать, а для "best effort" (очередь 0) — более низкий.
- Отличие от `qos policer`**:** `qos policer` ограничивает **весь** входящий трафик на порту, без разделения по очередям. `qos queue-policer`

SEC.RU | Короткий путь к информации Скачано с sec.ru

queue ограничивает трафик **в конкретной очереди** (после классификации).

Удаление конфигурации:

text
(config-if)# no qos queue-policer queue <queue>

Удаляет настройку ограничителя для указанной очереди.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.20 (config-if)# qos queue-shaper queue

Настройка формирователя (шейпера) для исходящей очереди на интерфейсе

Синтаксис:

```
(config-if)# qos queue-shaper queue <queue> <rate> [ excess ]
```

Параметры:

- <queue: 0-7>: Укажите номер очереди (или диапазон) для шейпера.
- <rate: 100-3300000>: Укажите скорость шейпера в килобитах в секунду (kbps).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [excess]: Разрешить использование всей избыточной полосы пропускания (excess bandwidth).

Объяснение: Настройка скорости формирователя (Egress Queue Shaper Rate) для QoS на конкретном интерфейсе.

Рекомендации:

- Команда qos queue-shaper queue настраивает формирователь (шейпер, shaper) для конкретной исходящей очереди (или диапазона очередей) на данном порту. Шейпер ограничивает скорость исходящего трафика, буферизуя (сглаживая) избыточные пакеты, а не отбрасывая их (в отличие от ограничителя policer).
- **В отличие от ограничителя скорости (policer):**
    - ✓ **policer:** ограничивает скорость входящего трафика. Избыточные пакеты отбрасываются (или отправляются pause-кадры). Работает на входе (ingress).
    - ✓ **shaper:** ограничивает скорость исходящего трафика. Избыточные пакеты буферизуются и отправляются позже, сглаживая пики нагрузки. Работает на выходе (egress).
- **Параметр** excess**:**
    - ✓ Без excess**:** Очередь ограничена строго заданной скоростью <rate>. Если трафик превышает эту скорость, пакеты буферизуются (до определенного лимита) или могут отбрасываться при переполнении буфера.
    - ✓ С excess**:** Очередь может использовать всю неиспользуемую полосу пропускания (excess bandwidth)

SEC.RU | Короткий путь к информации Скачано с sec.ru

сверх заданной скорости, если другие очереди не используют свои лимиты. Это позволяет более эффективно использовать доступную пропускную способность, не "простаивая" лимит, если есть свободные ресурсы.

- **Типичные сценарии:**
  - ✓ **Ограничение исходящей скорости для разных классов трафика:** Например, для голоса (очередь 5) установить гарантированную скорость 1 Мбит/с с возможностью использовать избыток (excess), для видео (очередь 4) — 10 Мбит/с, для best effort (очередь 0) — оставшуюся полосу.
  - ✓ **Сглаживание пиков трафика:** Предотвращает "взрывной" характер трафика, делая его более равномерным.

Удаление конфигурации:

```
(config-if)# no qos queue-shaper queue <queue>
```

Удаляет настройку шейпера для указанной очереди.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.21 (config-if)# qos shaper

Настройка формирователя (шейпера) для всего исходящего трафика на интерфейсе

Синтаксис:

```
(config-if)# qos shaper <rate>
```

Параметры:

- <rate: 100-3300000>: Укажите скорость шейпера в килобитах в секунду (kbps).

Объяснение: Настройка скорости формирователя (Egress Queue Policers Rate) для QoS на конкретном интерфейсе.

Рекомендации:

- Команда qos shaper настраивает формирователь (шейпер, shaper) для всего исходящего трафика на данном порту. Шейпер ограничивает общую скорость исходящего трафика, **буферизуя (сглаживая) избыточные пакеты**, а не отбрасывая их.
- **В отличие от** queue-shaper**:** queue-shaper ограничивает скорость **конкретной очереди**. qos shaper ограничивает **суммарную скорость всех очередей** на порту.
- **Как это работает:**
    1. Шейпер "сглаживает" исходящий трафик, ограничивая его скорость до заданного значения <rate>.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Если трафик превышает эту скорость, избыточные пакеты помещаются в буфер и отправляются позже, как только освободится полоса пропускания.
3. Это предотвращает "взрывной" характер трафика и позволяет соблюдать соглашения о пропускной способности (например, с вышестоящим оператором связи).

- **Типичные сценарии:**
    1. **Ограничение исходящей скорости на порту:** Например, на порту, подключенном к интернет-провайдеру, можно установить шейпер, чтобы не превышать купленную полосу пропускания (например, 100 Мбит/с).
    2. **Сглаживание трафика:** Предотвращает потерю пакетов из-за резких скачков трафика.
- **Отличие от ограничивателя скорости (policer):** Ограничиватель работает на входе (ingress) и отбрасывает избыточные пакеты. Шейпер работает на выходе (egress) и буферизует избыточные пакеты, сглаживая трафик.

Удаление конфигурации:

```
(config-if)# no qos shaper
```

Отключает шейпер на интерфейсе.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.35.22 (config-if)# qos tag-remark

Настройка режима маркировки тега (PCP/DEI) на исходящем трафике интерфейса

Синтаксис:

```
(config-if)# qos tag-remark { pcp <pcp> dei <dei> | mapped }
```

Параметры:

- { pcp <pcp> dei <dei> | mapped }: Укажите режим маркировки.
    - ✓ pcp <pcp> dei <dei>: Указать фиксированные значения PCP и DEI для всех кадров.
    - ✓ mapped: Использовать отображение классифицированных значений QoS-класса (CoS) и уровня DP (Drop Precedence) в значения PCP/DEI.

Объяснение: Настройка соответствующего режима маркировки (remarking), используемого этим портом.

Рекомендации:

- Команда qos tag-remark определяет, **как коммутатор маркирует тег VLAN (поля PCP и DEI) для исходящих кадров** на данном порту.
- **Два режима:**
    - ✓ pcp <pcp> dei <dei> **(фиксированная маркировка):** Все исходящие кадры, независимо от их внутренней классификации QoS, получают **одинаковые**, статически заданные значения PCP и DEI. Это полезно, если

SEC.RU | Короткий путь к информации Скачано с sec.ru

требуется переопределить все метки на порту (например, на порту, подключенном к устройству, которое игнорирует PCP/DEI или требует определенных значений).

- ✓ mapped **(динамическое отображение):** Значения PCP и DEI для исходящих кадров определяются на основе **внутренних меток QoS (CoS и DPL)**, используя таблицу отображения, настроенную командой qos map cos-tag. Это стандартный и наиболее гибкий режим, обеспечивающий сквозную маркировку приоритетов на основе классификации трафика.

- **Как это работает:**

  1. Внутри коммутатора каждый пакет имеет внутренние метки: CoS (0-7) и DPL (0-1).
  2. Если выбран режим mapped, при отправке пакета на порт коммутатор использует таблицу cos-tag, чтобы определить, какие PCP и DEI записать в тег VLAN.
  3. Если выбран режим pcp <pcp> dei <dei>, все исходящие пакеты получают указанные фиксированные значения, независимо от их CoS/DPL.

- **Типичные сценарии:**

  1. mapped **(рекомендуется):** Для большинства портов, где требуется сохранить приоритеты, присвоенные в процессе классификации.
  2. **Фиксированная маркировка:** Для портов, подключенных к устаревшему оборудованию, которое не поддерживает динамическую маркировку, или для портов, где необходимо сбросить все метки в известное

SEC.RU | Короткий путь к информации Скачано с sec.ru

состояние (например, при передаче трафика внешнему оператору с жесткими требованиями).

Удаление конфигурации:

```
(config-if)# no qos tag-remark
```

Сбрасывает режим маркировки к значению по умолчанию (обычно mapped*).*

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.23 (config-if)# qos trust dscp

Включение классификации DSCP на интерфейсе

Синтаксис:

```
(config-if)# qos trust dscp
```

Объяснение: Включение классификации DSCP для QoS на конкретном интерфейсе.

Рекомендации:

- Команда qos trust dscp в режиме конфигурации интерфейса **включает режим доверия (trust) к DSCP-**

SEC.RU | Короткий путь к информации Скачано с sec.ru

меткам на входящем трафике порта. Это означает, что коммутатор будет использовать значения DSCP в заголовках IP-пакетов для классификации трафика и определения его приоритета.

- **Как это работает:**
    1. Когда на порту включено `trust dscp`, коммутатор считывает значение DSCP из каждого входящего IP-пакета.
    2. На основе этого значения, используя таблицы отображения `dscp-cos` (или `dscp-classify`), пакету присваиваются внутренние метки QoS (CoS и DPL).
    3. Это позволяет "доверять" DSCP-меткам, выставленным предыдущими устройствами в сети (например, маршрутизаторами на границе сети).
- **В отличие от других методов классификации:**
    1. Без `trust dscp` коммутатор может использовать другие критерии для классификации (например, порт по умолчанию, CoS из тега VLAN, правила QCE).
    2. Приоритет классификации обычно таков: QCE > trust dscp > trust cos (если включено) > настройки порта по умолчанию.
- **Когда использовать:**
    1. На портах, которые подключаются к доверенным устройствам (например, к другому коммутатору или маршрутизатору), которые правильно маркируют трафик DSCP.
    2. На границах сети, где требуется сохранить сквозные приоритеты.
- Включайте `trust dscp` только на портах, подключенных к доверенным устройствам. На портах доступа (к пользователям)

SEC.RU | Короткий путь к информации Скачано с sec.ru

это может позволить злоумышленнику подменить DSCP и получить неоправданно высокий приоритет для своего трафика.

Удаление конфигурации:

```
(config-if)# no qos trust dscp
```

Отключает доверие к DSCP на интерфейсе. Коммутатор не будет использовать DSCP для классификации трафика.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.24 (config-if)# qos trust tag

Включение классификации на основе тега VLAN (PCP/DEI) на интерфейсе

Синтаксис:

```
(config-if)# qos trust tag
```

Объяснение: Включение классификации на основе тега VLAN для QoS на конкретном интерфейсе.

Рекомендации:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Команда `qos trust tag` в режиме конфигурации интерфейса включает режим доверия (trust) к меткам тега VLAN (PCP и DEI) на входящем трафике порта. Это означает, что коммутатор будет использовать значения PCP (Priority Code Point) и DEI (Drop Eligible Indicator) из тега VLAN для классификации трафика и определения его приоритета.
- **Как это работает:**
    1. Когда на порту включено `trust tag`, коммутатор считывает значения PCP и DEI из входящих кадров, имеющих тег VLAN (tagged frames).
    2. На основе этих значений, используя таблицы отображения `tag-cos` (PCP/DEI в CoS/DPL), пакету присваиваются внутренние метки QoS (CoS и DPL).
    3. Это позволяет "доверять" PCP/DEI-меткам, выставленным предыдущими устройствами в сети.
- **В отличие от других методов классификации:**
    1. Без `trust tag` коммутатор может игнорировать PCP/DEI или использовать другие критерии для классификации (например, порт по умолчанию, DSCP, правила QCE).
    2. Приоритет классификации обычно таков: QCE > trust dscp > trust tag > настройки порта по умолчанию.
- **Когда использовать:**
    1. На портах, которые подключаются к доверенным устройствам, правильно маркирующим трафик PCP/DEI (например, к другому управляемому коммутатору, IP-телефону, поддерживающему маркировку).
    2. В сетях, где QoS реализован на уровне 2 (CoS) и не используется DSCP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Включайте trust tag только на портах, подключенных к доверенным устройствам. На портах доступа (к пользователям) это может позволить злоумышленнику подменить PCP и получить неоправданно высокий приоритет для своего трафика.

Удаление конфигурации:

```
(config-if)# no qos trust tag
```

Отключает доверие к PCP/DEI на интерфейсе. Коммутатор не будет использовать тег VLAN для классификации трафика.

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```

2.7.35.25 (config-if)# qos wrr

Настройка весов для метода WRR на интерфейсе

Синтаксис:

```
(config-if)# qos wrr <w0> <w1> <w2> <w3> <w4> <w5>
```

Параметры:

- <w0: 1-100>: Укажите вес для очереди 0.
- <w1: 1-100>: Укажите вес для очереди 1.
- <w2: 1-100>: Укажите вес для очереди 2.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- <w3: 1-100>: Укажите вес для очереди 3.
- <w4: 1-100>: Укажите вес для очереди 4.
- <w5: 1-100>: Укажите вес для очереди 5.

Объяснение (Explanation): Назначение весов для метода обслуживания очередей QoS. WRR (Weighted Round Robin) означает взвешенное круговое обслуживание и использует веса очередей по умолчанию. Количество пакетов, обслуживаемых за каждый проход очереди, зависит от процентов, которые вы настраиваете для очередей.

Рекомендации:

- Команда qos wrr в режиме конфигурации интерфейса настраивает **веса для метода WRR (Weighted Round Robin)**, который определяет, как исходящий трафик распределяется между очередями на порту. WRR — это алгоритм планирования (scheduling), который гарантирует, что каждая очередь получает определенную долю пропускной способности, пропорциональную заданному весу.
- **Как это работает:**
    1. На порту существует несколько очередей (обычно 8, но в данном случае настраиваются очереди 0-5).
    2. WRR циклически обслуживает очереди, но количество пакетов (или байт), взятых из каждой очереди за один цикл, пропорционально весу (w0 - w5).
    3. Например, если веса очередей 0, 1, 2, 3, 4, 5 равны 10, 20, 30, 40, 50, 60, то за один полный цикл из очереди 0 будет взято 10 пакетов (или байт), из очереди 1 — 20, из очереди 5 — 60 и т.д.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Веса позволяют гарантировать минимальную полосу пропускания для каждого класса трафика. Например, голосовому трафику (очередь 5) можно дать высокий вес, а трафику best effort (очередь 0) — низкий.
- Другие методы планирования включают строгий приоритет (Strict Priority, SP), где более высокие очереди обслуживаются полностью до того, как обслуживаются более низкие. Часто используется гибридный подход: несколько высокоприоритетных очередей обслуживаются по SP, а остальные — по WRR.

Удаление конфигурации:

```
(config-if)# no qos wrr
```

Сбрасывает веса WRR к значениям по умолчанию (обычно равномерное распределение или фиксированные значения).

Просмотр:

```
# show qos
# show qos [ { interface [ ( <port_type> [ <port> ] ) ] } | wred | { maps [ dscp-cos ] [ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ] } | storm | { qce [ <qce> ] } ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.36 Настройка RADIUS-сервера (config)# radius-server

2.7.36.1 (config)# radius-server attribute 32

Настройка строки атрибута 32 RADIUS

Синтаксис:

```
(config)# radius-server attribute 32 <id>
```

Объяснение: Настройка строки атрибута 32 RADIUS.

Параметры:

- <id>: Укажите идентификатор RADIUS-сервера. Допустимое количество символов: от 1 до 253.

Рекомендации:

- Команда radius-server attribute 32 настраивает значение **атрибута 32 (NAS-Identifier)** в RADIUS-пакетах, отправляемых коммутатором на RADIUS-сервер. Атрибут 32 идентифицирует сетевое устройство доступа (NAS — Network Access Server), которое отправляет запрос на аутентификацию.
- **NAS-Identifier**–это строка, которая однозначно идентифицирует устройство (коммутатор) среди всех NAS-устройств в сети. RADIUS-сервер может использовать этот атрибут для:
    - ✓ Выбора правильной конфигурации аутентификации (например, какой использовать метод или какие VLAN назначать).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Логирования и аудита — какой коммутатор обработал запрос.
- ✓ Применения различных политик для разных устройств.

- **Зачем это нужно:**
  - ✓ По умолчанию коммутатор может отправлять в этом атрибуте свое имя хоста (hostname) или другой идентификатор.
  - ✓ С помощью этой команды можно переопределить это значение, задав более осмысленный или соответствующий политике идентификатор (например, SW-Floor2-Rack3).
- Настройка атрибута 32 должна соответствовать конфигурации на RADIUS-сервере. Администратор RADIUS-сервера должен знать, какие значения NAS-Identifier используются для каких целей.

Удаление конфигурации:

```
(config)# no radius-server attribute 32
```

Удаляет настройку атрибута 32, возвращаясь к значению по умолчанию (обычно имя хоста).

Просмотр:

```
# show radius-server [statistics]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.36.2 (config)# radius-server attribute 4

Настройка IPv4-адреса NAS (атрибут 4 RADIUS)

Синтаксис:

(config)# radius-server attribute 4 <ipv4>

Объяснение: Настройка IPv4-адреса NAS (Network Access Server).

Параметры:

- <ipv4>: Укажите IPv4-адрес NAS.

Рекомендации:

- Команда radius-server attribute 4 настраивает значение **атрибута 4 (NAS-IP-Address)** в RADIUS-пакетах, отправляемых коммутатором на RADIUS-сервер. Атрибут 4 содержит IP-адрес устройства доступа (NAS), которое отправляет запрос на аутентификацию.
- **NAS-IP-Address** – Это IP-адрес, который RADIUS-сервер использует для идентификации устройства, отправившего запрос. Сервер может использовать этот адрес для:
    - ✓ Аутентификации самого NAS (чтобы убедиться, что запрос пришел от доверенного устройства).
    - ✓ Выбора правильной конфигурации (например, какие VLAN или политики применять).
    - ✓ Логирования и аудита — какой коммутатор обработал запрос.
- **Зачем это нужно:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ По умолчанию коммутатор может отправлять в этом атрибуте IP-адрес интерфейса, через который отправляется RADIUS-пакет (обычно адрес управления).
- ✓ С помощью этой команды можно переопределить это значение, задав конкретный IP-адрес (например, адрес loopback-интерфейса или другой постоянный адрес), чтобы RADIUS-сервер всегда идентифицировал устройство одинаково, независимо от того, через какой интерфейс отправляется пакет.

- Настройка атрибута 4 должна соответствовать конфигурации на RADIUS-сервере. RADIUS-сервер должен быть настроен на прием запросов от указанного IP-адреса (обычно в файле clients.conf или аналогичном).

Удаление конфигурации:

```
(config)# no radius-server attribute 4
```

Удаляет настройку атрибута 4, возвращаясь к использованию IP-адреса исходящего интерфейса по умолчанию.

Просмотр:

```
# show radius-server [statistics]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.36.3 (config)# radius-server attribute 95

Настройка IPv6-адреса NAS (атрибут 95 RADIUS)

Синтаксис:

```
(config)# radius-server attribute 95 <ipv6>
```

Объяснение: Настройка IPv6-адреса NAS (Network Access Server).

Параметры:

- <ipv6>: Укажите IPv6-адрес NAS.

Рекомендации:

- Команда radius-server attribute 95 настраивает значение **атрибута 95 (NAS-IPv6-Address)** в RADIUS-пакетах, отправляемых коммутатором на RADIUS-сервер. Атрибут 95 содержит IPv6-адрес устройства доступа (NAS), которое отправляет запрос на аутентификацию. Этот атрибут является IPv6-аналогом атрибута 4 (NAS-IP-Address).
- **Что такое NAS-IPv6-Address?** Это IPv6-адрес, который RADIUS-сервер использует для идентификации устройства, отправившего запрос, в сетях IPv6. Сервер может использовать этот адрес для:
    - ✓ Аутентификации самого NAS (чтобы убедиться, что запрос пришел от доверенного устройства).
    - ✓ Выбора правильной конфигурации (например, какие VLAN или политики применять).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Логирования и аудита — какой коммутатор обработал запрос.

- **Зачем это нужно:**
  - ✓ По умолчанию коммутатор может отправлять в этом атрибуте IPv6-адрес интерфейса, через который отправляется RADIUS-пакет (обычно адрес управления).
  - ✓ С помощью этой команды можно переопределить это значение, задав конкретный IPv6-адрес (например, адрес loopback-интерфейса или другой постоянный адрес), чтобы RADIUS-сервер всегда идентифицировал устройство одинаково, независимо от того, через какой интерфейс отправляется пакет.
- Настройка атрибута 95 должна соответствовать конфигурации на RADIUS-сервере. RADIUS-сервер должен быть настроен на прием запросов от указанного IPv6-адреса.

Удаление конфигурации:

```
(config)# no radius-server attribute 95
```

Удаляет настройку атрибута 95, возвращаясь к использованию IPv6-адреса исходящего интерфейса по умолчанию.

Просмотр:

```
# show radius-server [statistics]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.36.4 (config)# radius-server deadtime

Настройка времени ожидания перед повторной попыткой соединения с недоступным RADIUS-сервером

Синтаксис:

```
(config)# radius-server deadtime <minutes>
```

Параметры:

- <deadtime>: Укажите значение времени ожидания для RADIUS-сервера. Допустимый диапазон: от 1 до 1440 минут.

Объяснение: Настройка значения времени ожидания (deadtime) для RADIUS-сервера. Deadtime – это период, в течение которого коммутатор не будет отправлять новые запросы на сервер, который не ответил на предыдущий запрос. Это предотвращает постоянные попытки коммутатора связаться с сервером, который уже определен как dead.

Рекомендации:

- Команда radius-server deadtime задает **периода** для RADIUS-сервера. Если RADIUS-сервер не отвечает на запросы (например, из-за сбоя или сетевых проблем), коммутатор помечает его как "dead" и в течение указанного времени (deadtime) не будет отправлять на него новые запросы, переключаясь на другие настроенные RADIUS-серверы.
- **Как это работает:**
    1. Коммутатор отправляет RADIUS-запрос на сервер.
    2. Если ответ не получен в течение тайм-аута (radius-server timeout), коммутатор помечает сервер как (dead).

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. В течение deadtime коммутатор не отправляет новые запросы на этот сервер.
4. По истечении deadtime сервер снова считается потенциально доступным, и коммутатор может отправлять на него запросы.

- **Зачем это нужно:**
    1. **Эффективность:** Предотвращает трату времени на ожидание ответа от заведомо недоступного сервера, ускоряя обработку запросов аутентификации.
    2. **Снижение нагрузки:** Уменьшает количество бесполезных запросов к недоступному серверу.
- **Выбор значения:**
    1. **Короткое значение (например, 5-10 минут):** Быстрое восстановление после временного сбоя сервера, но может привести к частым попыткам соединения, если сервер реально недоступен.
    2. **Длинное значение (например, 30-60 минут и более):** Экономит ресурсы при длительном отказе сервера, но увеличивает время восстановления после того, как сервер снова станет доступен.
- Обычно используется значение от 5 до 30 минут.

Удаление конфигурации:

```
(config)# no radius-server deadtime
```

Сбрасывает значение deadtime к значению по умолчанию (зависит от реализации).

Просмотр:

```
# show radius-server [statistics]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.36.5 (config)# radius-server host

Настройка хоста (сервера) RADIUS

Синтаксис:

```
(config)# radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ] [ timeout <seconds> ] [ retransmit <retries> ] [ key <key> ]
```

Параметры:

- <host_name>: Укажите имя хоста или IP-адрес для RADIUS-сервера. Допустимое количество символов: от 1 до 255.
- [auth-port <auth_port>]: Укажите UDP-порт, используемый на RADIUS-сервере для аутентификации. По умолчанию 1812.
- [acct-port <acct_port>]: Укажите UDP-порт, используемый на RADIUS-сервере для аккаунтинга (учета). По умолчанию 1813.
- [timeout <seconds>]: Укажите значение тайм-аута. Если значение тайм-аута указано здесь, оно заменит глобальное значение тайм-аута. Если вы хотите использовать глобальное значение, оставьте это поле пустым.
- [retransmit <retries>]: Укажите значение количества повторных попыток (retries). Если значение указано здесь, оно заменит глобальное значение. Если вы хотите использовать глобальное значение, оставьте это поле пустым.
- [key <key>]: Укажите секретный ключ. Если секретный ключ указан здесь, он заменит глобальный секретный ключ. Если вы хотите использовать глобальное значение, оставьте это поле пустым.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Эта команда используется для настройки RADIUS-сервера.

Рекомендации:

- Команда `radius-server host` является **основной для добавления RADIUS-сервера** в конфигурацию коммутатора. RADIUS (Remote Authentication Dial-In User Service) используется для централизованной аутентификации, авторизации и учета (AAA) пользователей (например, для административного доступа или 802.1X).
- **Параметры:**
  - ✓ `host_name`: Может быть IPv4-адресом, IPv6-адресом или доменным именем. При использовании доменного имени необходимо настроить DNS (`ip name-server`).
  - ✓ `auth-port`: Порт для аутентификации. Стандартный порт RADIUS — 1812. Более старые реализации могут использовать 1645.
  - ✓ `acct-port`: Порт для аккаунтинга (учета действий). Стандартный порт — 1813. Более старые реализации могут использовать 1646.
  - ✓ `timeout`: Время ожидания ответа от сервера (в секундах). Если сервер не отвечает в течение этого времени, коммутатор либо переходит к следующему серверу, либо повторяет попытку (в зависимости от настроек).
  - ✓ `retransmit`: Количество повторных попыток отправки запроса перед тем, как сервер будет считаться недоступным.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ key: Секретный ключ (shared secret), используемый для шифрования обмена между коммутатором и RADIUS-сервером. Должен совпадать с ключом, настроенным на RADIUS-сервере.

- **Приоритет параметров:** Параметры, указанные для конкретного хоста (timeout, retransmit, key), имеют приоритет над глобальными настройками (radius-server timeout, radius-server retransmit, radius-server key). Это позволяет гибко настраивать разные серверы.
- Для отказоустойчивости обычно настраивают несколько RADIUS-серверов. Коммутатор будет опрашивать их в порядке добавления.

Удаление конфигурации:

```
(config)# no radius-server host <host_name> [ auth-port <auth_port> ] [ acct-port <acct_port> ]
```

Удаляет указанный RADIUS-сервер из конфигурации.

Просмотр:

```
# show radius-server [statistics]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.36.6 (config)# radius-server key

Настройка глобального секретного ключа RADIUS

Синтаксис:

```
(config)# radius-server key <key>
```

Параметры:

- <key>: Укажите значение секретного ключа RADIUS-сервера. Допустимый диапазон: от 1 до 63 символов.

Объяснение: Настройка значения ключа RADIUS-сервера. Этот ключ является общим (shared secret) между RADIUS-сервером и коммутатором.

Рекомендации:

- Команда radius-server key задает **глобальный секретный ключ (shared secret)** для всех RADIUS-серверов, настроенных на коммутаторе. Этот ключ используется для шифрования обмена данными между коммутатором и RADIUS-сервером, включая пароли пользователей.
- Ключ должен **полностью совпадать** на коммутаторе и на RADIUS-сервере. Несовпадение ключа приведет к тому, что RADIUS-сервер не сможет расшифровать и обработать запросы от коммутатора, и аутентификация будет невозможна.
- Если для конкретного RADIUS-сервера (в команде radius-server host) указан свой ключ, он имеет приоритет над глобальным.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Это позволяет использовать разные ключи для разных серверов.

- **Рекомендации по выбору ключа:**
  - ✓ Используйте сложные, трудно подбираемые ключи (не менее 10-15 символов, включая буквы разного регистра, цифры и специальные символы).
  - ✓ Не используйте словарные слова или легко угадываемые комбинации.
  - ✓ Ключ хранится в конфигурации коммутатора. В некоторых реализациях он может отображаться в зашифрованном виде, но все же его компрометация может привести к нарушению безопасности.
- **Взаимодействие с AAA:** Для использования RADIUS-аутентификации необходимо также включить AAA (`aaa new-model` или аналогично) и настроить список аутентификации.

Удаление конфигурации:

```
(config)# no radius-server key
```

Удаляет глобальный секретный ключ RADIUS.

Просмотр:

```
# show radius-server [statistics]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.36.7 (config)# radius-server retransmit

Настройка количества повторных попыток отправки запросов RADIUS

Синтаксис:

```
(config)# radius-server retransmit <retries>
```

Параметры:

- <retries>: Укажите значение количества повторных попыток для RADIUS-сервера. Допустимый диапазон: от 1 до 1000.

Объяснение: Настройка количества повторных попыток отправки запросов на сервер аутентификации, который не отвечает. Если сервер не отвечает после отправки последней повторной попытки, коммутатор считает сервер аутентификации недоступным (dead).

Рекомендации:

- Команда radius-server retransmit задает **глобальное количество повторных попыток (retransmits)** для RADIUS-запросов. Если RADIUS-сервер не отвечает в течение заданного тайм-аута (radius-server timeout), коммутатор повторяет запрос указанное количество раз (retries). Только после исчерпания всех попыток сервер считается недоступным.
- **Как это работает:**
    1. Коммутатор отправляет RADIUS-запрос на сервер.
    2. Если ответ не получен в течение timeout (например, 5 секунд), коммутатор повторяет запрос.
    3. Процесс повторяется retries раз.

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. Если после всех повторных попыток ответа нет, сервер помечается как "мертвый" (dead), и коммутатор переключается на следующий сервер в списке (если он настроен).

- **Влияние на общее время ожидания:** Общее время, которое коммутатор будет ждать ответа от сервера, прежде чем переключиться на другой, можно рассчитать как: `timeout * (retries + 1)` (например, 5 секунд * 6 попыток = 30 секунд).
- **Выбор значения:**

    1. **Меньшее количество (например, 1-3):** Быстрее переключается на резервный сервер, но может ошибочно считать сервер недоступным при временных задержках в сети.
    2. **Большее количество (например, 5-10):** Более устойчив к временным сбоям сети, но увеличивает время реакции при реальной недоступности сервера.
- **Приоритет:** Значение, указанное для конкретного RADIUS-сервера (в команде `radius-server host`), имеет приоритет над глобальным значением.

Удаление конфигурации:

```
(config)# no radius-server retransmit
```

Сбрасывает значение глобального количества повторных попыток к значению по умолчанию (обычно 2-3).

Просмотр:

```
# show radius-server [statistics]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.37 Настройка RMON (Remote Network Monitoring) (config)# rmon

2.7.37.1 (config)# rmon alarm

Настройка оповещений (alarms) RMON

Синтаксис:

```
(config)# rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [ <rising_event_id> ] falling-threshold <falling_threshold> [ <falling_event_id> ] { [ rising | falling | both ] }
text
```

```
(config)# rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [ <rising_event_id> ] falling-threshold <falling_threshold> [ <falling_event_id> ] { [ rising | falling | both ] }
```

Объяснение: Настройка параметров оповещений RMON. Конфигурация оповещений RMON определяет конкретные критерии, которые будут генерировать события-отклики. Может быть настроена для проверки данных за любой указанный интервал времени и может отслеживать абсолютные или изменяющиеся значения. Оповещения также могут быть настроены для реагирования на превышение восходящего или нисходящего порогов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- <id>: Индекс записи. Диапазон от 1 до 65535.
- <oid_str>: Номер объекта MIB-переменной для выборки. Могут быть выбраны только переменные типа ifEntry.n.n. Возможные переменные: ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutDiscards, ifErrors, ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors.
- <interval>: Интервал опроса для выборки и сравнения с восходящим и нисходящим порогами. Диапазон от 1 до 2^31 (2147483647) секунд.
- { absolute | delta }: Проверка абсолютного или относительного изменения указанной переменной.
    - ✓ absolute: Переменная сравнивается с порогами в конце периода выборки.
    - ✓ delta: Из текущего значения вычитается последнее значение выборки, и разница сравнивается с порогами.
- rising-threshold <rising_threshold>: Если текущее значение больше восходящего порога, а значение последней выборки меньше этого порога, то генерируется оповещение. После того как восходящее событие сгенерировано, другое такое событие не будет генерироваться, пока выбранное значение не упадет ниже восходящего порога, не достигнет нисходящего порога и снова не поднимется до восходящего порога. Диапазон порога от -2147483647 до 2147483647.
- [<rising_event_id>]: Указывает индекс восходящего события. Диапазон от 1 до 65535.
- falling-threshold <falling_threshold>: Если текущее значение меньше нисходящего порога, а значение последней выборки

SEC.RU | Короткий путь к информации Скачано с sec.ru

было больше этого порога, то генерируется оповещение. После того как нисходящее событие сгенерировано, другое такое событие не будет генерироваться, пока выбранное значение не поднимется выше нисходящего порога, не достигнет восходящего порога и снова не опустится до нисходящего порога. Диапазон от -2147483647 до 2147483647.

- [<falling_event_id>]: Указывает индекс нисходящего события. Диапазон от 0 до 65535.
- { [rising | falling | both] }: Укажите метод, используемый для выборки выбранной переменной и расчета значения для сравнения с порогами.
    - ✓ rising: Запуск оповещения, когда первое значение больше восходящего порога.
    - ✓ falling: Запуск оповещения, когда первое значение меньше нисходящего порога.
    - ✓ both: Запуск оповещения, когда первое значение больше восходящего порога или меньше нисходящего порога.

Рекомендации:

- Команда rmon alarm является частью стандарта **RMON (Remote Network Monitoring)** и используется для **мониторинга сетевых счетчиков** на коммутаторе. Она позволяет отслеживать значения MIB-переменных (например, количество входящих/исходящих октетов, ошибок, отброшенных пакетов) и генерировать события при превышении заданных порогов.
- **Как это работает:**
    1. Коммутатор периодически (каждые <interval> секунд) считывает значение указанной MIB-переменной (например, ifInErrors для определенного порта).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Вычисляется значение для сравнения: либо абсолютное (absolute), либо изменение с предыдущего измерения (delta).
3. Это значение сравнивается с восходящим (rising-threshold) и нисходящим (falling-threshold) порогами.
4. При пересечении порога генерируется **событие** (event), которое может быть связано с действием (например, отправкой SNMP-ловушки, записью в лог). События настраиваются отдельно (команда rmon event).

- **Зачем это нужно:**
  1. **Проактивный мониторинг:** Позволяет обнаруживать аномалии (например, резкий рост ошибок на порту) без необходимости постоянно опрашивать коммутатор через SNMP.
  2. **Автоматизация:** Оповещения могут запускать внешние системы управления для анализа и реагирования.
- **Пример использования:** Настройка оповещения, если количество ошибок на порту превышает 100 за 60 секунд.

Удаление конфигурации:

```
(config)# no rmon alarm <id>
```

Удаляет оповещение RMON с указанным ID.

Просмотр:

```
# show rmon alarm [ <id_list> ]
# show rmon history [ <id_list> ]
# show rmon statistics [ <id_list> ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.37.2 (config)# rmon event

Настройка событий RMON

Синтаксис:

```
(config)# rmon event <id> [ log ] [ trap <community> ] { [ description <descrip
tion> ] }
```

Объяснение: Настройка параметров событий RMON.

Параметры:

- <id>: Укажите индекс ID. Диапазон: от 1 до 65535.
- [log]: При срабатывании события будет создана запись в журнале RMON (RMON log entry).
- [trap <community>]: Строка community (пароль), отправляемая вместе с SNMP-ловушкой (trap). Хотя строка community может быть задана на этой странице конфигурации, рекомендуется определить её на странице конфигурации SNMP-ловушек перед настройкой здесь. Допустимое количество символов: от 0 до 127.
- { [description <description>] }: Введите описательный комментарий для этой записи.

Рекомендации:

- Команда rmon event настраивает **события (events)** RMON, которые определяют, какое действие должно быть выполнено при срабатывании оповещения (alarm), настроенного командой rmon alarm. Событие связывает срабатывание порога с конкретным действием.
- **Действия при событии:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ log: Создание записи в локальном журнале RMON (который можно просмотреть через SNMP). Это полезно для локального аудита событий.
- ✓ trap <community>: Отправка SNMP-ловушки (trap) на настроенные SNMP-менеджеры.
  Параметр <community> задает строку community для этой ловушки (часто используется та же, что и для SNMP-менеджера). Рекомендуется предварительно настроить SNMP-ловушки глобально.
- ✓ Можно комбинировать log и trap (указав оба параметра).

- **Взаимосвязь alarm и event:**
  1. Alarm определяет *что* и *когда* отслеживать (какую MIB-переменную, с каким интервалом, какие пороги).
  2. Alarm ссылается на event ID (через rising_event_id и falling_event_id).
  3. Event определяет *как* реагировать (логирование, отправка trap).
- **Зачем это нужно:** Позволяет автоматизировать мониторинг сети: при достижении определенных условий (например, рост ошибок на порту) коммутатор сам отправляет уведомление администратору или записывает событие.

Удаление конфигурации:

```
(config)# no rmon event <id>
```

Удаляет указанное событие RMON.

Просмотр:

```
# show rmon alarm [ <id_list> ]
# show rmon history [ <id_list> ]
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.37.3 (config-if)# rmon collection history

Настройка сбора исторических данных RMON на интерфейсе

Синтаксис:

```
(config-if)# rmon collection history <id> [ buckets <buckets> ] [ interval <interval> ]
```

Объяснение: Конфигурация истории RMON используется для сбора статистики на физическом интерфейсе для мониторинга использования сети, типов пакетов и ошибок. Запись исторических данных RMON может использоваться для мониторинга периодических (интермиттирующих) проблем.

Параметры:

- <id>: Укажите индекс ID. Диапазон: от 1 до 65535.
- [buckets <buckets>]: Количество "корзин" (слотов для хранения данных), запрошенных для этой записи. Допустимый диапазон: от 1 до 65535.
- [interval <interval>]: Указывает интервал опроса. По умолчанию указано 1800 секунд. Допустимый диапазон: от 1 до 3600 секунд.

Рекомендации:

- Команда rmon collection history в режиме конфигурации интерфейса **включает сбор исторических данных RMON** на указанном порту. Эта функция периодически собирает статистику о трафике на интерфейсе (количество байт, пакетов,

SEC.RU | Короткий путь к информации Скачано с sec.ru

ошибок, широковещательных пакетов и т.д.) и сохраняет её в виде записей (samples) в буфере.

- **Зачем это нужно:**
  - ✓ **Анализ:** Позволяет отслеживать изменение загрузки порта, количества ошибок и других параметров во времени.
  - ✓ **Поиск периодических проблем:** Помогает выявить проблемы, которые возникают не постоянно, а время от времени (например, кратковременные всплески ошибок).
  - ✓ **Исторические данные:** Данные могут быть получены через SNMP RMON MIB (RFC 2819) для построения графиков и отчетов.
- **Параметры:**
  - ✓ `buckets`: Количество слотов для хранения собранных данных. По мере заполнения буфера новые записи перезаписывают самые старые. Нужно выбирать в зависимости от того, как долго вы хотите хранить историю.
  - ✓ `interval`: Частота опроса (в секундах). Более частый опрос дает более детальную картину, но требует больше ресурсов. Суммарное время хранения данных = `buckets * interval`.
- **Пример использования:** Если настроить `buckets 60` и `interval 60`, буфер будет хранить данные за последний час с опросом каждую минуту.

Удаление конфигурации:

```
(config-if)# no rmon collection history <id>
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Останавливает и удаляет сбор исторических данных RMON для указанной записи.

Просмотр:

```
# show rmon history [ <id_list> ]
```

Отображает собранные исторические данные RMON.

2.7.37.4 (config-if)# rmon collection stats

Настройка сбора статистики RMON на интерфейсе

Синтаксис:

```
(config-if)# rmon collection stats <id>
```

Объяснение: Настройка таблицы статистики RMON с помощью этой команды.

Параметры:

- <id>: Укажите индекс ID. Диапазон: от 1 до 65535.

Рекомендации:

- Команда rmon collection stats в режиме конфигурации интерфейса **включает сбор текущей (моментальной) статистики RMON** на указанном порту. Эта функция отслеживает накопительные счетчики трафика на интерфейсе с момента последнего сброса (или с момента включения

SEC.RU | Короткий путь к информации Скачано с sec.ru

устройства), в отличие от истории, которая сохраняет выборки за определенные интервалы времени.

- **Что такое Statistics Group в RMON?** Это базовая группа RMON (RFC 2819), которая предоставляет текущие значения счетчиков для интерфейса:
    - ✓ etherStatsOctets – количество байт (октетов).
    - ✓ etherStatsPkts – количество пакетов.
    - ✓ etherStatsBroadcastPkts – количество широковещательных пакетов.
    - ✓ etherStatsMulticastPkts – количество многоадресных пакетов.
    - ✓ etherStatsCRCAlignErrors – количество ошибок CRC.
    - ✓ etherStatsUndersizePkts – количество слишком коротких пакетов.
    - ✓ etherStatsOversizePkts – количество слишком длинных пакетов.
    - ✓ etherStatsFragments – количество фрагментов.
    - ✓ etherStatsJabbers – количество "джабберов" (длинные ошибочные пакеты).
    - ✓ etherStatsCollisions – количество коллизий.
    - ✓ И другие.
- **В отличие от** rmon collection history**:** История сохраняет выборки значений за определенные интервалы времени (периодически). Statistics (статистика) предоставляет **текущее накопленное значение** счетчиков с момента последнего сброса. На основе статистики могут создаваться оповещения (alarms) для отслеживания порогов.
- **Зачем это нужно:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Базовый мониторинг:** Позволяет через SNMP получать информацию о состоянии порта и накопленных ошибках.
- ✓ **Источник для оповещений (Alarms):** Без включенной статистики оповещения, отслеживающие счетчики интерфейса (например, ifInErrors), не будут работать.

Удаление конфигурации:

```
(config-if)# no rmon collection stats <id>
```

Отключает сбор статистики RMON на интерфейсе.

Просмотр:

```
# show rmon statistics [ <id_list> ]
```

2.7.38 Настройка Spanning Tree Protocol (STP) (config)# spanning-tree

2.7.38.1 (config)# spanning-tree aggregation

Включение режима агрегации для Spanning Tree

Синтаксис:

```
(config)# spanning-tree aggregation
```

Объяснение: Включение режима агрегации для Spanning Tree.

Рекомендации:

- Команда spanning-tree aggregation **активирует режим агрегации** для протокола Spanning Tree на коммутаторе. Эта

SEC.RU | Короткий путь к информации Скачано с sec.ru

команда, вероятно, переводит коммутатор в режим, где он участвует в работе Spanning Tree на уровне агрегированных каналов (LAG, Port Channels) как единое целое, а не для отдельных физических портов в агрегате.

- **Зачем это нужно:**
    - ✓ Когда несколько физических портов объединены в агрегированный канал (LAG), протокол Spanning Tree должен рассматривать этот логический канал как один порт (а не как несколько отдельных). Это предотвращает неправильную блокировку отдельных линков внутри агрегата и обеспечивает корректную работу защиты от петель.
    - ✓ Режим агрегации гарантирует, что STP обрабатывает агрегированные каналы корректно, отправляя и получая BPDU через любой из физических портов в агрегате, но принимая решения на уровне логического канала.
- **После выполнения команды:**
    - ✓ Приглашение командной строки может измениться на `(config-stp-aggr)#`, указывая на вход в режим конфигурации параметров агрегации STP.
    - ✓ В этом режиме могут быть доступны специфические настройки для работы STP с агрегированными каналами (например, стоимость порта для агрегата, приоритет и т.д.).
- Если агрегированные каналы не используются в сети, включение этой функции не требуется.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
# show spanning-tree
```

Показывает статус и информацию о работе Spanning Tree, включая состояние агрегированных портов (если режим агрегации включен).

2.7.38.2 (config-stp-aggr)# spanning-tree

Включение Spanning Tree в режиме агрегации

Синтаксис:

```
(config-stp-aggr)# spanning-tree
```

Объяснение: Включение Spanning Tree в режиме агрегации.

Рекомендации:

- Команда spanning-tree в режиме конфигурации агрегации (config-stp-aggr)# **активирует протокол Spanning Tree** для агрегированных каналов (LAG, Port Channels). Это дополнение к глобальному включению STP, специфичное для работы с агрегированными портами.
- **Как это работает:**
    - ✓ Когда агрегированный канал (LAG) создан и режим агрегации STP включен (spanning-tree aggregation), эта команда включает обработку STP для этого логического канала.
    - ✓ Коммутатор рассматривает весь LAG как один логический порт для целей Spanning Tree. BPDU могут

SEC.RU | Короткий путь к информации Скачано с sec.ru

отправляться и приниматься через любой из физических портов, входящих в агрегат.

- ✓ Если STP отключен на уровне агрегации (no spanning-tree), то логический канал не участвует в работе протокола, что может привести к образованию петель, если агрегат соединяет два коммутатора.

- Обычно перед выполнением этой команды необходимо:

1. Глобально включить STP на коммутаторе (spanning-tree в глобальном режиме).
2. Включить режим агрегации (spanning-tree aggregation).
3. Создать агрегированный канал и добавить в него физические порты.
4. Затем в режиме (config-stp-aggr)# включить STP для этого агрегированного канала с помощью команды spanning-tree.

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree
```

Отключает Spanning Tree для агрегированных каналов. Агрегированный канал не будет участвовать в работе протокола, что может создать риск петель.

Просмотр:

```
# show spanning-tree
```

Показывает статус STP для всех портов, включая агрегированные каналы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.3 (config-stp-aggr)# spanning-tree auto-edge

Включение функции автоматического определения граничного порта (auto-edge) в режиме агрегации

Синтаксис:

```
(config-stp-aggr)# spanning-tree auto-edge
```

Объяснение: Включение функции автоматического определения граничного порта (auto edge). Когда функция включена, порт автоматически определяется как граничный (edge) порт сети, если он не получает BPDU.

Рекомендации:

- Команда spanning-tree auto-edge в режиме агрегации (config-stp-aggr)# включает функцию **автоматического определения edge портов** для агрегированных каналов. Эта функция аналогична spanning-tree portfast для обычных портов, но применяется к логическим каналам (LAG).
- **Что такое edge порт?** Граничный порт — это порт, который подключен к конечному устройству (например, компьютеру, принтеру, серверу), а не к другому коммутатору. На таких портах нет необходимости проходить через состояния Listening и Learning Spanning Tree (30+ секунд ожидания), что значительно ускоряет подключение устройства.
- **Как работает auto-edge:**
    - ✓ Когда порт поднимается (link up), коммутатор включает режим PortFast (переводит порт сразу в состояние Forwarding).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Если на порт приходит BPDU (что указывает на подключение к другому коммутатору), функция auto-edge автоматически отключается, и порт начинает работать в обычном режиме STP.
- ✓ Это позволяет безопасно использовать преимущества PortFast на портах, подключенных к конечным устройствам, без риска создания петли.

- **Зачем это нужно для агрегированных каналов:** При подключении серверов или других устройств через агрегированный канал, включение auto-edge гарантирует, что логический канал будет быстро переведен в состояние Forwarding, но при этом сохраняется защита от петель в случае, если за агрегатом окажется коммутатор.

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree auto-edge
```

Отключает функцию автоматического определения граничного порта для агрегированных каналов.

Просмотр:

```
# show spanning-tree
```

Показывает статус STP для всех портов, включая агрегированные каналы, и их тип (Edge / Non-Edge).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.4 (config-stp-aggr)# spanning-tree bpdu-guard

Включение защиты BPDU Guard для агрегированных каналов

Синтаксис:

```
(config-stp-aggr)# spanning-tree bpdu-guard
```

Объяснение: Включение функции BPDU Guard. Эта функция защищает порты от получения BPDU. Она может предотвращать петли, отключая порт при получении BPDU, вместо того чтобы переводить его в состояние Discarding. Если функция включена, порт отключает себя при получении валидных BPDU.

Рекомендации:

- Команда spanning-tree bpdu-guard в режиме агрегации (config-stp-aggr)# включает функцию **BPDU Guard** для агрегированных каналов. BPDU Guard — это механизм безопасности, который защищает от случайного или намеренного подключения коммутатора к порту, который должен быть граничным (edge) портом (например, порт, подключенный к серверу или рабочей станции).
- **Как это работает:**
    1. BPDU Guard применяется к портам, которые должны быть граничными (edge) портами (обычно это порты с включенным PortFast или auto-edge).
    2. Если на такой порт приходит BPDU (что означает, что к порту подключен коммутатор, а не конечное устройство), порт немедленно переводится в

SEC.RU | Короткий путь к информации Скачано с sec.ru

состояние **errdisable** (отключается административно) и не участвует в работе сети.

3. Это предотвращает возможные петли (loops), которые могли бы возникнуть, если бы порт с PortFast был случайно подключен к другому коммутатору.

- **Сочетание с auto-edge:** Часто BPDU Guard используется вместе с `auto-edge`. Когда порт автоматически определяется как граничный (auto-edge), BPDU Guard гарантирует, что если все же будет получен BPDU, порт отключится.
- **Восстановление порта после срабатывания BPDU Guard:** Порт, отключенный BPDU Guard, можно восстановить:

  1. Выполнив команду `no spanning-tree bpdu-guard` на порту.
  2. Выполнив команду `errdisable recovery` (глобально или на порту).
  3. Физически переподключив кабель (в некоторых реализациях).
  4. Перезагрузив коммутатор.

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree bpdu-guard
```

Отключает BPDU Guard для агрегированных каналов. Порт не будет отключаться при получении BPDU.

Просмотр:

```
# show spanning-tree
```

Показывает статус STP для всех портов, включая агрегированные каналы, и состояние BPDU Guard.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.5 (config-stp-aggr)# spanning-tree edge

Ручное назначение агрегированного канала как граничного (edge) порта

Синтаксис:

```
(config-stp-aggr)# spanning-tree edge
```

Объяснение: Если интерфейс подключен к конечным узлам (end nodes), вы можете установить его как "Edge" (граничный).

Рекомендации:

- Команда spanning-tree edge в режиме агрегации (config-stp-aggr)# **вручную назначает агрегированный канал (логический порт) как граничный (edge) порт**. Это эквивалент команды spanning-tree portfast для обычных физических портов, но применяемый к LAG.
- **Что такое граничный (edge) порт?** Граничный порт — это порт, который подключен к конечному устройству (компьютеру, серверу, принтеру) и не должен участвовать в топологии Spanning Tree (не должен создавать петель). На таких портах пропускаются состояния Listening и Learning, и порт переходит в режим Forwarding практически мгновенно после поднятия линка.
- **В отличие от** auto-edge**:**
    - ✓ auto-edge автоматически определяет, является ли порт граничным, на основе отсутствия BPDU.
    - ✓ edge (ручное назначение) принудительно указывает, что порт является граничным, независимо от того, приходят BPDU или нет.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Когда использовать ручное назначение:**
    - ✓ Если точно известно, что порт всегда будет подключен к конечному устройству (например, порт доступа для сервера).
    - ✓ Если требуется гарантировать, что порт никогда не будет участвовать в STP (например, для ускорения работы протоколов, чувствительных к задержкам).
- Ручное назначение edge порта **отключает защиту от петель** на этом порту. Если к порту, назначенному как edge, будет подключен коммутатор (или создана петля), это может привести к широковещательному шторму и коллапсу сети. Рекомендуется сочетать ручное назначение edge с `bpdu-guard` для автоматического отключения порта в случае получения BPDU.

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree edge
```

Отменяет ручное назначение граничного порта. Порт возвращается к обычному режиму работы STP.

Просмотр:

```
# show spanning-tree
```

Показывает статус STP для всех портов, включая агрегированные каналы, и их тип (Edge / Non-Edge).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.6 (config-stp-aggr)# spanning-tree link-type

Настройка типа линка, подключенного к интерфейсу (агрегированному каналу)

Синтаксис:

```
(config-stp-aggr)# spanning-tree link-type { point-to-point | shared | auto }
```

Объяснение: Настройка типа линка, подключенного к интерфейсу.

Параметры:

- { point-to-point | shared | auto }: Выберите тип линка, подключенного к интерфейсу.
    - ✓ point-to-point: Точка-точка (например, соединение двух коммутаторов напрямую или через агрегированный канал).
    - ✓ shared: Разделяемая среда (например, старый Ethernet на коаксиальном кабеле или соединение через хаб). В современных сетях практически не встречается.
    - ✓ auto: Коммутатор автоматически определяет, подключен ли интерфейс к линку типа point-to-point или к разделяемой среде (рекомендуется).

Рекомендации:

- Команда spanning-tree link-type в режиме агрегации (config-stp-aggr)# определяет **тип линка для агрегированного канала (логического порта)**, который используется протоколом Rapid

SEC.RU | Короткий путь к информации Скачано с sec.ru

Spanning Tree Protocol (RSTP) и Multiple Spanning Tree Protocol (MSTP) для ускорения сходимости.

- **Зачем это нужно:**
  - ✓ В RSTP и MSTP тип линка влияет на то, как быстро порт может перейти в состояние Forwarding.
  - ✓ **Point-to-point (точка-точка):** Позволяет использовать механизм быстрой сходимости (proposal/agreement). Порт может немедленно перейти в состояние Forwarding после согласования.
  - ✓ **Shared (разделяемая среда):** Требует более медленного перехода через состояния Listening и Learning, как в классическом STP.
- **Когда выбирать:**
  - ✓ auto **(рекомендуется):** Коммутатор автоматически определяет тип линка на основе дуплексного режима (полный дуплекс обычно означает point-to-point, полудуплекс — shared). Это подходит для большинства случаев.
  - ✓ point-to-point **(ручное назначение):** Может потребоваться, если автоматическое определение ошибается (например, при использовании агрегированных каналов). Агрегированный канал (LAG) всегда должен рассматриваться как point-to-point.
  - ✓ shared **(ручное назначение):** Крайне редко, только для устаревших полудуплексных сред.

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree link-type
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Сбрасывает тип линка к значению по умолчанию (auto).

Просмотр:

```
# show spanning-tree
```

Отображает тип линка для каждого порта (включая агрегированные каналы).

2.7.38.7 (config-stp-aggr)# spanning-tree mst <instance> cost

Настройка стоимости пути (path cost) для экземпляра MST

Синтаксис:

```
(config-stp-aggr)# spanning-tree mst <instance> cost { <cost> | auto }
```

Объяснение: Настройка MSTI (MST Instance) и значения стоимости пути (path cost) для него.

Параметры:

- mst <instance: 0-15>: Укажите номер экземпляра MST. Укажите 0 для обозначения CIST (Common and Internal Spanning Tree). Укажите 1-15 для обозначения MSTI 1-15.
- cost { <cost> | auto }: Укажите значение стоимости пути (path cost), которое используется для определения наилучшего пути между устройствами. Допустимые значения: от 1 до 200 000 000. Если указан режим auto, система автоматически определяет скорость и дуплексный режим для расчета стоимости пути. Обратите внимание, что стоимость пути имеет приоритет над приоритетом порта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда spanning-tree mst cost в режиме агрегации (config-stp-aggr)# задает **стоимость пути (path cost) для указанного экземпляра MST** на агрегированном канале (логическом порту). Это ключевой параметр, влияющий на выбор корневого порта (root port) и назначенных портов (designated ports) в топологии MSTP.
- **Как это работает:**
    - ✓ Spanning Tree Protocol (STP, RSTP, MSTP) использует стоимость пути для расчета кратчайшего пути к корневому мосту (root bridge).
    - ✓ Чем ниже стоимость, тем более предпочтительным является путь (или порт).
    - ✓ Разные экземпляры MST (MSTI) могут иметь разные стоимости пути на одном и том же порту, что позволяет балансировать нагрузку, направляя разные VLAN (разные экземпляры) через разные порты.
- **Режимы:**
    - ✓ auto **(по умолчанию):** Стоимость рассчитывается автоматически на основе скорости порта. Стандартные значения: 10 Мбит/с = 2 000 000, 100 Мбит/с = 200 000, 1 Гбит/с = 20 000, 10 Гбит/с = 2 000.
    - ✓ **Ручной (**<cost>**):** Позволяет переопределить автоматическую стоимость. Используется для:
        - **Балансировки нагрузки:** Назначить более низкую стоимость для одного экземпляра MST на одном порту и более высокую для другого экземпляра на том же порту.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Управления маршрутами:** Сделать путь через определенный порт более предпочтительным (меньшая стоимость) или менее предпочтительным (большая стоимость).

- Стоимость пути имеет приоритет над приоритетом порта (spanning-tree priority).

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree mst <instance> cost
```

*Сбрасывает стоимость пути для указанного экземпляра MST к значению по умолчанию (*auto*).*

Просмотр:

```
# show spanning-tree
```

Отображает стоимость пути для каждого порта в каждом экземпляре MST.

2.7.38.8 (config-stp-aggr)# spanning-tree mst <instance> port-priority

Настройка приоритета порта для экземпляра MST

Синтаксис:

```
(config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>
```

Объяснение: Настройка MSTI (MST Instance) и его приоритета порта (port priority).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- mst <instance: 0-15>: Укажите номер экземпляра MST. Укажите 0 для обозначения CIST (Common and Internal Spanning Tree). Укажите 1-15 для обозначения MSTI 1-15.
- port-priority <prio>: Укажите значение приоритета порта.

Рекомендации:

- Команда spanning-tree mst port-priority в режиме агрегации (config-stp-aggr)# задает **приоритет порта для указанного экземпляра MST** на агрегированном канале (логическом порту). Этот параметр используется в алгоритме Spanning Tree для выбора корневого порта (root port) и назначенных портов (designated ports), когда несколько портов имеют одинаковую стоимость пути (path cost).
- **Как это работает:**
  - ✓ Приоритет порта (port priority) — это значение, которое используется как критерий выбора (tie-breaker) после сравнения стоимости пути.
  - ✓ **Меньшее значение приоритета означает более высокий приоритет** (более вероятно, что порт станет корневым или назначенным).
  - ✓ Приоритет порта является локальной настройкой для каждого порта и каждого экземпляра MST.
- **Диапазон значений:** Обычно от 0 до 240 с шагом 16 (0, 16, 32, ..., 240). Меньшие значения имеют более высокий приоритет. Значения, не кратные 16, могут быть округлены вниз до ближайшего кратного 16.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    - ✓ **Тонкая настройка выбора портов:** Позволяет влиять на то, какой порт будет выбран корневым (root port) или назначенным (designated port) в рамках конкретного экземпляра MST.
    - ✓ **Балансировка нагрузки:** Разные экземпляры MST могут иметь разные приоритеты портов, что позволяет направлять трафик разных VLAN через разные агрегированные каналы.
- **Отличие от** cost**:** Стоимость пути (cost) имеет приоритет над приоритетом порта. Приоритет порта используется только тогда, когда стоимости путей совпадают.

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree mst <instance> port-priority
```

Сбрасывает приоритет порта для указанного экземпляра MST к значению по умолчанию (обычно 128).

Просмотр:

```
# show spanning-tree
```

Отображает приоритет порта для каждого порта в каждом экземпляре MST.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.9 (config-stp-aggr)# spanning-tree restricted-role

Включение функции ограничения роли (restricted role) для порта

Синтаксис:

```
(config-stp-aggr)# spanning-tree restricted-role
```

Объяснение: Включение функции ограничения роли (restricted role). Если функция включена, порт не может быть выбран как корневой порт (Root Port) для CIST или любого MSTI, даже если он имеет наилучший приоритет Spanning Tree.

Рекомендации:

- Команда spanning-tree restricted-role в режиме агрегации (config-stp-aggr)# включает функцию **Restricted Role** для агрегированного канала. Эта функция предотвращает назначение порту роли корневого порта (Root Port).
- **Зачем это нужно:**
    - ✓ **Безопасность:** Предотвращает возможность атаки, при которой злоумышленник, подключив свой коммутатор с более низким (лучшим) приоритетом, может стать корневым мостом (root bridge) и перехватить трафик (атака "root bridge takeover").
    - ✓ **Контроль топологии:** Гарантирует, что порт никогда не будет выбран как корневой, независимо от BPDU, полученных от соседних устройств. Это полезно на границах сети, где не должно быть корневых портов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Стабильность:** Предотвращает нежелательные переключения ролей порта при временных изменениях в топологии.

- **Как это работает:**
  - ✓ Обычно порт, который получает лучшие BPDU (с наименьшей стоимостью пути к корню), становится корневым портом.
  - ✓ При включенной restricted-role, порт игнорирует приоритет BPDU и не позволяет себе стать корневым портом. Он может стать назначенным портом (Designated Port) или альтернативным (Alternate Port), но не корневым.
- **Сочетание с** restricted-tcn**:** Часто используется вместе с spanning-tree restricted-tcn (ограничение на отправку TCN — Topology Change Notification).

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree restricted-role
```

Отключает функцию ограничения роли. Порт может быть выбран как корневой порт, если это будет предпочтительно по алгоритму STP.

Просмотр:

```
# show spanning-tree
```

Отображает статус функции Restricted Role для порта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.10 (config-stp-aggr)# spanning-tree restricted-tcn

Включение функции ограничения распространения TCN (Topology Change Notification)

Синтаксис:

(config-stp-aggr)# spanning-tree restricted-tcn

Объяснение: Включение функции ограничения TCN (Restricted TCN). Если функция включена, порт не будет распространять полученные уведомления об изменении топологии (Topology Change Notifications) и изменения топологии на другие порты.

Рекомендации:

- Команда spanning-tree restricted-tcn в режиме агрегации (config-stp-aggr)# включает функцию **Restricted TCN** для агрегированного канала. Эта функция предотвращает распространение уведомлений об изменении топологии (TCN) от соседнего устройства через данный порт на остальную часть сети.
- **Как это работает:**
    - ✓ В стандартном режиме, когда порт получает TCN BPDU (Topology Change Notification), он пересылает его корневому мосту (root bridge), который затем распространяет изменение топологии по всей сети, заставляя коммутаторы сокращать время жизни MAC-записей.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ При включенной restricted-tcn, порт не пересылает полученные TCN дальше. Он также не участвует в генерации собственных TCN при изменениях на порту.

- **Зачем это нужно:**
  - ✓ **Безопасность:** Предотвращает атаки, при которых злоумышленник может постоянно генерировать TCN BPDU, вызывая частые сбросы MAC-таблиц по всей сети (MAC flooding, DoS-атака).
  - ✓ **Изоляция сегментов:** Позволяет изолировать периферийные сегменты сети, где часто происходят изменения топологии (например, подключение/отключение пользователей), от ядра сети, чтобы частые TCN не влияли на производительность ядра.
  - ✓ **Стабильность:** Предотвращает лавинное распространение TCN при нестабильных линках.
- **Сочетание с** restricted-role**:** Часто используется вместе с spanning-tree restricted-role для полной изоляции порта от влияния на топологию STP.

Удаление конфигурации:

```
(config-stp-aggr)# no spanning-tree restricted-tcn
```

Отключает функцию ограничения распространения TCN. Порт может пересылать TCN на другие порты.

Просмотр:

```
# show spanning-tree
```

Отображает статус функции Restricted TCN для порта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.11 (config)# spanning-tree edge bpdu-filter

Глобальное включение фильтрации BPDU на граничных портах

Синтаксис:

```
(config)# spanning-tree edge bpdu-filter
```

Объяснение: Включение функции фильтрации BPDU на граничных (edge) портах. Цель фильтрации BPDU на порту — предотвратить отправку коммутатором BPDU-кадров на порты, которые подключены к конечным устройствам.

Рекомендации:

- Команда spanning-tree edge bpdu-filter **глобально включает функцию фильтрации BPDU** на граничных портах (edge ports), т.е. на портах с включенным PortFast/auto-edge.
- **Что такое BPDU Filter?**
    - ✓ **Отправка:** Предотвращает отправку BPDU из порта. Порт не генерирует и не отправляет BPDU.
    - ✓ **Получение:** Если на порту включен BPDU Filter, он также может игнорировать входящие BPDU (в зависимости от реализации, но обычно фильтр применяется к исходящим BPDU). В некоторых реализациях получение BPDU на порту с фильтром может отключить фильтр.
- **Отличие от** bpdu-guard**:**
    - ✓ bpdu-guard **отключает порт** при получении BPDU (защита от подключения коммутатора к edge порту).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ bpdu-filter **предотвращает отправку BPDU** из порта (порт "молчит" с точки зрения STP).

- **Зачем это нужно:**
  - ✓ **Безопасность:** На портах, подключенных к конечным устройствам, избыточные BPDU не нужны. Фильтрация может предотвратить утечку информации о топологии STP.
  - ✓ **Производительность:** Некоторые конечные устройства могут некорректно реагировать на BPDU.
  - ✓ **Снижение нагрузки:** Уменьшает количество служебных BPDU-кадров в сети.
- Используйте bpdu-filter с осторожностью. Если порт с фильтром BPDU подключить к другому коммутатору, STP не будет работать, что может привести к петлям. Рекомендуется применять только на портах, где вы абсолютно уверены, что устройство не является коммутатором.

Удаление конфигурации:

```
(config)# no spanning-tree edge bpdu-filter
```

Отключает глобальную фильтрацию BPDU на граничных портах.

Просмотр:

```
# show spanning-tree
```

Отображает статус глобальных настроек STP, включая состояние BPDU Filter.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.12 (config)# spanning-tree edge bpdu-guard

Глобальное включение защиты BPDU Guard на граничных портах

Синтаксис:

```
(config)# spanning-tree edge bpdu-guard
```

Объяснение: Включение функции защиты BPDU Guard на граничных (edge) портах. Граничные порты обычно подключаются напрямую к ПК, файловым серверам или принтерам. Поэтому граничные порты настраиваются для быстрого перехода (PortFast). В нормальных условиях граничные порты не должны получать конфигурационные BPDU. Однако, если они их получают, это, вероятно, вызвано злонамеренными атаками или неправильными настройками. Когда граничные порты получают конфигурационные BPDU, они автоматически становятся не-граничными (non-edge) портами и запускают новый процесс расчета Spanning Tree. BPDU Guard поэтому используется для защиты устройства от злонамеренных атак. При включении этой функции, когда граничные порты получают конфигурационные BPDU, STP отключает эти затронутые граничные порты. После периода восстановления эти отключенные порты снова активируются.

Рекомендации:

- Команда spanning-tree edge bpdu-guard **глобально включает функцию BPDU Guard** для всех граничных портов (edge ports) на коммутаторе. BPDU Guard — это механизм безопасности, который защищает сеть от случайного или намеренного подключения коммутатора к порту, который должен оставаться граничным.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Как это работает:**
    1. BPDU Guard применяется к портам, которые настроены как граничные (edge) порты (т.е. с включенным PortFast или auto-edge).
    2. Если на такой порт приходит BPDU (что означает, что к порту подключен коммутатор, а не конечное устройство), порт немедленно переводится в состояние **errdisable** (отключается административно).
    3. Это предотвращает возможные петли (loops), которые могли бы возникнуть при подключении коммутатора к порту с PortFast.
- **Восстановление порта:** После периода восстановления (recovery time) порты, отключенные BPDU Guard, могут быть автоматически реактивированы. Время восстановления настраивается с помощью глобальной команды `errdisable recovery cause bpduguard`.
- **Отличие от** `bpdu-filter`**:**
    1. `bpdu-guard` **отключает порт** при получении BPDU.
    2. `bpdu-filter` **предотвращает отправку BPDU**, но может не отключать порт при получении BPDU.

Удаление конфигурации

```
(config)# no spanning-tree edge bpdu-guard
```

Отключает глобальную защиту BPDU Guard на граничных портах.

Просмотр:

```
# show spanning-tree
```

Отображает статус глобальных настроек STP, включая состояние BPDU Guard.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.13 (config)# spanning-tree mode

Настройка версии протокола Spanning Tree

Синтаксис:

```
(config)# spanning-tree mode { stp | rstp | mstp }
```

Параметры:

- { stp | rstp | mstp }: Укажите одну из версий протокола STP.

Объяснение: Настройка желаемой версии протокола Spanning Tree.

Рекомендации:

- Команда spanning-tree mode выбирает **версию протокола Spanning Tree**, которая будет использоваться на коммутаторе.
- **Варианты:**
  - ✓ stp **(802.1D, Spanning Tree Protocol):** Классический протокол. Обеспечивает защиту от петель, но имеет медленную сходимость (30-50 секунд при изменении топологии). Устаревший, но может использоваться для совместимости со старым оборудованием.
  - ✓ rstp **(802.1w, Rapid Spanning Tree Protocol):** Улучшенная версия с быстрой сходимостью (менее 10 секунд, часто 1-3 секунды). Рекомендуется для большинства сетей, где не требуется поддержка нескольких экземпляров VLAN.
  - ✓ mstp **(802.1s, Multiple Spanning Tree Protocol):** Расширенная версия, которая позволяет

SEC.RU | Короткий путь к информации Скачано с sec.ru

группировать VLAN в несколько экземпляров Spanning Tree. Это обеспечивает балансировку нагрузки (разные VLAN могут использовать разные пути) и более эффективное использование пропускной способности. Рекомендуется для сетей с большим количеством VLAN, где требуется оптимизация трафика.

- **Выбор режима:**
  - ✓ Если в сети есть устаревшее оборудование, поддерживающее только STP (802.1D), необходимо использовать режим `stp` (или RSTP/MSTP в режиме обратной совместимости).
  - ✓ Для большинства современных сетей рекомендуется `rstp`, если не требуется балансировка нагрузки между VLAN.
  - ✓ Если сеть использует множество VLAN и важно оптимально использовать магистральные линки (т.е. разные VLAN должны идти по разным путям), выбирайте `mstp`.

Удаление конфигурации:

```
(config)# no spanning-tree mode
```

Сбрасывает версию протокола к значению по умолчанию (обычно `rstp` *или* `stp`*).*

Просмотр:

```
# show spanning-tree
```

Отображает текущий режим Spanning Tree и информацию о его работе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.14 (config)# spanning-tree mst <instance> priority

Настройка приоритета моста для экземпляра MST

Синтаксис:

```
(config)# spanning-tree mst <instance> priority <prio>
```

Параметры

- <instance: 0-7>: Укажите идентификатор экземпляра. 0 означает CIST (Common and Internal Spanning Tree). 1-7 означает MSTI 1-7.
- <prio: 0-61440>: Укажите значение приоритета.

Объяснение: Укажите соответствующий приоритет для экземпляра MSTI. Приоритет моста используется при выборе корневого устройства (root device), корневого порта (root port) и назначенного порта (designated port). Устройство с наивысшим приоритетом (наименьшим числовым значением) становится корневым устройством. Однако, если все устройства имеют одинаковый приоритет, устройство с наименьшим MAC-адресом станет корневым устройством. Обратите внимание, что меньшие числовые значения указывают на более высокий приоритет. Приоритет моста, объединенный с номером экземпляра MSTI и 6-байтовым MAC-адресом коммутатора, образует идентификатор моста (Bridge Id).

Рекомендации:

- Команда spanning-tree mst priority задает **приоритет моста (bridge priority) для указанного экземпляра MST** (MSTI). Этот

SEC.RU | Короткий путь к информации Скачано с sec.ru

приоритет определяет, какой коммутатор в сети будет выбран корневым мостом (root bridge) для данного экземпляра.

- **Как это работает:**
  - ✓ В MSTP каждый экземпляр (MSTI) может иметь свой собственный корневой мост.
  - ✓ Коммутатор с **наименьшим значением приоритета** (наивысшим приоритетом) становится корневым для этого экземпляра.
  - ✓ Если приоритеты совпадают, выбирается коммутатор с **наименьшим MAC-адресом**.
- **Диапазон значений:** От 0 до 61440 с шагом 4096 (0, 4096, 8192, ..., 61440). Значения, не кратные 4096, обычно округляются до ближайшего кратного. Меньшие значения = более высокий приоритет.
- **CIST (instance 0):** Это общий экземпляр, который охватывает всю сеть MSTP. Его приоритет определяет корневой мост для всей сети MSTP.
- **MSTI (instance 1-7):** Дополнительные экземпляры для группировки VLAN. Каждый может иметь своего корневого моста, что позволяет балансировать нагрузку.
- **Рекомендация:** Назначайте наименьший приоритет (наивысший) коммутатору, который должен быть корневым. Например, для CIST (instance 0) назначьте приоритет 4096 или 8192.

Удаление конфигурации:

```
(config)# no spanning-tree mst <instance> priority
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Сбрасывает приоритет для указанного экземпляра MST к значению по умолчанию (32768).

Просмотр:

```
# show spanning-tree
```

Отображает приоритет моста для каждого экземпляра MST.

2.7.38.15 (config)# spanning-tree mst <instance> vlan

Назначение VLAN экземпляру MST

Синтаксис:

```
(config)# spanning-tree mst <instance> vlan <v_vlan_list>
```

Параметры:

- <instance: 0-7>: Укажите идентификатор экземпляра. 0 означает CIST (Common and Internal Spanning Tree). 1-7 означает MSTI (MST Instance) 1-7.
- <v_vlan_list>: Укажите список VLAN для указанного экземпляра MST. Разделяйте VLAN запятыми и используйте дефис для обозначения диапазона VLAN. (Пример: 2,5,20-40)

Объяснение: Назначение VLAN определенному экземпляру MSTI. Допускается как одна VLAN, так и диапазон VLAN.

Рекомендации:

- Команда spanning-tree mst vlan является **ключевой для конфигурации MSTP (Multiple Spanning Tree Protocol)**.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Она **назначает VLAN (или диапазон VLAN) определенному экземпляру MST (MSTI)**.

- **Как это работает:**
  - ✓ В MSTP VLAN группируются в экземпляры (MSTI). Каждый экземпляр создает независимую топологию Spanning Tree.
  - ✓ Все VLAN, назначенные одному экземпляру, используют одну и ту же топологию (одинаковые блокированные порты).
  - ✓ Разные экземпляры могут иметь разные топологии, что позволяет VLAN, назначенным разным экземплярам, использовать разные пути в сети, обеспечивая **балансировку нагрузки**.
- **CIST (Instance 0):** По умолчанию все VLAN, которые явно не назначены другим экземплярам (1-7), автоматически принадлежат CIST (Instance 0). CIST является "корневым" экземпляром и существует всегда.
- **Пример использования:**
  - ✓ Можно назначить VLAN 10, 20, 30 на MSTI 1, а VLAN 40, 50, 60 на MSTI 2.
  - ✓ Затем настроить разные коммутаторы как корневые для этих разных экземпляров (например, SW1 — корень для MSTI 1, SW2 — корень для MSTI 2).
  - ✓ В результате трафик VLAN 10,20,30 будет следовать к SW1, а трафик VLAN 40,50,60 — к SW2, используя разные магистральные линки и балансируя нагрузку.
- **Внимание:** Перед настройкой MSTP необходимо включить режим MSTP (`spanning-tree mode mstp`).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no spanning-tree mst <instance> vlan
```

Удаляет назначение VLAN для указанного экземпляра. Эти VLAN вернутся в CIST (Instance 0).

Просмотр:

```
# show spanning-tree
```

Отображает текущие назначения VLAN экземплярам MST.

2.7.38.16 (config)# spanning-tree mst forward-time

Настройка времени задержки перехода (Forward Delay) для MSTP

Синтаксис:

```
(config)# spanning-tree mst forward-time <fwdtime>
```

Параметры:

- <fwdtime: 4-30>: Укажите значение задержки перехода (forward delay) от 4 до 30 секунд.

Объяснение: Для мостов STP, задержка перехода (Forward Delay) — это время, проводимое в каждом из состояний Listening и Learning перед переходом в состояние Forwarding. Эта задержка возникает, когда новый мост появляется в сети.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда spanning-tree mst forward-time задает **таймер Forward Delay** для протоколов STP и MSTP. Этот таймер определяет, сколько времени порт будет находиться в состояниях **Listening** и **Learning** перед переходом в состояние **Forwarding**.
- **Состояния порта:**
    - ✓ **Listening** (15 секунд по умолчанию): Порт прослушивает BPDU, чтобы определить активную топологию, но не передает пользовательский трафик.
    - ✓ **Learning** (15 секунд по умолчанию): Порт изучает MAC-адреса из проходящих кадров, но еще не передает их.
    - ✓ **Forwarding:** Порт передает пользовательский трафик.
- **Зачем это нужно:**
    - ✓ Задержка перехода предотвращает временные петли в сети, которые могли бы возникнуть, если бы порт начал пересылать трафик слишком рано, до того, как все коммутаторы в сети согласуют топологию.
- **Взаимосвязь с другими таймерами:**
    - ✓ В STP и MSTP таймеры должны быть согласованы по всей сети. Рекомендуется не менять значения по умолчанию, так как они взаимосвязаны с max-age и hello-time.
    - ✓ Если требуется изменить таймеры, обычно это делается только на корневом мосту (root bridge), который распространяет их через BPDU.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Рекомендуемые значения:** Стандартное значение 15 секунд. При изменении убедитесь, что 2 * (Forward Delay - 1 секунда) >= Max Age, иначе сеть может стать нестабильной.

Удаление конфигурации:

```
(config)# no spanning-tree mst forward-time
```

Сбрасывает таймер Forward Delay к значению по умолчанию (15 секунд).

Просмотр:

```
# show spanning-tree
```

Отображает текущие значения таймеров STP, включая Forward Delay.

2.7.38.17 (config)# spanning-tree mst max-age

Настройка максимального времени жизни (Max Age) для MSTP

Синтаксис

```
(config)# spanning-tree mst max-age <maxage> [ forward-time <fwdtime> ]
```

Параметры:

- <maxage: 6-40>: Укажите значение максимального времени жизни (max age). Допустимый диапазон: от 6 до 40 секунд.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [forward-time <fwdtime>]: Для мостов STP задержка перехода (Forward Delay) — это время, проводимое в каждом из состояний Listening и Learning перед переходом в состояние Forwarding. Эта задержка возникает, когда новый мост появляется в сети. Допустимые значения: 4-30 секунд.

Объяснение: Если другой коммутатор в Spanning Tree не отправляет hello-пакет в течение определенного периода времени, он считается отключенным (disconnected). Допустимые значения: от 6 до 40 секунд, и значения Max Age должны быть меньше или равны (Forward Delay - 1) * 2.

Рекомендации:

- Команда spanning-tree mst max-age задает **таймер Max Age (максимальное время жизни)** для протоколов STP и MSTP. Этот таймер определяет, как долго коммутатор будет хранить хранить полученную информацию о топологии (конфигурацию BPDU), прежде чем отбросить её, если не получит новую BPDU от корневого моста.
- **Как это работает:**
  - ✓ Корневой мост отправляет BPDU каждые hello-time секунд (по умолчанию 2 секунды).
  - ✓ Если коммутатор не получает BPDU в течение max-age (по умолчанию 20 секунд), он считает, что путь к корневому мосту потерян, и инициирует пересчет топологии (изменение состояния портов).
- **Взаимосвязь с другими таймерами:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ max-age должно быть **больше**, чем hello-time, чтобы не происходило ложных срабатываний.
- ✓ Критическое соотношение: max-age **≤ (Forward Delay - 1) * 2**. Это необходимо для корректной работы алгоритма предотвращения петель.
- ✓ Стандартные значения: hello-time = 2 сек, max-age = 20 сек, forward-delay = 15 сек. При этом условие выполняется: 20 ≤ (15-1)*2 = 28.

- **Рекомендации:** Изменять таймеры max-age и forward-delay следует только на корневом мосту (root bridge), который распространяет их через BPDU. В большинстве сетей значения по умолчанию являются оптимальными.

Удаление конфигурации:

```
(config)# no spanning-tree mst max-age
```

Сбрасывает таймер Max Age к значению по умолчанию (20 секунд).

Просмотр:

```
# show spanning-tree
```

Отображает текущие значения таймеров STP, включая Max Age.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.18 (config)# spanning-tree mst max-hops

Настройка максимального количества переходов (Max Hops) для MSTP

Синтаксис:

```
(config)# spanning-tree mst max-hops <maxhops>
```

Параметры:

- <maxhops>: Укажите значение максимального количества переходов (hop count). Допустимый диапазон: от 6 до 40.

Объяснение: Максимальное количество переходов (hops), разрешенное для региона MST, прежде чем BPDU будет отброшен. Каждый коммутатор уменьшает счетчик переходов на единицу перед передачей BPDU дальше. Когда счетчик переходов достигает нуля, BPDU отбрасывается. Значение счетчика переходов по умолчанию: 20. Допустимый диапазон: 6-40.

Рекомендации:

- Команда spanning-tree mst max-hops задает **максимальное количество переходов (hop count)** для BPDU в пределах региона MST (Multiple Spanning Tree). Этот параметр ограничивает "радиус" действия BPDU и предотвращает бесконечное распространение служебных сообщений в больших топологиях.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Как это работает:**
    1. Корневой мост (root bridge) в регионе MST отправляет BPDU со значением `max-hops` (например, 20) в поле hop count.
    2. Каждый следующий коммутатор (сосед) в регионе уменьшает этот счетчик на 1 при пересылке BPDU.
    3. Если счетчик достигает 0, BPDU отбрасывается (т.е. его "жизнь" истекла).
- **Зачем это нужно:**
    1. **Ограничение размера региона MST:** Значение `max-hops` определяет диаметр региона MST (максимальное количество коммутаторов между любыми двумя устройствами).
    2. **Предотвращение бесконечных циклов:** Ограничивает распространение устаревшей информации.
    3. **Управление сходимостью:** Меньшее значение `max-hops` ускоряет обнаружение потери связности с корневым мостом в больших сетях.
- **Выбор значения:**
    1. `max-hops` должно быть достаточно большим, чтобы охватить все коммутаторы в регионе MST.
    2. Слишком большое значение может привести к тому, что устаревшие BPDU будут "бродить" по сети дольше, чем нужно.
    3. Рекомендуемое значение по умолчанию — 20, что подходит для большинства сетей.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Внимание:** Этот параметр применяется **только в пределах одного региона MST**. BPDU, покидающие регион, управляются другими механизмами (CIST).

Удаление конфигурации:

```
(config)# no spanning-tree mst max-hops
```

Сбрасывает максимальное количество переходов к значению по умолчанию (20).

Просмотр:

```
# show spanning-tree
```

Отображает текущее значение максимального количества переходов для MSTP.

2.7.38.19 (config)# spanning-tree mst name

Настройка имени и номера ревизии для региона MST

Синтаксис:

```
(config)# spanning-tree mst name <name> revision <v_0_to_65535>
```

Параметры:

- name <name>: Укажите имя для этого MSTI (MST Instance). По умолчанию используется MAC-адрес коммутатора. Максимальная длина — 32 символа. Для совместного использования деревьев Spanning Tree для MSTI, мосты

SEC.RU | Короткий путь к информации Скачано с sec.ru

должны иметь одинаковое имя конфигурации и значение ревизии.

- revision <v_0_to_65535>: Укажите номер ревизии для этого MSTI. Допустимый диапазон: от 0 до 65535.

Объяснение: Настройка имени и номера ревизии для этого MSTI.

Рекомендации:

- Команда spanning-tree mst name определяет **имя региона MST (MST Region)** и **номер ревизии** (revision number). Эти параметры являются ключевыми для формирования региона MST — группы коммутаторов, которые совместно используют одинаковые настройки MSTP (одинаковые имена, ревизии и отображения VLAN в MSTI).
- **Что такое регион MST?** Регион MST — это логическая группа коммутаторов, которые:
    1. Имеют одинаковое имя конфигурации (MST Configuration Name).
    2. Имеют одинаковый номер ревизии (Revision Number).
    3. Имеют одинаковое отображение VLAN в экземпляры MST (MSTI).
- **Зачем это нужно:**
    1. Коммутаторы внутри одного региона MST взаимодействуют как единое целое, обмениваясь BPDU, которые содержат информацию о всех экземплярах MST (MSTI).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Коммутаторы из разных регионов MST взаимодействуют через CIST (Common and Internal Spanning Tree), который работает как RSTP между регионами.

- **Важное требование:** Все коммутаторы в одном регионе MST должны иметь **строго одинаковые** значения:
    1. Имя конфигурации (`name`).
    2. Номер ревизии (`revision`).
    3. Отображение VLAN в MSTI (`spanning-tree mst <instance> vlan`).
    4. Если хотя бы один из этих параметров отличается, коммутаторы будут считаться находящимися в разных регионах, и между ними будет работать только CIST (без возможности балансировки нагрузки между MSTI).
- Задавайте осмысленное имя региона (например, "Region-1", "DataCenter") и номер ревизии (например, 1). При изменении конфигурации MSTP (например, переназначении VLAN) можно увеличить номер ревизии.

Удаление конфигурации:

```
(config)# no spanning-tree mst name
```

Сбрасывает имя и номер ревизии к значениям по умолчанию (имя = MAC-адрес, ревизия = 0).

Просмотр:

```
# show spanning-tree
```

Отображает имя региона MST и номер ревизии.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.20 (config)# spanning-tree recovery interval

Настройка интервала автоматического восстановления портов, отключенных из-за ошибок STP

Синтаксис:

```
(config)# spanning-tree recovery interval <interval>
```

Параметры:

- <interval>: Время, которое должно пройти, прежде чем порт в состоянии error-disabled может быть включен. Допустимый диапазон: от 30 до 86400 секунд (1 сутки).

Объяснение: При включении, порт, находящийся в состоянии error-disabled, может быть автоматически включен (восстановлен) через определенное время.

Рекомендации:

- Команда spanning-tree recovery interval задает **интервал автоматического восстановления** для портов, которые были переведены в состояние **error-disabled** (ошибка отключения) функциями безопасности STP, такими как **BPDU Guard** или другими механизмами (например, port-security).
- **Как это работает:**
    1. При срабатывании BPDU Guard (получен BPDU на порту с PortFast) порт переводится в состояние error-disabled и блокируется.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Если настройка recovery interval включена, коммутатор запускает таймер на указанное время.
3. По истечении этого времени порт автоматически реактивируется (выполняется no shutdown) и возвращается к нормальной работе.
4. Если проблема (например, BPDU все еще поступают) не устранена, порт может снова быть отключен.

- **Зачем это нужно:**
  1. **Автоматизация восстановления:** Избавляет администратора от необходимости вручную включать порты (команда no shutdown или через веб-интерфейс) после временных проблем.
  2. **Удобство:** Особенно полезно в больших сетях, где порты могут часто отключаться из-за случайных подключений коммутаторов.
- **Выбор значения:**
  1. **Короткое значение (30-120 секунд):** Быстрое восстановление, но если проблема не устранена, порт будет часто переключаться (flapping), что может создавать дополнительный трафик STP.
  2. **Большое значение (600-3600 секунд и более):** Порт остается отключенным дольше, что дает администратору время на диагностику, но замедляет восстановление сервиса.
- **Внимание:** Для работы автоматического восстановления необходимо также включить глобальную функцию errdisable recovery (иногда отдельной командой, например, errdisable recovery cause bpduguard).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no spanning-tree recovery interval
```

Отключает автоматическое восстановление портов из состояния error-disabled.

Просмотр:

```
# show spanning-tree
```

Отображает статус настройки восстановления и текущий интервал (если включен).

2.7.38.21 (config)# spanning-tree transmit hold-count

Настройка максимального количества BPDU, передаваемых портом в секунду

Синтаксис:

```
(config)# spanning-tree transmit hold-count <holdcount>
```

Параметры:

- <holdcount: 1-10>: Укажите значение счетчика удержания передачи (transmit hold-count). Допустимый диапазон: от 1 до 10.

Объяснение: Количество BPDU, отправляемых портом моста в секунду. При превышении этого значения передача следующего BPDU будет задержана. По умолчанию установлено 6. Учтите, что увеличение

SEC.RU | Короткий путь к информации Скачано с sec.ru

этого значения может существенно повлиять на загрузку CPU в коммутаторе, а уменьшение может замедлить сходимость. Рекомендуется оставить параметр Transmit Hold Count равным значению по умолчанию.

Рекомендации:

- Команда `spanning-tree transmit hold-count` задает **максимальное количество BPDU (Bridge Protocol Data Units)**, которое порт может отправить в течение одной секунды. Это механизм ограничения скорости (rate limiting) для BPDU на уровне протокола STP.
- **Как это работает:**
  - ✓ Каждый порт имеет внутренний счетчик отправленных BPDU.
  - ✓ Если порт пытается отправить больше BPDU, чем установлено `hold-count` в секунду, отправка лишних BPDU задерживается (они помещаются в очередь).
- **Зачем это нужно:**
  - ✓ **Защита CPU:** Предотвращает перегрузку процессора (CPU) коммутатора при всплесках BPDU (например, во время массового изменения топологии или при атаке).
  - ✓ **Стабильность:** Ограничивает количество служебного трафика STP в сети.
- **Рекомендации по настройке:**
  - ✓ **Значение по умолчанию (6):** Оптимально для большинства сетей.
  - ✓ **Увеличение (7-10):** Может ускорить сходимость при очень быстрых изменениях топологии, но увеличивает

SEC.RU | Короткий путь к информации Скачано с sec.ru

нагрузку на CPU. Рекомендуется только при наличии веской причины и понимании последствий.

- ✓ **Уменьшение (1-5):** Уменьшает нагрузку на CPU, но может замедлить сходимость STP (порту потребуется больше времени, чтобы отправить необходимое количество BPDU для согласования).

- **Внимание:** Изменять этот параметр следует с осторожностью и, как правило, только в крупных сетях с большим количеством портов на коммутаторе. В большинстве случаев оставляйте значение по умолчанию.

Удаление конфигурации:

```
(config)# no spanning-tree transmit hold-count
```

Сбрасывает параметр transmit hold-count *к значению по умолчанию (6).*

Просмотр:

```
# show spanning-tree
```

Отображает текущее значение transmit hold-count

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.22 (config-if)# spanning-tree

Включение Spanning Tree на интерфейсе

Синтаксис:

(config-if)# spanning-tree

Объяснение: Включение протокола Spanning Tree на данном интерфейсе.

Рекомендации:

- Команда spanning-tree в режиме конфигурации интерфейса **активирует протокол Spanning Tree (STP) на конкретном порту**. По умолчанию STP обычно включен на всех портах коммутатора. Однако эта команда позволяет явно включить его (если ранее был отключен) или восстановить работу STP на порту.
- **Когда может потребоваться отключение STP (**no spanning-tree**):**
    - ✓ На порту, к которому подключено только одно устройство (и отсутствует риск петли), и требуется сэкономить ресурсы CPU (очень редко).
    - ✓ В специальных конфигурациях, где другой протокол (например, ERPS) обеспечивает защиту от петель, или в средах с полным контролем топологии (например, в дата-центрах с определенными требованиями к производительности).
- **Вимание:** Отключение STP на порту **создает риск образования петель** в сети. Если два порта с отключенным

SEC.RU | Короткий путь к информации Скачано с sec.ru

STP будут соединены или если порт будет подключен к сети с возможными петлями, это может вызвать широковещательный шторм и парализовать работу сети.

- Обычно STP должен быть включен на **всех портах** коммутатора. Исключения делаются только при глубоком понимании сетевой топологии и альтернативных механизмах защиты.
- **Проверка состояния:** После включения STP порт будет проходить состояния **Blocking** → **Listening** → **Learning** → **Forwarding** (или быстро переходить в Forwarding, если включен PortFast).

Удаление конфигурации:

```
(config-if)# no spanning-tree
```

Отключает протокол Spanning Tree на данном интерфейсе. Порт не будет участвовать в STP, что может привести к образованию петель.

Просмотр:

```
# show spanning-tree
```

Отображает состояние STP для всех портов, включая статус (включен/отключен), роль и состояние.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.23 (config-if)# spanning-tree auto-edge

Включение функции автоматического определения граничного порта (auto-edge) на интерфейсе

Синтаксис:

```
(config-if)# spanning-tree auto-edge
```

Объяснение: Включение функции автоматического определения граничного порта (auto-edge) на данном интерфейсе. Когда функция включена, порт автоматически определяется как граничный (edge) порт сети, если он не получает BPDU.

Рекомендации:

- Команда `spanning-tree auto-edge` в режиме конфигурации интерфейса включает функцию **автоматического определения граничных портов (auto-edge)** для конкретного порта (или агрегированного канала). Эта функция является аналогом `spanning-tree portfast` (PortFast), но с автоматическим определением.
- **Что делает auto-edge:**
    - ✓ При поднятии линка (link up) порт немедленно переводится в состояние Forwarding (как PortFast).
    - ✓ Если на порт приходит BPDU (что указывает на подключение к другому коммутатору), функция auto-edge автоматически отключается, и порт начинает работать в обычном режиме STP (проходя через состояния Listening, Learning, Forwarding).
    - ✓ Это позволяет безопасно использовать преимущества быстрого перехода на портах, подключенных к конечным

SEC.RU | Короткий путь к информации Скачано с sec.ru

устройствам, но автоматически переходить в обычный режим при подключении коммутатора.

- **Когда использовать:**
  - ✓ На портах доступа (access ports), к которым подключаются конечные устройства (компьютеры, принтеры, серверы).
  - ✓ Это **рекомендуемая альтернатива** ручному включению `spanning-tree edge` (ручному PortFast), так как auto-edge обеспечивает и быстрый переход, и защиту от потенциальных петель.
- **В отличие от** `spanning-tree edge`**:**
  - ✓ `edge` (ручной PortFast) — порт всегда считается граничным, даже если приходят BPDU (что может привести к петле). Требует дополнительной защиты `bpdu-guard`.
  - ✓ `auto-edge` — порт автоматически определяет, является ли он граничным, на основе наличия BPDU. Более безопасный вариант.

Удаление конфигурации:

```
(config-if)# no spanning-tree auto-edge
```

Отключает функцию автоматического определения граничного порта на данном интерфейсе. Порт будет работать в обычном режиме STP.

Просмотр:

```
# show spanning-tree
```

Отображает статус порта (Edge/Non-Edge) и тип определения (auto/manual).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.24 (config-if)# spanning-tree bpdu-guard

Включение защиты BPDU Guard на интерфейсе

Синтаксис:

```
(config-if)# spanning-tree bpdu-guard
```

Объяснение: Включение функции BPDU Guard на данном интерфейсе. Эта функция защищает порты от получения BPDU. Она может предотвращать петли, отключая порт при получении BPDU, вместо того чтобы переводить его в состояние Discarding. Если функция включена, порт отключает себя при получении валидных BPDU.

Рекомендации:

- Команда spanning-tree bpdu-guard в режиме конфигурации интерфейса включает функцию **BPDU Guard** на конкретном порту (или агрегированном канале). BPDU Guard — это механизм безопасности, который защищает сеть от случайного или намеренного подключения коммутатора к порту, который должен оставаться граничным (edge).
- **Как это работает:**
    1. BPDU Guard применяется к портам, которые должны быть граничными (edge) портами (обычно это порты с включенным auto-edge или edge).
    2. Если на такой порт приходит BPDU (что означает, что к порту подключен коммутатор, а не конечное устройство), порт немедленно переводится в состояние **error-disabled** (административно отключается).

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Это предотвращает возможные петли (loops), которые могли бы возникнуть при подключении коммутатора к порту с PortFast.

- **Восстановление порта:** Порт, отключенный BPDU Guard, можно восстановить:
    1. Выполнив команду `no shutdown` в режиме конфигурации интерфейса.
    2. Настроив автоматическое восстановление с помощью `errdisable recovery cause bpduguard` и `spanning-tree recovery interval`.
- **Где включать:** Рекомендуется включать BPDU Guard на **всех портах доступа**, к которым подключаются конечные пользователи (компьютеры, принтеры, телефоны). Это предотвращает случайное или злонамеренное подключение коммутатора к стене.
- **Сочетание с `auto-edge`:** BPDU Guard часто используется вместе с `auto-edge` (PortFast): `auto-edge` ускоряет переход порта в состояние Forwarding, а `bpdu-guard` обеспечивает безопасность, отключая порт при получении BPDU.

Удаление конфигурации:

```
(config-if)# no spanning-tree bpdu-guard
```

Отключает BPDU Guard на данном интерфейсе. Порт не будет отключаться при получении BPDU.

Просмотр:

```
# show spanning-tree
```

Отображает статус BPDU Guard для порта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.25 (config-if)# spanning-tree edge

Ручное назначение интерфейса как граничного (edge) порта

Синтаксис:

```
(config-if)# spanning-tree edge
```

Объяснение: Если интерфейс подключен к конечным узлам (end nodes), вы можете установить его как "Edge" (граничный).

Рекомендации:

- Команда spanning-tree edge в режиме конфигурации интерфейса **вручную назначает порт как граничный (edge) порт**. Это эквивалент классической команды spanning-tree portfast (PortFast) — порт, помеченный как edge, сразу переходит в состояние Forwarding при поднятии линка, пропуская состояния Listening и Learning.
- **Что такое граничный (edge) порт?** Это порт, который подключен к конечному устройству (компьютеру, серверу, принтеру) и не должен участвовать в топологии Spanning Tree (не должен создавать петель).
- **В отличие от** auto-edge**:**
    - ✓ edge (ручное назначение): Порт **всегда** считается граничным, даже если на него приходят BPDU. Без дополнительной защиты (bpdu-guard) это может привести к петле.
    - ✓ auto-edge: Порт автоматически определяет, является ли он граничным, на основе наличия BPDU, и может переключиться в обычный режим при получении BPDU.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Когда использовать ручное назначение:**
    - ✓ Если точно известно, что порт всегда будет подключен к конечному устройству и никогда к коммутатору.
    - ✓ Если требуется гарантировать немедленный переход в Forwarding без автоматического переключения.
- **Внимание:** Ручное назначение edge порта **отключает защиту от петель** на этом порту. Если к порту, назначенному как edge, будет подключен коммутатор (или создана петля), это может привести к широковещательному шторму. **Рекомендуется сочетать ручное назначение edge с** bpdu-guard для автоматического отключения порта в случае получения BPDU.

Удаление конфигурации:

```
(config-if)# no spanning-tree edge
```

Отменяет ручное назначение граничного порта. Порт возвращается к обычному режиму работы STP.

Просмотр:

```
# show spanning-tree
```

Отображает статус порта (Edge/Non-Edge) и тип определения (auto/manual).

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.26 (config-if)# spanning-tree link-type

Настройка типа линка, подключенного к интерфейсу

Синтаксис:

```
(config-if)# spanning-tree link-type { point-to-point | shared | auto }
```

Параметры:

- { point-to-point | shared | auto }: Выберите тип линка, подключенного к интерфейсу.
    - ✓ point-to-point: Соединение точка-точка (например, соединение двух коммутаторов напрямую или через агрегированный канал).
    - ✓ shared: Разделяемая среда (например, старый Ethernet на коаксиальном кабеле или соединение через хаб). В современных сетях практически не встречается.
    - ✓ auto: Коммутатор автоматически определяет, подключен ли интерфейс к линку типа point-to-point или к разделяемой среде (рекомендуется).

Объяснение: Настройка типа линка, подключенного к интерфейсу.

Рекомендации:

- Команда spanning-tree link-type в режиме конфигурации интерфейса определяет **тип линка для порта**, который используется протоколом **Rapid Spanning Tree Protocol (RSTP)** и **Multiple Spanning Tree Protocol (MSTP)** для ускорения сходимости.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    - ✓ В RSTP и MSTP тип линка влияет на то, как быстро порт может перейти в состояние Forwarding.
    - ✓ **Point-to-point (точка-точка):** Позволяет использовать механизм быстрой сходимости (proposal/agreement). Порт может немедленно перейти в состояние Forwarding после согласования.
    - ✓ **Shared (разделяемая среда):** Требует более медленного перехода через состояния Listening и Learning, как в классическом STP.
- **Когда выбирать:**
    - ✓ `auto` **(рекомендуется):** Коммутатор автоматически определяет тип линка на основе дуплексного режима (полный дуплекс обычно означает point-to-point, полудуплекс — shared). Это подходит для большинства случаев.
    - ✓ `point-to-point` **(ручное назначение):** Может потребоваться, если автоматическое определение ошибается (например, при использовании агрегированных каналов, на которых полный дуплекс, но они не являются классическим point-to-point). Агрегированный канал (LAG) всегда должен рассматриваться как point-to-point для оптимальной производительности.
    - ✓ `shared` **(ручное назначение):** Крайне редко, только для устаревших полудуплексных сред (например, соединение через хаб).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no spanning-tree link-type
```

*Сбрасывает тип линка к значению по умолчанию (*auto*).*

Просмотр:

```
# show spanning-tree
```

Отображает тип линка для каждого порта.

2.7.38.27 (config-if)# spanning-tree mst <instance> cost

Настройка стоимости пути (path cost) для экземпляра MST на интерфейсе

Синтаксис:

```
(config-if)# spanning-tree mst <instance> cost { <cost> | auto }
```

Объяснение: Настройка MSTI (MST Instance) и значения стоимости пути (path cost) для него.

Параметры:

- mst <instance: 0-15>: Укажите номер экземпляра MST. Укажите 0 для обозначения CIST (Common and Internal Spanning Tree). Укажите 1-15 для обозначения MSTI 1-15.
- cost { <cost> | auto }: Укажите значение стоимости пути (path cost), которое используется для определения наилучшего пути

SEC.RU | Короткий путь к информации Скачано с sec.ru

между устройствами. Допустимые значения: от 1 до 200 000 000. Если указан режим auto, система автоматически определяет скорость и дуплексный режим для расчета стоимости пути. Обратите внимание, что стоимость пути имеет приоритет над приоритетом порта.

Рекомендации:

- Команда spanning-tree mst cost в режиме конфигурации интерфейса задает **стоимость пути (path cost) для указанного экземпляра MST** на конкретном порту. Это ключевой параметр, влияющий на выбор корневого порта (root port) и назначенных портов (designated ports) в топологии MSTP.
- **Как это работает:**
    - ✓ Spanning Tree Protocol (STP, RSTP, MSTP) использует стоимость пути для расчета кратчайшего пути к корневому мосту (root bridge).
    - ✓ **Чем ниже стоимость, тем более предпочтительным является путь (или порт).**
    - ✓ Разные экземпляры MST (MSTI) могут иметь разные стоимости пути на одном и том же порту, что позволяет балансировать нагрузку, направляя разные VLAN (разные экземпляры) через разные порты.
- **Режимы:**
    - ✓ auto **(по умолчанию):** Стоимость рассчитывается автоматически на основе скорости порта. Стандартные значения (в новой методологии IEEE 802.1t): 10 Мбит/с = 2 000 000, 100 Мбит/с = 200 000, 1 Гбит/с = 20 000, 10 Гбит/с = 2 000, 40 Гбит/с = 1 000, 100 Гбит/с = 500.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Ручной (**<cost>**):** Позволяет переопределить автоматическую стоимость. Используется для:
    - **Балансировки нагрузки:** Назначить более низкую стоимость для одного экземпляра MST на одном порту и более высокую для другого экземпляра на том же порту.
    - **Управления маршрутами:** Сделать путь через определенный порт более предпочтительным (меньшая стоимость) или менее предпочтительным (большая стоимость).
- **Приоритет:** Стоимость пути имеет приоритет над приоритетом порта (spanning-tree port-priority).

Удаление конфигурации:

```
(config-if)# no spanning-tree mst <instance> cost
```

*Сбрасывает стоимость пути для указанного экземпляра MST к значению по умолчанию (*auto*).*

Просмотр:

```
# show spanning-tree
```

Отображает стоимость пути для каждого порта в каждом экземпляре MST.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.29 (config-if)# spanning-tree mst <instance> port-priority

Настройка приоритета порта для экземпляра MST на интерфейсе

Синтаксис:

```
(config-if)# spanning-tree mst <instance> port-priority <prio>
```

Объяснение: Настройка MSTI (MST Instance) и его приоритета порта (port priority).

Параметры:

- mst <instance: 0-15>: Укажите номер экземпляра MST. Укажите 0 для обозначения CIST (Common and Internal Spanning Tree). Укажите 1-15 для обозначения MSTI 1-15.
- port-priority <prio>: Укажите значение приоритета порта.

Рекомендации:

- Команда spanning-tree mst port-priority в режиме конфигурации интерфейса задает **приоритет порта для указанного экземпляра MST** на конкретном порту. Этот параметр используется в алгоритме Spanning Tree для выбора корневого порта (root port) и назначенных портов (designated ports), когда несколько портов имеют одинаковую стоимость пути (path cost).
- **Как это работает:**
    - ✓ Приоритет порта (port priority) — это значение, которое используется как критерий выбора (tie-breaker) после сравнения стоимости пути.
    - ✓ **Меньшее значение приоритета означает более высокий приоритет** (более вероятно, что порт станет корневым или назначенным).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Приоритет порта является локальной настройкой для каждого порта и каждого экземпляра MST.

- **Диапазон значений:** Обычно от 0 до 240 с шагом 16 (0, 16, 32, ..., 240). Меньшие значения имеют более высокий приоритет. Значения, не кратные 16, могут быть округлены вниз до ближайшего кратного 16.
- **Зачем это нужно:**
  - ✓ **Тонкая настройка выбора портов:** Позволяет влиять на то, какой порт будет выбран корневым (root port) или назначенным (designated port) в рамках конкретного экземпляра MST.
  - ✓ **Балансировка нагрузки:** Разные экземпляры MST могут иметь разные приоритеты портов, что позволяет направлять трафик разных VLAN через разные порты (при одинаковых стоимостях путей).
- **Отличие от** cost**:** Стоимость пути (cost) имеет приоритет над приоритетом порта. Приоритет порта используется только тогда, когда стоимости путей совпадают.

Удаление конфигурации:

```
(config-if)# no spanning-tree mst <instance> port-priority
```

Сбрасывает приоритет порта для указанного экземпляра MST к значению по умолчанию (обычно 128).

Просмотр:

```
# show spanning-tree
```

Отображает приоритет порта для каждого порта в каждом экземпляре MST.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.38.29 (config-if)# spanning-tree restricted-role

Включение функции ограничения роли (restricted role) на интерфейсе

Синтаксис:

```
(config-if)# spanning-tree restricted-role
```

Объяснение: Включение функции ограничения роли (restricted role). Если функция включена, порт не может быть выбран как корневой порт (Root Port) для CIST или любого MSTI, даже если он имеет наилучший приоритет Spanning Tree.

Рекомендации:

- Команда `spanning-tree restricted-role` в режиме конфигурации интерфейса включает функцию **Restricted Role** для данного порта. Эта функция предотвращает назначение порту роли корневого порта (Root Port).
- **Зачем это нужно:**
    - ✓ **Безопасность:** Предотвращает возможность атаки, при которой злоумышленник, подключив свой коммутатор с более низким (лучшим) приоритетом, может стать корневым мостом (root bridge) через этот порт (атака "root bridge takeover").
    - ✓ **Контроль топологии:** Гарантирует, что порт никогда не будет выбран как корневой, независимо от BPDU, полученных от соседних устройств. Это полезно на границах сети, где не должно быть корневых портов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Стабильность:** Предотвращает нежелательные переключения ролей порта при временных изменениях в топологии.

- **Как это работает:**
  - ✓ Обычно порт, который получает лучшие BPDU (с наименьшей стоимостью пути к корню), становится корневым портом.
  - ✓ При включенной restricted-role, порт игнорирует приоритет BPDU и не позволяет себе стать корневым портом. Он может стать назначенным портом (Designated Port) или альтернативным (Alternate Port), но не корневым.
- **Где применять:**
  - ✓ На портах, подключенных к недоверенным сетям (например, к сегменту, где могут подключаться пользователи).
  - ✓ На портах, где административно нежелательно, чтобы порт стал корневым.
- **Сочетание с** restricted-tcn**:** Часто используется вместе с spanning-tree restricted-tcn для полной изоляции порта от влияния на топологию STP.

Удаление конфигурации:

```
(config-if)# no spanning-tree restricted-role
```

Отключает функцию ограничения роли. Порт может быть выбран как корневой порт, если это будет предпочтительно по алгоритму STP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
# show spanning-tree
```

Отображает статус функции Restricted Role для порта.

2.7.38.30 (config-if)# spanning-tree restricted-tcn

Включение функции ограничения распространения TCN (Topology Change Notification) на интерфейсе

Синтаксис:

```
(config-if)# spanning-tree restricted-tcn
```

Объяснение: Включение функции ограничения TCN (Restricted TCN). Если функция включена, порт не будет распространять полученные уведомления об изменении топологии (Topology Change Notifications) и изменения топологии на другие порты.

Рекомендации:

- Команда spanning-tree restricted-tcn в режиме конфигурации интерфейса включает функцию **Restricted TCN** для данного порта. Эта функция предотвращает распространение уведомлений об изменении топологии от соседнего устройства через данный порт на остальную часть сети.
- **Как это работает:**
    - ✓ В стандартном режиме, когда порт получает TCN BPDU (Topology Change Notification), он пересылает его корневому мосту (root bridge), который затем

SEC.RU | Короткий путь к информации Скачано с sec.ru

распространяет изменение топологии по всей сети, заставляя коммутаторы сокращать время жизни MAC-записей.

- ✓ При включенной restricted-tcn, порт **не пересылает** полученные TCN дальше. Он также не участвует в генерации собственных TCN при изменениях на порту.

- **Зачем это нужно:**
  - ✓ **Безопасность:** Предотвращает атаки, при которых злоумышленник может постоянно генерировать TCN BPDU, вызывая частые сбросы MAC-таблиц по всей сети (MAC flooding, DoS-атака).
  - ✓ **Изоляция сегментов:** Позволяет изолировать периферийные сегменты сети, где часто происходят изменения топологии (например, подключение/отключение пользователей), от ядра сети, чтобы частые TCN не влияли на производительность ядра.
  - ✓ **Стабильность:** Предотвращает лавинное распространение TCN при нестабильных линках.
- **Где применять:**
  - ✓ **На портах доступа, подключенных к пользовательским сегментам**, где частые включения/выключения устройств могут генерировать много TCN. Это защищает ядро сети от лишних пересчетов MAC-таблиц.
  - ✓ **На портах, подключенных к недоверенным сетям.**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Сочетание с** restricted-role**:** Часто используется вместе с spanning-tree restricted-role для полной изоляции порта от влияния на топологию STP.

Удаление конфигурации:

```
(config-if)# no spanning-tree restricted-tcn
```

Отключает функцию ограничения распространения TCN. Порт может пересылать TCN на другие порты.

Просмотр:

```
# show spanning-tree
```

Отображает статус функции Restricted TCN для порта.

2.7.39 (config-if)# speed

Настройка скорости порта

Синтаксис:

```
(config-if)# speed { 1000 | 100 | 10 | auto { [ 10 ] [ 100 ] [ 1000 ] } }
```

Объяснение: Настройка скорости порта для данного конкретного интерфейса.

Параметры:

- { 1000 | 100 | 10 | auto { [10] [100] [1000] } }: Укажите желаемую скорость порта.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда speed в режиме конфигурации интерфейса задает **скорость работы физического порта** в мегабитах в секунду (Мбит/с). Это один из ключевых параметров, который должен быть согласован с подключенным устройством для обеспечения стабильной связи.
- **Варианты:**
    - ✓ 10: Скорость 10 Мбит/с (обычно для устаревшего оборудования). Выберите это значение, если подключенное устройство не поддерживает более высокие скорости.
    - ✓ 100: Скорость 100 Мбит/с (Fast Ethernet).
    - ✓ 1000: Скорость 1000 Мбит/с (Gigabit Ethernet).
    - ✓ auto: Автоматическое согласование скорости (auto-negotiation). Порт будет пытаться согласовать оптимальную скорость с подключенным устройством. Можно также указать, какие скорости должны предлагаться при автосогласовании, например, auto 10 100 (предлагать только 10 и 100 Мбит/с) или auto 100 1000.
- **Критически важно для стабильности:** Настройки скорости (и дуплекса) должны **полностью совпадать** на обоих концах соединения. Несоответствие приводит к проблемам:
    - ✓ Если один порт настроен на auto, а другой — на фиксированную скорость (1000), автосогласование может не сработать, и порт может работать на неправильной скорости или не работать вообще.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Если оба порта настроены на фиксированные, но разные скорости, связи не будет.

- Для большинства современных устройств рекомендуется использовать auto (автосогласование). В случаях, когда автосогласование не работает (например, соединение с устаревшим или нестандартным оборудованием), можно вручную задать фиксированную скорость и дуплекс.

Удаление конфигурации:

```
(config-if)# no speed
```

Сбрасывает настройку скорости к значению по умолчанию (обычно auto*).*

Просмотр:

```
# show interface ( <port_type> [ <v_port_type_list> ] ) status
```

Отображает текущую скорость порта и другую информацию о состоянии интерфейса.

Примеры настройки:

1. **Настройка порта на автосогласование (рекомендуется):**

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# speed auto
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2. **Принудительная установка скорости 1000 Мбит/с (полный дуплекс также должен быть настроен):**

```
(config)# interface GigabitEthernet 1/24
(config-if)# speed 1000
(config-if)# duplex full
```

3. **Автосогласование с ограничением предлагаемых скоростей (только 100 и 1000 Мбит/с):**

```
(config)# interface GigabitEthernet 1/5
(config-if)# speed auto 100 1000
```

4. **Проверка текущей скорости:**

```
# show interface GigabitEthernet 1/24 status
Port      Name  Status       Vlan  Duplex  Speed  Type
Gi1/24          Connected    1     Full    1000   1000Base-T
```

5. **Сброс настроек скорости к значениям по умолчанию:**

```
(config)# interface GigabitEthernet 1/24
(config-if)# no speed
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.40 (config)# switchport

2.7.41.1 (config)# switchport vlan mapping

Настройка отображения (трансляции) VLAN

Синтаксис :

```
(config)# switchport vlan mapping <group ID> <vlan_list> <translation_vlan>
```

Объяснение: Трансляция VLAN полезна для пользователей, которые хотят преобразовать исходный VLAN ID в новый VLAN ID для обмена данными между разными VLAN и улучшения масштабирования VLAN. Трансляция VLAN заменяет входящий тег C-VLAN на тег S-VLAN вместо добавления дополнительного тега. При настройке трансляции VLAN оба конца соединения обычно должны быть способны соответствующим образом заменять теги. Другими словами, оба конца должны быть настроены на трансляцию тега C-VLAN в тег S-VLAN и тега S-VLAN в тег C-VLAN соответствующим образом в сети. Обратите внимание, что **только порты доступа (access ports)** поддерживают трансляцию VLAN. Не рекомендуется настраивать трансляцию VLAN на транковых портах (trunk ports).

Параметры:

- <group ID: 1-28>: Укажите идентификатор группы, который применяется к данному правилу трансляции.
- <vlan_list>: Укажите идентификатор VLAN, который будет отображен на новый VID.
- <translation_vlan>: Укажите новый VID, на который будет изменен VID входящих кадров.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда switchport vlan mapping настраивает **трансляцию (замену) VLAN ID**. Функция принимает кадр с одним VLAN ID (исходный, C-VLAN) и **заменяет его на другой VLAN ID** (целевой, S-VLAN) при входе (ingress) на порт. Это отличается от тегирования (Q-in-Q), где добавляется дополнительный тег.
- **Когда используется:**
    - ✓ **Совместимость разных сетей:** Когда два разных домена используют одинаковые VLAN ID для разных целей, трансляция позволяет им взаимодействовать, не меняя конфигурацию на обеих сторонах. Например, у одного провайдера VLAN 100 используется для одного клиента, а у другого — для другого. Трансляция позволяет "склеить" их.
    - ✓ **Упрощение управления:** Позволяет использовать локальные VLAN ID внутри организации, которые транслируются в глобальные VLAN ID при передаче провайдеру.
    - ✓ **Миграция:** При переходе с одной схемы нумерации VLAN на другую, трансляция позволяет временно поддерживать обе схемы.
- **Внимание:**
    - ✓ **Только порты доступа (access ports):** Трансляция VLAN работает только на портах, настроенных как switchport mode access. Не используйте на транках.
    - ✓ **Двусторонняя настройка:** Как указано в описании, для корректной работы трансляция должна быть настроена

SEC.RU | Короткий путь к информации Скачано с sec.ru

на **обоих концах соединения** для обеспечения двустороннего преобразования (исходный -> целевой при входе на один конец, и целевой -> исходный при входе на другой).

- **Группы (groups):** Параметр <group ID> позволяет группировать несколько правил трансляции на одном порту.

Удаление конфигурации:

```
(config)# no switchport vlan mapping <group> <v_vlan_id_from>
```

Удаляет указанное правило трансляции VLAN для группы.

Примеры настройки:

1. **Создание правила трансляции: VLAN 100 на порту отображается в VLAN 201:**

```
# configure terminal
(config)# switchport vlan mapping 5 100 201
```

2. **Применение правила к порту доступа (настройка порта):**

```
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 201
(config-if)# switchport vlan mapping enable
(config-if)# switchport vlan mapping 5
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.2 (config-if)# switchport access vlan

Настройка идентификатора VLAN доступа (Access VLAN) для интерфейса

Синтаксис:

```
(config-if)# switchport access vlan <pvid>
```

Объяснение: Настройка идентификатора VLAN доступа (Access VLAN ID, PVID) для данного интерфейса.

Параметры:

- <pvid>: Укажите идентификатор VLAN доступа (PVID) для этого интерфейса.

Рекомендации:

- Команда switchport access vlan в режиме конфигурации интерфейса задает **идентификатор VLAN доступа (Access VLAN, PVID)** для порта, работающего в режиме доступа (access mode). PVID (Port VLAN ID) определяет, к какой VLAN принадлежит порт.
- **Работа в режиме доступа (access mode):**
    - ✓ Порт работает в одном VLAN (нетегированный трафик).
    - ✓ Все нетегированные (untagged) кадры, поступающие на порт, считаются принадлежащими к указанному Access VLAN (PVID).
    - ✓ При отправке кадров из этого VLAN на порт, коммутатор отправляет их без тега VLAN (untagged).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Если на порт приходит тегированный кадр с VLAN ID, отличным от PVID, он обычно отбрасывается (в зависимости от конфигурации).

- **Требуется:**
  1. Предварительно **создать** VLAN с указанным ID (команда `vlan <vlan_id>`).
  2. Убедиться, что порт настроен в режиме доступа: `switchport mode access`.
- **Значение по умолчанию:** Обычно Access VLAN = 1 (VLAN по умолчанию).
- **Смена VLAN:** При изменении Access VLAN на порту, все устройства, подключенные к этому порту, переходят в новую VLAN.

Удаление конфигурации:

```
(config-if)# no switchport access vlan
```

Сбрасывает настройку Access VLAN к значению по умолчанию (обычно VLAN 1).

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Отображает информацию о VLAN на порту, включая режим (access/trunk) и Access VLAN (PVID).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примеры настройки:

1. **Создание VLAN 10 и настройка порта Gi1/1 в режим доступа с VLAN 10:**

```
# configure terminal
(config)# vlan 10
(config-vlan)# name Sales
(config-vlan)# exit
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
```

2. **Настройка нескольких портов в одну VLAN:**

```
(config)# interface GigabitEthernet 1/1-20
(config-if)# switchport mode access
(config-if)# switchport access vlan 100
```

2.7.41.3 (config-if)# switchport forbidden vlan

Добавление или удаление порта из списка запрещенных VLAN

Синтаксис:

```
(config-if)# switchport forbidden vlan { add | remove } <vlan_list>
```

Параметры:

- { add | remove }: Добавить или удалить данный конкретный интерфейс из списка запрещенных VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- <vlan_list>: Укажите идентификатор VLAN (или список VLAN).

Объяснение: Добавление или удаление порта из списка запрещенных VLAN.

Рекомендации:

- Команда switchport forbidden vlan в режиме конфигурации интерфейса управляет **списком запрещенных VLAN** для порта, работающего в режиме транка (trunk). Эта функция предотвращает динамическое изучение и добавление указанных VLAN на порт, даже если протоколы динамического VLAN (например, GVRP или VTP) пытаются это сделать.
- **Как это работает:**
    - ✓ На транковом порту обычно разрешены все VLAN (по умолчанию) или определенные VLAN (через switchport trunk allowed vlan).
    - ✓ Команда forbidden vlan задает **черный список** VLAN, которые **не могут быть добавлены на порт**.
    - ✓ Если протокол динамического VLAN (например, GVRP) пытается добавить VLAN из запрещенного списка на порт, это будет отклонено.
- **Зачем это нужно:**
    - ✓ **Безопасность:** Предотвращает непреднамеренное или злонамеренное добавление критически важных VLAN (например, управляющей VLAN) на порт через динамические протоколы.
    - ✓ **Контроль:** Обеспечивает, что только определенные администратором VLAN могут присутствовать на порту,

SEC.RU | Короткий путь к информации Скачано с sec.ru

даже если в сети используются динамические протоколы.

- **В отличие от** allowed vlan**:**
  - ✓ allowed vlan — это **белый список**. VLAN, не указанные в разрешенных, не пропускаются.
  - ✓ forbidden vlan — это **черный список**. Все VLAN, не входящие в запрещенный список, могут быть пропущены (с учетом других ограничений). Если не указано allowed vlan, разрешены все VLAN, кроме запрещенных.
- **Внимание:** Запрещенные VLAN также не могут быть добавлены статически. Если порт является членом VLAN через статическую конфигурацию (например, switchport access vlan или switchport trunk allowed vlan), команда forbidden vlan не удалит его оттуда автоматически.

Удаление конфигурации:

```
(config-if)# no switchport forbidden vlan
```

Удаляет список запрещенных VLAN с порта (или удаляет отдельную VLAN из списка, если указана).

Просмотр:

```
> show switchport forbidden [ { vlan <vid> } | { name <name> } ]
# show switchport forbidden [ { vlan <vid> } | { name <name> } ]
```

Отображает список VLAN, запрещенных на порту.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Примеры настройки:

1. **Запрет VLAN 1 на транковом порту (для безопасности управления):**

```
# configure terminal
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport forbidden vlan add 1
```

2. **Запрет нескольких VLAN (10, 20, 30):**

```
(config-if)# switchport forbidden vlan add 10,20,30
```

3. **Удаление VLAN 1 из списка запрещенных:**

```
(config-if)# switchport forbidden vlan remove 1
```

2.7.41.4 (config-if)# switchport hybrid acceptable-frame-type

Настройка типов кадров, принимаемых гибридным портом

Синтаксис:

```
(config-if)# switchport hybrid acceptable-frame-type { all | tagged | untagged }
```

Параметры:

- { all | tagged | untagged }: Укажите тип кадра для данного интерфейса. Доступные варианты: all (принимать все кадры), tagged (принимать только тегированные кадры), untagged (принимать только нетегированные кадры).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Настройка типов кадров, принимаемых портом. Доступные варианты включают: all (принимать все кадры), tagged (принимать только тегированные кадры), untagged (принимать только нетегированные кадры). Этот параметр влияет на обработку входящих VLAN. Если порт принимает только тегированные кадры, нетегированные кадры, полученные на порту, отбрасываются. По умолчанию тип кадра установлен в all.

Рекомендации:

- Команда switchport hybrid acceptable-frame-type используется на **гибридных портах (hybrid ports)** для указания, какие типы кадров (тегированные, нетегированные или все) будут приниматься портом.
- **Гибридный порт (hybrid port):** Это порт, который может одновременно обрабатывать как тегированные, так и нетегированные кадры (в отличие от access-порта, который работает только с нетегированными, и trunk-порта, который работает только с тегированными). Гибридные порты используют PVID для нетегированных кадров и принимают/отправляют тегированные кадры для других VLAN.
- **Варианты:**
    - ✓ all **(по умолчанию):** Порт принимает и тегированные, и нетегированные кадры. Нетегированные кадры назначаются в PVID (switchport hybrid pvid). Тегированные — в соответствующие VLAN.
    - ✓ tagged**:** Порт принимает **только тегированные кадры**. Нетегированные кадры отбрасываются.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ untagged**:** Порт принимает **только нетегированные кадры**. Тегированные кадры отбрасываются.

- **Когда использовать:**
  - ✓ tagged**:** Когда подключенное устройство всегда отправляет тегированные кадры (например, другой коммутатор или сервер, настроенный на тегирование). Это может предотвратить случайное подключение нетегированных устройств.
  - ✓ untagged**:** Когда подключенное устройство отправляет только нетегированные кадры (например, конечный пользователь) и нужно гарантировать, что тегированные кадры (возможно, с неправильной конфигурации) не будут приняты.

Удаление конфигурации:

```
(config-if)# no switchport hybrid acceptable-frame-type
```

*Сбрасывает настройку к значению по умолчанию (*all*).*

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Настройка гибридного порта на прием только тегированных кадров:**

```
# configure terminal
(config)# interface GigabitEthernet 1/24
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid acceptable-frame-type tagged
```

2. **Настройка гибридного порта на прием только нетегированных кадров:**

```
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid pvid 10
(config-if)# switchport hybrid acceptable-frame-type untagged
```

2.7.41.5 (config-if)# switchport hybrid allowed vlan

Настройка разрешенных VLAN для гибридного порта

Синтаксис:

```
(config-if)# switchport hybrid allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
```

Параметры:

- { all | none | [add | remove | except] <vlan_list> }: Укажите один из вариантов.
    - ✓ all: Все VLAN.
    - ✓ none: Никакие VLAN.
    - ✓ add: Добавить VLAN к текущему списку.
    - ✓ remove: Удалить VLAN из текущего списка.
    - ✓ except: Все VLAN, кроме указанных в <vlan_list>.
- <vlan_list>: Укажите список VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Настройка разрешенных VLAN, когда данный интерфейс находится в гибридном режиме (hybrid mode).

Рекомендации:

- Команда `switchport hybrid allowed vlan` используется на **гибридных портах (hybrid ports)** для указания, какие тегированные VLAN разрешены для прохождения через порт. Нетегированные кадры обрабатываются отдельно с помощью PVID (команда `switchport hybrid pvid`).
- **Гибридный порт (hybrid mode):** В отличие от trunk-порта (который обычно пропускает все VLAN или явно разрешенные, но только тегированные), гибридный порт может одновременно:
  - ✓ Отправлять и принимать **нетегированные** кадры для PVID.
  - ✓ Отправлять и принимать **тегированные** кадры для VLAN, указанных в `allowed vlan`.
- **Параметры:**
  - ✓ `all`: Разрешить все VLAN (тегированный трафик для любых VLAN). Использование всех VLAN на гибридном порту аналогично trunk.
  - ✓ `none`: Не разрешать ни одной VLAN (только нетегированный трафик PVID).
  - ✓ `add`: Добавить VLAN к текущему списку разрешенных (например, `switchport hybrid allowed vlan add 10,20`).
  - ✓ `remove`: Удалить VLAN из текущего списка.
  - ✓ `except`: Разрешить все VLAN, кроме указанных (например, `switchport hybrid allowed vlan except 1` — запретить VLAN 1).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Типичный сценарий использования гибридного порта:**
    - ✓ Подключение IP-телефона: телефон может использовать тегированную VLAN для голоса (например, VLAN 100) и передавать нетегированный трафик для компьютера (который подключается к телефону) в PVID (например, VLAN 10). Порт коммутатора настроен как гибридный: PVID = 10 (нетегированный), allowed vlan add 100 (тегированный для голоса).

Удаление конфигурации:

```
(config-if)# no switchport hybrid allowed vlan
```

Сбрасывает список разрешенных VLAN к значению по умолчанию (обычно all *или* none*, зависит от реализации).*

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Настройка гибридного порта с PVID 10 и разрешением тегированной VLAN 100 для IP-телефона:**

```
# configure terminal
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid pvid 10
(config-if)# switchport hybrid allowed vlan add 100
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2. **Разрешить все VLAN, кроме VLAN 1 (безопасность):**

```
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid allowed vlan except 1
```

2.7.41.6 (config-if)# switchport hybrid egress-tag

Настройка тегирования исходящих кадров на гибридном порту

Синтаксис:

```
(config-if)# switchport hybrid egress-tag { none | all [ except-native ] }
```

Параметры:

- { none | all [except-native] }: Определяет тегирование исходящих кадров порта.
    - ✓ none: Все VLAN отправляются без тега (нетегированными).
    - ✓ all: Все VLAN отправляются с тегом (тегированными).
    - ✓ all except-native: Все VLAN, кроме настроенной PVID (Native VLAN), отправляются с тегом. PVID отправляется без тега.

Объяснение: Определяет тегирование исходящих кадров порта.

Рекомендации:

- Команда switchport hybrid egress-tag на **гибридном порту (hybrid port)** определяет, какие исходящие кадры будут

SEC.RU | Короткий путь к информации Скачано с sec.ru

отправляться с тегом VLAN (tagged), а какие — без тега (untagged).

- **Гибридный порт** может одновременно отправлять как тегированные, так и нетегированные кадры для разных VLAN, в отличие от access-порта (только нетегированные) и trunk-порта (обычно все тегированные, кроме native VLAN).
- **Варианты:**
  - ✓ `none`: Все исходящие кадры отправляются без тега VLAN (нетегированными). Это поведение, аналогичное access-порту, но с возможностью принимать тегированные кадры на входе (если `acceptable-frame-type` не ограничивает). Используется редко.
  - ✓ `all`: Все исходящие кадры отправляются с тегом VLAN (тегированными). Это поведение, аналогичное trunk-порту. Обычно используется, когда гибридный порт подключен к устройству, которое ожидает тегированные кадры.
  - ✓ `all except-native` **(наиболее распространенный вариант для гибридных портов):** Все VLAN, кроме **PVID (Native VLAN)**, отправляются с тегом. Кадры, принадлежащие PVID, отправляются без тега (как на access-порту). Это стандартный режим для подключения IP-телефонов: телефон получает тегированный трафик голоса (VLAN X), а компьютер, подключенный к телефону, получает нетегированный трафик (PVID).
- **Типичный сценарий (IP-телефон):**
  - ✓ PVID = 10 (нетегированный трафик для компьютера).
  - ✓ `allowed vlan` содержит 100 (тегированный голосовой трафик).
  - ✓ `egress-tag all except-native`: Трафик VLAN 100 отправляется тегированным (телефон его понимает).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Трафик VLAN 10 (PVID) отправляется нетегированным (компьютер его понимает).

Удаление конфигурации:

```
(config-if)# no switchport hybrid egress-tag
```

Сбрасывает настройку тегирования к значению по умолчанию (зависит от реализации).

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Настройка гибридного порта для IP-телефона (PVID=10, тегированная VLAN 100):**

```
# configure terminal
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid pvid 10
(config-if)# switchport hybrid allowed vlan add 100
(config-if)# switchport hybrid egress-tag all except-native
```

2. **Настройка гибридного порта, где все VLAN тегированы (режим trunk):**

```
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid egress-tag all
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.7 (config-if)# switchport hybrid ingress-filtering

Включение фильтрации входящего трафика (ingress filtering) на гибридном порту

Синтаксис:

```
(config-if)# switchport hybrid ingress-filtering
```

Объяснение: Включение функции фильтрации входящего трафика (ingress filtering) на данном конкретном интерфейсе. Если фильтрация входящего трафика включена и входящий порт не является членом VLAN, кадр с входящего порта отбрасывается. По умолчанию фильтрация входящего трафика отключена.

Рекомендации:

- Команда switchport hybrid ingress-filtering в режиме конфигурации интерфейса **включает фильтрацию входящего трафика (ingress filtering)** на гибридном порту. Эта функция является дополнительным механизмом безопасности и управления, который проверяет, принадлежит ли порт к той VLAN, из которой пришел кадр.
- **Как это работает:**
    - ✓ **Включено (**switchport hybrid ingress-filtering**):** Когда порт получает кадр, коммутатор проверяет, является ли этот порт членом VLAN, указанной в кадре (для тегированных кадров) или PVID (для нетегированных). Если порт **не является членом** этой VLAN, кадр **отбрасывается**.
    - ✓ **Отключено (**no switchport hybrid ingress-filtering**, по умолчанию):** Коммутатор не выполняет эту проверку.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Кадры могут быть приняты на порт, даже если порт не является членом VLAN кадра (хотя дальнейшая обработка может зависеть от других настроек).

- **Зачем это нужно:**
  - ✓ **Безопасность:** Предотвращает проникновение трафика из VLAN, в которые порт не должен входить.
  - ✓ **Изоляция:** Гарантирует, что порт будет принимать только трафик из тех VLAN, членами которых он является явно (через PVID или allowed vlan).
  - ✓ **Соответствие стандартам:** Функция ingress filtering определена в стандарте IEEE 802.1Q и рекомендуется к включению для повышения безопасности.
- **Рекомендация:** Включать ingress-filtering на всех портах, где требуется строгая изоляция VLAN. Особенно это важно на транковых и гибридных портах, где порт может быть членом не всех VLAN.

Удаление конфигурации:

```
(config-if)# no switchport hybrid ingress-filtering
```

Отключает фильтрацию входящего трафика на порту (поведение по умолчанию).

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Примеры настройки:

1. **Включение ingress-filtering на гибридном порту для безопасности:**

```
# configure terminal
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid pvid 10
(config-if)# switchport hybrid allowed vlan add 100
(config-if)# switchport hybrid ingress-filtering
```

2.7.41.8 (config-if)# switchport hybrid native vlan

Настройка идентификатора нативной VLAN (PVID) для гибридного порта

Синтаксис:

```
(config-if)# switchport hybrid native vlan <pvid>
```

Параметры:

- <pvid>: Укажите идентификатор VLAN порта (Port VLAN ID, PVID) для данного конкретного интерфейса.

Объяснение: Настраивает идентификатор VLAN в гибридном режиме (Hybrid mode) для порта. Допустимые значения: от 1 до 4095. Значение по умолчанию: 1.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда switchport hybrid native vlan (также известная как switchport hybrid pvid) задает **идентификатор нативной VLAN (Native VLAN, PVID)** для гибридного порта. PVID определяет, к какой VLAN относятся нетегированные (untagged) кадры, принимаемые портом, и как отправляются кадры из этой VLAN (обычно без тега, в зависимости от настройки egress-tag).
- **Нативная VLAN (Native VLAN) в контексте гибридного порта:**
  - ✓ Нетегированные (untagged) кадры, поступающие на порт, автоматически назначаются в нативную VLAN.
  - ✓ Кадры, отправляемые из нативной VLAN на порт, обычно отправляются без тега (если egress-tag не настроен иначе, например, all except-native).
- **В отличие от access-порта:** На access-порту также есть PVID, но порт не принимает тегированные кадры (по умолчанию). На гибридном порту PVID сосуществует с возможностью принимать и отправлять тегированные кадры для других VLAN (указанных в allowed vlan).
- **Типичный сценарий (IP-телефон):**
  - ✓ PVID = 10 (нетегированный трафик для компьютера).
  - ✓ allowed vlan содержит 100 (тегированный голосовой трафик).
  - ✓ egress-tag all except-native: Трафик VLAN 100 отправляется тегированным (телефон его понимает). Трафик VLAN 10 (PVID) отправляется нетегированным (компьютер его понимает).
- **По умолчанию:** PVID = 1 (VLAN по умолчанию).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no switchport hybrid native vlan
```

Сбрасывает PVID к значению по умолчанию (1).

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Настройка гибридного порта для IP-телефона (PVID=10, тегированная VLAN 100):**

```
# configure terminal
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid native vlan 10
(config-if)# switchport hybrid allowed vlan add 100
(config-if)# switchport hybrid egress-tag all except-native
```

2. **Изменение PVID для гибридного порта:**

```
(config)# interface GigabitEthernet 1/5
(config-if)# switchport hybrid native vlan 20
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.9 (config-if)# switchport hybrid port-type

Настройка типа порта в гибридном режиме

Синтаксис:

```
(config-if)# switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
```

Объяснение: Настройка типа порта в гибридном режиме (Hybrid mode) для порта.

Параметры:

- { unaware | c-port | s-port | s-custom-port }: Доступны четыре типа порта. Действия каждого типа порта на входе (ingress) и выходе (egress) описаны в таблице ниже.

Тип порта (Port Type)	Действие на входе (Ingress Action)	Действие на выходе (Egress Action)
Unaware	При получении тегированного кадра: если TPID = 0x8100, кадр становится дважды тегированным (double-tag) и передается. Если TPID не 0x8100 (например, 0x88A8), кадр отбрасывается. При получении нетегированного кадра: добавляется тег (PVID) и кадр передается.	TPID кадра, передаваемого портом Unaware, устанавливается в 0x8100. Конечное состояние кадра после выхода также зависит от правил выхода (egress rules).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Тип порта (Port Type)	Действие на входе (Ingress Action)	Действие на выходе (Egress Action)
C-port	При получении тегированного кадра: если TPID = 0x8100, кадр передается. Если TPID не 0x8100 (например, 0x88A8), кадр отбрасывается. При получении нетегированного кадра: добавляется тег (PVID) и кадр передается.	TPID кадра, передаваемого портом C-port, устанавливается в 0x8100.
S-port	При получении тегированного кадра: если TPID = 0x88A8, кадр передается. Если TPID не 0x88A8 (например, 0x8100), кадр отбрасывается. При получении нетегированного кадра: добавляется тег (PVID) и кадр передается.	TPID кадра, передаваемого портом S-port, устанавливается в 0x88A8.
S-custom-port	При получении тегированного кадра: если TPID = 0x88A8, кадр передается. Если TPID не 0x88A8 (например, 0x8100), кадр отбрасывается. При получении нетегированного кадра: добавляется тег (PVID)	TPID кадра, передаваемого портом S-custom-port, устанавливается в пользовательское значение (self-customized), которое

SEC.RU | Короткий путь к информации Скачано с sec.ru

Тип порта (Port Type)	Действие на входе (Ingress Action)	Действие на выходе (Egress Action)
	и кадр передается.	может быть задано пользователем в поле Ethertype для Custom S-ports.

Рекомендации:

- Команда switchport hybrid port-type определяет **тип порта** в гибридном режиме. Этот параметр влияет на обработку тегов VLAN на уровне физического порта, в частности, на значение **TPID (Tag Protocol Identifier)**.
- **TPID (Tag Protocol Identifier):** Это 16-битное поле в теге VLAN, которое идентифицирует протокол тегирования. Стандартный TPID для 802.1Q (C-VLAN) — **0x8100**. TPID для провайдерского тегирования (S-VLAN, Q-in-Q) — **0x88A8**.
- **Типы портов:**
  - ✓ unaware: У порта нет сведений о VLAN. Обычно используется на портах доступа, но в гибридном режиме позволяет, например, принимать тегированные кадры и преобразовывать их в двойное тегирование.
  - ✓ c-port **(Customer port):** Порт клиента. Ожидает стандартные теги 802.1Q (TPID=0x8100). При получении нетегированных кадров добавляет тег с PVID. Используется в сетях операторов на стороне клиента.
  - ✓ s-port **(Service port):** Порт оператора (провайдера). Ожидает провайдерские теги (TPID=0x88A8).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Используется для Q-in-Q (тегирование трафика клиентов).

- ✓ s-custom-port **(Custom Service port):** Порт оператора с пользовательским TPID. Позволяет задать нестандартное значение TPID для взаимодействия с оборудованием, использующим отличные от стандарта значения.

- **Типичные сценарии:**
  - ✓ В обычной корпоративной сети (без Q-in-Q) используются типы unaware или c-port.
  - ✓ В сети провайдера для разграничения клиентов (Q-in-Q) на стороне клиента используется c-port, а на стороне провайдера — s-port.

Удаление конфигурации:

```
(config-if)# no switchport hybrid port-type
```

Сбрасывает тип порта к значению по умолчанию (зависит от реализации).

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Настройка порта оператора (S-port) для Q-in-Q:**

```
# configure terminal
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid port-type s-port
```

2. **Настройка порта клиента (C-port) для стандартного тегирования:**

```
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid port-type c-port
```

2.7.41.10 (config-if)# switchport mode

Настройка режима VLAN для интерфейса

Синтаксис:

```
(config-if)# switchport mode { access | trunk | hybrid }
```

Параметры:

- { access | trunk | hybrid }: Укажите режим VLAN.

Объяснение: Настройка режима VLAN для данного конкретного интерфейса.

Рекомендации:

- Команда switchport mode является **основной для определения роли порта** в контексте VLAN. Она задает, как порт обрабатывает тегированные и нетегированные кадры.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Режимы:**
  - ✓ `access` **(порт доступа):**
    - Порт принадлежит **одной** VLAN (настраивается командой `switchport access vlan`).
    - Обычно используется для подключения конечных устройств (компьютеров, принтеров, IP-телефонов в конфигурации без голосовой VLAN).
    - Все исходящие кадры отправляются **без тега** (untagged).
    - Входящие нетегированные кадры назначаются в Access VLAN.
    - Входящие тегированные кадры обычно отбрасываются (если только порт не настроен на прием тегированных, например, для голосовой VLAN).
  - ✓ `trunk` **(транковый порт):**
    - Порт может передавать трафик для **нескольких VLAN** (настраивается командой `switchport trunk allowed vlan`).
    - Обычно используется для соединения между коммутаторами, а также для подключения серверов и другого оборудования, поддерживающего тегирование.
    - Все исходящие кадры (кроме Native VLAN) отправляются **с тегом** (tagged).
    - Native VLAN (по умолчанию VLAN 1) отправляется без тега (если не настроено иное).

SEC.RU | Короткий путь к информации Скачано с sec.ru

        - Входящие тегированные кадры принимаются, если VLAN разрешена. Входящие нетегированные кадры назначаются в Native VLAN.
    - ✓ hybrid **(гибридный порт):**
        - Порт может одновременно работать как access и trunk.
        - Поддерживает **одну нетегированную VLAN (Native/PVID)** и произвольное количество **тегированных VLAN**.
        - Наиболее гибкий режим. Используется, например, для подключения IP-телефонов, когда телефон использует тегированную VLAN для голоса, а компьютер, подключенный к телефону, — нетегированную (PVID).
- **Выбор режима:**
    - ✓ access: Подключение конечных устройств (компьютеры, принтеры).
    - ✓ trunk: Соединение коммутаторов, подключение серверов с тегированием VLAN.
    - ✓ hybrid: Подключение IP-телефонов или устройств, которым нужна одна нетегированная и несколько тегированных VLAN.

Удаление конфигурации:

```
(config-if)# no switchport mode
```

Сбрасывает режим к значению по умолчанию (обычно access*).*

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Настройка порта доступа (Access) для VLAN 10:**

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
```

2. **Настройка транкового порта (Trunk):**

```
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20,30
(config-if)# switchport trunk native vlan 1
```

3. **Настройка гибридного порта (Hybrid) для IP-телефона:**

```
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid native vlan 10
(config-if)# switchport hybrid allowed vlan add 100
(config-if)# switchport hybrid egress-tag all except-native
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.11 (config-if)# switchport trunk allowed vlan

Настройка разрешенных VLAN для транкового порта

Синтаксис:

```
(config-if)# switchport trunk allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
```

Параметры:

- { all | none | [add | remove | except] <vlan_list> }: Укажите один из вариантов.
    - ✓ all: Все VLAN.
    - ✓ none: Никакие VLAN.
    - ✓ add: Добавить VLAN к текущему списку.
    - ✓ remove: Удалить VLAN из текущего списка.
    - ✓ except: Все VLAN, кроме указанных в <vlan_list>.
- <vlan_list>: Укажите список VLAN.

Объяснение: Настройка разрешенных VLAN, когда данный интерфейс находится в транковом режиме (trunk mode).

Рекомендации:

- Команда switchport trunk allowed vlan используется на **транковых портах (trunk mode)** для указания, какие VLAN могут проходить через порт. По умолчанию транковый порт разрешает все VLAN (1-4094).
- **Зачем это нужно:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Безопасность:** Ограничение VLAN, которые могут проходить через транк, предотвращает несанкционированный доступ к VLAN из других сегментов сети. Особенно важно ограничивать VLAN управления (обычно VLAN 1).
- ✓ **Эффективность:** Уменьшает количество служебного трафика (BPDU для каждого VLAN в случае MSTP) и широковещательного трафика, который должен обрабатывать порт.
- ✓ **Контроль:** Позволяет администратору явно указать, какие VLAN должны быть доступны на данном транке.

- **Параметры:**
  - ✓ `all`: Разрешить все VLAN. Это настройка по умолчанию.
  - ✓ `none`: Запретить все VLAN (порт не будет передавать трафик ни одной VLAN). Используется редко.
  - ✓ `add`: Добавить VLAN к текущему списку разрешенных (например, `switchport trunk allowed vlan add 10,20`).
  - ✓ `remove`: Удалить VLAN из текущего списка.
  - ✓ `except`: Разрешить все VLAN, кроме указанных (например, `switchport trunk allowed vlan except 1` — запретить VLAN 1).
- **Рекомендация:** Всегда ограничивайте транковые порты. Минимально — удаляйте VLAN 1 (native VLAN) из разрешенного списка, если он не используется.
- **Внимание:** Native VLAN (настраивается командой `switchport trunk native vlan`) не обязательно должна быть в списке разрешенных? Обычно native VLAN всегда считается разрешенной (так как ее кадры идут без тега), но лучшая

SEC.RU | Короткий путь к информации Скачано с sec.ru

практика — включать native VLAN в список разрешенных для ясности.

Удаление конфигурации:

```
(config-if)# no switchport trunk allowed vlan
```

*Сбрасывает список разрешенных VLAN к значению по умолчанию (*all*).*

Просмотр:

```
# show vlan status
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Ограничение транка только VLAN 10,20,30:**

```
# configure terminal
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 10,20,30
```

2. **Добавление VLAN 40 к существующему списку:**

```
(config-if)# switchport trunk allowed vlan add 40
```

3. **Удаление VLAN 20 из списка:**

```
(config-if)# switchport trunk allowed vlan remove 20
```

4. **Разрешить все VLAN, кроме VLAN 1 (безопасность):**

```
(config-if)# switchport trunk allowed vlan except 1
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.12 (config-if)# switchport trunk native vlan

Настройка нативной VLAN (Native VLAN) для транкового порта

Синтаксис:

```
(config-if)# switchport trunk native vlan <pvid>
```

Параметры:

- <pvid>: Укажите идентификатор VLAN порта (Port VLAN ID, PVID) для данного конкретного интерфейса.

Объяснение: Настройка идентификатора нативной VLAN в транковом режиме (trunk mode) для данного конкретного интерфейса.

Рекомендации:

- Команда switchport trunk native vlan задает **нативную VLAN (Native VLAN)** для транкового порта. Native VLAN — это VLAN, чей трафик **не тегируется** (отправляется без тега) на транковом порту.
- **Как это работает:**
  - ✓ **Входящие (ingress) нетегированные кадры:** Полученные на транковом порту нетегированные кадры автоматически назначаются в нативную VLAN.
  - ✓ **Исходящие (egress) кадры:** Кадры, принадлежащие нативной VLAN, отправляются **без тега (untagged)**. Все остальные VLAN, разрешенные на транке, отправляются с тегом (tagged).
- **Значение по умолчанию:** Native VLAN по умолчанию – VLAN 1.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**
    - ✓ **Совместимость:** Некоторые устаревшие устройства или приложения могут не поддерживать тегированные кадры. Использование native VLAN позволяет им взаимодействовать через транк.
    - ✓ **Управление:** Native VLAN (обычно VLAN 1) часто используется для трафика управления (CDP, VTP, PAgP, DTP). Если native VLAN не совпадает на двух концах транка, это может вызвать проблемы.
- **Внимание:** Нативная VLAN **должна быть одинаковой** на обоих концах транкового соединения (на обоих коммутаторах). Несовпадение native VLAN может привести к уязвимостям безопасности (VLAN hopping) из-за неправильной интерпретации нетегированных кадров.
- **Рекомендация по безопасности:** Измените native VLAN с VLAN 1 на другой неиспользуемый VLAN (например, VLAN 999) и явно запретите VLAN 1 на транке (`switchport trunk allowed vlan except 1`).

Удаление конфигурации:

```
(config-if)# no switchport trunk native vlan
```

Сбрасывает нативную VLAN к значению по умолчанию (VLAN 1).

Просмотр:

```
# show running-config
# show interfaces GigabitEthernet 1/1 switchport
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Команда show interfaces switchport *отображает нативную VLAN для транкового порта.*

Примеры настройки:

1. **Изменение native VLAN с 1 на 999 (рекомендуется для безопасности):**

```
# configure terminal
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport trunk native vlan 999
(config-if)# switchport trunk allowed vlan except 1
```

2. **Настройка native VLAN для транка между двумя коммутаторами:**

```
# configure terminal
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport trunk native vlan 100
```

2.7.41.13 (config-if)# switchport trunk vlan tag native

Настройка тегирования трафика нативной VLAN на транковом порту

Синтаксис:

```
(config-if)# switchport trunk vlan tag native
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Настройка данного конкретного интерфейса на тегирование трафика нативной VLAN (Native VLAN).

Рекомендации:

- Команда switchport trunk vlan tag native включает **тегирование (tagging) для нативной VLAN** на транковом порту. По умолчанию трафик нативной VLAN отправляется **без тега** (untagged). Эта команда изменяет это поведение, заставляя порт отправлять кадры нативной VLAN с тегом (tagged).
- **Как это работает:**
    - ✓ **По умолчанию (**no switchport trunk vlan tag native**):** Кадры, принадлежащие нативной VLAN, отправляются без тега. Нетегированные кадры, полученные на порту, считаются принадлежащими нативной VLAN.
    - ✓ **При включенном тегировании (**switchport trunk vlan tag native**):** Кадры, принадлежащие нативной VLAN, отправляются **с тегом**. Нетегированные кадры, полученные на порту, **отбрасываются** (поскольку порт больше не ожидает нетегированные кадры).
- **Зачем это нужно:**
    - ✓ **Безопасность:** Предотвращает атаки "VLAN hopping" через двойное тегирование (double-tagging), когда злоумышленник отправляет специально сформированный кадр, который использует нетегированную природу native VLAN для проникновения в другие VLAN.
    - ✓ **Упрощение:** Устраняет понятие "native VLAN" (нетегированной VLAN), делая транк полностью

SEC.RU | Короткий путь к информации Скачано с sec.ru

тегированным. Это упрощает конфигурацию и анализ трафика.

- ✓ **Стандартизация:** В некоторых сетевых стандартах и в средах провайдеров требуется тегирование всего трафика, включая native VLAN.

- **Внимание:** При включении этой функции **оба конца транкового соединения** должны быть настроены одинаково (оба с switchport trunk vlan tag native). Если один конец ожидает нетегированные кадры native VLAN, а другой отправляет их с тегом, связь будет нарушена.

Удаление конфигурации:

```
(config-if)# no switchport trunk vlan tag native
```

Отключает тегирование нативной VLAN (поведение по умолчанию — native VLAN отправляется без тега).

Просмотр:

```
# show running-config
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Включение тегирования native VLAN на транковом порту для безопасности:**

```
# configure terminal
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport trunk native vlan 999
(config-if)# switchport trunk vlan tag native
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.14 (config-if)# switchport vlan ip-subnet id

Настройка сопоставления IP-подсети с VLAN (IP Subnet-based VLAN)

Синтаксис:

```
(config-if)# switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>
```

Параметры:

- <vce_id: 1-128>: Укажите индекс записи. Допустимый диапазон: 1-128.
- <ipv4>: Укажите IP-адрес и маску подсети в формате xx.xx.xx.xx/mm.mm.mm.mm.
- <vid>: Укажите идентификатор VLAN.

Объяснение: Конфигурация VLAN на основе IP-подсети (IP Subnet-based VLAN) предназначена для отображения нетегированных (untagged) входящих кадров в определенную VLAN, если исходный IP-адрес найден в таблице сопоставления IP-подсети с VLAN. Когда классификация на основе IP-подсети включена, исходный адрес нетегированных входящих кадров проверяется по таблице сопоставления IP-подсети с VLAN. Если запись для этой подсети найдена, кадры назначаются в VLAN, указанную в записи. Если ни одна IP-подсеть не совпадает, нетегированные кадры классифицируются как принадлежащие VLAN ID принимающего порта (PVID).

Рекомендации:

- Команда switchport vlan ip-subnet id настраивает **правило классификации VLAN на основе IP-подсети**. Это позволяет

SEC.RU | Короткий путь к информации Скачано с sec.ru

автоматически назначать нетегированный трафик в определенную VLAN в зависимости от исходного IP-адреса устройства.

- **Как это работает:**
    1. На порту, где включена классификация по IP-подсети, коммутатор перехватывает первый пакет от устройства.
    2. Он анализирует исходный IP-адрес и сравнивает его с настроенными правилами (`ip-subnet id`).
    3. Если найдено совпадение (адрес принадлежит указанной подсети), все последующие кадры от этого устройства (пока активно соединение) назначаются в указанную VLAN.
    4. Если совпадений не найдено, используется PVID порта (стандартная VLAN доступа).
- **Зачем это нужно:**
    1. **Гибкость:** Позволяет автоматически сегментировать трафик на основе IP-адресации, не требуя от пользователя настройки VLAN на его устройстве.
    2. **Миграция:** Позволяет постепенно переводить устройства из одной VLAN в другую, изменяя их IP-адреса (и правило), без физического переключения портов.
    3. **Совместимость:** Полезно для сетей, где используются устаревшие устройства, не поддерживающие тегирование VLAN.
- **Порядок классификации:** Обычно классификация осуществляется в следующем порядке (если несколько методов включено): MAC-based VLAN → IP-subnet-based VLAN → Port-based VLAN (PVID).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config-if)# no switchport vlan ip-subnet id <vce_id_list>
```

Удаляет указанное правило сопоставления IP-подсети с VLAN.

Просмотр:

```
# show vlan ip-subnet [ id <subnet_id> ]
```

Примеры настройки:

1. **Настройка правила: все устройства из подсети 192.168.10.0/24 помещать в VLAN 10:**

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport vlan ip-subnet id 1 192.168.10.0/255.255.255.0 vlan 10
```

2. **Настройка нескольких правил на порту (разные подсети в разные VLAN):**

```
(config-if)# switchport vlan ip-subnet id 2 10.1.1.0/255.255.255.0 vlan 20
(config-if)# switchport vlan ip-subnet id 3 172.16.1.0/255.255.255.0 vlan 30
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.15 (config-if)# switchport vlan mac

Настройка сопоставления MAC-адреса с VLAN (MAC-based VLAN)

Синтаксис:

```
(config-if)# switchport vlan mac <mac_addr> vlan <vid>
```

Параметры:

- <mac_addr>: Укажите исходный MAC-адрес. Обратите внимание, что исходный MAC-адрес может быть сопоставлен только с одним идентификатором VLAN.
- vlan <vid>: Сопоставьте этот MAC-адрес с соответствующим идентификатором VLAN.

Объяснение: Эта команда используется для настройки VLAN на основе исходных MAC-адресов. Когда порт получает нетегированные (untagged) входящие кадры, обрабатывается исходный MAC-адрес, чтобы определить, какой VLAN принадлежат эти нетегированные кадры. Если исходные MAC-адреса не соответствуют созданным правилам, нетегированные кадры назначаются на идентификатор нативной VLAN принимающего порта (PVID).

Рекомендации:

- Команда switchport vlan mac настраивает **правило классификации VLAN на основе MAC-адреса (MAC-based VLAN)**. Это позволяет автоматически назначать нетегированный трафик в определенную VLAN в зависимости от MAC-адреса источника устройства.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Как это работает:**
    1. На порту, где включена классификация по MAC-адресу, коммутатор перехватывает кадры.
    2. Он анализирует исходный MAC-адрес (source MAC) в заголовке кадра.
    3. Если MAC-адрес совпадает с одним из настроенных правил, кадр назначается в соответствующую VLAN.
    4. Если совпадений не найдено, используется PVID порта (стандартная VLAN доступа).
- **Зачем это нужно:**
    1. **Гибкость:** Позволяет назначать разные VLAN устройствам, подключенным к одному порту (например, через неуправляемый коммутатор), на основе их MAC-адресов.
    2. **Безопасность:** Можно привязать конкретное устройство (с известным MAC-адресом) к определенной VLAN, даже если оно подключено к "чужому" порту.
    3. **Миграция:** Позволяет постепенно переводить устройства из одной VLAN в другую, не меняя физическое подключение порта, а просто добавляя правило для MAC-адреса.
- **Внимание:**
    1. Правило сопоставляет **исходный MAC-адрес** (то есть адрес устройства-источника) с VLAN.
    2. Один MAC-адрес может быть сопоставлен только с одной VLAN.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Обычно для работы MAC-based VLAN требуется включить эту функцию на порту (отдельной командой, например, switchport vlan mac enable).

Удаление конфигурации:

```
(config-if)# no switchport vlan mac <mac_addr> vlan <vid>
```

Удаляет правило сопоставления MAC-адреса с VLAN.

Просмотр:

```
# show vlan mac [ address <mac_addr> ]
```

Примеры настройки:

1. **Сопоставление MAC-адреса aa:bb:cc:dd:ee:ff с VLAN 10:**

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport vlan mac aa:bb:cc:dd:ee:ff vlan 10
```

2. **Настройка нескольких правил на одном порту:**

```
(config-if)# switchport vlan mac 00:11:22:33:44:55 vlan 20
(config-if)# switchport vlan mac 00:aa:bb:cc:dd:ee vlan 30
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.41.16 (config-if)# switchport vlan mapping

Применение группы VLAN mapping к интерфейсу

Синтаксис:

```
(config-if)# switchport vlan mapping <group>
```

Параметры:

- <group: 1-20>: Укажите идентификатор группы, который применяется к данному правилу.

Объяснение: Настройка таблицы группового отображения VLAN (group VLAN mapping) для данного конкретного интерфейса.

Рекомендации:

- Команда switchport vlan mapping в режиме конфигурации интерфейса **применяет предварительно созданную группу правил VLAN mapping** (трансляции VLAN) к данному порту. Сами правила трансляции создаются глобальной командой switchport vlan mapping <group ID> <vlan_list> <translation_vlan>
- **Как это работает:**
    1. Администратор создает глобальное правило трансляции VLAN, указывая группу ID, исходный VLAN и целевой VLAN (например, switchport vlan mapping 5 100 201).
    2. Затем на порту, который должен выполнять эту трансляцию, применяется группа командой switchport vlan mapping 5.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. После этого все входящие кадры на этом порту с исходным VLAN ID 100 будут заменены на VLAN ID 201.

- **Внимание:** только порты доступа (access ports) поддерживают трансляцию VLAN. Не рекомендуется настраивать трансляцию VLAN на транковых портах (trunk ports).
- **Двусторонняя настройка:** Для корректной двусторонней трансляции необходимо настроить соответствующие правила и применить их к портам на **обоих концах** соединения.
- **Группы:** Параметр <group> позволяет сгруппировать несколько правил трансляции (один групповой ID может содержать несколько пар "исходный VLAN → целевой VLAN") и применить их к порту одной командой.

Удаление конфигурации (Negation):

```
(config-if)# no switchport vlan mapping
```

Удаляет применение группы VLAN mapping с порта.

Просмотр:

```
# show running-config
# show interfaces GigabitEthernet 1/1 switchport
```

Примеры настройки:

1. **Создание глобального правила трансляции и применение его к порту доступа:**

```
# configure terminal
(config)# switchport vlan mapping 5 100 201
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

```
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport vlan mapping 5
```

2. **Применение группы к порту (если группа уже создана):**

```
(config)# interface GigabitEthernet 1/5
(config-if)# switchport mode access
(config-if)# switchport vlan mapping 10
```

2.7.41.17 (config-if)# switchport vlan protocol group

Настройка группы протоколов VLAN для интерфейса

Синтаксис:

```
(config-if)# switchport vlan protocol group <grp_id> vlan <vid>
```

Параметры:

- <grp_id: word 16>: Укажите описательное имя для этой записи. Это поле допускает только 16 буквенных символов (a-z; A-Z) или целых чисел (0-9).
- <vid>: Укажите идентификатор VLAN, который применяется к этому правилу.

Объяснение: Настройка группы протоколов VLAN для данного конкретного интерфейса.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда switchport vlan protocol group настраивает **правило классификации VLAN на основе протокола (Protocol-based VLAN)**. Это позволяет автоматически назначать нетегированные (untagged) кадры в определенную VLAN в зависимости от типа протокола в кадре.
- **Как это работает:**
    1. Администратор создает правило, указывая идентификатор группы (grp_id) и целевой VLAN (vid).
    2. Само правило классификации (какой протокол соответствует какой группе) настраивается отдельно (вероятно, глобальными командами, такими как vlan protocol group).
    3. На порту с помощью данной команды группа привязывается к VLAN.
    4. Когда порт получает нетегированный кадр, он анализирует тип протокола (например, IP, ARP, IPX, AppleTalk). Если тип протокола соответствует правилу, кадр назначается в указанную VLAN.
    5. Для кадров, тип протокола которых не соответствует ни одному правилу, используется PVID порта.
- **Типы протоколов (как видно из команды** show vlan protocol**):**
    1. **Ethernet II (**eth2**):** Протоколы на основе EtherType (IP, ARP, IPX, AppleTalk и т.д.).
    2. **SNAP (SubNetwork Access Protocol):** Протоколы SNAP с указанием OUI и PID.
    3. **LLC (Logical Link Control):** Протоколы LLC с указанием DSAP и SSAP.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Зачем это нужно:**

    1. **Сегментация трафика:** Разные протоколы можно направлять в разные VLAN. Например, IP-трафик в VLAN 10, IPX-трафик в VLAN 20.
    2. **Безопасность:** Изоляция устаревших или небезопасных протоколов.
    3. **Миграция:** Постепенный перевод трафика разных протоколов на новую VLAN.

Удаление конфигурации:

```
(config-if)# no switchport vlan protocol group <grp_id> vlan <vid>
```

Удаляет привязку группы протоколов к VLAN на интерфейсе.

Просмотр:

```
# show vlan protocol [ eth2 { <etype> | arp | ip | ipx | at } ] [ snap { <oui> | rfc-1042 | snap-8021h } <pid> ] [ llc <dsap> <ssap> ]
```

Примеры настройки:

1. **Настройка группы "IP_TRAFFIC" для VLAN 10 (предполагая, что глобальное правило для IP уже создано):**

    ```
    # configure terminal
    (config)# interface GigabitEthernet 1/1
    (config-if)# switchport vlan protocol group IP_TRAFFIC vlan 10
    ```

2. **Настройка группы "IPX_TRAFFIC" для VLAN 20:**

    ```
    (config-if)# switchport vlan protocol group IPX_TRAFFIC vlan 20
    ```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.42 Настройка TACACS+ сервера (config)# tacacs-server

2.7.42.1 (config)# tacacs-server timeout

Настройка тайм-аута ожидания ответа от TACACS+ сервера

Синтаксис:

```
(config)# tacacs-server timeout <seconds>
```

Параметры:

- <seconds:1-1000>: Укажите значение тайм-аута. Допустимый диапазон тайм-аута от 1 до 1000 секунд.

Объяснение: Время, в течение которого коммутатор ожидает ответа от TACACS+ сервера перед повторной отправкой запроса.

Рекомендации:

- Команда tacacs-server timeout задает **глобальное значение тайм-аута (timeout)** для TACACS+ запросов. Это максимальное время ожидания ответа от TACACS+ сервера. Если ответ не получен в течение этого времени, коммутатор либо повторяет запрос (если остались попытки, заданные tacacs-server retransmit), либо переключается на следующий сервер.
- **TACACS+** (Terminal Access Controller Access Control System Plus) — это протокол AAA (Authentication, Authorization, Accounting), используемый для централизованного управления доступом к сетевым устройствам. В отличие от RADIUS, TACACS+

SEC.RU | Короткий путь к информации Скачано с sec.ru

разделяет аутентификацию, авторизацию и учет, а также шифрует весь пакет, а не только пароль.

- **Как это работает:**
    1. Коммутатор отправляет TACACS+ запрос на сервер и запускает таймер.
    2. Если ответ получен до истечения тайм-аута, процесс завершается успешно.
    3. Если тайм-аут истекает, коммутатор повторяет запрос (если `retransmit` > 0) или помечает сервер как недоступный.
- **Выбор значения:**
    1. **Слишком короткий тайм-аут (например, 1-2 секунды):** Может привести к ложному определению сервера как недоступного при нормальных задержках в сети или при высокой нагрузке на сервер.
    2. **Слишком длинный тайм-аут (например, 30-60 секунд):** Замедляет процесс аутентификации при проблемах с сервером и увеличивает время переключения на резервный сервер.
    3. **Рекомендуемое значение:** Обычно используется от 3 до 10 секунд в зависимости от условий сети.

Удаление конфигурации:

```
(config)# no tacacs-server timeout
```

Сбрасывает значение глобального тайм-аута к значению по умолчанию (обычно 5 секунд).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
# show tacacs-server
```

Отображает текущие настройки TACACS+ серверов, включая тайм-аут.

Примеры настройки:

1. **Установка глобального тайм-аута 10 секунд:**

   ```
   # configure terminal
   (config)# tacacs-server timeout 10
   ```

2. **Установка более короткого тайм-аута (3 секунды) для быстрого переключения:**

   ```
   (config)# tacacs-server timeout 3
   ```

2.7.42.2 (config)# tacacs-server deadtime

Настройка времени ожидания перед повторной попыткой соединения с мертвым (dead) TACACS+ сервером

Синтаксис:

```
(config)# tacacs-server deadtime <minutes>
```

Параметры:

- <minutes:1-1440>: Укажите значение времени ожидания (deadtime) для TACACS+ сервера. Допустимый диапазон: от 1 до 1440 минут.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Объяснение: Deadtime – это период, в течение которого коммутатор не будет отправлять новые запросы на сервер, который не ответил на предыдущий запрос. Это предотвращает постоянные попытки коммутатора связаться с сервером, который уже определен как "мертвый".

Рекомендации:

- Команда tacacs-server deadtime задает **время "мертвого" периода** для TACACS+ сервера. Если TACACS+ сервер не отвечает на запросы (например, из-за сбоя или сетевых проблем), коммутатор помечает его как "мертвый" и в течение указанного времени (deadtime) не будет отправлять на него новые запросы, переключаясь на другие настроенные TACACS+ серверы.
- **Как это работает:**
    1. Коммутатор отправляет TACACS+ запрос на сервер.
    2. Если ответ не получен в течение тайм-аута (tacacs-server timeout), коммутатор помечает сервер как "мертвый" (dead).
    3. В течение deadtime коммутатор не отправляет новые запросы на этот сервер.
    4. По истечении deadtime сервер снова считается потенциально доступным, и коммутатор может отправлять на него запросы.
- **Зачем это нужно:**
    1. **Эффективность:** Предотвращает трату времени на ожидание ответа от заведомо недоступного сервера, ускоряя обработку запросов аутентификации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. **Снижение нагрузки:** Уменьшает количество бесполезных запросов к недоступному серверу.

- **Выбор значения:**
    1. **Короткое значение (например, 5-10 минут):** Быстрое восстановление после временного сбоя сервера, но может привести к частым попыткам соединения, если сервер реально недоступен.
    2. **Длинное значение (например, 30-60 минут и более):** Экономит ресурсы при длительном отказе сервера, но увеличивает время восстановления после того, как сервер снова станет доступен.
- Обычно используется значение от 5 до 30 минут.

Удаление конфигурации:

```
(config)# no tacacs-server deadtime
```

Сбрасывает значение deadtime к значению по умолчанию (зависит от реализации, может быть 0 – отключено).

Просмотр:

```
# show tacacs-server
```

Примеры настройки:

1. **Установка deadtime 10 минут:**

```
# configure terminal
(config)# tacacs-server deadtime 10
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2. **Установка deadtime 30 минут (для длительного отказа сервера):**

```
(config)# tacacs-server deadtime 30
```

2.7.42.3 (config)# tacacs-server key

Настройка глобального секретного ключа TACACS+

Синтаксис:

```
(config)# tacacs-server key <key>
```

Параметры:

- <key:1-63>: Укажите значение секретного ключа. Допустимая длина: от 1 до 63 символов.

Объяснение: Укажите секретный ключ длиной до 63 символов. Этот ключ используется совместно между TACACS+ сервером и коммутатором.

Рекомендации:

- Команда tacacs-server key задает **глобальный секретный ключ (shared secret)** для всех TACACS+ серверов, настроенных на коммутаторе. Этот ключ используется для шифрования всего обмена данными между коммутатором и TACACS+ сервером, включая пароли и другие атрибуты.
- Ключ должен **полностью совпадать** на коммутаторе и на TACACS+ сервере. Несовпадение ключа приведет к тому, что

SEC.RU | Короткий путь к информации Скачано с sec.ru

TACACS+ сервер не сможет расшифровать и обработать запросы от коммутатора, и аутентификация будет невозможна.

- **TACACS+ vs RADIUS:** В отличие от RADIUS, который шифрует только пароль, TACACS+ шифрует **весь** пакет (кроме заголовка TACACS+), что обеспечивает более высокий уровень безопасности.
- **Приоритет:** Если для конкретного TACACS+ сервера (в команде tacacs-server host) указан свой ключ, он имеет приоритет над глобальным. Это позволяет использовать разные ключи для разных серверов.
- **Рекомендации по выбору ключа:**
    - ✓ Используйте сложные, трудно подбираемые ключи (не менее 10-15 символов, включая буквы разного регистра, цифры и специальные символы).
    - ✓ Не используйте словарные слова или легко угадываемые комбинации.
    - ✓ Ключ хранится в конфигурации коммутатора. В некоторых реализациях он может отображаться в зашифрованном виде, но все же его компрометация может привести к нарушению безопасности.

Удаление конфигурации:

```
(config)# no tacacs-server key
```

Удаляет глобальный секретный ключ TACACS+.

Просмотр:

```
# show tacacs-server
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Отображает текущие настройки TACACS+ серверов (ключ обычно отображается в зашифрованном виде).

Примеры настройки:

1. **Установка глобального секретного ключа "MySecretKey123":**

```
# configure terminal
(config)# tacacs-server key MySecretKey123
```

2. **Установка более сложного ключа:**

```
(config)# tacacs-server key "T@cAc$+S3cr3tK3y!2024"
```

2.7.42.4 (config)# tacacs-server host

Настройка хоста (сервера) TACACS+

Синтаксис:

```
(config)# tacacs-server host <host_name> [ port <port> ] [ timeout <seconds> ] [ key <key> ]
```

Параметры:

- <host_name>: Укажите имя хоста или IP-адрес для TACACS+ сервера.
- [port <port>]: Укажите номер TCP-порта, используемого на TACACS+ сервере для аутентификации. По умолчанию 49.
- [timeout <seconds>]: Если значение тайм-аута указано здесь, оно заменит глобальное значение тайм-аута. Если вы хотите использовать глобальное значение, оставьте это поле пустым.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- [key <key>]: Если секретный ключ указан здесь, он заменит глобальный секретный ключ. Если вы хотите использовать глобальное значение, оставьте это поле пустым.

Объяснение: Настройка параметров TACACS+ сервера.

Рекомендации:

- Команда tacacs-server host является **основной для добавления TACACS+ сервера** в конфигурацию коммутатора. TACACS+ (Terminal Access Controller Access Control System Plus) — это протокол AAA (Authentication, Authorization, Accounting), используемый для централизованного управления доступом к сетевым устройствам.
- **Параметры:**
  - ✓ host_name: Может быть IPv4-адресом, IPv6-адресом или доменным именем. При использовании доменного имени необходимо настроить DNS (ip name-server).
  - ✓ port: TCP-порт TACACS+ сервера. Стандартный порт — **49**. В отличие от RADIUS (UDP), TACACS+ использует TCP, что обеспечивает более надежную доставку.
  - ✓ timeout: Время ожидания ответа от сервера (в секундах) для данного конкретного сервера. Если не указано, используется глобальное значение (tacacs-server timeout).
  - ✓ key: Секретный ключ (shared secret), используемый для шифрования обмена между коммутатором и TACACS+ сервером. Должен совпадать с ключом, настроенным на TACACS+ сервере. Если не указан, используется глобальный ключ (tacacs-server key).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **TACACS+ vs RADIUS:**
    - ✓ TACACS+ использует **TCP** (обычно порт 49), что обеспечивает более надежную доставку.
    - ✓ TACACS+ шифрует **весь пакет**, а не только пароль.
    - ✓ TACACS+ разделяет аутентификацию, авторизацию и учет (три отдельных процесса).
- **Отказоустойчивость:** Для повышения надежности можно настроить несколько TACACS+ серверов. Коммутатор будет опрашивать их в порядке добавления.

Удаление конфигурации:

```
(config)# no tacacs-server host <host_name> [ port <port> ]
```

Удаляет указанный TACACS+ сервер из конфигурации.

Просмотр:

```
# show tacacs-server
```

Примеры настройки:

1. **Добавление TACACS+ сервера с IP-адресом 192.168.1.100, ключом "secret123", портом по умолчанию:**

```
# configure terminal
(config)# tacacs-server host 192.168.1.100 key secret123
```

2. **Добавление TACACS+ сервера с нестандартным портом и тайм-аутом:**

```
(config)# tacacs-server host 10.10.10.50 port 49 timeout 10 key MyS
ecretKey
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

3. **Добавление TACACS+ сервера по доменному имени (требуется DNS):**

```
(config)# ip name-server 8.8.8.8
(config)# tacacs-server host tacacs.company.com key securekey
```

2.7.43 Настройка UPnP (Universal Plug and Play) (config)# upnp

2.7.43.1 (config)# upnp

Глобальное включение UPnP

Синтаксис:

```
(config)# upnp
```

Объяснение: Включение работы UPnP (Universal Plug and Play).

Рекомендации:

- Команда upnp **глобально активирует** функцию UPnP на коммутаторе. UPnP — это набор сетевых протоколов, которые позволяют устройствам в сети автоматически обнаруживать друг друга и взаимодействовать без необходимости ручной настройки.
- UPnP может использоваться для:
    - ✓ **Автоматического обнаружения:** Позволяет другим UPnP-устройствам (например, маршрутизаторам, медиа-серверам, принтерам) обнаруживать коммутатор в сети.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **Управления через UPnP:** Некоторые коммутаторы поддерживают базовое управление (например, получение информации о статусе) через UPnP-клиенты.
- ✓ **Поддержки QoS (Quality of Service):** UPnP QoS (также известный как UPnP Qos Device Architecture) может использоваться для управления приоритетами трафика от приложений, поддерживающих UPnP (например, стриминговые сервисы, игры).

- **Безопасность:** UPnP известен уязвимостями безопасности. Злоумышленники могут использовать UPnP для обхода файрволов, выполнения атак с подменой DNS, перехвата трафика или использования устройства в качестве части ботнета. **Рекомендуется отключать UPnP на сетевых устройствах, если в нем нет явной необходимости.** Включайте UPnP только в доверенных сетях и если приложения требуют его наличия.
- После включения UPnP можно проверить его статус командой `show upnp`.

Удаление конфигурации:

```
(config)# no upnp
```

Глобально отключает UPnP на коммутаторе.

Просмотр:

```
# show upnp
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

Отображает статус UPnP (включен/отключен) и, возможно, другую информацию о работе протокола.

Примеры настройки:

1. **Глобальное включение UPnP:**

```
# configure terminal
(config)# upnp
```

2.7.43.2 (config)# upnp advertising-duration

Настройка интервала отправки UPnP-объявлений

Синтаксис:

```
(config)# upnp advertising-duration <v_100_to_86400>
```

Параметры:

- <v_100_to_86400>: Укажите интервал (длительность) отправки объявлений. Допустимый диапазон: от 100 до 86400 секунд.

Объяснение: Этот параметр определяет, как часто отправляется UPnP-объявление (advertisement). Длительность указывается в пакетах SSDP (Simple Service Discovery Protocol), которые информируют управляющую точку (control point) о том, как часто она должна получать SSDP-объявления от коммутатора. По умолчанию интервал отправки объявлений установлен в 100 секунд. Рекомендуется устанавливать более короткий интервал, так как чем короче интервал, тем более актуальным является UPnP-статус.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда `upnp advertising-duration` задает **интервал (в секундах)**, с которым коммутатор отправляет SSDP-объявления (advertisements) о своем присутствии и предоставляемых сервисах по протоколу UPnP.
- **Как это работает:**
    - ✓ SSDP работает поверх UDP и является "ненадежным" протоколом (без подтверждения доставки).
    - ✓ Управляющие точки (UPnP-клиенты) слушают эти объявления, чтобы обнаружить UPnP-устройства в сети.
    - ✓ Значение `advertising-duration` указывается в SSDP-пакете и говорит клиенту, **как часто он должен ожидать следующее объявление**. Это не частота отправки в секундах, а время жизни объявления (TTL).
    - ✓ Реальная частота отправки объявлений коммутатором определяется этим значением (обычно объявления отправляются с интервалом `advertising-duration / 2` или `advertising-duration * 0.75`, в зависимости от реализации).
- **Выбор значения:**
    - ✓ **Короткий интервал (например, 100-300 секунд):** Обеспечивает более быстрое обнаружение устройства и более актуальную информацию, но увеличивает сетевой трафик (хотя объем SSDP-трафика невелик).
    - ✓ **Длинный интервал (например, 1800-86400 секунд):** Снижает служебный трафик, но замедляет обнаружение устройства и может привести к тому, что

SEC.RU | Короткий путь к информации Скачано с sec.ru

клиенты "потеряют" коммутатор при временных проблемах с сетью.

- Значение по умолчанию (100 секунд) является разумным компромиссом. Увеличивайте его, если UPnP не критичен, или уменьшайте, если требуется более быстрое обнаружение.

Удаление конфигурации:

```
(config)# no upnp advertising-duration
```

Сбрасывает интервал отправки объявлений к значению по умолчанию (100 секунд).

Просмотр:

```
# show upnp
```

Примеры настройки:

1. **Установка интервала 150 секунд:**

```
# configure terminal
(config)# upnp advertising-duration 150
```

2. **Установка более длинного интервала (1 час = 3600 секунд) для снижения трафика:**

```
(config)# upnp advertising-duration 3600
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.43.3 (config)# upnp ttl

Настройка времени жизни (TTL) для UPnP-объявлений

Синтаксис:

```
(config)# upnp ttl <v_1_to_255>
```

Параметры:

- <v_1_to_255>: Укажите значение TTL (Time to Live). Допустимый диапазон: от 1 до 255.

Объяснение: TTL (Time to Live) используется для настройки того, через какое количество шагов (маршрутизаторов) UPnP-объявление может пройти, прежде чем исчезнуть.

Рекомендации:

- Команда upnp ttl задает **значение TTL (Time to Live)** в IP-заголовке SSDP-пакетов (Simple Service Discovery Protocol), отправляемых коммутатором в рамках работы UPnP.
- **Как это работает:**
  - ✓ Каждый маршрутизатор на пути пакета уменьшает TTL на 1.
  - ✓ Когда TTL становится равным 0, пакет отбрасывается.
  - ✓ TTL ограничивает "радиус" распространения SSDP-объявлений в сети.
- **TTL = 1 (значение по умолчанию для многих UPnP-реализаций):** Объявления не покидают локальную подсеть. Это настройка по умолчанию, рекомендуемая для большинства сетей, так как UPnP обычно предназначен для работы в пределах одного широковещательного домена (VLAN).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **TTL > 1:** Позволяет SSDP-объявлениям проходить через маршрутизаторы и достигать других подсетей. Используется редко, так как UPnP не предназначен для работы через маршрутизаторы (многие маршрутизаторы не перенаправляют SSDP-пакеты).
- **Выбор значения:**
    - ✓ **1 (рекомендуется):** Ограничивает объявления локальной подсетью. Это минимально возможное значение, которое обеспечивает работу в пределах одного широковещательного домена.
    - ✓ **Больше 1:** Может понадобиться в сетях, где SSDP-пакеты должны проходить через несколько коммутаторов с маршрутизацией (например, если управляющая точка находится в другой подсети). Однако это нестандартно для UPnP.

Удаление конфигурации:

```
(config)# no upnp ttl
```

Сбрасывает TTL к значению по умолчанию (обычно 1).

Просмотр:

```
# show upnp
```

Примеры настройки:

1. **Установка TTL = 1 (рекомендуемое значение):**

```
# configure terminal
(config)# upnp ttl 1
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.44 Настройка учетных записей пользователей (username) (config)# username

2.7.44.1 (config)# username <username> privilege <priv> password encrypted

Создание новой учетной записи пользователя с зашифрованным паролем

Синтаксис:

```
(config)# username <username> privilege <priv> password encrypted <encry_password>
```

Объяснение: По умолчанию существует только один пользователь 'admin', которому назначен наивысший уровень привилегий 15. Используйте эту команду для настройки новой учетной записи пользователя.

Параметры:

- username <username: word31>: Укажите новое имя пользователя. Допустимое количество символов: 31.
- privilege <priv: 0-15>: Укажите уровень привилегий для этой новой учетной записи. Допустимый диапазон: от 1 до 15.
    - ✓ **Уровень 15:** Полный доступ ко всем группам команд. Предоставляет полный контроль над устройством.
    - ✓ **Другие уровни:** Доступ определяется настройками уровня привилегий для каждой группы команд.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ Принцип: Уровень привилегий пользователя должен быть равен или превышать уровень привилегий группы команд для получения доступа к этой группе.
- ✓ Настройки по умолчанию: Уровень 5 обычно предоставляет доступ только для чтения (read-only). Уровень 10 обычно предоставляет доступ для чтения и записи (read-write). Обслуживание системы (загрузка ПО, сброс к заводским настройкам) требует уровня 15.
- ✓ **Рекомендации:** Уровень 15 — для администратора; уровень 10 — для стандартного пользователя; уровень 5 — для гостевого аккаунта.

- password encrypted <encry_password: 4-44>: Укажите зашифрованный пароль для этой новой учетной записи. Зашифрованный (скрытый) пароль пользователя. Обратите внимание, что зашифрованный пароль будет расшифрован системой внутренне. Вы не можете использовать его напрямую как обычный текст, и он обычно не является человеко-читаемым.

Рекомендации:

- Команда username (с параметром password encrypted) используется для **создания или изменения учетных записей пользователей** для доступа к CLI (консоль, Telnet, SSH) и веб-интерфейсу. Пароль указывается в **уже зашифрованном виде**.
- **Внимание:** Параметр encrypted означает, что вы должны ввести пароль в том виде, в котором он хранится в конфигурации (например, полученный из другой конфигурации или сгенерированный системой).
- **Уровни привилегий (Privilege Levels):**

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **15 (Администратор):** Полный доступ ко всем командам, включая конфигурационные, управление прошивкой, сброс настроек.
- ✓ **10 (Продвинутый пользователь):** Обычно доступ для чтения и записи к большинству команд, кроме критических (обновление ПО, управление учетными записями).
- ✓ **5 (Гость):** Обычно доступ только для чтения (команды `show`, `ping` и т.д.).

- **Удаление пользователя:** `no username <username>` удаляет учетную запись.

Удаление конфигурации:

```
(config)# no username <username>
```

Удаляет учетную запись указанного пользователя.

Просмотр

```
> show users
# show users
```

Отображает список активных сессий пользователей. Для просмотра списка всех пользователей (не только активных) может использоваться `show running-config | include username`.

Примеры настройки:

1. **Создание пользователя с уровнем привилегий 15 и зашифрованным паролем:**

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
# configure terminal
(config)# username mis4jack privilege 15 password encrypted jack3
0125
```

2. **Создание пользователя "operator" с уровнем 10 (чтение/запись):**

```
(config)# username operator privilege 10 password encrypted operP
@ss123
```

3. **Создание гостевого пользователя "guest" с уровнем 5 (только чтение):**

```
(config)# username guest privilege 5 password encrypted guest123
```

2.7.44.2 (config)# username <username> privilege <priv> password none

Создание новой учетной записи пользователя без пароля

Синтаксис:

```
(config)# username <username> privilege <priv> password none
```

Объяснение: По умолчанию существует только один пользователь 'admin', которому назначен наивысший уровень привилегий 15. Используйте эту команду для настройки новой учетной записи пользователя без пароля.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- username <username: word31>: Укажите новое имя пользователя. Допустимое количество символов: 31.
- privilege <priv: 0-15>: Укажите уровень привилегий для этой новой учетной записи. Допустимый диапазон: от 1 до 15.
    - ✓ **Уровень 15:** Полный доступ ко всем группам команд. Предоставляет полный контроль над устройством.
    - ✓ **Другие уровни:** Доступ определяется настройками уровня привилегий для каждой группы команд.
    - ✓ Принцип: Уровень привилегий пользователя должен быть равен или превышать уровень привилегий группы команд для получения доступа к этой группе.
    - ✓ Настройки по умолчанию: Уровень 5 обычно предоставляет доступ только для чтения (read-only). Уровень 10 обычно предоставляет доступ для чтения и записи (read-write). Обслуживание системы (загрузка ПО, сброс к заводским настройкам) требует уровня 15.
    - ✓ **Рекомендации:** Уровень 15 — для администратора; уровень 10 — для стандартного пользователя; уровень 5 — для гостевого аккаунта.
- password none: Отсутствие пароля для этой учетной записи.

Рекомендации:

- Команда username ... password none создает учетную запись пользователя, которая **не требует ввода пароля** при входе в систему. Это небезопасно и **не рекомендуется** для использования особенно с высокими уровнями привилегий.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Сценарии использования (только в изолированных, тестовых средах):**
    - ✓ Временная учетная запись для отладки.
    - ✓ Доступ для автоматизированных скриптов, если другие механизмы аутентификации недоступны (хотя даже в этом случае лучше использовать SSH-ключи или учетные данные с паролями).
    - ✓ Обучающие или демонстрационные цели.
- **Безопасность:** Учетная запись без пароля является серьезной уязвимостью. Любой, кто имеет доступ к консоли или сети (если разрешен удаленный доступ по Telnet/SSH с такой учетной записью), может войти в систему с уровнем привилегий, заданным для этой учетной записи.
- Всегда используйте учетные записи с паролями. Если требуется доступ без пароля для автоматизации, рассмотрите использование аутентификации на основе ключей SSH.

Удаление конфигурации:

```
(config)# no username <username>
```

Удаляет учетную запись указанного пользователя.

Просмотр:

```
> show users
# show users
```

Отображает список активных сессий пользователей. Для просмотра списка всех пользователей (не только активных) может использоваться `show running-config | include username`*.*

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.44.3 (config)# username <username> privilege <priv> password unencrypted

Создание новой учетной записи пользователя с незашифрованным паролем

Синтаксис:

```
(config)# username <username> privilege <priv> password unencrypted <password>
```

Объяснение: По умолчанию существует только один пользователь 'admin', которому назначен наивысший уровень привилегий 15. Используйте эту команду для настройки новой учетной записи пользователя с незашифрованным паролем.

Параметры:

- username <username: word31>: Укажите новое имя пользователя. Допустимое количество символов: 31.
- privilege <priv: 0-15>: Укажите уровень привилегий для этой новой учетной записи. Допустимый диапазон: от 1 до 15.
    - ✓ **Уровень 15:** Полный доступ ко всем группам команд. Предоставляет полный контроль над устройством.
    - ✓ **Другие уровни:** Доступ определяется настройками уровня привилегий для каждой группы команд.
    - ✓ Принцип: Уровень привилегий пользователя должен быть равен или превышать уровень привилегий группы команд для получения доступа к этой группе.
    - ✓ Настройки по умолчанию: Уровень 5 обычно предоставляет доступ только для чтения (read-only).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Уровень 10 обычно предоставляет доступ для чтения и записи (read-write). Обслуживание системы (загрузка ПО, сброс к заводским настройкам) требует уровня 15.

- ✓ **Рекомендации:** Уровень 15 – для администратора; уровень 10 – для стандартного пользователя; уровень 5 – для гостевого аккаунта.

- password unencrypted <password: line31>: Укажите незашифрованный пароль для этой учетной записи. Пароль в открытом тексте. Допускаются любые печатные символы, включая пробелы.

Рекомендации:

- Команда username ... password unencrypted создает учетную запись пользователя с паролем, введенным в **открытом виде (plain text)**. Этот пароль будет храниться в конфигурации в незашифрованном виде (или в слабо зашифрованном, но все равно уязвимом к чтению).
- **Безопасность:** Пароли в открытом виде могут быть прочитаны любым, кто имеет доступ к просмотру конфигурации (например, через show running-config). Это создает серьезную угрозу безопасности.
- В большинстве современных систем рекомендуется использовать команду username ... password encrypted (зашифрованный пароль) или username ... secret.
- **Уровни привилегий:** Как и в других вариантах команды username, уровни 5 (гость), 10 (стандартный пользователь) и 15 (администратор) являются рекомендуемыми.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Удаление конфигурации:

```
(config)# no username <username>
```

Удаляет учетную запись указанного пользователя.

Просмотр:

```
> show users
# show users
```

Отображает список активных сессий пользователей. Для просмотра списка всех пользователей (не только активных) может использоваться show running-config | include username*.*

2.7.45 Настройка VLAN (config)# vlan

2.7.45.1 (config)# vlan

Создание и настройка VLAN

Синтаксис:

```
(config)# vlan <vlist>
```

Объяснение: Настройка разрешенных VLAN.

Параметры:

- <vlist>: Показывает разрешенные VLAN доступа. Этот параметр влияет только на порты, установленные в режим "Access".

SEC.RU | Короткий путь к информации Скачано с sec.ru

Порты в других режимах являются членами всех VLAN, указанных в поле "Allowed VLANs". По умолчанию указана только VLAN 1. Можно добавить больше разрешенных VLAN доступа, указав отдельные идентификаторы VLAN через запятую. Если вы хотите указать диапазон, разделите его дефисом. Например: 1,5,10,12-15,100. После нажатия Enter приглашение командной строки изменится на (config-vlan)#.

Рекомендации:

- Команда vlan используется для **создания VLAN** (Virtual Local Area Network) и перехода в режим конфигурации VLAN (config-vlan)#. В этом режиме можно задать имя VLAN и другие параметры.
- **Внимание:** Прежде чем назначать порты в VLAN, эта VLAN должна быть создана на коммутаторе. Исключение составляет VLAN 1 (по умолчанию).
- **Синтаксис:**
    - ✓ Одна VLAN: vlan 10
    - ✓ Несколько VLAN через запятую: vlan 10,20,30
    - ✓ Диапазон VLAN: vlan 100-200
    - ✓ Комбинация: vlan 2,5,10-20,50
- **После создания VLAN** (т.е. после выполнения команды vlan <vlist>) вы попадаете в режим (config-vlan)#, где можно:
    - ✓ Задать имя VLAN: name <vlan_name>.
    - ✓ Настроить другие параметры (например, состояние, медиа-тип).
- **Стандартная VLAN 1:** Существует по умолчанию, не может быть удалена или переименована.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Диапазоны VLAN:** В стандарте 802.1Q допустимы VLAN от 1 до 4094. Некоторые VLAN (например, 1002-1005) могут быть зарезервированы

Удаление конфигурации:

```
(config)# no vlan { { ethertype s-custom-port } | <vlan_list> }
```

Удаляет указанные VLAN. При этом порты, назначенные в удаленную VLAN, теряют связь (обычно переводятся в неактивное состояние или в VLAN 1).

Примеры настройки:

1. **Создание VLAN 10 и переход в режим конфигурации VLAN:**

```
# configure terminal
(config)# vlan 10
(config-vlan)#
```

2. **Создание нескольких VLAN:**

```
(config)# vlan 20,30,40
(config-vlan)#
```

3. **Создание диапазона VLAN (100-150):**

```
(config)# vlan 100-150
(config-vlan)#
```

4. **Создание VLAN с именем:**

```
(config)# vlan 100
(config-vlan)# name Sales
(config-vlan)# exit
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

2.7.45.2 (config)# vlan ethertype s-custom-port

Настройка типа EtherType для пользовательских S-портов

Синтаксис:

```
(config)# vlan ethertype s-custom-port <etype>
```

Параметры:

- ethertype s-custom-port <etype>: Укажите тип EtherType, используемый для пользовательских S-портов (customer s-ports). Допустимый диапазон: от 0x0600 до 0xffff (шестнадцатеричные значения).

Объяснение: Настройка типа EtherType (Ethernet type), используемого для пользовательских S-портов.

Рекомендации:

- Команда vlan ethertype s-custom-port задает **значение TPID (Tag Protocol Identifier)** для портов, настроенных как s-custom-port (тип порта "S-custom-port" в гибридном режиме). TPID — это 16-битное поле в теге VLAN, которое идентифицирует протокол тегирования.
- **Используется:**
  - ✓ **C-port (Customer port):** Ожидает стандартные клиентские теги с TPID = 0x8100 (802.1Q).
  - ✓ **S-port (Service port):** Ожидает провайдерские теги с TPID = 0x88A8 (стандарт для Q-in-Q).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ **S-custom-port:** Позволяет задать **пользовательское (custom) значение TPID** для взаимодействия с оборудованием других производителей, которое может использовать нестандартные TPID (например, 0x9100, 0x9200 и т.д.).

- **Когда это нужно:**
  - ✓ При подключении к устаревшему или проприетарному оборудованию, которое использует нестандартные значения TPID для тегирования VLAN.
  - ✓ При работе в среде, где требуется нестандартный EtherType для разграничения клиентов в сетях провайдеров.
- **Диапазон значений:** Допустимы любые значения от 0x0600 до 0xFFFF, но стандартными являются 0x8100 (802.1Q) и 0x88A8 (802.1ad — Q-in-Q).
- **Внимание:** Это глобальная настройка для всех портов, имеющих тип s-custom-port. Изменение этого значения повлияет на обработку тегированных кадров на всех таких портах.

Удаление конфигурации:

```
(config)# no vlan ethertype s-custom-port
```

Сбрасывает EtherType для S-custom-port к значению по умолчанию (обычно 0x88A8).

Примеры настройки:

1. **Установка EtherType для S-custom-port в 0x88A8 (стандарт Q-in-Q):**

SEC.RU | Короткий путь к информации Скачано с sec.ru

```
# configure terminal
(config)# vlan ethertype s-custom-port 0x88a8
```

2. **Установка нестандартного EtherType (например, 0x9100 для оборудования некоторых производителей):**

```
(config)# vlan ethertype s-custom-port 0x9100
```

2.7.45.3 (config)# vlan protocol

Настройка классификации VLAN на основе протокола

Синтаксис:

```
(config)# vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>
```

Объяснение: Сетевые устройства, которым требуется поддержка нескольких протоколов, не могут быть легко сгруппированы в общую VLAN. Это может потребовать использования нестандартных устройств для передачи трафика между разными VLAN, чтобы охватить все устройства, участвующие в конкретном протоколе. Такая конфигурация лишает пользователей основных преимуществ VLAN, включая безопасность и простоту доступа.

Чтобы избежать этих проблем, есть возможность настроить на этом коммутаторе VLAN на основе протокола (protocol-based VLANs), которые разделяют физическую сеть на логические группы VLAN для каждого требуемого протокола. Когда кадр получен на порту, его принадлежность к VLAN может быть определена на основе типа протокола, используемого входящими пакетами.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Параметры:

- protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } }: Доступны три типа кадров: "Ethernet", "SNAP" и "LLC". Поле значения необходимо изменить соответствующим образом.
    - ✓ eth2 **(Ethernet):** Значение Ether Type (etype). По умолчанию установлено 0x0800. Допустимый диапазон: от 0x0600 до 0xffff.
    - ✓ snap**:** Включает значения OUI (Organizationally Unique Identifier) и PID (Protocol ID).
        - OUI: Значение в формате xx-xx-xx, где каждая пара (xx) в строке является шестнадцатеричным значением в диапазоне 0x00-0xff.
        - PID: Если OUI равен шестнадцатеричному 000000, идентификатор протокола является значением поля EtherType для протокола, работающего поверх SNAP. Если OUI принадлежит определенной организации, PID является значением, назначенным этой организацией для протокола, работающего поверх SNAP.
    - ✓ llc **(Logical Link Control):** Включает значения DSAP (Destination Service Access Point) и SSAP (Source Service Access Point). По умолчанию значение 0xff. Допустимый диапазон: от 0x00 до 0xff.
- group <grp_id>: Укажите имя для этой записи. Это поле допускает только 16 буквенных символов (a-z; A-Z) или целых чисел (0-9).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Рекомендации:

- Команда vlan protocol создает **правило классификации VLAN на основе протокола**, которое затем может быть применено к порту (с помощью switchport vlan protocol group <grp_id> vlan <vid>). Это позволяет автоматически назначать нетегированные кадры в определенную VLAN в зависимости от типа протокола кадра.
- **Зачем это нужно:**
    - ✓ В сетях, использующих несколько протоколов (например, IP, IPX, AppleTalk), можно сегментировать трафик по протоколам, размещая их в разных VLAN без изменения конфигурации конечных устройств.
    - ✓ Повышает безопасность, изолируя устаревшие или менее безопасные протоколы.
    - ✓ Упрощает управление в средах с нестандартными протоколами.
- **Типы кадров:**
    - ✓ eth2 **(Ethernet II):** Наиболее распространенный тип. Идентифицирует протокол по значению EtherType (например, 0x0800 = IPv4, 0x0806 = ARP, 0x86DD = IPv6).
    - ✓ snap **(SubNetwork Access Protocol):** Используется в некоторых сетях (например, Token Ring, FDDI) или для инкапсуляции протоколов, не имеющих EtherType.
    - ✓ llc **(Logical Link Control):** Используется для протоколов без явного EtherType, идентифицируемых по DSAP/SSAP (например, NetBIOS, SNA).

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Применение на порту:** После создания группы командой vlan protocol ... group <grp_id>, на порту доступа можно привязать эту группу к VLAN: switchport vlan protocol group <grp_id> vlan <vid>.

Удаление конфигурации:

```
(config)# no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>
```

Удаляет указанное правило классификации протоколов.

Просмотр:

```
# show vlan protocol [ eth2 { <etype> | arp | ip | ipx | at } ] [ snap { <oui> | rfc-1042 | snap-8021h } <pid> ] [ llc <dsap> <ssap> ]
```

Примеры настройки:

1. **Создание правила для IP-протокола (EtherType 0x0800) с группой "IP_TRAFFIC":**

```
# configure terminal
(config)# vlan protocol eth2 ip group IP_TRAFFIC
```

2. **Создание правила для ARP-протокола (EtherType 0x0806) с группой "ARP_TRAFFIC":**

```
(config)# vlan protocol eth2 arp group ARP_TRAFFIC
```

3. **Создание правила для пользовательского EtherType 0x88a8 с группой "CUSTOM":**

```
(config)# vlan protocol eth2 0x88a8 group CUSTOM
```


SEC.RU | Короткий путь к информации Скачано с sec.ru

4. **Применение группы к порту и VLAN (после создания группы):**

```
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport vlan protocol group IP_TRAFFIC vlan 10
```

2.7.46 (config)# web privilege group

Назначение уровня привилегий для групп веб-интерфейса

Синтаксис:

```
(config)# web privilege group <group_name> level { [ cro <cro> ] [ crw <crw> ] [ sro <sro> ] [ srw <srw> ] }
```

Объяснение: Назначение группы агрегации (Aggregation group) для уровня crw (configuration/execute read-write) 15.

Параметры:

- group <group_name>: Это имя идентифицирует группу привилегий. Допустимые слова: 'Aggregation', 'DHCP', 'Debug', 'Dhcp_Client', 'Diagnostics', 'EPS', 'ERPS', 'ETH_LINK_OAM', 'EVC', 'IP2', 'IPMC_Snooping', 'LACP', 'LLDP', 'Loop_Protect', 'MAC_Table', 'MEP', 'MVR', 'Maintenance', 'Mirroring', 'NTP', 'POE', 'PTP', 'Ports', 'Private_VLANs', 'QoS', 'RPC', 'Security', 'Spanning_Tree', 'System', 'Timer', 'UPnP', 'VCL', 'VLAN_Translation', 'VLANs', 'Voice_VLAN'.
- level { [cro <cro: 0-15>] [crw <crw: 0-15>] [sro <sro: 0-15>] [srw <srw: 0-15>] }: Каждая группа имеет уровень авторизации для следующих подгрупп:

SEC.RU | Короткий путь к информации Скачано с sec.ru

- ✓ cro (configuration read-only): Доступ к конфигурации только для чтения. Уровень: 1-15.
- ✓ crw (configuration/execute read-write): Доступ к конфигурации и выполнению команд для чтения и записи. Уровень: 1-15.
- ✓ sro (status/statistics read-only): Доступ к статусу и статистике только для чтения. Уровень: 1-15.
- ✓ srw (status/statistics read-write): Доступ к статусу и статистике для чтения и записи. Уровень: 1-15.

- Уровень привилегий пользователя должен быть равен или превышать уровень авторизации, чтобы иметь доступ к этой группе.

Рекомендации:

- Команда web privilege group используется для **настройки уровня привилегий, необходимого для доступа к различным функциональным группам в веб-интерфейсе (GUI)** коммутатора. Это позволяет тонко настраивать права доступа для пользователей с разными уровнями привилегий (например, администраторов, операторов, гостей).
- **Четыре уровня доступа для каждой группы:**
  - ✓ cro **(Configuration Read-Only):** Позволяет только просматривать конфигурацию (но не изменять её).
  - ✓ crw **(Configuration Read-Write):** Позволяет просматривать и изменять конфигурацию.
  - ✓ sro **(Status/Statistics Read-Only):** Позволяет только просматривать статус и статистику.
  - ✓ srw **(Status/Statistics Read-Write):** Позволяет просматривать и, возможно, сбрасывать статистику.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **Как это работает:**
    1. Администратор задает для каждой функциональной группы (например, VLANs, QoS, Spanning_Tree) требуемый уровень привилегий для каждого типа доступа (cro, crw, sro, srw).
    2. Когда пользователь входит в веб-интерфейс, его уровень привилегий (заданный в учетной записи `username privilege <priv>`) сравнивается с этими значениями.
    3. Пользователь видит и может выполнять только те действия, для которых его уровень привилегий равен или превышает настроенный уровень доступа для соответствующей группы.
- **Пример:** Если для группы `VLANs` установить `crw 10`, то только пользователи с уровнем привилегий 10 и выше смогут создавать/изменять VLAN через веб-интерфейс. Пользователи с уровнем 5 увидят эту группу, возможно, только для чтения (если `sro 5`), или не увидят вовсе.
- **Значения по умолчанию:** Обычно для большинства групп `crw` требует уровень 15 (только администраторы), `cro` и `sro` — уровень 5 или ниже (гости), `srw` — уровень 10 (операторы).

Удаление конфигурации:

```
(config)# no web privilege group <group_name> level
```

Сбрасывает уровни привилегий для указанной группы к значениям по умолчанию.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Просмотр:

```
> show web privilege group <group_name> level
# show web privilege group <group_name> level
```

Примеры настройки:

1. **Назначение группе "Aggregation" (агрегация каналов) уровня crw 15 (только администраторы могут настраивать агрегацию):**

```
# configure terminal
(config)# web privilege group aggregation level crw 15
```

2. **Настройка прав для группы "VLANs":**

```
(config)# web privilege group vlan level crw 15 cro 10 sro 5 srw 10
```

3. **Настройка прав для группы "QoS":**

```
(config)# web privilege group qos level crw 15 cro 10 sro 5 srw 10
```

2

SEC.RU | Короткий путь к информации Скачано с sec.ru