НПО “Телеком”
Разработка, производство и внедрение
цифровых систем передачи данных

Руководство по эксплуатации

Коммутаторы Ethernet серии NTS

тел. +7 (3412) 573-040
https://npotelecom.ru
тех. поддержка:
+7 (3412) 57-30-32
help@npotelecom.ru

Версия 1.01

Целевая аудитория

Данное руководство по эксплуатации предназначено для технического персонала, выполняющего настройку и мониторинг устройства посредством WEB/CLI конфигуратора, а также процедуры по его установке и обслуживанию. Квалификация технического персонала предполагает знание работы протоколов и принципов построения Ethernet сетей, а также правила электробезопасности.

Данное руководство распространяется на модели: NTS-25080, NTS-25160, NTS-25240, NTS-25480, NTS-25080 (AC_R), NTS-25160 (AC_R), NTS-25240 (AC_R), NTS-25480 (AC_R), NTS-25080P, NTS-25160P, NTS-25240P, NTS-25480P, NTS-25080P (AC_R), NTS-25160P (AC_R), NTS-25240P (AC_R), NTS-25480P (AC_R), NTS-3508F, NTS-3516F, NTS-3524F, NTS-3532F, NTS-3548F, NTS-5508F, NTS-5516F, NTS-5520F.

Данное руководство включает общую информацию по настройке коммутаторов NTS, функционал устройств может отличаться в зависимости от модели.

Информация об уязвимостях программного обеспечения, рекомендации по их устранению и необходимости перехода на новую версию ПО, осуществляется путем рассылки на электронную почту заказчика.

№	Номер версии руководства и дата изм.	Внесенные изменения
1	1.00 от 22.06.2021	Первая версия
2	1.01 от 10.11.2026	Добавлены разделы: 1.3.1 Подключение аккумуляторной батареи; 4.2.65. Green Ethernet (Настройка энергосбережения); 4.1.14. Мониторинг и диагностика системных ресурсов. Дополнены разделы: 4.1.6. Конфигурация интерфейсов; 4.1.7. Настройка параметров физических интерфейсов; 4.2.31. MVR; 4.1.11.1. Настройка NTP и SNTP.

Оглавление

Целевая аудитория 2
1. Описание изделия 8
1.1. Назначение 8
1.2. Основные технические характеристики 8
1.3. Конструктивное исполнение 23
1.3.1. Подключение аккумуляторной батареи 29
1.4. Комплектация 30
1.5. Установка 31
2. Подключение к коммутатору 31
2.1. Подключение через Console (RS-232) 31
2.2. Подключение через Telnet, SSH 32
2.3. Подключение через Web-интерфейс 33
3. Загрузка ПО, изменение пароля доступа, сброс конфигурации через меню загрузчика. 35
3.1. Загрузка ПО через меню загрузчика uboot 35
3.2. Сброс настроек в заводские через меню загрузчика uboot. 35
3.3. Загрузка ПО через CLI 36
3.4. Загрузка ПО через WEB 37
4. CLI интерфейс 37
4.1. Базовые настройки 37
4.1.1. Режимы конфигурирования 37
4.1.2. Работа в командной строке 37
4.1.3. Создание учетной записи 38
4.1.4. Сохранение конфигурации, перезагрузка и возврат к заводским настройкам 38
4.1.4.1. Версионирование и откат конфигурации. 39
4.1.5. Настройка имени устройства 41
4.1.6. Конфигурация интерфейсов 42
4.1.7. Настройка параметров физических интерфейсов 43
4.1.8. Настройка L3 интерфейсов коммутатора 44
4.1.9. Настройка маршрутов 46
4.1.10. Настройка DNS и Domain Name 46
4.1.11. Настройка времени 48
4.1.11.1. Настройка NTP и SNTP 48
4.1.11.2. Конфигурация часового пояса 49
4.1.12. Конфигурация журнала системных сообщений 49
4.1.13. VLAN 50
4.1.14. Мониторинг и диагностика системных ресурсов 55

4.2. Расширенные настройки 56
4.2.1. DHCP 56
4.2.2. DHCPv4 56
4.2.3. DHCPv6 61
4.2.4. DHCPv6 опции 37 и 38....62
4.2.5. DHCP snooping и опция 82 66
4.2.6. DHCP-опции 60 и 61 69
4.2.7. DHCP Relay для IPv4 70
4.2.8. BOOTP....73
4.2.9. Уровни привилегий. Privilege Levels....74
4.2.10. Механизмы управления парольной политикой безопасности. Ограничение неуспешных попыток входа.....75
4.2.11. Конфигурация аутентификации, авторизации и учета. Authentication, Authorization, Accounting....77
4.2.12. Конфигурация SSH, Telnet, HTTP, HTTPS 78
4.2.13. Конфигурация управления доступом. Access Management Configuration.....80
4.2.14. SNMP 80
4.2.15. RMON 87
4.2.16. Port Security 88
4.2.17. NAS (Network Access Server)....91
4.2.18. ACL. Списки доступа....95
4.2.19. IP Source Guard. Защита IP-адреса источника 98
4.2.20. IP Source Guard....99
4.2.21. IPv6 Source Guard....99
4.2.22. ARP inspection. Инспекция ARP 100
4.2.23. Настройка Gratuitous ARP....101
4.2.24. ARP Proxy....102
4.2.25. Radius 104
4.2.26. Настройка TACACS+ 105
4.2.27. LAG....106
4.2.28. LACP....106
4.2.29. Настройка loop-protect (Loop Protection) 107
4.2.30. IPMC Profile....110
4.2.31. MVR....110
4.2.32. IPMC 114
4.2.33. IGMP Snooping....114
4.2.34. MLD Snooping....125
4.2.35. LLDP 128
4.2.36. LLDP MED 129

4.2.37. Таблица mac –адресов 132
4.2.38. Privatevlan 133
4.2.39. Изоляция портов (Protected ports) 135
4.2.40. VCL 135
4.2.41. Voice VLAN 136
4.2.42. QoS (Качество обслуживания) 138
4.2.43. Mirroring (Зеркалирование) 145
4.2.44. UPnP 146
4.2.45. GVRP 147
4.2.46. sFlow 148
4.2.47. UDLD 148
4.2.48. DDMI (интерфейс цифрового диагностического мониторинга) 149
4.2.49. MRP и MVRP 149
4.2.50. Link OAM 151
4.2.51. CFM 153
4.2.52. APS 156
4.2.53. ERPS 159
4.2.54. Настройка Spanning Tree 160
4.2.55. POE 174
4.2.56. Selective QinQ и Double QinQ 175
4.2.57. Динамическая маршрутизация 176
4.2.57.1. OSPF 176
4.2.57.2. RIP 180
4.2.57.3. IS-IS 184
4.2.57.4. BGP 187
4.2.57.5. BFD 195
4.2.57.6. PIM 197
4.2.57.7. PBR 199
4.2.58. VRF 201
4.2.59. Настройка протокола VRRP 205
4.2.60. Стекирование 206
4.2.61. Обновление ПО и автоматическая конфигурация 207
4.2.62. Конфигурация PPPoE Intermediate Agent 207
4.2.63. Настройка bpdu-tunnel-protocol (l2pt/BPDU Tunneling) 208
4.2.64. Control Plane Policing (CoPP) 213
4.2.65. Green Ethernet (Настройка энергосбережения) 214
5. Web-интерфейс 215
5.1. Основные команды управления настройками 216

5.2. Конфигурация 216
5.2.1. System. Системные настройки 217
5.2.2. Green Ethernet. Настройка энергосбережения. Настройка энергосбережения. ..224
5.2.3. Thermal Protection Configuration. Настройка защиты от перегрева. 225
5.2.4. Конфигурация портов. Ports 226
5.2.5. CFM Global Configuration 228
5.2.6. Автоматическое защитное переключение (APS) 232
5.2.7. ERPS 234
5.2.8. Конфигурирование DHCPv4 сервера 235
5.2.9. DHCPv6 239
5.2.10. Конфигурация пользователей. Users Configuration. 240
5.2.11. Уровни привилегий. Privilege Levels 241
5.2.12. Конфигурация аутентификации, авторизации и учета. Authentication, Authorization, Accounting 243
5.2.13. Конфигурация SSH 245
5.2.14. Конфигурация HTTPS 245
5.2.15. Конфигурация управления доступом. Access Management Configuration 246
5.2.16. SNMP 246
5.2.17. RMON 252
5.2.18. Network. Сеть 254
5.2.19. NAS (Network Access Server) 257
5.2.20. ACL. Списки доступа 261
5.2.21. IP Source Guard. Защита IP-адреса источника 265
5.2.22. IPv6 Source Guard. Защита IPv6-адреса источника 266
5.2.23. ARP inspection. Инспекция ARP 267
5.2.24. RADIUS 269
5.2.25. TACACS+ 271
5.2.26. Aggregation. Агрегирование 272
5.2.27. Link OAM. 274
5.2.28. Loop protection. Защита от петель 275
5.2.29. Spanning Tree 277
5.2.30. IPMC Profile (Профиль IPMC) 282
5.2.31. MVR 283
5.2.32. IPMC 285
5.2.32.1. IGMP Snooping 285
5.2.32.2. MLD Snooping 289
5.2.33. LLDP 292
5.2.34. POE 297

5.2.35. MAC Table. Таблица MAC-адресов 298
5.2.36. VLANs 299
5.2.37. VLAN Translation 303
5.2.38. Private VLANs (Частные VLAN) 303
5.2.39. VCL 304
5.2.40. QoS (Качество обслуживания) 307
5.2.41. Mirroring (Зеркалирование) 315
5.2.42. Voice VLAN. Голосовой VLAN 317
5.2.43. UPnP 318
5.2.44. MRP и MVRP 319
5.2.45. GVRP 320
5.2.46. sFlow 321
5.2.47. DDMI (интерфейс цифрового диагностического мониторинга) 323
5.2.48. UDLD 323
Приложение 1 – Обращение в службу технической поддержки 324

1. Описание изделия

1.1. Назначение

Коммутаторы Ethernet серии NTS-3508F, NTS-3516F, NTS-3524F, NTS-3532F, NTS-3548F, NTS-5508F, NTS-5516F, NTS-5520F – это высокопроизводительные коммутаторы концентрации (агрегации) уровня L3, разработанные ЗАО НПО «Телеком». Коммутаторы предназначены для использования в операторских сетях в качестве устройств агрегации и в центрах обработки данных. Порты коммутаторов поддерживают работу на скоростях 1 Гбит/с (SFP), 10 Гбит/с (SFP+), 25 Гбит/с (SFP28).

Коммутаторы Ethernet серии NTS-25080, NTS-25160, NTS-25240, NTS-25480, NTS-25080 (AC_R), NTS-25160 (AC_R), NTS-25240 (AC_R), NTS-25480 (AC_R), NTS-25080P, NTS-25160P, NTS-25240P, NTS-25480P, NTS-25080P (AC_R), NTS-25160P (AC_R), NTS-25240P (AC_R), NTS-25480P (AC_R) - управляемые коммутаторы уровня L3, разработанные ЗАО НПО «Телеком». Коммутаторы осуществляют подключение конечных пользователей и сетей предприятий малого и среднего бизнеса к сетям операторов связи с помощью высокоскоростных интерфейсов. Модели с индексом «P» в названии поддерживают функцию PoE\PoE+ для электропитания подключенных устройств, например, IP камер, беспроводных точек доступа, и других устройств, к которым невозможно или нежелательно проводить силовой электрический кабель.

1.2. Основные технические характеристики

Основные технические характеристики приведены в таблице 1.2.1.

Таблица 1.2.1 - Основные технические характеристики

Интерфейсы	
NTS-25080, NTS-25080 (AC_R)	8 портов 10/100/1000Base-T (RJ-45,8P8C) 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-25160, NTS-25160 (AC_R)	16 портов 10/100/1000Base-T (RJ-45,8P8C) 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-25240, NTS-25240 (AC_R)	24 порта 10/100/1000Base-T (RJ-45,8P8C) 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-25480, NTS-25480 (AC_R)	48 – 10/100/1000Base-T (RJ-45,8P8C) 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-25080P, NTS-25080P (AC_R)	8 портов 10/100/1000Base-T (RJ-45,8P8C POE/POE+) 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45)

	1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-25160P, NTS-25160P (AC_R)	16 портов 10/100/1000Base-T (RJ-45,8P8C) PoE/PoE+ 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-25240P, NTS-25240P (AC_R)	24 – 10/100/1000Base-T (RJ-45,8P8C) PoE/PoE+ 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-25480P, NTS-25480P (AC_R)	48 портов 10/100/1000Base-T (RJ-45, POE/POE+) 4 – 1000BASE-X/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-3508F	4 – Combo10/100/1000Base-T (RJ-45,8P8C) 8– 100BASE-FX/1000BASE-X 4 – 1000BASE-X/100BASE-FX/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-3516F	4 – Combo10/100/1000Base-T (RJ-45,8P8C) 16 – 100BASE-FX/1000BASE-X 4 – 1000BASE-X/100BASE-FX/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-3524F	4 – Combo10/100/1000Base-T (RJ-45,8P8C) 24 – 100BASE-FX/1000BASE-X 4 – 1000BASE-X/100BASE-FX/10GBASE-R (SFP/SFP+, 10G) 1 консольный порт RS-232 (RJ-45) 1 – 10/100/1000Base-TNPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-3532F	8 – 10/100/1000Base-T (RJ-45,8P8C) 12 – Combo 100BASE-FX/1000BASE-X (SFP) 12 – 1000BASE-X/10G BASE-R (SFP+, 10G) 1 – порт Console (отдельный консольный порт для управления) 1 – 10/100/1000Base-T NPI (RJ-45) 1 порт USB (доступен не во всех ревизиях)
NTS-3548F	48 портов 100Base-FX/1000Base-X 4 порта 1000/10000 Base-X (SFP/SFP+) 1 консольный порт RS-232 (RJ-45) 1 порт 10/100/1000 BASE-T (NPI) 1 порт USB (доступен не во всех ревизиях)
NTS-5508F	8 – 100BASE-FX/1000BASE-X/10GBASE-R (SFP/SFP+) 1 – порт Console, RS-232 (RJ-45) 1 – 10/100/1000Base-T NPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)

NTS-5516F	16 – 100BASE-FX/1000BASE X/10GBASE-R (SFP/SFP+) 1 – порт Console, RS-232 (RJ-45) 1 – 10/100/1000Base-T NPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
NTS-5520F	Поддерживает загружаемую программную конфигурацию основных портов: Конфигурация 1 20 –100BASE-FX/1000BASE-X/10GBASE-R (SFP/SFP+) Конфигурация 2 8 –100BASE-FX/1000BASE-X/10GBASE-R (SFP/SFP+) 4 – 25GBASE-xR Конфигурация 3 8 – 25GBASE-xR 1 – порт Console, RS-232 (RJ-45) 1 – 10/100/1000Base-T NPI (RJ-45) 1 – порт USB (доступен не во всех ревизиях)
Производительность	
NTS-25080, NTS-25080P, NTS-25080 (AC_R), NTS-25080P (AC_R)	Пропускная способность – 96 Гигабит в секунду Производительность на пакетах длиной 64 байта – 71,43 MPPS
NTS-25160, NTS-25160P, NTS-25160 (AC_R), NTS-25160P (AC_R)	Пропускная способность – 112 Гигабит в секунду Производительность на пакетах длиной 64 байта – 88,33 MPPS
NTS-25240, NTS-25240P, NTS-25240 (AC_R), NTS-25240P (AC_R)	Пропускная способность – 128 Гигабит в секунду (опционально 400 Гигабит в секунду) Производительность на пакетах длиной 64 байта – 95,23 MPPS (опционально 297,6 MPPS)
NTS-25480, NTS-25480P, NTS-25480 (AC_R), NTS-25480P (AC_R)	Пропускная способность – 176 Гигабит в секунду (опционально 400 Гигабит в секунду) Производительность на пакетах длиной 64 байта – 130,95 MPPS (опционально 297,6 MPPS)
NTS-3508F	Пропускная способность – 96 Гигабит в секунду (опционально 400 Гигабит в секунду) Производительность на пакетах длиной 64 байта – 71,42 MPPS (опционально 297,6 MPPS)
NTS-3516F	Пропускная способность – 112 Гигабит в секунду (опционально 400 Гигабит в секунду) Производительность на пакетах длиной 64 байта – 83,33 MPPS (опционально 297,6 MPPS)
NTS-3524F	Пропускная способность – 128 Гигабит в секунду (опционально 400 Гигабит в секунду) Производительность на пакетах длиной 64 байта – 95,23 MPPS (опционально 297,6 MPPS)
NTS-3532F	Пропускная способность – 400 Гигабит в секунду Производительность на пакетах длиной 64 байта – 297,6 MPPS
NTS-3548F	Пропускная способность – 176 Гигабит в секунду Производительность на пакетах длиной 64 байта – 130,95 MPPS (опционально 297,6 MPPS)

NTS-5508F	Пропускная способность – 176 Гигабит в секунду (опционально 400 Гигабит в секунду) Производительность на пакетах длиной 64 байта – 130,95 MPPS (опционально 297,6 MPPS)
NTS-5516F, NTS-5520F	Пропускная способность – 400 Гигабит в секунду Производительность на пакетах длиной 64 байта – 297,6 MPPS
Потребляемая мощность	
NTS-25080, NTS-25080 (AC_R)	Не более 13 Вт
NTS-25160, NTS-25160 (AC_R)	Не более 17 Вт
NTS-25240, NTS-25240 (AC_R)	Не более 30 Вт
NTS-25080P, NTS-25080P (AC_R)	Потребляемая мощность, без учета нагрузки PoE – 30 Вт Бюджет PoE – 240 Вт (опционально может быть увеличен или снижен)
NTS-25480, NTS-25480 (AC_R)	Не более 45 Вт
NTS-25160P, NTS-25240P, NTS-25160P (AC_R), NTS-25240P (AC_R)	Потребляемая мощность, без учета нагрузки PoE – 30 Вт Бюджет PoE – 350 Вт (опционально может быть увеличен или снижен)
NTS-25480P, NTS-25480P (AC_R)	Потребляемая мощность, без учета нагрузки PoE – 45 Вт Бюджет PoE – 720 Вт (опционально 760, 800, 1440 Вт)
NTS-3508F	Не более 29 Вт
NTS-3516F	Не более 33 Вт
NTS-3524F	Не более 35 Вт
NTS-5508F, NTS-5516F, NTS-5520F, NTS-3532F	Не более 45 Вт
NTS-3548F	Не более 90 Вт
Физические характеристики	
NTS-25080, NTS-25160, NTS-25240	Размеры (ВхШхГ), мм: 44x440x315 Масса: 3,9 кг
NTS-25080 (AC_R), NTS-25160 (AC_R), NTS-25240 (AC_R)	Размеры (ВхШхГ), мм: 44x440x372 Масса: 4,3 кг
NTS-25080P, NTS-25160P, NTS-25240P	Размеры (ВхШхГ), мм: 44x440x309 Масса: 4,5 кг
NTS-25480	Размеры (ВхШхГ), мм: 44x440x380 44x440x260 Масса: 4,6 кг
NTS-25480 (AC_R)	Размеры (ВхШхГ), мм: 44x440x384 Масса: 4,9 кг

NTS-25080P (AC_R), NTS-25160P (AC_R), NTS-25240P (AC_R)	Размеры (ВхШхГ), мм: 44x440x390 Масса: 6,5 кг
NTS-25480P	Размеры (ВхШхГ), мм: 44x440x371 Масса: 4,5 кг
NTS-25480P (AC_R)	Размеры (ВхШхГ), мм: 44x440x373 Масса: 6,75 кг
NTS-3508F, NTS-3516F, NTS-3524F, NTS-5508F, NTS-5516F, NTS-5520F	Размеры (ВхШхГ), мм: 44x440x310 Масса: 4 кг
NTS-3532F	Размеры (ВхШхГ), мм: 44x440x310 Масса: 4 кг
NTS-3548F	Размеры (ВхШхГ), мм: 44x440x310 Масса: 4,3 кг
Охлаждение	
NTS-25080, NTS-25160, NTS-25240, NTS-25080 (AC_R), NTS-25160 (AC_R), NTS-25240 (AC_R)	Активное, с помощью вентиляторов (опционально пассивное)
NTS-25480, NTS-25480 (AC_R)	Активное, с помощью вентиляторов (опционально пассивное)
NTS-25080P, NTS-25160P, NTS-25240P, NTS-25080P (AC_R), NTS-25160P (AC_R), NTS-25240P (AC_R)	Активное, с помощью вентиляторов (опционально пассивное)
NTS-25480P, NTS-25480P (AC_R)	Активное, с помощью вентиляторов
NTS-3508F, NTS-3516F, NTS-3524F, NTS-5508F, NTS-5516F, NTS-5520F	Активное, с помощью вентиляторов
NTS-3532F	2 вентилятора
NTS-3548F	2 вентилятора
Питание	
NTS-25080, NTS-25160, NTS-25240, NTS-25480P,	220 В AC (встроенный 1 блок питания)

NTS-3508F, NTS-3516F, NTS-3524F, NTS-5508F, NTS-5516F, NTS-5520F, NTS-3532F, NTS-3548F NTS-25080 (AC_R), NTS-25160 (AC_R), NTS-25240 (AC_R), NTS-25480 (AC_R), NTS-25080P (AC_R), NTS-25160P (AC_R), NTS-25240P (AC_R), NTS-25480P (AC_R)	– Один источник питания постоянного или переменного тока. – До двух источников питания постоянного или переменного тока с возможностью горячей замены.

Производительность:

- Размер буфера кадров – 4 Мегабайта
- Объем оперативной памяти – 2 Гигабайта
- Объем постоянного запоминающего устройства – 384 Мегабайта (Опционально 512 Мегабайт или 1024 Мегабайт)
- Таблица MAC-адресов – 32,768
- Таблица VLAN – 4096
- Количество правил MAC ACL (ingress/egress) – 2998 шт.
- Количество правил IPv4/IPv6 ACL – 2998/1499 шт./шт.
- Количество L2 Multicast групп – параметр является настраиваемым, возможные значения: 4,096; 2,200; 2,048; 1,200; 1,024
- Количество ARP-записей – 2048 (опционально до 10000)
- Link Aggregation Groups (LAG) – до 128 групп
- Количество портов в одном LAG – до 8
- Количество ECMP-групп – до 1024 шт.
- Качество обслуживания QoS – 32K
- Количество ACL (списков/записей) – 1024
- Количество маршрутов L3 IPv4 Unicast – до 15 000 шт.
- Количество маршрутов L3 IPv6 Unicast – до 7 500 шт.
- Количество маршрутов L3 IPv4 Multicast (IGMP Proxy, PIM) – 1028 шт.
- Количество маршрутов L3 IPv6 Multicast (IGMP Proxy, PIM) – 1656 шт.
- Количество OSPF-instance (сессий) – 20 шт.
- Максимальное количество OSPF соседств - 256 шт.
- Количество VRRP-маршрутизаторов – до 255
- Количество экземпляров MSTP – до 64
- Максимальное количество GRE туннелей –16 шт.
- Максимальный MTU для джамбо-фреймов, байт – до 14000
- Количество 802.1ad правил – от 8 до 4 096 шт
- Объем TCAM, шт – на вход до 4096 – на выход до 8192

– Размер Jumbo Frame – до 14000 байт

Физические характеристики:
– Рабочая температура окружающей среды – от -20 до +60°C AC
– Температура хранения – от -40 до +70°C
– Рабочая влажность – не более 80%
– Исполнение – 19″, 1U

Функции портов:
– Port Speed/Duplex Mode/Flow Ctrl
– Поддержка Auto MDI/MDIX
– 802.1Qbb Per Priority Flow Control
– Port Frame Size (Jumbo frames)
– Port State (administrative status)
– Port Status (link monitoring)
– Port Statistics (MIB counters)
– Port VeriPHY (Виртуальное тестирование кабеля)
– NPI port
– On-the-fly SFP detection
– DDMI
– UDLD
– IEEE 802.3ap 10G-KR
– IEEE 802.3ap 25G-KR (на коммутаторах с поддержкой 25G)
– POE/POE+ с поддержкой LLDP
– PoE IEEE802.3bt без поддержки LLDP
– Защита от блокировки очереди (HOL)
– Поддержка сверхдлинных кадров (Jumbo frames)
– Управление потоком (IEEE 802.3X)

Функции при работе с MAC-адресами:

– Независимый режим обучения в каждой VLAN
– Поддержка многоадресной рассылки (MAC Multicast Support)
– Регулируемое время хранения MAC-адресов
– Статические записи MAC (Static MAC Entries)
– Отслеживание событий MAC change на портах
– Логирование событий MAC Flapping

Поддержка IPv6:
– Функциональность IPv6 Host
– Совместное использование IPv4, IPv6

QoS:
– Прозрачный режим
– Классификация трафика (8 активных приоритетов)
– Default Priority для порта

- Пользовательский приоритет
- Маппинг входных приоритетов
- RR (Round Robin)
- SP (Strict Priority)
- WRR (Weighted Round Robin)
- WFQ
- FIFO
- PQ
- WFQ (weighted fair queuing)
- DWRR (deficit weighted round robin)
- DRR (deficit round robin)
- CBQ (Class-Based Queueing)
- Три цвета маркировки трафика
- Поддержка QoS Control List (QCL Mode)
- Назначение меток CoS/DSCP на основании QCL
- Перемаркировка DSCP to COS, COS to DSCP
- Настройка приоритета 802.1p для VLAN управления
- Global Storm Control для UniCast, MultiCast и BroadCast
- Управление полосой пропускания
- Поддержка алгоритма управления очередями RED (Random Early Discard)
- Port policers
- Назначение VLAN на основании QCL
- Queue policers очередей
- Global/VCAP (ACL) policers
- QoS классификация трафика на основании ACL
- Port egress shaper
- Queue egress shapers
- Перемаркировка DiffServ (RFC2474)
- Tag remarking
- Режим планировщика

Функции L2:

- Auto MAC addr. Learning/Ageing
- Статические MAC адреса
- Virtual LAN (VLAN)
- Двухсторонний VLAN translation
- Односторонний VLAN translation (входной/выходной)
- Объем TCAM – до 4096
- Стекирование
- Private VLAN Static
- Port Isolation Static
- MAC-based VLAN
- Protocol-based VLAN
- IP subnet-based VLAN
- VLAN Trunking

- iPVLAN Trunking
- Поддержка GARP VLAN registration (GVRP)
- Поддержка Multiple Registration Protocol (MRP)
- Поддержка Multiple VLAN Registration Protocol (MVRP)
- GMRP (GARP Multicast Registration Protocol)
- Поддержка IEEE-802.1ad Provider Bridge (Native or Translated VLAN)
- PVSTP+ (экземпляр связующего дерева, при котором в каждом VLAN работает отдельный экземпляр STP)
- RPVSTP+
- Поддержка протокола STP (Spanning Tree Protocol, IEEE 802.1d)
- Поддержка протокола RSTP (Rapid Spanning Tree Protocol, IEEE 802.1w)
- Поддержка протокола MSTP (Multiple Spanning Tree Protocol, IEEE 802.1s)
- Поддержка протокола Rapid-PVST+
- MAC Flapping
- Loop Guard
- Link Aggregation статический (без протокола)
- Link Aggregation протокол LACP
- AGGR/LACP user interface alignment with Industry standard
- UNI LAG (LACP) 1:1 Active/Standby
- LACP Revertive/Non-revertive
- LACP loop free operation
- BPDU Guard & Restricted Role
- IGMPv2 snooping
- IGMPv3 snooping
- MLDv1 snooping
- MLDv2 snooping
- Профили фильтрации IGMP
- IPMC throttling, filtering, leave proxy
- MVR
- Поддержка MVR profile
- Voice VLAN
- Поддержка Q-in-Q
- Поддержка Selective Q-in-Q
- DHCP snooping
- ARP inspection
- Port Mirroring
- Flow mirroring
- Rmirror (Удаленное зеркалирование)
- PIM-Snooping, Flex-link
- Multi-Switch Link Aggregation Group (MLAG)
- IP SLA
- Поддержка стекирования, количество устройств в стеке до 8 штук (опционально до 12)
- Количество отдельно работающих экземпляров протокола связующего дерева – 64

- Loopback Detection
- STP Root Guard
- Spanning Tree Fast Link option
- STP BPDU Guard
- G.8032v2 ERPS
- BPDU Filtering

Функции:
- STP Loop Guard
- Изоляция портов
- Поддержка Layer 2 Protocol Tunneling (L2PT)
- IGMP proxy fast-leave
- Поддержка протокола VRRP
- Поддержка LAG Balancing Algorithm
- Диагностика оптического трансивера
- Поддержка IGMP Snooping fast-leave
- Поддержка функций IGMP Proxy-report
- Поддержка авторизации IGMP через RADIUS
- Поддержка IGMP Querier
- Автоматическое резервирование (backup) файла конфигурации по TFTP/SFTP
- SNTP (Simple Network Time Protocol)
- Traceroute
- Возможность обработки трафика управления с двумя заголовками IEEE 802.1Q
- Управление доступом к коммутатору – уровни привилегий для пользователей
- Блокировка интерфейса управления
- Локальная аутентификация
- Фильтрация IP-адресов для SNMP
- Клиент Telnet, клиент SSH
- Сервер Telnet, сервер SSH
- Поддержка макрокоманд
- Журналирование вводимых команд по протоколу TACACS+
- Автоматическая настройка DHCP
- Добавление тега PPPoE Circuit-ID
- Flash File System
- Команды отладки
- Механизм ограничения трафика в сторону CPU
- Шифрование пароля
- Ping (поддержка IPv4/IPv6)
- Поддержка нескольких версий файлов конфигурации
- Поддержка IP Sourse Goard
- Наличие механизмов управления UniCast, MultiCast и BroadCast-трафиком для предотвращения UniCast, MultiCast и BroadCast-штормов
- Функция фильтрации трафика, предназначенная для модуля управления

- Наличие механизмов фильтрации трафика без сохранения информации о сессии (stateless)
- Проверка подлинности на основе MAC-адреса Port Security
- Поддержка алгоритма управления очередями WRR (weighted round robin)
- Поддержка доступа к веб-интерфейсу по SSL
- Наличие механизма обнаружения отказа системы охлаждения.
- Наличие механизма обнаружения отказа блоков питания
- Наличие связи IP-MAC-Port
- Версии поддерживаемых MLD Snooping 1,2
- MLD Snooping fast-leave
- Поддержка автосогласования (autonegotiation)
- Наличие функции Proxy ARP
- Функции L2 Multicast: MLD Snooping Querier, IGMP Snooping v1,2,3, IGMP Snooping Fast Leave, MLD Snooping v1,2, IGMP и MLD Snooping Querier, MVR, GMRP
- Наличие функций защиты от подмены IP-адреса (IP-spoofing)
- Возможность загрузки файлов на устройство по нешифрованному протоколу передачи файлов
- Поддержка механизма полисинга трафика (traffic policing)
- Наличие защиты от смены корневого коммутатора в домене STP (Root Guard/Protection)
- Поддержка стандарта Selective Double (VLAN)
- Поддержка виртуальных таблиц коммутации и маршрутизации (Virtual Routing and Forwarding)
- Поддержка стандарта STP Loopback Detection
- Наличие дополнительной защиты от возникновения петель в домене STP (Loop Guard/Protection
- Поддержка стандарта Multicast VLAN registration
- Поддержка механизма маркировки трафика Type of Service (ToS)
- Возможность загрузки файлов на устройство по шифрованному протоколу передачи файлов
- Наличие связи IP-MAC-Port
- Поддержка стандарта 802.3az
- Наличие аппаратного ускорителя маршрутизации/пересылки (hardware routing/forwarding accelerator)
- Поддержка гранулярного контроля доступа к устройству (granular access control)

Функции мониторинга:
- Статистика интерфейсов
- Поддержка мониторинга загрузки CPU по задачам и очередям
- Мониторинг загрузки оперативной памяти (RAM)
- Мониторинг температуры
- Мониторинг TCAM

Резервирование:
- G.8031 – 1:1 Port protection (резервирование портов)

- G.8032 – Ring protection (Кольцевое резервирование)
- G.8032 – Ring protection v2 (Кольцевое резервирование)

Функции L3 и маршрутизация:
- Функция DHCP relay Option 82
- Поддержка протокола BFD
- Количество L3 интерфейсов, штук – параметр является настраиваемым, возможные значения: до 2050
- Количество L3 интерфейсов -20 vlan, 5 IPv4-адресов в каждом vlan, 512 IPv6 GUA суммарно для всех vlan
- VRRP v2, v3
- Количество VRRP маршрутизаторов 255
- Количество Loopback-интерфейсов, штук – параметр является настраиваемым, возможные значения: от 1 до 1024
- Поддержка протокола BGP
- UPNP
- IPv4 L3 Static Routing (Статическая маршрутизация)
- RFC2992 (ECMP) поддержка HW based L3 static routing
- Динамическая маршрутизация RIPv2 (RFC 2453)
- Динамическая маршрутизация OSPFv2 (RFC 2328)
- Динамическая маршрутизация OSPFv3 (IPv6) (RFC 5340)
- RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option
- RFC 3137 OSPF Stub Router Advertisement
- IPv6 L3 Static Routing
- RFC-1812 L3 checking (version, IHL, checksum, etc)
- Количество поддерживаемых VRF до 1023 шт.
- Поддержка мультипротокольного расширения протокола динамической маршрутизации BGP (Multiprotocol Extensions for BGP; MBGP)
- MSDP, IP Unnumbered
- Поддержка маршрутизации на основе политик (Policy-Based Routing; PBR)

Функции обеспечения безопасности:
- Port-Based 802.1X
- Критерии фильтрации ACL Port, Vlan ID, Ethertype, CoS, MAC source address, MAC destination address, IPv4 source address, IPv4 destination address, IPv4 DSCP, IPv4 Preference, IPv4 ToS, IPv4 security option, IPv4 protocol numbers, IPv4 custom field, IPv6 source address, IPv6 destination address, TCP/UDP source port, TCP/UDP destination port, TCP/UDP flags, Time-base
- Тип организации списков контроля доступа (ACL): DSCP, IP-протокол, MAC/IP/IPv6-адресов источника/назначения, Номер порта TCP/UDP, Порт коммутатора, Приоритет IEEE 802.1p, VLAN ID, EtherType, TOS, Preference, Содержимого пакета, определяемого пользователем (User Defined Bytes), типа IP-протокола
- Аппаратная обработка ACL: Фильтрация и классификация трафика L2–L4 осуществляются аппаратно на базе встроенной ассоциативной памяти TCAM (ASIC) без

вовлечения центрального процессора (CPU) устройства, что обеспечивает обработку данных на полной скорости физических портов (без потери производительности)
- Основные функции качества обслуживания (QoS) и ограничения скорости: Ограничение скорости на портах (shaping), Ограничение скорости (policing) согласно sr-TCM и tr-TCM, Поддержка класса обслуживания IEEE 802.1p, Обработка очередей по алгоритмам Strict Priority/Weighted
- Single 802.1X
- Multiple 802.1X
- MAC-Based Authentication
- VLAN Assignment
- QoS Assignment
- Guest VLAN (Гостевой VLAN)
- RADIUS Authentication and Authorization
- RADIUS Accounting
- MAC Address Limit
- Persistent MAC learning
- IP MAC binding
- IP/MAC binding dynamic to static
- TACACS+ Authentication and Authorization
- TACACS+ Command Authorization
- TACACS+ Accounting
- Web & CLI Authentication
- Авторизация (15 уровней доступа)
- ACLs for filtering/policing/port copy
- Защита от DoS-атак
- IP source guard
- Secure FTP Client
- Поддержка Radius EAP
- Поддержка протоколов AAA: Local, Radius, 802.1x Tacacs+
- Проверка подлинности на основе MAC-адреса, ограничение количества MAC-адресов, статические MAC-адреса
- Проверка подлинности по портам на основе IEEE 802.1x
- Сегментация трафика
- Предотвращение атак BPDU
- PPPoE Intermediate agent
- Dynamic ARP Inspection
- DHCPv6 Snooping
- DHCP Option 43
- Фильтрация DHCP-клиентов
- IPv6 Source Guard
- Поддержка функции IPv6 ND Inspection
- Поддержка функции IPv6 RA Guard
- L2-L3-L4 ACL (Access Control List)

– IPv6 ACL

Синхронизация:
– NTPv4 Client
– Возможность работы в качестве NTP-сервера (NTP server)

OAM & Тестирование:
– 802.3ah: Variable, request, response
– 802.3ah: Discovery process, information. Event notification, loopback
– 802.3ah: Dying Gasp Enhanced
– 802.3ah: Dying Gasp SNMP Trap
– 802.3ah Ethernet Link OAM
– 802.3ah Unidirectional Link Detection (протокол обнаружения однонаправленных линков) UDLD
– Continuity Check (ETH-CCM) проверка целостности
– IS-, OS-, PS-, SID-TLV
– ERPS с использованием ETH-CCM и ETH-RAPS
– Аппаратное ускорение OAM
– Встроенный датчик отказа блока питания
– Встроенный датчик отказа системы охлаждения

Управление:
– Поддержка зеркалирования трафика RSPAN; sFlow; SPAN
– Dual CPU (Application variant with JSON)
– DHCP Client (RFC 2131)
– DHCP Server (RFC 2131)
– DHCP Server support for DHCP relay packets
– Per port DHCP
– DHCPv6 Client (RFC 3315)
– DHCPv6 Relay Agent (RFC 3315)
– DHCPv6-ShieldProtecting against Rogue DHCPv6 Servers (RFC 7610)
– DNS client, relay (RFC 1035)
– Сервер DNS (Resolver)
– IPv4/IPv6 Ping
– IPv4/IPv6 Traceroute
– HTTP сервер
– CLI – Console Port
– CLI – Telnet
– Соответствие промышленному стандарту CLI
– Списки контроля доступа (Management ACL)
– Industrial Standard Configuration
– Industrial Standard CLI debug commands
– Port Description CLI
– Фильтры доступа к управлению

- Поддержка HTTPS
- Поддержка SSHv2
- Управление по IPv6
- IPv6 Ready Logo PHASE2 (только host)
- ICMPv6 (RFC4884)
- Системный Syslog
- Восстановление пароля
- ZTP (Zero-touch provisioning)
- Загрузка обновления ПО через web интерфейс
- SNMP агент v1/v2c/v3
- RMON (Группы 1, 2, 3 и 9)
- RMON аварии и события (CLI, web)
- IEEE 802.1AB-2005 Link Layer Discovery LLDP
- TIA 1057 LLDP-MED
- sFlow
- FTP Client
- Поддержка загрузки и выгрузки конфигурации по промышленному стандарту
- Возможность загрузки и выгрузки конфигурации и программного обеспечения TFTP: SCP, SFTP, SSH, TFTP, локально на внешний носитель
- Поддержка протоколов и средств управления DHCP client, LACP, BFD, BGP, BGPv6, IS-IS, OSPFv2, OSPFv3, RIPv1, RIPv2, AAA, TSN, Static, DHCP server, DHCP relay, DHCPv6 client, BootP client, Active Directory, IGMP Proxy(RFC 4605), PIM SM, Local, NTP client, Стандарт ERPS(G.8032v2), Стандарт MSTP IEE 802.1s, SSHv1, Telnet, SSHv2, PIM, MRP, IGMP , sFlow , Diameter, LDAP , LLDP , PPP PPPoE, RADIUS, SNMPv1, SNMPv2c, SNMPv3, HTTP, HTTPS, SFTP, NTP, DHCP, DNS, ICMP, 802.1X, TCP, SNMP, FTP, SSH, RMON, SMON, SCP, IPv4

Поддержка стандартных MIBов:
- RFC 2674 VLAN MIB
- IEEE 802.1Q Bridge MIB 2008
- RFC 2819 RMON (Group 1, 2. 3 и 9)
- RFC 1215 TRAPS MIB
- RFC 4188 Bridge MIB
- RFC 4292 IP Forwarding Table MIB
- RFC 4293 Management Information Base for the Internet Protocol (IP)
- RFC 5519 Multicast Group Membership Discovery MIB
- RFC 4668 RADIUS auth. Client MIB
- RFC 4670 RADIUS Accounting MIB
- RFC 3635 Ethernet-like MIB
- RFC 2863 Interface Group MIB using SMI v2
- RFC 3636 802.3 MAU MIB
- RFC 4133 Entity MIB version 3
- RFC 4878 Link OAM MIB
- RFC 3411 SNMP Management Frameworks

– RFC 3414 User-based Security Model for SNMPv3
– RFC 3415 View-based access Control Model for SNMP
– RFC 2613 SMON – PortCopy
– IEEE 802.1 MSTP MIB
– Private MIB
– IEEE 802.1AB LLDP-MIB (LLDP MIB included in a clause of the STD)
– IEEE 802.3ad (LACP MIB included in a clause of the STD)
– IEEE 802.1X (PAE MIB included in a clause of the STD)
– TIA 1057 LLDP-MED (MIB is part of the STD)

Восстановление:
– Холодный старт
– Теплый старт

1.3. Конструктивное исполнение

Коммутаторы Ethernet серии NTS моделей NTS-25080, NTS-25160, NTS-25240, NTS-25480, NTS-25080 (AC_R), NTS-25160 (AC_R), NTS-25240 (AC_R), NTS-25480 (AC_R), NTS-25080P, NTS-25080P (AC_R), NTS-25160P, NTS-25160P (AC_R), NTS-25240P, NTS-25240P (AC_R), NTS-25480P, NTS-25480P (AC_R), NTS-3508F, NTS-3516F, NTS-3524F, NTS-3532F, NTS-3548F, NTS-5508F, NTS-5516F, NTS-5520F выполнены в металлическом корпусе 1U и предназначены для установки в стойку 19”. Внешний вид изделий представлен на рисунках 1.3.1-1.3.16. Внешний вид изделий может отличаться от фактического в зависимости от модификации и типа электропитания.

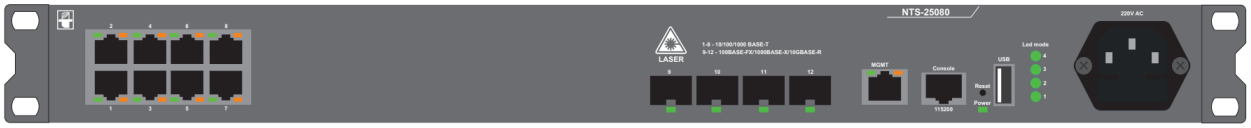


Рисунок 1.3.1 – Внешний вид NTS-25080/NTS-25080 (AC_R)

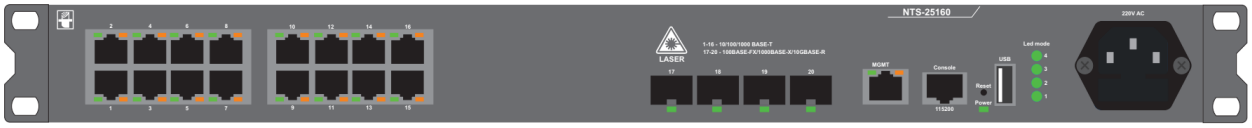


Рисунок 1.3.2 – Внешний вид NTS-25160/NTS-25160 (AC_R)

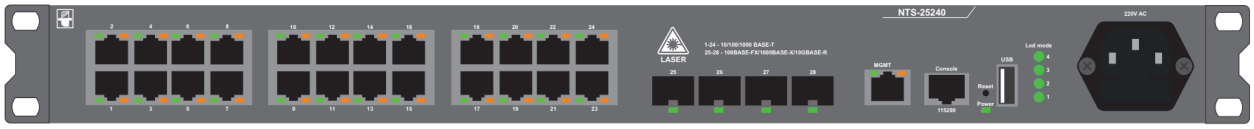


Рисунок 1.3.3 – Внешний вид NTS-25240/NTS-25240 (AC_R)

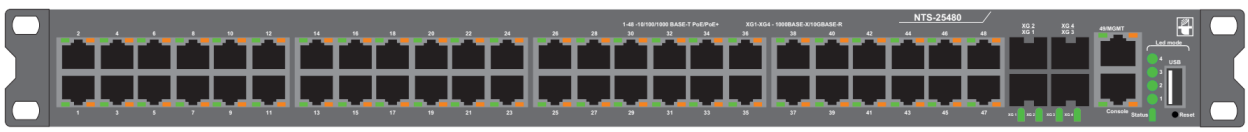


Рисунок 1.3.4 – Внешний вид NTS-25480/NTS-25480 (AC_R)



Рисунок 1.3.5 – Внешний вид NTS-25080P/NTS-25080P (AC_R)

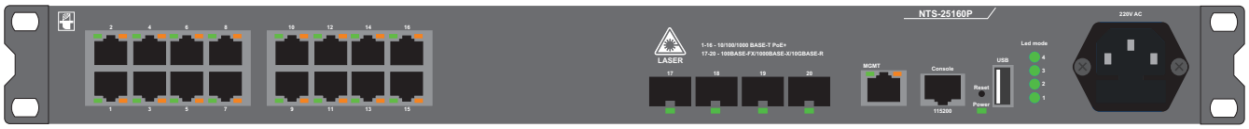


Рисунок 1.3.6 – Внешний вид NTS-25160P/NTS-25160P (AC_R)

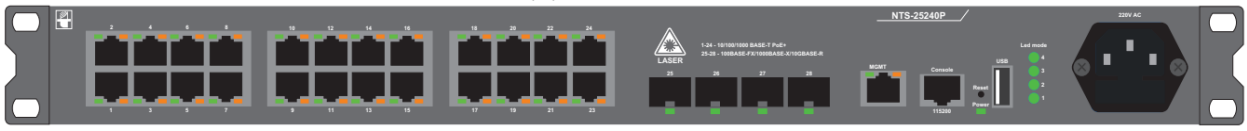


Рисунок 1.3.7 – Внешний вид NTS-25240P/NTS-25240P (AC_R)

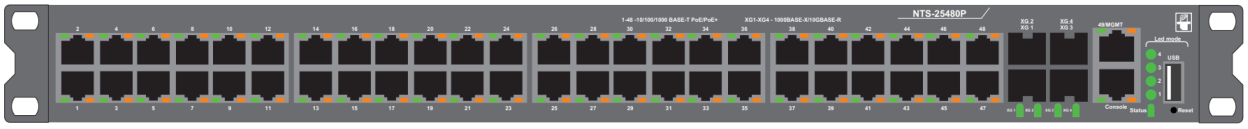


Рисунок 1.3.8 – Внешний вид NTS-25480P/NTS-25480P (AC_R)



Рисунок 1.3.9 – Внешний вид NTS-5508F



Рисунок 1.3.10 – Внешний вид NTS-5516F



Рисунок 1.3.11 – Внешний вид NTS-5520F



Рисунок 1.3.12 – Внешний вид NTS-3508F



Рисунок 1.3.13 – Внешний вид NTS-3516F



Рисунок 1.3.14 – Внешний вид NTS-3524F

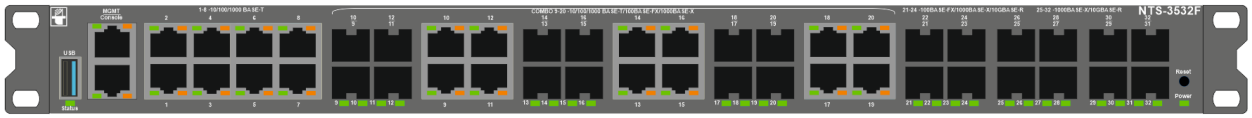


Рисунок 1.3.15 – Внешний вид NTS-3532F

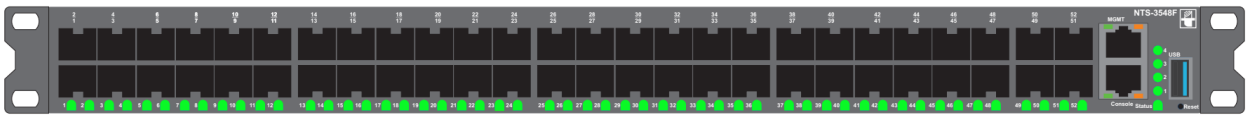


Рисунок 1.3.16 – Внешний вид NTS-3548F

Описание функциональных элементов лицевой панели для NTS-25080/NTS-25080 (AC_R)/NTS-25080P/NTS-25080P (AC_R), NTS-25160/NTS-25160 (AC_R)/NTS-25160P/NTS-25160P (AC_R), NTS-25240/NTS-25240 (AC_R)/NTS-25240P/NTS-25240P (AC_R) приведено в таблице 1.3.3, рисунок 1.3.17-1.3.19.

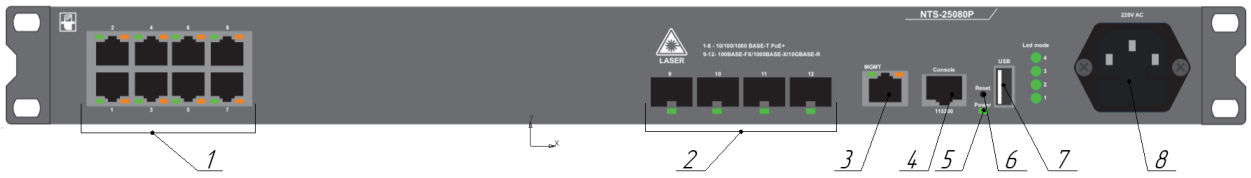


Рисунок 1.3.17 – Описание элементов лицевой панели NTS-25080/NTS-25080 (AC_R)/NTS-25080P/NTS-25080P (AC_R)

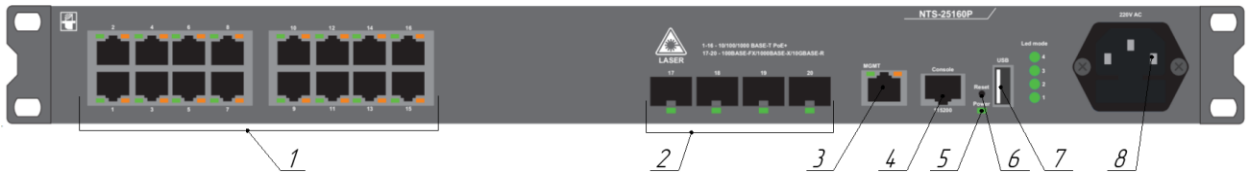


Рисунок 1.3.18 – Описание элементов лицевой панели NTS-25160/NTS-25160 (AC_R)/NTS-25160P/NTS-25160P (AC_R)

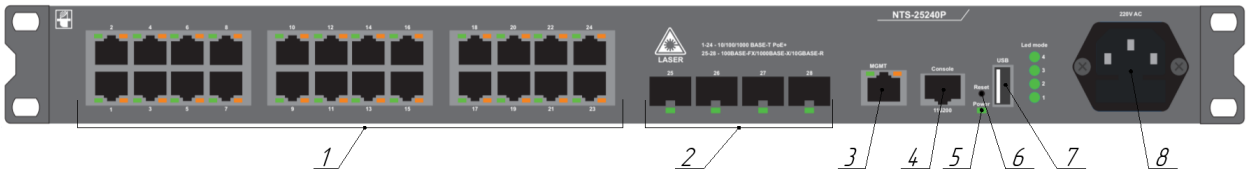


Рисунок 1.3.19 – Описание элементов лицевой панели NTS-25240/NTS-25240 (AC_R)/NTS-25240P/NTS-25240P (AC_R)

Таблица 1.3.3 – Описание элементов лицевой панели NTS-25080/NTS-25080 (AC_R)/NTS-25080P/NTS-25080P (AC_R), NTS-25160/NTS-25160 (AC_R)/NTS-25160P/NTS-25160P (AC_R), NTS-25240/NTS-25240 (AC_R)/NTS-25240P/NTS-25240P (AC_R)

№	Наименование	Описание
1	1-24	Для NTS-25080, NTS-25080 (AC_R), NTS-25160, NTS-25240 – порты 10/100/1000BASE-T (RJ-45) Для NTS-25080P, NTS-25160P, NTS-25240P, NTS-25080P (AC_R), NTS-25160P (AC_R), NTS-25240P (AC_R) – порты 10/100/1000BASE-T (RJ-45), с поддержкой POE по стандартам IEEE 802.3af-2003, IEEE 802.3at-2009
2	XG1-XG4	Слоты для установки трансиверов 1000BASE-X/10GBASE-R (SFP/SFP+, 10G)
3	NPI	NPI порт 10/100/1000Base-T (RJ-45)
4	Console	Консольный порт для подключения по протоколу RS-232
5	Power	Индикатор электропитания
6	Reset Factory	Функциональная кнопка сброса
7	USB	USB порт, доступен не во всех ревизиях
8	220V AC	Разъем подключения электропитания от сети переменного тока 220 В

Описание функциональных элементов лицевой панели для NTS-25480/NTS-25480P/NTS-25480P (AC_R) приведено в таблице 1.3.4, рисунок 1.3.20.

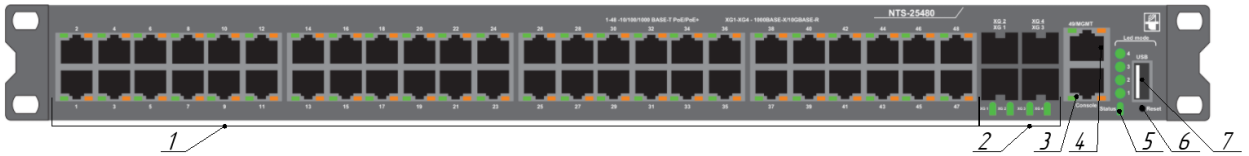


Рисунок 1.3.20 – Описание элементов лицевой панели NTS-25480/NTS-25480 (AC_R)/NTS-25480P/NTS-25480P (AC_R)

Таблица 1.3.4 – Описание элементов лицевой панели NTS-25480/NTS-25480 (AC_R)/NTS-25480P/NTS-25480P (AC_R)

№	Наименование	Описание
1	1-48	Для NTS-25480/NTS-25480 (AC_R) – порты 10/100/1000BASE-T (RJ-45) Для NTS-25480P/NTS-25480P (AC_R) – порты 10/100/1000BASE-T (RJ-45), с поддержкой POE по

		стандартам IEEE 802.3af-2003, IEEE 802.3at-2009
2	XG1-XG4	Слоты для установки трансиверов 1000BASE-X/10GBASE-R (SFP/SFP+, 10G)
3	Console	Консольный порт для подключения по протоколу RS-232
4	NPI	NPI порт 10/100/1000Base-T (RJ-45)
5	Status	Индикатор состояния
6	Reset Factory	Функциональная кнопка сброса
7	USB	USB порт, доступен не во всех ревизиях

Описание функциональных элементов лицевой панели для NTS-3524F, NTS-3532F приведено в таблице 1.3.5, рисунок 1.3.21.

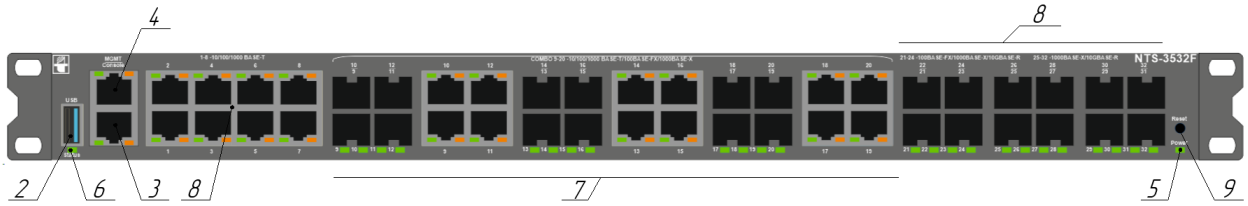


Рисунок 1.3.21 – Описание элементов лицевой панели

Таблица 1.3.5 – Описание элементов лицевой панели

№	Наименование	Описание
2	USB	USB порт (доступен не во всех ревизиях)
3	Console	Консольный порт для подключения по протоколу RS-232
4	NPI	NPI порт 10/100/1000Base-T (RJ-45) для управления
5	Power	Индикатор электропитания
6	Status	Индикатор состояния устройства
7	Combo порты	Порты Combo 10/100/1000Base-T (RJ-45,8P8C) - 100BASE-FX/1000BASE-X/10GBASE-R (SFP/SFP+)
8	Основные порты	Порты устройства с соответствующими индикаторами подключения: 1-8 – 10/100/1000Base-T 21-24 – 100BASE-FX/1000BASE-X/10GBASE-R (SFP/SFP+) 25-32 – 1000BASE-X/10GBASE-R (SFP/SFP+)
9	Reset	Кнопка сброса

Описание функциональных элементов лицевой панели для NTS-3508F, NTS-3516F, NTS-5508F, NTS-5516F, NTS-5520F приведено в таблице 1.3.6, рисунок 1.3.22.

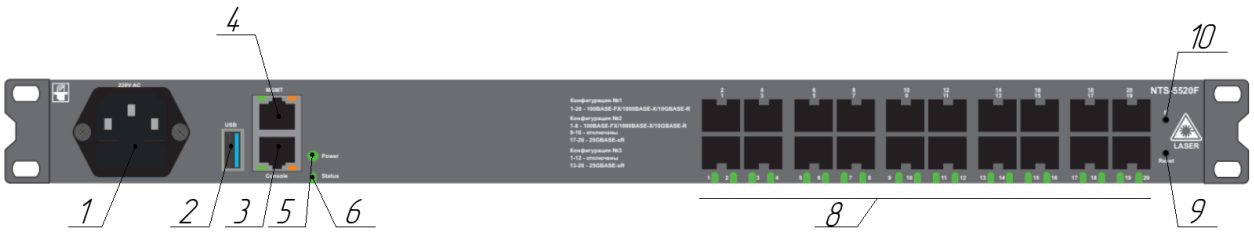


Рисунок 1.3.22 – Описание элементов лицевой панели

Таблица 1.3.6– Описание элементов лицевой панели

№	Наименование	Описание
1	220V AC	Разъем подключения электропитания от сети переменного тока 220 В, при вариантах питания DC, DC-DC разъем отсутствует
2	USB	USB порт (доступен не во всех ревизиях)
3	Console	Консольный порт для подключения по протоколу RS-232
4	NPI	NPI порт 10/100/1000Base-T (RJ-45) для управления
5	Power	Индикатор электропитания
6	Status	Индикатор состояния устройства
8	Основные порты	Порты устройства с соответствующими индикаторами подключения: NTS-3516F: 1-16 – 100BASE-FX/1000BASE-X 17-20 –1000BASE-X/10GBASE-R (SFP/SFP+) NTS-3508F: 1-8 – 100BASE-FX/1000BASE-X 9-12 –1000BASE-X/10GBASE-R (SFP/SFP+) NTS-5508F: 1-8 –1000BASE-X/10GBASE-R (SFP/SFP+) NTS-5516F: 1-16 –1000BASE-X/10GBASE-R (SFP/SFP+) NTS-5520F: Поддерживает загружаемую программную конфигурацию основных портов: Конфигурация 1 1-20 – 100BASE-FX/1000BASE-X/10GBASE-R (SFP/SFP+) Конфигурация 2 1-8 – 100BASE-FX/1000BASE-X/10GBASE-R (SFP/SFP+) 9-16 - отключены 17-20 – 25GBASE-xR Конфигурация 3 1-12 - отключены

		13-20 – 25GBASE-xR
9	Reset	Кнопка сброса
10	F	Функциональная кнопка

Описание функциональных элементов лицевой панели для NTS-3548F приведено в таблице 1.3.7, рисунок 1.3.23.

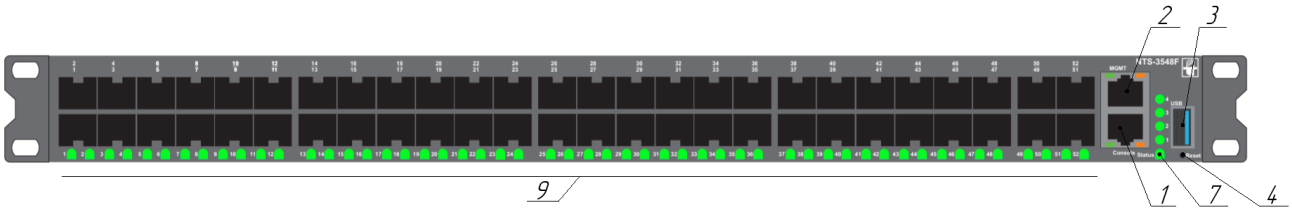


Рисунок 1.3.23 – Описание элементов лицевой панели

Таблица 1.3.7 – Описание элементов лицевой панели

№	Наименование	Описание
1	Console	Консольный порт для подключения по протоколу RS-232
2	NPI	NPI порт 10/100/1000Base-T (RJ-45) для управления
3	USB	USB порт (доступен не во всех ревизиях)
4	Reset	Кнопка сброса
7	Status/System status	Индикатор состояния устройства
9	Основные порты	1-52 – 100BASE-FX/1000BASE-X 49-52 –1000BASE-X/10GBASE-R (SFP/SFP+)

1.3.1. Подключение аккумуляторной батареи

Некоторые модели коммутаторов, для обеспечения бесперебойной работы в случае непродолжительного отсутствия электропитания от сети, оборудованы разъемом для подключения аккумуляторной батареи (Рисунок 1.3.1.1).

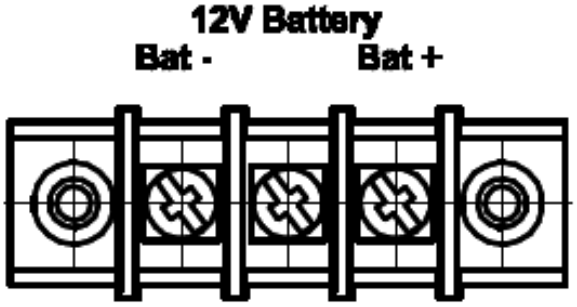


Рисунок 1.3.1.1

При наличии основного питания от сети подключенная аккумуляторная батарея находится в режиме автоматического подзаряда (при наличии такой необходимости, определяемой контроллером). В случае прекращения подачи основного питания устройство переходит на автономную работу от АКБ. Переключение на резервный источник

происходит без прерывания рабочих процессов оборудования, что гарантирует полную сохранность текущих данных и исключает программные сбои.

Подключение внешней резервной аккумуляторной батареи (рисунок 1.3.1.2) к устройству производится к клеммам BAT+ (положительный полюс) и BAT- (отрицательный полюс) с обязательным соблюдением полярности. Для обеспечения безопасности и надежности системы на линии подключения АКБ рекомендуется установить внешний автоматический выключатель.

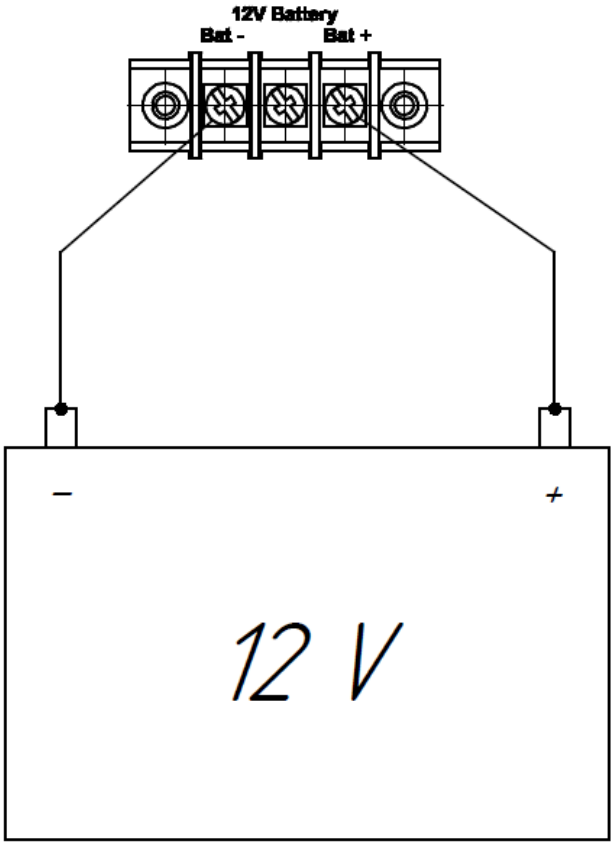


Рисунок 1.3.1.2

1.4. Комплектация

Комплектация может быть изменена в зависимости от условий поставки и пожеланий заказчика.

Базовая комплектация изделия:

–Паспорт;

–Комплект крепежа для установки в стойку;

–Кабель питания;

–Предохранитель (при необходимости);

–Руководство по эксплуатации – * шт;

*Доступно для скачивания по ссылке https://npotelecom.ru/download/, поставляется опционально на CD диске.

1.5. Установка

При работе с оборудованием необходимо соблюдение требований «Правил техники безопасности при эксплуатации электроустановок потребителей». Запрещается работать с оборудованием лицам, не допущенным к работе в соответствии с требованиями техники безопасности в установленном порядке. Эксплуатация устройства должна производиться инженерно-техническим персоналом, прошедшим специальную подготовку.

При получении коробки с устройством необходимо проверить целостность упаковки, эксплуатационной документации, упаковки с комплектом монтажных частей и их количества. Перед установкой устройство должно быть выдержано определенный период времени в том помещении, в котором будет установлено, для выравнивания температуры и избегания образования конденсата.

Расположите изделие в стойке 19” таким образом, чтобы расстояние между соседними устройствами было не менее 1U. При необходимости отрегулируйте положение кронштейнов относительно корпуса. Избегайте перекрывания вентиляционных отверстий в устройстве.

Зафиксируйте изделие в стойке при помощи комплекта крепежа (рисунок 1.5.1).



1 – гайка скоба, 2 – шайба, 3 – винт.

Рисунок 1.5.1 – Фиксация изделия в стойке вид сбоку

Заземлите изделие. Подключите провод заземления к специальному винту на корпусе изделия. Подключите электропитание. Индикатор «Power» должен загореться зеленым. Подключите патч корды в соответствии с требуемой конфигурацией.

2. Подключение к коммутатору

Настройка параметров и управление коммутатором осуществляется: через порт Console при подключении к нему внешнего терминала, в качестве которого может использоваться персональный компьютер; через порт Ethernet, управление осуществляется посредством SNMP, Telnet, SSH или Web-интерфейса.

2.1. Подключение через Console (RS-232)

Для установления соединения между консольным портом коммутатора и ПК, необходимо выполнить действия:

– соединить Serial-порт ПК с портом Consoleкоммутатора консольным кабелем.
– запустить на ПК программу (Putty, HyperTerminal), установить настройки:
– выбрать соответствующий Serialпорт компьютера.
– установить скорость передачи данных 115200.
– задать формат данных: 8 бит данных, 1 стоповый бит, без контроля четности.
– включить питание коммутатора.

Если вы выполнили действия правильно, в окне терминала появится лог загрузки коммутатора:

```
DDR3 initializing, ECC mode=4, clk_div=06, 2T=on init_by_pub=0
<>DDR3 up
CIict

U-Boot 2019.10 (Apr 06 2020 - 11:30:43 +0200)fireant

CPU:   ARM A53
Model: FireAnt PCB135/eMMC Reference Board
DRAM:  2 GiB
MMC:   sdhci@600800000: 0
Loading Environment from SPI Flash... SF: Detected mx66l1g45g
with page size 256 Bytes, erase size 4 KiB, total 128 MiB
OK
In:    serial@600100000
Out:   serial@600100000
Err:   serial@600100000
Net:   eth0: switch@0
Hit any key to stop autoboot:  0
SF: Detected mx66l1g45g with page size 256 Bytes, erase size
4 KiB, total 128 MiB
Reading 20971520 byte(s) at offset 0x00000000
```

После окончания загрузки необходимо ввести имя пользователя (Username) и пароль (Password) (по умолчанию Username – “admin” Password – отсутствует (поле оставить пустым, нажав клавишу «Enter»). В окне терминала появится приглашение к вводу команд в виде символа «#»:

```
Username: admin
Password:
#
```

По умолчанию учетная запись admin наделена 15 уровнем (наивысший) привилегий системного администратора.

2.2. Подключение через Telnet, SSH

Для подключения к коммутатору, используя протокол Telnet или SSH. Необходимо чтобы на коммутаторе был сконфигурирован ipv4 или ipv6 адрес и хост с Telnetклиентом был доступен с коммутатора (находился в одной сети с ним или был доступен через маршрутизатор).

В текущем примере коммутатор имеет ip-адрес 192.168.0.186, маска 255.255.255.0**.** Сначала необходимо настроить IP-адрес на ПК, с которого будет осуществляться управление. Настроим адрес 192.168.0.176, маска 255.255.255.0**.** Соединим ПК и

коммутатор патч кордом Ethernet. Выполним команду: `telnet192.168.0.186` в командной строке ОС или подключимся через Putty. Затем введем Usernameи Password (по умолчанию Username – “admin” Password - отсутствует).

```
Username: admin
Password:
#
```

2.3. Подключение через Web-интерфейс

Для доступа к коммутатору через WEB-интерфейс откройте WEB-браузер и введите в адресной строке http://ip-коммутатора. По умолчанию на коммутаторе получение ip-адреса настроено через DHCP, если получить ip-адрес не удалось, устанавливается ip-адрес 192.168.1.1 и маской подсети 255.255.255.0.

В данном примере ip-адрес коммутатора 192.168.0.186. В открывшейся странице введите имя пользователя и пароль (по умолчанию Имя пользователя – “admin” Пароль - отсутствует).

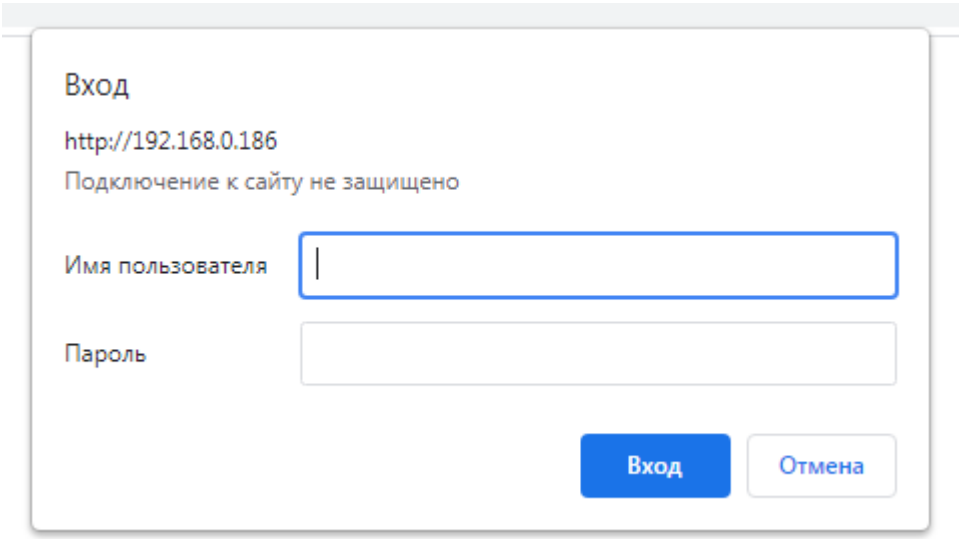


Рисунок 2.3.1 Страница авторизации

При верном вводе имени пользователя и пароля откроется основной WEB-интерфейс.

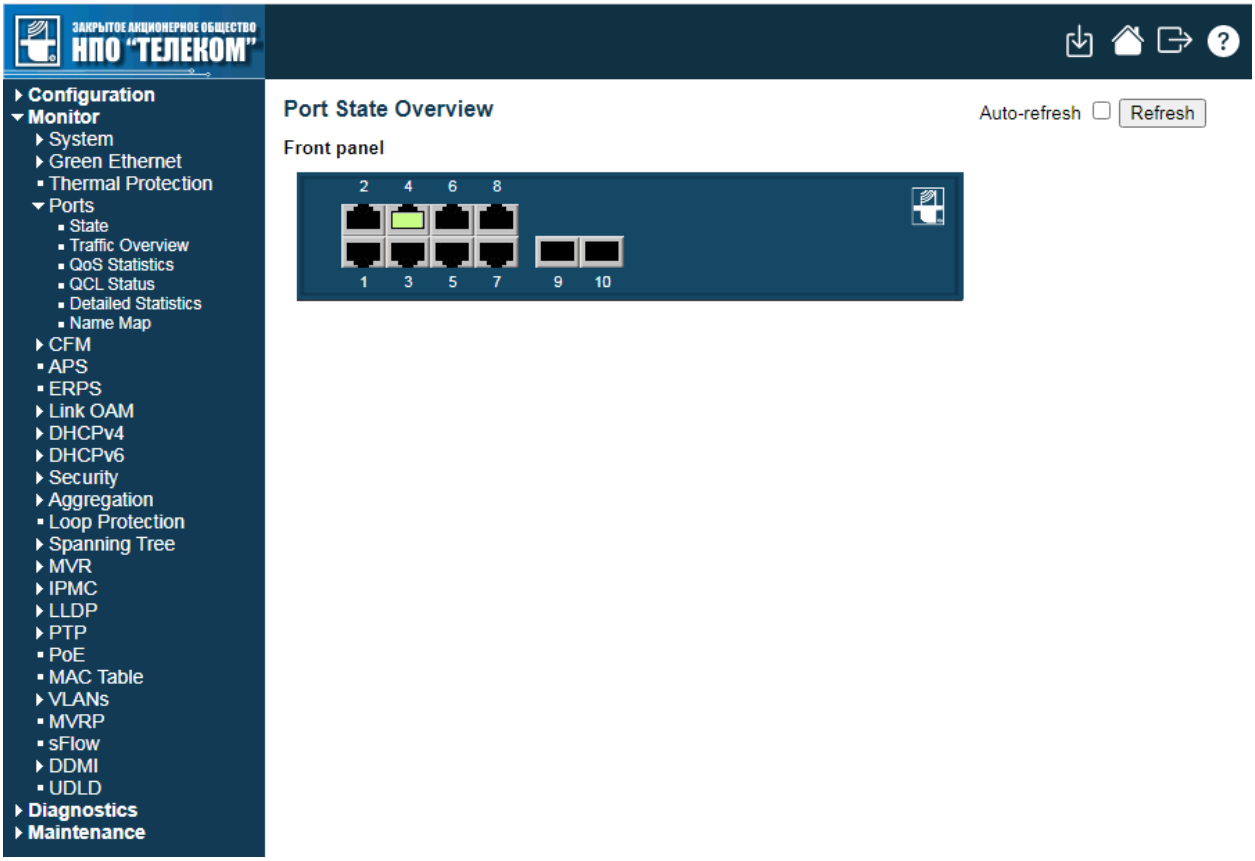


Рисунок 2.3.2 Основное меню WEB-интерфейса

3. Загрузка ПО, изменение пароля доступа, сброс конфигурации через меню загрузчика.

3.1. Загрузка ПО через меню загрузчика uboot

Для процедуры загрузки ПО через загрузчик uboot потребуется консольный кабель и tftp-сервер с файлом прошивки.

- Подключить консольный кабель в порт "Console" на коммутаторе, tftp-сервер подключить в порт "MGMT". Включить/перезагрузить коммутатор.
- После сообщения в терминале **Autobooting in 10 seconds, enter password to stop:** ввести пароль `nts`. В терминале появится символ для ввода команд **=>**.
- Задать ip-адрес коммутатора командой `setenv ipaddr 192.168.102.2`
- Задать ip-адрес tftp-сервера командой `setenv serverip 192.168.102.1`
- Загрузить прошивку командой `tftpboot` имя файла прошивки например `tftpboot istax_nts25.itb.`
- По завершении передачи файла ввести команду загрузки в оперативной памяти `run ramboot`
- При успешной загрузке коммутатора выполнить повторную загрузку ПО штатным способом через web-интерфейс или CLI командой `firmware upgrade tftp://192.168.102.1/istax_nts25.itb`

Примечание1: для изменения пароля доступа в меню загрузчика, введите команду `password`, после соответствующего приглашения `"Enter new password:"` введите новый пароль, аналогично после приглашения `"Retype new password:"` повторите введенный пароль. При успешном изменении пароля в терминал выведется запись `"Password successfully changed"`

Примечание2: для выхода из меню загрузчика и рестарта коммутатора, введите команду `reset`

3.2. Сброс настроек в заводские через меню загрузчика uboot.

Перезагрузить коммутатор, после сообщения `Autobootingin 10 seconds,`

`Enter password to stop`: ввести пароль `nts`

Вариант 1. Сброс настроек для ранних версий ПО (через затирание Flash-памяти)

1. Ввести команду `sf probe`
2. Ввести команду `mtd erase rootfs_data`
3. Перезагрузить `reset`
4. После перезагрузки в `cli` ввести команду `platform debug allow`, далее `debug firmware bootstrap nor`
5. Перезагрузить reload cold

Вариант 2. Сброс настроек и восстановление доступа для актуальных версий ПО

В новых версиях программного обеспечения реализован механизм селективного сброса параметров без необходимости полного затирания секторов Flash-памяти. В зависимости от текущей задачи используются следующие команды:

– **Временный обход пароля администратора:**

```
=> setenv ignore_config_password 1
```

Команда активирует режим игнорирования пароля локальной конфигурации исключительно для встроенной учетной записи **admin. Действие команды не затрагивает** остальных созданных в системе пользователей и их уровни привилегий. После последующей загрузки операционной системы будет осуществлен вход под учетной записью admin без пароля (по умолчанию), что позволяет восстановить доступ к интерфейсу CLI без потери текущей рабочей конфигурации коммутатора.

=> sa – сохранить переменную

– **Очистка базы данных пользователей:**

```
=> restore password
```

Команда полностью удаляет всех созданных в системе пользователей из локальной базы данных учетных записей. После применения команды в системе остается только одна встроенная учетная запись по умолчанию – admin без пароля. Текущая сетевая конфигурация интерфейсов (IP-адреса, VLAN, маршруты) при этом сохраняется.

– **Полный сброс конфигурации устройства:**

```
=> restore config
```

Команда инициализирует процедуру полного удаления файла конфигурации коммутатора. Все настройки сбрасываются к заводским значениям по умолчанию.
После ввода требуемых команд из списка выше выполнить команду перезагрузки:
```
=> reset
```

3.3. Загрузка ПО через CLI

Примеры загрузки ПО через протоколы tftp, ftp, scp, sftp, http:

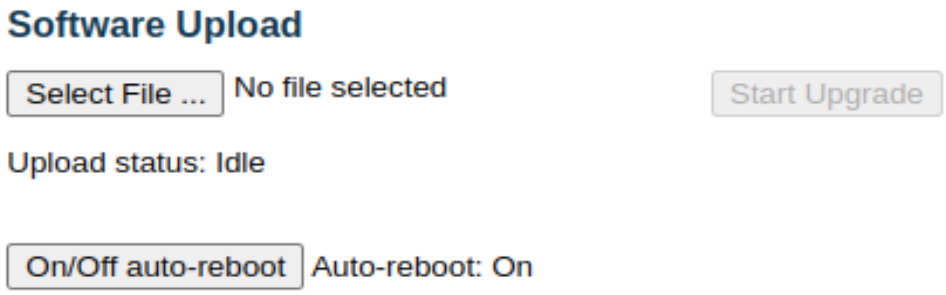
```
firmware upgrade tftp://192.168.102.1/istax_nts25.itb
firmware upgrade
ftp://user1:password@192.168.102.1/istax_nts25.itb
firmware upgrade
scp://user:password@192.168.102.1/istax_nts25.itb save-host-key
```

```
firmware upgrade http://host[:port]/filename
firmware upgrade
sftp://user:password@192.168.102.1:22/istax_nts25.itb save-host-
key
```

3.4. Загрузка ПО через WEB

Для обновления ПО нужно перейти во вкладку:

Maintenance→Software→Upload→Кликнуть по Select File, выбрать файл прошивки.
Нажать кнопку «`Start Upgrade`».



4. CLI интерфейс

Для настройки, управления и мониторинга через CLI интерфейс, подключитесь к устройству через порт Console (смотри п.1.1), через telnet, SHH (смотри п.1.2).

4.1. Базовые настройки

Данный раздел содержит описание и рекомендации по базовым настройке коммутатора.

4.1.1. Режимы конфигурирования

В интерфейсе командной строки доступно три базовых режима:

- Пользовательский режим
- Привилегированный режим
- Режим глобальной конфигурации (для перехода требуется 15 уровень привилегий и ввод команды “`configure terminal`”, для выхода из режима требуется ввести команду “exit”)

4.1.2. Работа в командной строке

Интерфейс CLI коммутатора выполнен по промышленным стандартам и обладает типовым наборам команд. Доступны следующие клавиши для редактирования:

Клавиша	Функция
Backspace	Удаляет символ после курсора, позицию курсора не сдвигает.
Вверх	История введенных команд. Выводит предыдущую введенную команду. Многократное нажатие выводит ранее введенные команды по порядку.
Вниз	История введенных команд.

	Выводит следующую введенную команду.
Влево	Сдвиг курсора на один символ влево
Вправо	Сдвиг курсора на один символ вправо
Ctrl + P	То же что и клавиша «Вверх»
Ctrl + N	То же что и клавиша «Вниз»
Ctrl + Z	Возврат в Adminрежим из любого конфигурационного режима
Ctrl + C	Остановка запущенной команды, например ping
Tab	При частичном вводе команды, при нажатии клавиши Tab, выводятся все допустимые варианты продолжения команды.

Для вызова справки в CLI предусмотрены команды:

"help" – доступна в любом режиме, выводит краткую информацию по использованию функции справки.

"?" – доступна в любом режиме, выводит список всех допустимых команд с их описанием.

В случае некорректного ввода команды возвращается информация об ошибке:

% Incomplete command. - команда введена не полностью либо отсутствует обязательный параметр.

% Invalid word detected at '^' marker. – неправильный ввод команды. Маркер '^' указывает на место неправильного ввода.

% Ambiguous word detected at '^' marker. - Введенная команда имеет два и более варианта интерпретации. Маркер '^' указывает на место неправильного ввода.

CLIподдерживает сокращенный ввод команд, если введенная строка может быть однозначно дополнена до полной команды и интерпретирована в случае единственно возможного варианта интерпретации. В ином случае вернется ошибка вида: "% Ambiguous word detected at '^' marker."

4.1.3. Создание учетной записи

Пример создания учетной записи через интерфейс командной строки:

```
# configure terminal
(config)# username operator privilege 15 password unencrypted operator
(config)#
```

Разберем введённые команды:

configure terminal – переход в режим глобальной конфигурации.

user name operator privilege 15 password unencrypt ed operator- создание пользователя с именем **operator**, наивысшим уровнем привилегий (15) и паролем **operator**

4.1.4. Сохранение конфигурации, перезагрузка и возврат к заводским настройкам

Для сохранения внесенных изменений в конфигурацию коммутатора требуется выйти из режима глобальной конфигурации и ввести команду "copy running - config

startup - config", либо в режиме глобальной конфигурации ввести команду "do copy running – config start up - config".

Пример сохранения конфигурации в энергонезависимую память:

```
(config)# do copy running-config startup-config
Building configuration...
% Saving 1631 bytes to flash: startup-config
```

Пример сохранения конфигурации в tftp-сервер:

```
# copy startup-config tftp://192.168.30.8/config.txt
Building configuration...
% Saving 1631 bytes to flash: startup-config
```

Пример выгрузки конфигурации с tftp-сервера:

```
# copy tftp://192.168.30.8/config.txt startup-config
Building configuration...
% Saving 1631 bytes to flash: startup-config
```

Для перезагрузки устройства воспользуйтесь командой `reloadcold` в привилегированном режиме.

Пример ввода в терминале:

```
# reloadcold
% Cold reload in progress, please stand by.
Rebooting system...
```

Для возврата к заводским установкам выполните команду `reload defaults`. В данном случае коммутатор не будет перезагружен.

Пример ввода в терминале:

```
# reload defaults
% Reloading defaults. Please stand by.
```

4.1.4.1. Версионирование и откат конфигурации.

Использование системы версионирования и отката конфигурации является надежным и эффективным способом обеспечения отказоустойчивости сетевого оборудования. Система позволяет изолировать сбои путем автоматического и ручного сохранения снимков настроек в локальной энергонезависимой Flash-памяти устройства, а также организации их выгрузки на внешние серверы.

Система предотвращает потерю управления над коммутатором при внесении ошибочных изменений. Благодаря механизму безопасного отката с таймером ожидания, устройство автоматически возвращается к заведомо рабочей конфигурации, если администратор не подтвердит доступность коммутатора после применения новых параметров.

Для доступа к настройкам необходимо перейти в режим глобальной конфигурации, а также настроить необходимые параметры.

Команда	Описание
Привилегированный режим	
`archive config save`	Создание точки сохранения (checkpoint) во внутренней памяти без комментария

archive config save comment <string>	Создание точки сохранения во внутренней памяти с добавлением текстового комментария
show archive list	Вывод таблицы сохраненных версий (ID, Дата/Время, Размер, Комментарий)
show archive diff <ID1> <ID2>	Сравнение двух версий конфигурации
archive upload <ID>	Ручная выгрузка определенной локальной версии по её ID на внешний сервер
archive upload checkpoint <ID>	Ручная выгрузка локальной версии с использованием ключевого слова checkpoint
archive download <url_file> [apply]	Скачивание файла конфигурации по URL извне с возможностью немедленного применения
archive clear <ID>	Удаление конкретной записи архива по её идентификатору
archive clear all	Полная очистка локального архива конфигураций
archive clear older-than <1-3650> days	Удаление из локальной памяти архивов старше указанного количества дней (от 1 дня до 10 лет)
archive verify <ID>	Расчет и проверка контрольной суммы (SHA256) архивного файла по его числовому ID
Режим глобальной конфигурации	
ip archive-server <word> protocol <scp|sftp|tftp> [user <word>] [port <uint>] [path <word>] [filename-template <word>]	Комплексная настройка параметров подключения к серверу резервного копирования
ip archive-server password <secure_pass>	Установка пароля для авторизации на внешнем сервере
archive auto-backup enable	Включение автовыгрузки на сервер при каждой команде copy running-config startup-config
archive auto-backup disable	Настройка периодической выгрузки актуального конфига по расписанию (интервал от 1 минуты до 7 суток)
archive max-files <1-15>	Установка жесткого лимита количества удерживаемых файлов в локальной памяти
Режим конфигурации (configure)	
configure rollback to <ID>	Немедленный откат системы на конфигурацию с указанным ID
configure rollback to <ID> time <1-10080>	Безопасный откат на указанный ID с таймером отмены (от 1 минуты до 7 суток)
configure confirm	Подтверждение изменений и остановка таймера обратного отсчета

Пример настройки:

Ниже приведен практический сценарий настройки параметров автоматического резервного копирования на внешний SFTP-сервер, создание локальной точки, а также выполнение безопасного отката на конфигурацию №1 с последующим подтверждением.

1. Переход в режим глобальной конфигурации, настройка параметров внешнего сервера, лимитов архива и периодичности выгрузки: NTS-#

```
configure terminal
(config)# ip archive-server 192.168.1.8 protocol sftp user backup_admin port 22 path /home/backup/ filename-template switch_{hostname}_{date}.cfg
(config)# ip archive-server password MySecurePassword123
(config)# archive max-files 10
(config)# archive auto-backup enable
(config)# archive auto-backup period 1440
(config)# exit
```

Примечание: Значение period 1440 задает резервное копирование по расписанию один раз в сутки (1440 минут).

2. Создание контрольной точки вручную перед внесением критических изменений:

```
# archive config save comment Before core infrastructure changes
```

3. Просмотр списка доступных точек восстановления:

```
# show archive list
ID  Date/Time            Size    Comment
1   2026-05-13 10:15:22  45KB    Base configuration
2    2026-05-13 10:35:00  48KB     Before core infrastructure changes
```

4. Выполнение безопасного отката на предыдущую конфигурацию (ID 1) на 5 минут:

```
# configure rollback to 1 time 5
```

Система временно применила конфигурацию ID 1. Запущен таймер отката: 5 минут.

5. Подтверждение корректности работы примененной конфигурации:

```
# configure confirm
```

Таймер отката остановлен. Конфигурация ID 1 успешно зафиксирована как основная рабочая.

4.1.5. Настройка имени устройства

Пример создания учетной записи через интерфейс командной строки:

```
# configure terminal
(config)# hostname switch
```

```
switch(config)#
```

Задание имени хоста выполняется вводом команды `hostname <имя устройства>`. Ввод команды доступен из режима глобальной конфигурации. После выполнения команды, в терминале, перед символом “#” будет отображаться имя вашего устройства. Для отмены команды введите “`nohostname`”

4.1.6. Конфигурация интерфейсов

Для перехода в режим конфигурации интерфейсов необходимо в режиме глобальной конфигурации ввести команду `interface <type> <list>`. В зависимости от типа настраиваемого интерфейса поддерживаются следующие команды:

Команда	Описание
Глобальные настройки	
`interface *`	Одновременная настройка всех физических портов (на всех коммутаторах в стеке);
`interface GigabitEthernet <port_list>`	Настройка параметров физических интерфейсов 1 Гбит/с;
`interface 10GigabitEthernet <port_list>`	Настройка параметров физических интерфейсов 10 Гбит/с;
`interface 25GigabitEthernet <port_list>`	Настройка параметров физических интерфейсов 25 Гбит/с;
`interface Port-channel <channel_list>` `no interface Port-channel <channel_list>`	Настройка агрегированных интерфейсов (LAG); удаление агрегированных интерфейсов (LAG);
`interface loopback <loopback_list>` `no interface loopback <loopback_list>`	Настройка виртуальных Loopback-интерфейсов; удаление виртуальных Loopback-интерфейсов;
`interface vlan <vlan_list>` `no interface vlan <vlan_list>`	Настройка L3-интерфейсов VLAN коммутатора. удаление L3-интерфейсов VLAN коммутатора.

Для сброса настроек одного или нескольких интерфейсов к значениям по умолчанию (заводским параметрам) используется команда `default interface <type> <list>` в режиме глобальной конфигурации `(config)#`

Команда	Описание
Глобальные настройки	
`default interface *`	Сброс настроек всех физических интерфейсов (и всех коммутаторов в стеке) к значениям по умолчанию.

default interface GigabitEthernet <port_list>	Сброс параметров указанных портов 1 Гбит/с до значений по умолчанию.
default interface 10GigabitEthernet <port_list>	Сброс параметров указанных портов 10 Гбит/с до значений по умолчанию.
default interface 25GigabitEthernet <port_list>	Сброс параметров указанных портов 25 Гбит/с до значений по умолчанию.
default interface Port-channel <channel_list>	Сброс настроек агрегированных интерфейсов (LAG) к значениям по умолчанию.
default interface loopback <loopback_list>	Сброс параметров указанных Loopback-интерфейсов.
default interface vlan <vlan_list>	Сброс параметров L3-интерфейсов VLAN (удаление IP-адресов и возврат к базовым настройкам).

Пример ввода в терминале:
сброс одного интерфейса

```
# configure terminal
(config)# default interface GigabitEthernet 1/1
% Configuration for these interfaces will be set to default
Are you sure you want to proceed? [y/N] y
(config)#
```

сброс диапазона интерфейсов

```
# configure terminal
(config)# default interface GigabitEthernet 1/1-3
% Configuration for these interfaces will be set to default
Are you sure you want to proceed? [y/N] y
(config)#
```

сброс диапазона интерфейсов

```
# configure terminal
(config)# default interface GigabitEthernet 1/1,3
% Configuration for these interfaces will be set to default
Are you sure you want to proceed? [y/N] y
(config)#
```

сброс нескольких интерфейсов в стеке

```
# configure terminal
(config)# default interface GigabitEthernet 1/1 GigabitEthernet
2/1
% Configuration for these interfaces will be set to default
Are you sure you want to proceed? [y/N] y
(config)#
```

4.1.7. Настройка параметров физических интерфейсов

Для настройки параметров физических интерфейсов,необходимо перейти в режим глобальной конфигурации и ввести команду interface GigabitEthernet

<port_type_list> (где <port_type_list> – это номер или диапазон интерфейс(а)(ов), допустимы несколько вариантов ввода:

– (config)# interface GigabitEthernet 1/1
  (config-if)#
– (config)# interface GigabitEthernet 1/1-4
  (config-if)#
– (config)# interface GigabitEthernet 1/1,4
  (config-if)#

При работе со стеком коммутаторов или для массовой настройки однотипных портов поддерживается использование символа * (групповой выбор) в параметре <port_type_list> (формат <номер_коммутатора>/<номер_порта>):

– Выбор одного и того же порта (в данном примере – порта №2) одновременно на всех коммутаторах в стеке.
  (config)# interface GigabitEthernet */2
– Выбор всех портов данного типа (1 Гбит/с) на конкретном коммутаторе (в данном примере – на коммутаторе №2 в стеке).
  (config)# interface GigabitEthernet 2/*

Примечание: аналогичный синтаксис группового выбора поддерживается для интерфейсов 10GigabitEthernet и 25GigabitEthernet, а также при сбросе настроек командой default interface.

Команда	Описание
shutdown no shutdown	Выключение интерфейса Включение интерфейса
speed {10|100|1000|auto}	Настройка скорости физического порта: 10 – 10mb/s 100-100mb/s 1000-1000mb/s auto – автоматическое согласование скорости (есть возможность дополнительно указать какие скорости разрешить при автосогласовании)
duplex{auto|full|half}	Настройка режима дуплекса auto – автоматическое согласование дуплекса full - полный дуплекс half - полудуплекс
description <описание> no description	назначение описания интерфейса удаление описания интерфейса

4.1.8. Настройка L3 интерфейсов коммутатора

По умолчанию на коммутаторе создан L3 интерфейс “vlan 1” с ip-адресом 192.168.1.1 и маской подсети 255.255.255.0.

Для настройки параметров L3 интерфейсов необходимо перейти в режим глобальной конфигурации и ввести команду interface vlan <vlan_list> (где <vlan_list> – это номер или диапазон интерфейс(а)(ов), если такого номера интерфейса еще нет на коммутаторе, то он будет создан автоматически), допустимы несколько вариантов ввода:

– (config)# interface vlan 1

```
    (config-if-vlan)#
```

– `(config)# interface interface vlan 1-4`

```
    (config-if-vlan)#
```

– `(config)# interface interface vlan 1,4`

```
    (config-if-vlan)#
```

Команда	Описание
`ip address <ipv4_addr><ipv4_subnet>`	Назначение интерфейсу статического ipv4-адреса, где `<ipv4_addr>`- ip-адрес, а `<ipv4_subnet>`– маска подсети
`no ip address <ipv4_addr><ipv4_subnet>`	Удаление статического ip-адреса с интерфейса
`ip address dhcp`	Получение ipv4-адреса автоматически от сервера dhcp
`no ip address dhcp`	Удаляет динамический IP-адрес, полученный через протокол DHCP, с интерфейса.
`add ip address <ipv4_addr><ipv4_subnet>`	Назначение интерфейсу дополнительного статического ipv4-адреса, где `<ipv4_addr>`- ip-адрес, а `<ipv4_subnet>`– маска подсети
`no ip address<ipv4_addr><ipv4_subnet>`	Удаление статического ip-адреса с интерфейса
`no ip address secondary`	Удаляет все вторичные IP-адреса с интерфейса. Вторичные адреса применяются для назначения дополнительного диапазона адресов на одном интерфейсе.
`no ip address`	Полностью удаляет основной и все вторичные IP-адреса с интерфейса, делая его неактивным для взаимодействия с сетью.
`ipv6 address <ipv6_subnet>`	Назначение интерфейсу статического ipv6-адреса, где `<ipv6_subnet>`- ip-адрес_ маска подсети
`no ip address <ipv6_subnet>`	Удаление статического ip-адреса с интерфейса
`ipv6 address dhcp`	Получение ipv6-адреса автоматически от сервера dhcp

ip cos <0-7>	Настройка маркировки исходящего трафика с интерфейса управления.
no ip cos	Отмена команды.

Для удаления L3 интерфейса в режиме глобальной конфигурации введите команду: no interface vlan <vlan_list> (где <vlan_list>- это номер или диапазон интерфейс(а)(ов)).

4.1.9. Настройка маршрутов

Для создания статического маршрута используется команда ip route <ipv4_addr> <ipv4_subnet> <ipv4_ucast>, где <ipv4_addr> – целевой адрес для удаленной сети, <ipv4_subnet> – маска подсети для удаленной сети, <ipv4_ucast> – ip-адрес следующего перехода для пересылки пакетов в удаленную сеть. Доступна в режиме глобальной конфигурации.

Пример настройки статического маршрута:

```
(config)# ip route 192.168.10.0 255.255.255.0 192.168.10.1
```

Для удаления маршрута применяется команда no ip route

```
(config)# no ip route 192.168.10.0 255.255.255.0 192.168.10.1
```

4.1.10. Настройка DNS и Domain Name

Команда	Описание
Глобальные настройки DNS	
ip name-server <0-2> dhcp interface vlan <vlan_id>	Команда настраивает DHCP-клиент на интерфейсе VLAN для автоматического получения адреса DNS-сервера. Когда интерфейс получает конфигурацию по протоколу DHCP, он автоматически получит информацию о DNS-серверах и применит её локально на устройстве. Параметры: - <0-2> – индекс сервера (может иметь значения от 0 до 2). - dhcp – режим динамического получения конфигурации DNS через DHCP. - interface vlan <vlan_id> – указание интерфейса VLAN, через который будут получены DNS-конфигурации.
ip name-server <0-2> dhcp [ipv4|ipv6]	Команда устанавливает автоматическое получение DNS-сервера по протоколу DHCP с указанием версии протокола IPv4 или IPv6. Параметры: - <0-2> – индекс сервера (может иметь значения от 0 до 2).

	- dhcp – указание режима динамической конфигурации DNS через DHCP. - [ipv4|ipv6] – выбор версии IP-протокола для получения DNS-сервера.
ip name-server <0-2> [<ipv4_ucast>|<ipv6_ucast>]	Команда используется для статической установки конкретного DNS-сервера вручную. Параметры: - <0-2> – индекс сервера (может иметь значения от 0 до 2). - <ipv4_ucast> – указывается адрес DNS-сервера в формате IPv4. - <ipv6_ucast> – указывается адрес DNS-сервера в формате IPv6.
ip dns proxy	Команда используется на коммутаторах для включения функции DNS Proxy. Этот режим позволяет устройству перехватывать DNS-запросы от подключённых узлов и самостоятельно обращаться к внешним DNS-серверам для их обработки.
no ip name-server <0-2>	Отменяет предыдущую настройку DNS-сервера для указанного индекса. Параметр: - <0-2> – индекс сервера, настройка которого должна быть удалена.
no ip dns proxy	Команда отключает функцию DNS Proxy на устройстве. Если раньше было включено переадресация DNS-запросов через прокси, эта команда отменяет данную настройку, возвращая обработку DNS-запросов клиентам непосредственно внешним DNS-серверам.
Команда просмотра информации DNS	
show ip name-server	Команда используется для отображения текущих настроек DNS-серверов на устройстве.
Глобальные настройки Domain Name	
ip domain name <domain_name>	Назначает доменное имя по умолчанию для устройства. Это имя используется совместно с DNS-запросами для разрешения неполных доменных имен. Параметры: - <domain_name> – имя домена, которое будет использоваться устройством.

`ip domain name dhcp [ipv4| ipv6]`	Устанавливает способ получения доменного имени через DHCP-протокол для соответствующей версии IP. Параметры: - `dhcp` – использование DHCP для получения доменного имени. - `[ipv4 | ipv6]` – версия IP-протокола (IPv4 или IPv6).
`ip domain name dhcp [ipv4| ipv6] interface vlan <vlan_id>`	Получает доменное имя через DHCP, привязанное к определенному интерфейсу VLAN. Параметры: - `dhcp` – получение доменного имени через DHCP. - `[ipv4 | ipv6]` – версия IP-протокола. - `interface vlan <vlan_id>` – идентификационный номер VLAN-интерфейса, откуда будет получено доменное имя.
`no ip domain name`	Удаляет ранее установленное имя домена.
Команда просмотра информации Domain Name	
`show ip domain`	Команда выводит текущие настройки доменной системы (DNS) на сетевом устройстве.

4.1.11. Настройка времени

4.1.11.1. Настройка NTP и SNTP

Команда	Описание
Глобальные настройки	
`ntp` `no ntp`	Включение функции ntp Выключение функции ntp
`ntp mode [ntp | sntp]`	`ntp` - NTP-клиент (по умолчанию) `sntp` - SNTP-клиент (RFC 4330)

`ntp server [1-5] ip-address [domain_name|ipv4_ucast|ipv6_ucast]`
 	
`no ntp server [1-5]`
	Позволяет указать адрес или доменное имя
	NTP-сервера. Возможно настроить до 5 адресов.
	
	Выключает указанный NTP-сервер.

`ntp source <ipv4_ucast>`
 	
`no ntp source`
	Для указания source-IP-адреса для NTP-пакетов для всех peer.
	
	Устанавливает source-IP-адрес для NTP-пакетов по умолчанию

Команда просмотра информации	
`show ntp status`	Отображает статус текущего состояния синхронизации времени устройства с серверами NTP. Информация включает состояние синхронизации, выбранный источник времени и точность синхронизации.

Примечание: для того, чтобы коммутатор выступал в роли NTP-сервера локально, необходимо включить ntp без указания внешнего сервера:

```
# configure terminal
(config)#ntp
```

Если необходимо вручную установить точное время на коммутаторе, это делается следующим образом:

```
time set [<date>Date yyyy/mm/dd, yyyy=1970-2037, mm=1-12, dd=1-31] [<time>Time HH:mm:ss, HH=0-23, mm=0-59, ss=0-59]
```

Пример:

```
# time set 2025/12/03 15:00:00
```

Важно: если устройство было перезагружено, ручные настройки времени теряются, поскольку они хранятся в оперативной памяти.

Если один из коммутаторов имеет доступ во внешнюю сеть, но будет в роли NTP-сервера, необходимо синхронизировать время коммутатора с внешним сервером.

```
# configure terminal
(config)#ntp
(config)#ntp server [1-5]
ip-address [domain_name|ipv4_ucast|ipv6_ucast]
```

4.1.11.2. Конфигурация часового пояса

Команда	Описание
`clock timezone <word16><-23-23>`	`<word16>`- акроним для определения часового пояса `<-23-23>`- соответствующий часовой пояс
`clock summer-time <word16> date <start time><end time><offset>`	Конфигурация перехода на летнее время `<word16>`- акроним для определения часового пояса `<starttime>` - время начала действия в формате (MMDDYYYYHH:MM) `<endtime>` - время окончания действия в формате (MMDDYYYYHH:MM) `<offset>` - количество минут для добавления в летнее время

4.1.12. Конфигурация журнала системных сообщений

Systemlog (системный журнал) – стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP. Настройка доступна из режима глобальной конфигурации.

Команда	Описание
logging on no logging on logging flash no logging flash debug logging flash debug logging erase platform debug allow	Режим работы: включен. Режим работы: выключен. сохранение лога в энергонезависимую память отмена команды просмотр журнала в энергонезависимой памяти удаление записей журнала из энергонезависимой памяти переход в режим debug
logging host {<domain_name> | <ipv4_ucast>}	Настройка адреса syslog-сервера где <domain_name>- имя сервера <ipv4_ucast> - ipv4-адрес сервера
logging level {error | informational | notice | warning} logging source <ipv4_ucast>	Выбор типа отправляемых сообщений. Error – отправлять только ошибки Informational – отправлять информ. сообщения, уведомления, предупреждения и ошибки. Notice – отправлять уведомления, предупреждения и ошибки. Warning – отправлять предупреждения и ошибки. Указать исходный IP-адрес для сообщений syslog.

Пример настройки в терминале (включение ведения журнала событий, установка адреса syslog-сервера с адресом 192.168.0.176, выбор типа сообщений для записи в журнале – все):

```
(config)# logging on
(config)# logging host 192.168.0.176
(config)# logging level in formational
```

4.1.13. VLAN

Использование виртуальных локальных сетей VLAN (Virtual Local Area Network) является популярным и недорогим способом сегментирования развернутой сети по логически сгруппированным устройствам безотносительно к их физическим соединениям. Сети VLAN также сегментируют сеть на различные 104 широковещательные домены таким образом, что пакеты передаются на порты внутри VLAN, которой они принадлежат.

Сети VLAN повышают безопасность. Устройства, которые часто связываются друг с другом группируются в одну и ту же VLAN. Если устройства данной VLAN желают

связаться с устройствами в другой VLAN, трафик должен пройти через устройство маршрутизации или коммутатор 3-го уровня.

Сети VLAN упрощают управление трафиком. В обычных сетях, не сегментированных на VLAN, легко возникает перегрузка, обусловленная широковещательным трафиком, адресованного всем устройствам. Сводя к минимуму распространение широковещательного трафика по всей сети, сети VLAN облегчают работу устройствам группы, часто связывающимся с другими устройствами в той же VLAN за счет деления всей сети на несколько доменов вещания.

Для доступа к настройкам необходимо перейти в режим глобальной конфигурации, а также настроить необходимые порты.

Команда	Описание
Глобальные настройки	

`vlan <vlan_list>`
 	
`no vlan <vlan_list>`
	Создание vlan и переход в режим конфигурации vlan
	
	Удаление vlan

`name <vword32>`
 	
`no name <vword32>`
	Настройка имени vlan
	
	Удаление имени

`vlan ethertype s-custom-port`	Настройка типа ethertype/TPID, используемого для специализированных s-портов
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`switchport mode {access | hybrid | trunk}`	Настройка режима работы порта `access` (Доступ): Порты доступа, как правило, используется для подключения к конечным станциям. Динамические функции, такие как Voice VLAN могут добавить порт к большему количеству VLAN. Порты доступа имеют следующие характеристики: - Принадлежит ровно к одной VLAN (port VLAN). - Принимает не тегированные и тегированные кадры. - Удаляет все кадры, которые не классифицируются как access VLAN. - На выходе все кадры, классифицированные как Access VLAN, передаются без тегов. Другие (динамически добавленные VLAN) передаются с тегами. `trunk` (Магистральные): Магистральные порты могут передавать трафик на несколько виртуальных локальных сетей одновременно и, как правило, используется для подключения

	к другим коммутаторам. Магистральные порты имеют следующие характеристики: - По умолчанию, trunk-порт является членом всех VLAN (1-4095). - VLAN, членом которых является магистральный порт, может быть ограничено путем использования Allowed VLAN. - Кадры, классифицированные с VLAN, членом которых порт не является, 106 отбрасываются. - По умолчанию, все кадры, кроме кадров, классифицированных как port VLAN, передаются тегированными. Кадры, классифицированные в port VLAN, не получают C-тегами на выходе - Можно настроить устройство тегировать на выходе все кадры, в этом случае только тегированные кадры будут приниматься на входе. hybrid(Гибридные): Гибридные порты схожи с портами типа Trunk во многих отношениях, но имеют дополнительные функции. В дополнение к характеристикам, описанным для trunk-портов, гибридные порты имеют следующие возможности: -Могут быть сконфигурирован как VLAN unaware, C-tag, S-tag или Scustom tag. - С возможностью фильтрации на входе. - Обработка входящих кадров и конфигурацию выходного тегирования можно настроить независимо.
switchport access vlan vlan_id> switchport trunk allowed vlan <vlan_list> switchport hybrid allowed vlan <vlan_list>	Настройка VLAN ID для порта. Допустимый диапазон значений: от 1 до 4095. По умолчанию задано. Команды приведены в зависимости от режима работы порта. Порты в режимах Trunk и Hybrid могут контролировать членами каких VLAN они могут становиться. Порты в режиме Access может быть членом только одной VLAN, access VLAN. Поле может быть оставлено пустым. В таком случае, порт не будет членом ни одной VLAN.
switchport forbidden vlan add <vlan_list>	Настройка порта для того чтобы никогда не становиться членом определенных VLAN. Это может быть полезно при

	использовании динамических протоколов, работающих с VLAN, например, GVRP. По умолчанию, поле оставлено пустым и ограничений не накладывается.
`switchport hybrid ingress-filtering`	Настройка фильтрации входящих кадров. Если фильтрация входящих кадров включена и входящий кадр не принадлежит VLAN, указанному на данном порту, такой кадр отбрасывается. Если фильтрация входящих кадров выключена и входящий кадр не принадлежит VLAN такой кадр принимается и передается в коммутатор. По умолчанию фильтрация входящих кадров включена для портов в режимах access и trunk.
`switchport hybrid acceptable-frame-type {all | tagged | untagged}`	Настройка режима обработки входящих кадров (доступно только для Hybrid портов) `All` – Тегированные и не тегированные кадры принимаются. `Tagged` – Только тегированные кадры принимаются. Не тегированные - отбрасываются `Untagged` – Только не тегированные кадры принимаются. Тегированные - отбрасываются.
`switchport hybrid egress-tag {all | none}`	Настройка тегирования на выходе для hybrid портов. All - Все кадры передаются с метками. None - Все кадры передаются без меток. По умолчанию - кадры с меткой VLAN совпадающей с port VLAN передаются не тегированными. Остальные кадры передаются со своими метками.
`switchport trunk vlan tag native`	Настройка тегирования на выходе для trunk портов. При такой команде все кадры передаются с метками.
`switchport {trunk | hybrid} native vlan <vlan_id>`	Настройка Port VLAN
`switchport hybrid port-type {c-port | s-custom-port | s-port | unaware}`	Конфигурация гибридных портов. `c-port` – если во входящем тегированном кадре TPID=0x8100, он передается. Если кадр не тегированный или приоритетно тегированный в него добавляется тег port VLAN. Исходящие кадры тегируются меткой C-tag.

	s-custom-port – если во входящем тегированном кадре TIPID=0x8100 или Ethertype for Custom Sports он передается. Если кадр не тегированный или приоритетно тегированный в него добавляется тег port VLAN. Исходящие кадры тегируются меткой Custom S-tag. s-port – если во входящем тегированном кадре TIPID=0x8100 или 0x88A8, он передается. Если кадр не тегированный или приоритетно тегированный в него добавляется тег port VLAN. Исходящие кадры тегируются меткой S-tag. unaware – все входящие кадры, вне зависимости от того есть ли у них тег или нет, тегируются меткой port VLAN (PVID). Разрешенные VLAN не удаляются на выходе

Пример создания vlan и настройки vlan на физическом интерфейсе:

```
# configure  terminal
(config)# vlan 90
(config-vlan)# name office
(config-vlan)# exit
(config)# interface GigabitEthernet 1/7-8
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 90
```

Разберем команды:

- Создание vlan 90 в глобальной конфигурации;
- Имя Vlan;
- Выбор необходимых интерфейсов для настройки (порт 7 и 8);
- Перевод интерфейсов в режим trunk;
- Добавление vlan 90 (tagged).

Пример настройки порта в hybrid:

```
# configure  terminal
(config)# vlan 10,20,30,40,50,60
(config-vlan)# exit
(config)# interface GigabitEthernet 1/1-4
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid allowed vlan 10,20,30,40,50,60
(config-if)# switchport hybrid tagged vlan add 10,20,30
(config-if)# switchport hybrid untagged vlan  add 40,50,60
(config-if)# switchport hybrid ingress-filtering
(config-if)# switchport hybrid native vlan 40
```

Пример настройки порта в **access**:

```
# configure  terminal
(config)# vlan 40
(config-vlan)# exit
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 40
```

4.1.14. Мониторинг и диагностика системных ресурсов

Команды данного раздела предназначены для контроля загрузки центрального процессора (CPU), использования оперативной и энергонезависимой памяти, анализа очередей трафика в сторону CPU, а также проверки статуса системной индикации.

Мониторинг памяти и индикации

Команда	Описание
Привилегированный режим	
`show memory`	Вывод информации об объеме и загрузке оперативной памяти (RAM), средней загрузке системы (Load average), распределении времени CPU (`usr`, `sys`, `idle`, `irq` и др.), а также объеме энергонезависимой памяти (NOR/NAND Flash).
`show system led status`	Отображение текущего состояния и режима работы системного светодиодного индикатора (Status/System LED) на лицевой панели коммутатора (или всех коммутаторов в стеке). В штатном режиме индикатор горит непрерывным зеленым светом (`green`, `solid`); при возникновении системных ошибок или аварийной ситуации индикатор мигает оранжевым светом.

Мониторинг загрузки центрального процессора (CPU)

Команда	Описание
Привилегированный режим	
`show system cpu status`	Отображение общей средней загрузки центрального процессора за интервалы 100 мс, 1 секунду и 10 секунд.
`show system cpu status all`	Вывод общей загрузки CPU с детализацией по всем системным потокам (задачам) коммутатора: ID, имя процесса, состояние (State), приоритет (Prio), нагрузка за 5 сек / 1 мин / 5 мин и время работы.

Детальная диагностика потоков и очередей пакетов CPU

Команда	Описание
Привилегированный режим	
`show system cpu packets status`	Вывод статистики приема/передачи L3-пакетов по программным модулям (LLDP, System_Log,

	DHCP_Helper, IP, IPMC_LIB и др.), максимального времени обработки (Max Rx Callback [ms]), а также загрузки аппаратных очередей извлечения кадров в CPU (Xtr Qu 0–6: sFlow, Port security, OAM, Management, IPMC, BPDU).
`show system cpu packets top [all | range <1-100>]`	Вывод списка программных модулей с наибольшим количеством пакетов в очереди обработки CPU (всех или первых 1–100).
show system cpu thread status [id {<uint> | all}]	Вывод подробного статуса системных потоков коммутатора (по конкретному числовому ID или по всем потокам).
show system cpu thread status backtrace [id {<uint> | all}]	Вывод трассировки стека вызовов (backtrace) для указанного потока или всех потоков (используется для углубленной отладки)
`show system cpu thread top [all | range <1-100>]`	Вывод рейтинга системных потоков, создающих наибольшую нагрузку на процессор (всех или первых 1–100).

4.2. Расширенные настройки

4.2.1. DHCP

4.2.2. DHCPv4

DHCP (протокол динамической настройки узла) – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации, клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры.

Команда	Описание
Глобальные настройки	

`ip dhcp server`
 	
`no ip dhcp server`
	Включить DHCP сервер
	
	Выключить DHCP сервер

`ip dhcp excluded-address <ipv4_addr><ipv4_addr>`
 	
`no ip dhcp excluded-address <ipv4_addr><ipv4_addr>`
	Добавить диапазон-группу исключаемых IP адресов. Обычно адреса шлюзов, так как DHCP сервер не должен раздавать адреса шлюзов клиентам
	
	Удалить диапазон-группу исключаемых IP адресов.

Настройка пула адресов	
`ip dhcp pool <word32>`	Создать пул IP-адресов или войти в режим настройки существующего пула. В качестве аргумента <word32> указывается уникальное буквенно-цифровое имя пула (различает заглавные и строчные буквы, длиной до 32 символов без пробелов).

no ip dhcp	Удалить пул IP-адресов со всеми его настройками.
{host | network} <ipv4_ucast><ipv4_netmask>	Задать сеть для пула (network) или настроить пул для одного хоста (host). Требует ввода IP-адреса хоста или подсети в формате <ipv4_ucast> и маски подсети в формате <ipv4_netmask> (например: 192.168.1.0 255.255.255.0).
no {host | network}	Отменить привязку сети или хоста к пулу. Выдача адресов из этого диапазона прекратится.
address <ipv4_ucast> interface <interface_id>	Выделить фиксированный IP-адрес формата <ipv4_ucast> и жестко закрепить его за клиентом, подключенным к указанному порту/интерфейсу <interface_id>
no address <ipv4_ucast> interface <interface_id>	Удалить привязку фиксированного IP-адреса к указанному интерфейсу. Адрес снова станет доступен для общей динамической выдачи.
lease {<0-365> [<0-23>] [<0-59>] | infinite}	Задать время аренды адреса. Можно указать срок в формате <Дни> [<Часы>] [<Минуты>] (например, lease 1 2 2 – 1 день 2 часа 2 минуты) или использовать ключевое слово infinite для бессрочной аренды. По умолчанию адрес выдается на 24 часа.
no lease	Сбросить время аренды адреса на системное значение по умолчанию (24 часа).
default-router <ipv4_ucast>	Указать IP-адреса основных шлюзов формата <ipv4_ucast>, которые клиенты получат вместе с IP-адресом.
no default-router	Удалить указанный IP-адрес шлюза из настроек пула.
dns-server <ipv4_ucast>	Указать IP-адреса DNS-серверов формата <ipv4_ucast> для разрешения доменных имен.
no dns-server <ipv4_ucast>	Удалить указанный IP-адрес DNS-сервера из настроек пула.
domain-name <word128>	Задать суффикс доменного имени для клиентов. Принимает текстовую строку <word128> длиной до 128 символов.
no domain-name	Удалить имя домена из настроек пула.
bootfile-name <word128>	**Опция 67.** Задать имя загрузочного

no bootfile-name	файла или файла прошивки с соответствующим расширением. Принимает текстовую строку <word128> длиной до 128 символов. Удалить имя загрузочного файла из настроек пула.
tftp-server <word128> no tftp-server	**Опция 66.** Задать IP-адрес или имя TFTP-сервера, где хранятся файлы загрузки. Принимает текстовую или адресную строку <word128> длиной до 128 символов. Удалить адрес TFTP-сервера из настроек пула.
vendor class-identifier <string64> specific-info <word66> no vendor class-identifier <string64>	**Опции 60 и 43.** 1. Компонент vendor class-identifier <string64> включает проверку идентификатора класса вендора (Option 60). Сервер ответит только тем клиентам, которые прислали точно такой же текст. **Строка длиной до 64 символов обязательно пишется в кавычках** "" (например: "Server"). 2. Компонент specific-info <word66> задает специфичные настройки вендора (Option 43). Значение принимает строку <word66> (HEX-код до 64 октетов) и **строго обязательно вводится с префиксом** 0x (например: 0x0104c0a80101). Удалить настройки 60-й и 43-й опций **для указанного класса**.
broadcast <ipv4_ucast> no broadcast	Задать конкретный широковещательный IP-адрес формата <ipv4_ucast> для использования в подсети клиента. Удалить широковещательный адрес. Сервер вернется к стандартному расчету по маске подсети.
client-identifier {mac-address <mac_addr> | name <line128> | fqdn <line128>} no client-identifier {mac-address <mac_addr> | name <line128> | fqdn <line128>}	Привязать IP-адрес к уникальному идентификатору DHCP-клиента (**Option 61**). Позволяет выполнить привязку по физическому MAC-адресу (mac-address), произвольному текстовому имени (name до 128 символов) или по устаревшему формату полного доменного имени (fqdn). Удалить привязку IP-адреса к указанному идентификатору клиента.

client-name <word128>	Задать фиксированное имя хоста для конкретного DHCP-клиента. Принимает строку <word128> длиной до 128 символов.
no client-name	Удалить имя хоста клиента из настроек пула.
hardware-address <mac_address>	Привязать IP-адрес к физическому аппаратному MAC-адресу сетевой карты клиента формата <mac_address>.
no hardware-address <mac_address>	Удалить привязку по MAC-адресу.
netbios-name-server <ipv4_ucast>	Указать IP-адреса серверов имен NetBIOS (WINS) формата <ipv4_ucast> для Windows-клиентов.
no netbios-name-server <ipv4_ucast>	Удалить IP-адрес сервера NetBIOS (WINS) из параметров пула.
netbios-node-type {b-node | h-node | m-node | p-node}	Задать тип узла NetBIOS для настройки порядка разрешения имен. • b-node – только широковещательные запросы (Broadcast) • p-node – только через сервер имён WINS (Peer-to-peer) • m-node – сначала широковещание, затем WINS (Mixed) • h-node – сначала WINS, затем широковещание (Hybrid)
no netbios-node-type	Сбросить тип узла NetBIOS на системное значение по умолчанию.
netbios-scope <word128>	Указать текстовую область NetBIOS (NetBIOS scope string). Принимает строку <word128> длиной до 128 символов.
no netbios-scope	Удалить область NetBIOS из параметров пула.
nis-domain-name <word128>	Задать имя домена службы сетевой информации NIS для Unix-клиентов. Принимает строку <word128> длиной до 128 символов.
no nis-domain-name	Удалить имя домена NIS.
nis-server <ipv4_ucast>	Указать IP-адреса серверов сетевой информации NIS формата <ipv4_ucast>.
no nis-server <ipv4_ucast>	Удалить IP-адрес сервера NIS.
ntp-server <ipv4_ucast>	Указать IP-адреса серверов сетевого времени NTP формата <ipv4_ucast> для синхронизации часов клиентов.

no ntp-server <ipv4_ucast>	Удалить IP-адрес сервера NTP.
Reserved-only no reserved-only	Перевести пул в режим выдачи адресов только для тех устройств, которые явно указаны в командах address. Запросы от всех остальных неизвестных устройств сервер будет игнорировать. Отключить строгий режим. Разрешить динамическую выдачу любых свободных адресов пула всем запрашивающим клиентам.
DHCP Relay	
ip dhcp relay no ip dhcp relay	Включение функции DHCP Relay Выключение функции DHCP Relay
ip dhcp relay server <ipv4_ucast> no ip dhcp relay server	Эта команда настраивает IP адрес сервера DHCP, которому будут перенаправляться запросы клиентов DHCP. Параметр <ipv4_ucast> – это IPv4 адрес сервера DHCP. Данная команда удаляет ранее настроенный адрес сервера DHCP Relay Agent. После выполнения команды устройство перестанет отправлять запросы DHCP данному серверу.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ip dhcp snooping max-client <1-2048>	Команда позволяет ограничить количество DHCP-клиентов, которым разрешено получать динамический IP-адрес на определённом интерфейсе
ip dhcp snooping trust no ip dhcp snooping trust	Настройка режима для порта: Доверенный (Trusted) – порт коммутатора, к которому подключен другой коммутатор или DHCPсервер. DHCP-пакеты, полученные с доверенного порта, не отбрасываются. Ненадёжный (Untrusted) – порт, к которому подключен клиент. DHCP-ответы, приходящие с этого порта, отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database).
Настройка interface vlan	

`ip dhcp snooping`
 	
`no ip dhcp snooping`
	Включение функции DHCP snooping
	
	Выключение функции DHCP snooping

`ip dhcp relay enable`
 	
`no ip dhcp relay enable`
	Данная команда включает режим DHCP Relay Agent на соответствующем интерфейсе устройства.
	
	Данная команда выключает режим DHCP Relay Agent на соответствующем интерфейсе устройства.

`ip helper-address <ipv4_ucast>`
 	
`no ip helper-address`
	Команда задаёт адрес DHCP-сервера, которому будут отправлены DHCP-запросы от клиентов, находящихся в данной подсети (VLAN).
	
	Команда no ip helper-address служит для удаления настройки DHCP Helper Address на интерфейсе.

`ip dhcp server`
 	
`no ip dhcp server`
	Включить DHCP сервер на интерфейсе.
	
	Выключить DHCP сервер на интерфейсе.

Пример настройки DHCP сервера:

```
# configure terminal
(config)# vlan 3
(config-vlan)# exit
(config)# ip dhcp server
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config-if)# exit
(config)# interface vlan 3
(config-if-vlan)#ip address 10.10.10.3 255.255.255.0
(config-if-vlan)#ip dhcp server
(config-if-vlan)# exit
(config)#ip dhcp pool 3
(config-dhcp-pool)#network 10.10.10.0 255.255.255.0
(config-dhcp-pool)#lease 1 0 0
```

4.2.3. DHCPv6

Команда	Описание
Глобальные настройки	
`ipv6 dhcp snooping`	Включить режим DHCPv6 snooping. Когда включен режим DHCPv6 snooping, сообщения запроса клиента DHCPv6 будут пересылаться на доверенные порты и разрешать ответные пакеты только от доверенных портов.

`no ipv6 dhcp snooping`	Выключить режим DHCPv6 snooping
`ipv6 dhcp snooping nh-unknown {allow | drop}`	Выбор обработки неизвестных значений заголовка IPv6. Коммутатор должен анализировать все пакеты IPv6 для клиента DHCPv6, чтобы определить, действительно ли это сообщение DHCPv6 Возможные варианты: `drop`- Отбрасывать пакеты с неизвестными заголовками расширения IPv6. Это наиболее безопасный вариант, но он может привести к перебоям в трафике. `allow`–Разрешить пакеты с неизвестными заголовками расширения IPv6. Это менее безопасный вариант, но он предотвращает перебои в трафике.
Dhcp6_Relay для определенного vlan.	
`interface vlan <vlan_list>`	Создание интерфейса Vlan
`ipv6 dhcp relay interface vlan <vlan_id>`	Указание идентификатора интерфейса, используемого для ретрансляции.
`ipv6 dhcp relay destination <ipv6_ucast>`	Указание адреса IPv6. IPv6-адрес сервера DHCPv6, на который должны быть ретранслированы запросы. Значение по умолчанию «ff05 :: 1: 3» означает «любой DHCP-сервер».
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

`ipv6 dhcp snooping trust`
 	
`no ipv6 dhcp snooping trust`
	Настройка режима работы порта как надежный источник сообщений DHCPv6.
	
	Отмена команды и установка режима работы как ненадежный источник сообщений DHCPv6.

4.2.4. DHCPv6 опции 37 и 38

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) применяется для автоматической выдачи клиентам IPv6-адресов, префиксов и прочих необходимых настроек. Если клиент запрашивает конфигурационные параметры у удалённого DHCPv6-сервера, расположенного вне своего сегмента сети, он обращается к нему через DHCPv6 Relay. Получив сообщение от клиента, реле отправляет его серверу в пакете типа “relay-forward”, а ответ от сервера возвращается аналогично в сообщении “relay-reply”.

Однако при использовании DHCPv6 Relay возникают проблемы, такие как защита от нелегальных присваиваний адресов и необходимость точного назначения IPv6-адреса конкретному устройству. Для их решения применяются дополнительные опции DHCPv6 – опции 37 ("Subscriber-ID") и 38 ("Remote ID"), подробно описанные в документах RFC4649 и RFC4580 соответственно.

Эти опции помогают идентифицировать пользователей и устройства, гарантируют прозрачность процедуры распределения адресов и упрощают отслеживание запросов в больших сетях. DHCPv6 Relay добавляет указанные опции к исходящим запросам клиента

и удаляет их из полученных ответов сервера, обеспечивая таким образом полную непрозрачность для конечного клиента.

Команда	Описание
В глобальном режиме	
`ipv6 dhcp snooping remote-id option` `no ipv6 dhcp snooping remote-id option`	Включить поддержку опции 37 в `DHCPv6-snooping`. Выключить поддержку опции 37 в `DHCPv6-snooping`.
`ipv6 dhcp snooping subscriber-id option` `no ipv6 dhcp snooping subscriber-id option`	Включить поддержку опции 38 в `DHCPv6-snooping`. Выключить поддержку опции 38 в `DHCPv6-snooping`.
`ipv6 dhcp snooping remote-id policy [drop|keep|replace]` `no ipv6 dhcp snooping remote-id policy`	Настроить режим политики при получении DHCPv6 запроса, который уже содержит опцию 37: `drop` - запрос будет отброшен; `keep` - запрос будет передан без обработки; `replace` - поле опции 37 будет добавлено агентом. Восстановить значение по умолчанию `(replace)`.
`ipv6 dhcp snooping subscriber-id policy [drop|keep|replace]` `no ipv6 dhcp snooping subscriber-id policy`	Настроить режим политики при получении DHCPv6 запроса, который уже содержит опцию 38: `drop` - запрос будет отброшен; keep - запрос будет передан без обработки; `replace` - поле опции 38 будет добавлено агентом. Восстановить значение по умолчанию `(replace)`.
`ipv6 dhcp snooping subscriber-id select pv delimiter [<cr>|<word>]` `no ipv6 dhcp snooping subscriber-id select pv delimiter`	Выбрать разделитель между наименованием порта для опции 38. Доступны символы `#|.|,|;|:|/|+|пробел`. Восстановить значения по умолчанию - без разделителя.
`ipv6 dhcp relay remote-id option` `no ipv6 dhcp relay remote-id option`	Включить поддержку опции 37 в `DHCPv6-relay`. Выключить поддержку опции 37 в `DHCPv6-relay`.
`ipv6 dhcp relay subscriber-id option` `no ipv6 dhcp relay subscriber-id option`	Включить поддержку опции 38 в `DHCPv6-relay` Выключить поддержку опции 38 в `DHCPv6-relay`
`ipv6 dhcp relay subscriber-id select pv delimiter [<cr>|<word>]` `no ipv6 dhcp relay subscriber-id select delimiter`	Выбрать разделитель между наименованием vlan для опции 38. Доступны символы `#|.|,|;|:|/|+|пробел`. Восстановить значения по умолчанию - без разделителя.

В режиме настройки порта коммутатора	
ipv6 dhcp snooping remote-id <word128> no ipv6 dhcp snooping remote-id	Задать содержание опции 37 строкой <remote-id>, не более 128 символов. Восстановить значение по умолчанию (VLAN MAC).
ipv6 dhcp snooping subscriber-id <word128> no ipv6 dhcp snooping subscriber-id	Задать содержание опции 38 строкой <subscrider-id>, не более 128 символов. Восстановить значение по умолчанию (VLAN+port)
В режиме настройки vlan интерфейса	
ipv6 dhcp relay remote-id <word128> no ipv6 dhcp relay remote-id	Задать содержание опции 37 строкой <remote-id>, не более 128 символов. Восстановить значение по умолчанию (VLAN MAC).
ipv6 dhcp relay subscriber-id <word128> no ipv6 dhcp relay subscriber-id	Задать содержание опции 38 строкой <subscrider-id>, не более 128 символов. Восстановить значение по умолчанию (VLAN+port)
Команды просмотра информации	
show ipv6 dhcp snooping[interface|<cr>]	Отображает общую информацию о состоянии функции DHCPv6 Snooping на коммутаторе. Показывает состояние активности, список доверенных интерфейсов. - interface – показать информацию по конкретному интерфейсу. - <cr> – завершить ввод командной строки и вывести общую информацию.
show ipv6 dhcp snooping statistics [interface|<cr>]	Показывает статистику работы функции DHCPv6 Snooping, включая количество обработанных пакетов, обнаруженных атак и отклонённых запросов. - [interface | <cr>] – просмотреть подробную статистику по указанному интерфейсу или вывести общий отчёт.
show ipv6 dhcp snooping statistics zero-suppress [interface|<cr>]	Показывает статистику работы функции DHCPv6 Snooping, включая количество обработанных пакетов, обнаруженных атак и отклонённых запросов. Однако выводит только ненулевые значения статистики, что удобно для быстрого анализа текущих показателей работы DHCPv6 Snooping. - [interface | <cr>] – просмотреть подробную статистику по указанному интерфейсу или вывести общий отчёт.

show ipv6 dhcp snooping table	Отображает подробную информацию по всем подключенным клиентам.
show ipv6 dhcp relay [interface vlan <vlan_id>|<cr>]	Используется для просмотра состояния и конфигурации DHCPv6 Relay агентов на коммутаторе. Эта команда покажет информацию о настроенных VLAN'ax и интерфейсах, используемых для перенаправления DHCPv6-запросов от клиентов к серверам. - interfacevlan<vlan_id> – посмотреть статус агента DHCPv6 Relay для указанного VLAN. - <cr> – вывести общее состояние DHCPv6 Relay.
show ipv6 dhcp relay statistics [interface vlan <vlan_id>|<cr>]	Выведет статистические данные о производительности DHCPv6 Relay, включая число переданных и принятых пакетов, ошибочные пакеты и прочее. - [interfacevlan<vlan_id> | <cr>] – просмотр статистики для конкретного VLAN или общего отчёта.

Пример настройки ipv6 dhcp snooping:

```
# configure terminal
(config)# hostname NTS
NTS(config)# vlan 200
NTS(config-vlan)# exit
NTS(config)# ipv6 dhcp snooping
NTS(config)# ipv6 dhcp snooping remote-id option
NTS(config)# ipv6 dhcp snooping subscriber-id option
NTS(config)# interface GigabitEthernet 1/1
NTS(config-if)# description "client"
NTS(config-if)# switchport access vlan 200
NTS(config-if)# no ipv6 dhcp snooping trust
NTS(config-if)# ipv6 dhcp snooping remote-id 00-03-0f-00-00-01
NTS(config-if)# ipv6 dhcp snooping subscriber-id
vlan200+GigabitEthernet1/1
NTS(config-if)# exit
NTS(config-if)# interface GigabitEthernet 1/24
NTS(config-if)# ipv6 dhcp snooping trust
NTS(config-if)# description "server"
NTS(config-if)# switchport access vlan 200
```

Пример настройки ipv6 dhcp relay:

```
# configure terminal
(config)# hostname NTS
NTS(config)# vlan 10,20
NTS(config-vlan)# exit
NTS(config)# ipv6 dhcp relay remote-id option
NTS(config)# ipv6 dhcp relay subscriber-id option
NTS(config)# interface vlan 10
```

```
NTS(config-if)# ipv6 address 2001:da8:10:1::1/64
NTS(config-if)# ipv6 dhcp relay destination 2001:da8:100:1::2
interface vlan 20
NTS(config-if)# ipv6 dhcp relay remote-id 00-03-0f-00-00-02
NTS(config-if)# ipv6 dhcp relay subscriber-id
vlan20+GigabitEthernet1/2
```

4.2.5. DHCP snooping и опция 82

DHCP snooping контролирует процесс получения DHCP-клиентом IP-адреса для предотвращения атак DHCP и появления нелегитимных DHCP-серверов в сети, устанавливая доверенные и не доверенные порты. Сообщения из доверенных портов передаются коммутатором без проверки. Доверенные порты используются для подключения DHCP-сервера или DHCP-ретранслятора, а не доверенные - для подключения DHCP-клиентов. Коммутатор передает сообщения DHCP-запросов из не доверенных портов, но не передает DHCP-ответы. Опция 82 позволяет коммутатору добавлять в DHCP-запросы клиента информацию remote-id (идентификатор коммутатора) и circuit-id (идентификатор порта коммутатора) перед передачей запроса на DHCP-сервер.

Команда	Описание
В глобальном режиме	
`ip dhcp snooping vlan <vlan_list>`	Включить контроль протокола DHCP в пределах выбранной vlan.
`ip dhcp snooping max-client <1-2048>`	Установить максимальное количество клиентов.
`ip dhcp snooping information option format [ascii|hex]`	Установить формат значений опции 82.
`ip dhcp snooping information option`	Разрешить коммутатору добавление опции 82 при работе протокола DHCP.
`ip dhcp snooping information option allowed-untrusted`	Разрешить принимать DHCP-пакеты с опцией 82 от «ненадежных» портов.
`ip dhcp snooping information option circuit-id`	Установить идентификатор CircuitID опции 82. **hostname** Системное имя **port** Порт в формате `Gigabitethernet<stacked>/<interfaceid>` **remote-mac** MAC-address клиента **string** формат определяется пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **switch-mac** MAC-address коммутатора **vlan** Идентификатор vlan <vid> При определении можно использовать шаблоны: **%h**: hostname; **%p**: короткое имя порта, например gi1/1; **%P**: длинное имя порта, например,

	gigabitethernet 1/1; **%m**: мак-адрес порта в формате H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H; **%s**: номер юнита в стеке; **%n**: номер порта; **%i**: IP адрес клиента; **%v**: идентификатор vlan; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
`ip dhcp snooping information option delimiter`	Установить формат разделителя **colon**Символ':' **dot**Символ'.' **none**без символа **slash**Символ '/' **space**Пробел
`ip dhcp snooping information option remote-id`	Установить идентификатор Remote agent ID опции 82. **hostname** Системное имя **string** формат определяется пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **mac** MAC-address коммутатора При определении можно использовать шаблоны: **%h**: hostname; **%m**: мак-адрес порта в формате H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
В режиме настройки интерфейса	
`ip dhcp snooping max-client <1-2048>`	Установить максимальное количество клиентов для этого порта.
`no ip dhcp snooping trust`	Установить порт, как не доверенный. По умолчанию все порты доверенные.
`ip dhcp snooping information option`	Разрешить добавление опции 82 при работе протокола DHCP для этого порта.
`ip dhcp snooping information option global`	Использовать настройки глобальной конфигурации опции 82 при работе протокола DHCP для этого порта.
`ip dhcp snooping information option circuit-id`	Установить идентификатор CircuitID опции 82. **hostname** Системное имя **port** Порт в формате Gigabitethernet<stacked>/<interfaceid> **remote-mac** MAC-address клиента

	string формат определяется пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **switch-mac** MAC-address коммутатора **vlan** Идентификатор vlan <vid> При определении можно использовать шаблоны: **%h**: hostname; **%p**: короткое имя порта, например gi1/1; **%P**: длинное имя порта, например, gigabitethernet 1/1; **%m**: мак-адрес порта в формате H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H; **%s**: номер юнита в стеке; **%n**: номер порта; **%i**: IP адрес клиента; **%v**: идентификатор vlan; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
`ip dhcp snooping information option delimiter`	Установить формат разделителя **colon**Символ':' **dot**Символ'.' **none**без символа **slash**Символ '/' **space**Пробел
`ip dhcp snooping information option format [ascii|hex]`	Установить формат значений опции 82 для этого порта.
`ip dhcp snooping information option remote-id`	Установить идентификатор Remote agent ID опции 82. **hostname** Системное имя **string** формат определяется пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **mac** MAC-address коммутатора При определении можно использовать шаблоны: **%h**: hostname; **%m**: мак-адрес порта в формате H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
Команды просмотра информации	
`show ip dhcp snooping [interface|vlan]`	Отображает информацию о включенном DHCP Snooping: статусе функции,

	доверенных портах, VLAN-ах на интерфейсах.
`show ip dhcp snooping status [interface]`	Отображает статус количества подключенных клиентов.
`show ip dhcp snooping table`	Отображает подробную информацию по всем подключенным клиентам.
`show ip dhcp detailed statistics snooping [interface]`	Отображает статистику по работе DHCPSnooping на интерфейсах.

Пример настройки:

```
# configure terminal
(config)# hostname NTS
NTS(config)# vlan 200
NTS(config-vlan)# exit
NTS(config)# ip dhcp snooping vlan 200
NTS(config)# ip dhcp snooping information option
NTS(config)# ip dhcp snooping information option remote-id %h
NTS(config)# ip dhcp snooping information option format ascii
NTS(config)# interface GigabitEthernet 1/1
NTS(config-if)# description "client"
NTS(config-if)# switchport access vlan 200
NTS(config-if)# no ip dhcp snooping trust
NTS(config-if)# ip dhcp snooping information option
NTS(config-if)#  ip dhcp snooping information option circuit-id
string "NTS_port1"
NTS(config-if)# exit
NTS(config-if)# interface GigabitEthernet 1/24
NTS(config-if)# description "server"
NTS(config-if)# switchport access vlan 200
```

4.2.6. DHCP-опции 60 и 61

Опции 60 и 61 – это параметры DHCP-протокола, используемые для идентификации сетевых устройств при получении IP-адреса.

Option 60 (Vendor Class Identifier) указывает тип устройства (например, IP-телефон, ТВ-приставка).

Option 61 (Client Identifier) указывает конкретное устройство (обычно MAC-адрес).

Команда	Описание
Команда в режиме конфигурирования interface vlan	
`ip address dhcp class-id [GigabitEthernet <port_type_id> | 10GigabitEthernet <port_type_id> | ascii <word31> | hex <word64>]`	Настройка формата и записи опции 60
`no ip address dhcp class-id`	Удаление пользовательской записи опции 60
`ip address dhcp client-id`	Настройка формата и записи опции 61

[GigabitEthernet <port_type_id> | 10GigabitEthernet <port_type_id> | ascii <word31> | hex <word64>]	
no ip address dhcp client-id	Удаление пользовательской записи опции 61

Пример настройки.

```
# configure terminal
(config)# vlan 100
(config)# ip address dhcp
(config)# ip address dhcp client-id ascii 00-00-00-00-00-01
(config)# ip address dhcp class-id ascii npo_telecom
```

4.2.7. DHCP Relay для IPv4

Функцией DHCP Relay-агента является передача DHCP-пакетов от клиента к серверу и обратно в случае, если сервер и клиент находятся в разных подсетях. Другой функцией является добавление дополнительных опций в DHCP-запросы клиента (например, опции 82).

Принцип работы DHCP Relay-агента: коммутатор принимает от клиента DHCP-запросы и передает их серверу от имени клиента (в зависимости от конфигурации, добавляя свои опции или оставляя принятые от клиента). Получив ответ от сервера, коммутатор передает его клиенту.

При настройке коммутатора в режиме DHCP Relay можно значительно повысить эффективность сети за счёт сокращения количества DHCP-серверов, которые при другой схеме понадобились бы для каждой подсети.

Команда	Описание
В глобальном режиме	
ip dhcp relay	Включить DHCP Relay-агент.
ip dhcp relay server <ipv4_ucast>	Задать IP-адрес DHCP-сервера для DHCP Relay - агента.
ip dhcp relay information policy	Выбрать режим обработки DHCP-пакетов с опцией 82: - keep – пропускает пакеты без изменений (настроено по умолчанию); - replace – замещает содержимое опции 82; - drop – отбрасывает пакеты с опцией 82.
ip dhcp relay information option	Разрешить добавление опции 82 при работе протокола DHCP.
ip dhcp relay information option circuit-id	Установить идентификатор CircuitID опции 82. **hostname** Системное имя **port** Порт в формате Gigabitethernet<stacked>/<interfaceid> **remote-mac** MAC-address клиента **string** формат определяется

	пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **switch-mac** MAC-address коммутатора **vlan** Идентификатор vlan <vid> При определении можно использовать шаблоны: **%h**: hostname; **%p**: короткое имя порта, например gi1/1; **%P**: длинное имя порта, например, gigabitethernet 1/1; **%m**: мак-адрес порта в формате H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H; **%s**: номер юнита в стеке; **%n**: номер порта; **%i**: IP адрес клиента; **%v**: идентификатор vlan; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
`ip dhcp relay information option remote-id`	Установить идентификатор Remote agent ID опции 82. **hostname** Системное имя **string** формат определяется пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **mac** MAC-address коммутатора При определении можно использовать шаблоны: **%h**: hostname; **%m**: мак-адрес порта в формате H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
`ip dhcp relay information option format [ascii|hex]`	Установить формат значений опции 82.
`ip dhcp relay information option delimiter`	Установить формат разделителя **colon**Символ':' **dot**Символ'.' **none**без символа **slash**Символ '/' **space**Пробел
В режиме настрйки интерфейса vlan	
`ip dhcp relay enable`	Включить работуDHCPRelay-агента на интерфейсе.
`ip dhcp relay information option`	Разрешить добавление опции 82 при

	работе протокола DHCPна интерфейсе.
ip dhcp relay information option circuit-id	Установить идентификатор CircuitID опции 82 на интерфейсе. **hostname** Системное имя **port** Порт в формате Gigabitethernet<stacked>/<interfaceid> **remote-mac** MAC-address клиента **string** формат определяется пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **switch-mac** MAC-address коммутатора **vlan** Идентификатор vlan <vid> При определении можно использовать шаблоны: **%h**: hostname; **%p**: короткое имя порта, например gi1/1; **%P**: длинное имя порта, например, gigabitethernet 1/1; **%m**: мак-адрес порта в формате H-H-H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H-H-H; **%s**: номер юнита в стеке; **%n**: номер порта; **%i**: IP адрес клиента; **%v**: идентификатор vlan; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
ip dhcp relay information option remote-id	Установить идентификатор Remote agent ID опции 82 на интерфейсе. **hostname** Системное имя **string** формат определяется пользователем, которое заключается в двойные кавычки (""). Строка может содержать любые символы, включая специальные символы и пробелы. **mac** MAC-address коммутатора При определении можно использовать шаблоны: **%h**: hostname; **%m**: мак-адрес порта в формате H-H-H-H-H-H-H-H; **%M**: мак-адрес системы в формате H-H-H-H-H-H-H-H; **%c**: мак-адрес клиента в формате H-H-H-H-H-H.
ip dhcp relay information option format [ascii|hex]	Установить формат значений опции 82 на интерфейсе.
ip dhcp relay information option delimiter	Установить формат разделителя **colon**Символ':'

	dotСимвол'.' **none**без символа **slash**Символ '/' **space**Пробел
`ip dhcp relay information option global`	Использовать настройки глобальной конфигурации опции 82 для этого порта.
Команды просмотра информации	
`show ip dhcp relay`	Просмотр конфигурации DHCP Relay-агента.
`show ip dhcp relay statistics`	Просмотр конфигурации и статистики по работе DHCPRelay-агента.
`show ip dhcp detailed statistics relay [interface]`	Просмотр детальной статистики работы DHCPRelay-агента на интерфейсах.

Пример настройки:

```
# configure terminal
(config)# ip routing
(config)# hostname NTS
NTS(config)# vlan 102,200
NTS(config-vlan)# exit
NTS(config)# ip dhcp relay
NTS(config)# ip dhcp relay server 192.168.200.1
NTS(config)# ip dhcp relay information option
NTS(config)# ip dhcp relay information policy replace
NTS(config)# ip dhcp relay information option circuit-id %v
NTS(config)# ip dhcp relay information option remote-id %c
NTS(config)# ip dhcp relay information option format hex
NTS(config)# interface GigabitEthernet 1/1
NTS(config-if)# description "client"
NTS(config-if)# switchport access vlan 102
NTS(config-if)# exit
NTS(config)# interface GigabitEthernet 1/24
NTS(config-if)# description "server"
NTS(config-if)# switchport access vlan 200
NTS(config-if)# exit
NTS(config)# interface vlan 102
NTS(config-if-vlan)# ip address 192.168.102.200 255.255.255.0
NTS(config-if-vlan)# ip dhcp relay enable
NTS(config-if-vlan)# exit
NTS(config)# interface vlan 200
NTS(config-if-vlan)#  ip address 192.168.200.2 255.255.255.0
```

4.2.8. BOOTP

BOOTP – сетевой протокол, используемый для автоматического получения клиентом IP-адреса.

Пример настройки ip-адреса 192.168.102.200 для bootp-клиента (коммутатора) с MAC адресом 1c:a0:d3:40:9d:b2 на DHCP-сервере.

```
allow bootp;
```

```
subnet 192.168.102.0 netmask 255.255.255.0 {
range 192.168.102.10 192.168.102.30;
default-lease-time 600;
max-lease-time 7200;
option routers 192.168.102.1;
host switch_NTS {
hardware ethernet 1c:a0:d3:40:9d:b2;
fixed-address 192.168.102.200;
}
}
```

Команда режима настройки interface vlan	Описание
`ip address bootp`	Включение получения ip-адреса по протоколу bootp
Команда просмотра информации о ip адресе	
`show interface vlan <vlan_list>`	

Пример настройки:

```
# configure terminal
(config)# interface vlan 2
(config-if-vlan)# ip address bootp
(config-if-vlan)# exit
(config)# interface GigabitEthernet 1/2
(config-if)# switchport access vlan 2
(config-if)# exit
(config)# exit
```

Просмотр информации:

```
# show interface vlan 2
VLAN 2
LINK: 1c-a0-d3-40-9d-b2 Mtu:1500 <BROADCAST MULTICAST>
IPv4: 192.168.102.200/16 192.168.255.255
IPv6: fe80::1ea0:d3ff:fe40:9db2/64 <>
BOOTP: State: BOUND server: 192.168.102.1
```

4.2.9. Уровни привилегий. Privilege Levels

Команда	Описание
Глобальные настройки	
`Web privilege group { APS | Aggregation | Alarm | CFM | DDMI | DHCP | DHCPv6_Client | Debug | Diagnostics | ERPS | ETH_LINK_OAM | Firmware | Green_Ethernet | IP | IPMC_Snooping | LACP | LLDP | Loop_Protect | MAC_Table | MRP | MVR | Miscellaneous | NTP | POE | Ports | Private_VLANs |`	Выбор группы и настройка уровня привилегий для одного или нескольких модулей: -System: Contact, Name, Location, Timezone, Daylight Saving Time, Log; -Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard;

QoS | RMirror | Security(access) | Security(network)| Spanning_Tree | System | UDLD | UPnP | VCL | VLAN_Translation | VLANs | Voice_VLAN | XXRP | sFlow | uFDMA_AIL | uFDMA_CIL} level {configRoPriv | configRwPriv | statusRoPriv | statusRwPriv} <0-15>	-IP: все, кроме ping; -Ports: все, кроме VeriPHY; -Diagnostics: ping и VeriPHY; - Maintenance: CLI - System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web - Users, Privilege Levels и все в Maintenance; -Debug configRoPriv – Конфигурация: толькочтение configRwPriv – Конфигурация: чтение и запись statusRoPriv – Статус/статистика: только чтение statusRwPriv – Статус/статистика: чтение и запись Уровень привилегий группы от 0 до 15. Привилегия пользователя должна быть такой же или больше, чем уровень этой группы, чтобы иметь доступ к этой группе.
ip dhcp excluded-address <ipv4_addr><ipv4_addr> no ip dhcp excluded-address <ipv4_addr><ipv4_addr>	Добавить диапазон-группу исключаемых IP адресов. Обычно адреса шлюзов, так как DHCP сервер не должен раздавать адреса шлюзов клиентам Удалить диапазон-группу исключаемых IP адресов.

4.2.10. Механизмы управления парольной политикой безопасности. Ограничение неуспешных попыток входа.

Настройка политики паролей.

Настроив политику паролей, вы повысите общую безопасность своей сети, сделав процесс аутентификации пользователей более надежным и защищенным.

Команда	Описание
Глобальные настройки	
password history no password history password history size <1-50> password min-length <0-128>	Включение истории паролей; Выключение истории паролей; Команда устанавливает размер хранилища истории паролей; Команда задаёт минимальное число символов, которое должно содержаться в пароле пользователя.;

`password complexity-level { medium| strong | weak}`	Задание уровня сложности пароля: - weak (слабый) – самый низкий уровень требований к сложности пароля. Пользователь может задать простой пароль, состоящий лишь из простых комбинаций символов (например, только маленькие буквы или только числа). - medium (средний) – средний уровень сложности. Пароль должен содержать сочетание различных типов символов, таких как большие и малые буквы, цифры и специальные символы. - strong (сильный) – высокий уровень сложности. Этот уровень требует наиболее строгих правил составления пароля, включающих разнообразные типы символов, что делает подбор пароля значительно труднее.
`password lifetime <0-90>`	Назначение срока жизни пароля Срок жизни пароля определяется числом месяцев, в течение которого пользователь обязан сменить пароль. По истечении установленного интервала система потребует смены пароля.

Настройка блокировки локальной учетной записи при неудачных попытках авторизации.

Реализован функционал блокировки локальной учетной записи при неудачных попытках авторизации. Настройка функционала реализована в глобальной конфигурации коммутатора.

(config)#passwords lockout <1-5> Установить количество идущих подряд попыток ввода пароля с ошибкой до блокировки локальной учетной записи пользователя.

(config)#passwords time block <0-7200> Установить время блокировки локальной учетной записи пользователя.

Пример конфигурации:

passwords lockout 2 passwords time block 90

Примечание: команда **no passwords lockout** и **nopasswords time block** сбросит значение по умолчанию на**:**

passwords lockout 3 passwords time block 0

После двух неудачных попыток авторизации заблокировать пользователя на 90 секунд.

#show users accounts Просмотр списка пользователей, статуса блокировки и таймера блокировки

#show users accounts

UserName Privilege Locked State Left time

-------- --------- ------------ ---------

user	15	locked	87
admin	15	usable	0

#set username username activeРазблокировать пользователя, заблокированного по причине неверного ввода пароля.

#set username user active

#show users accounts

UserName	Privilege	Locked State	Left time
--------	---------	------------	---------
user	15	usable	0
admin	15	usable	0

4.2.11. Конфигурация аутентификации, авторизации и учета. Authentication, Authorization, Accounting

Authentication (аутентификация) – сопоставление запроса существующей учётной записи в системе безопасности.

Authorization (авторизация, проверка уровня доступа) – сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий.

Accounting (учёт) – слежение за потреблением ресурсов пользователем.

Команда	Описание
Глобальные настройки	
`aaa authentication login {console | http | ssh | telnet} {local | radius | tacacs}`	`Local` - использовать локальную базу данных на коммутаторе для проверки подлинности; `Radius` - использовать удаленные серверы RADIUS для аутентификации; - `Tacacs` - использовать удаленные серверы TACACS для аутентификации;
`no aaa authentication login {console | http | ssh | telnet}`	Отключение аутентификации, и вход в систему невозможен;
`aaa authentication enable default { tacacs | radius } enable`	Данная команда настраивает порядок аутентификации администраторов при входе в привилегированный режим.
`aaa authorization {console | ssh | telnet } tacacs`	`Tacacs` – для авторизации команд используется один или несколько удаленных серверов TACACS+. Если все удаленные серверы находятся в автономном режиме, пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий.
`no aaa authorization {console`	Отключение авторизации. Пользователь получает доступ к командам CLI в

`| ssh | telnet }`
 	
`aaa authorization { console | ssh | telnet } commands {0-15} config-commands`
	соответствии со своим уровнем привилегий
	
	Авторизации команд позволяет ограничить количество команд CLI, доступных пользователю. Пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий 0-15. Использование удаленного сервера TACACS+ для авторизации команд. Если все удаленные серверы отключены, пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий.

`aaa accounting {console | ssh | telnet } tacacs commands {0-15} exec`
 	
`No aaa accounting {console | ssh | telnet }`
	`Commands` - Включает учет всех команд с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15. Оставьте поле пустым, чтобы отключить учет команд.
	`Exec` - Режим учета EXEC
	
	Отключение учета

Пример настройки TACACS для ssh с ограничением пользователей по вводу команд commands sets:

```
# configure  terminal
(config)# tacacs-server host 10.10.10.5 timeout 60 key
unencrypted test
(config)# aaa authentication login ssh tacacs local
(config)# aaa authorization ssh tacacs commands 15 config-
commands
(config)# aaa accounting ssh tacacs commands 15 exec
```

4.2.12. Конфигурация SSH, Telnet, HTTP, HTTPS

Команда	Описание
Глобальные настройки	

`ip ssh`
 	
`no ip ssh`
	Включить ssh
	
	Выключить ssh

`ip telnet`
 	
`no ip telnet`
	Включить `telnet`
	
	Выключить `telnet`

`ip http server`
 	
`no ip http server`
	Включение режима HTTP
	
	Выключение режима HTTP

`ip http secure-server`
 	
`no ip http secure-server`
	Включение режима HTTPS.
	
	Выключение режима HTTPS

ip http secure-certificate {delete | generate | upload} No ip http secure-certificate	Настройка обслуживания сертификации. Возможные действия: Delete – удалить сертификат Upload – загрузка сертификата, можно выбрать два метода загрузки. Необходимо ввести ссылку на сертификат. Generate – создание сертификата. Отключение сертификации
ip http secure-redirect No ip http secure-redirect	Включение режима автоматического перенаправления HTTPS. Применяется только, если для режима работы HTTPS включен. Автоматически направляет HTTP web-браузера на соединение HTTPS, когда включены оба режима работы – HTTPS и Automatic Redirect выключение режима автоматического перенаправления HTTPS
Настройка шифрования SHH	
crypto key generate dsa	Включение генерации пары ключей DSA (Digital Signature Algorithm). Фиксированная длина ключа составляет 1024 бита.
crypto key generate ecdsa	Служит для включения генерации пар криптографических ключей, использующих алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm). Этот алгоритм основан на математике эллиптических кривых и предназначен для создания цифровых подписей.
crypto key generate ecdsa size <256,384,521>	Число бит, определяющее размер создаваемого ключа для алгоритма ECDSA. По умолчанию 256 бит.
crypto key generate ed25519	Включение генерации пары асимметричных криптографических ключей с использованием алгоритма Ed25519. Данный алгоритм представляет собой разновидность схемы цифровой подписи, основанной на криптографии с использованием эллиптических кривых (ECC).
crypto key generate ed25519 size <256,384,521>	Число бит, определяющее размер создаваемого ключа для алгоритма Ed25519. По умолчанию 256 бит.
crypto key generate rsa	Включение генерации пары асимметричных криптографических ключей RSA (Rivest-Shamir-Adleman). Эти ключи применяются для шифрования данных, обеспечения конфиденциальности и аутентификации пользователей и

	устройств.
crypto key generate rsa size <1024-3072>	Диапазон бит, определяющее размер создаваемого ключа для алгоритма RSA. По умулчанию 1024 бит.

4.2.13. Конфигурация управления доступом. Access Management Configuration

Команда	Описание
access management no access management	Режим работы: включен. Режим работы: выключен.
access management <1-16><1-4095> {<ipv4_ucast> | <ipv6_ucast>} to <ipv4_ucast>} {telnet | web | snmp} no access management <1-16>	Пример настройки доступа <1-16> – указывает на порядковый номер правила (всего возможно настроить 16 правил) <1-4095> – номер vlan для элемента управления доступом. {<ipv4_ucast> | <ipv6_ucast>} to<ipv4_ucast>} – диапазон ip-адресов для управления доступом. Допускается запись только одного ip-адреса. Telnetweb snmp– сервисы к которым будет предоставлен доступ. Отключение указанного номера записи в списке управления доступом.

Пример настройки access management:

```
# configure  terminal
(config)# access management
(config)# access management 1 1 192.168.102.2 telnet
```

4.2.14. SNMP

Использование протокола управления сетями SNMP (Simple Network Management Protocol) является основным отраслевым стандартом для удаленного мониторинга состояния сетевого оборудования, сбора статистических метрик производительности и оперативного реагирования на аварийные события.

Система позволяет гибко разграничивать права доступа к переменным базы данных управления (MIB) с помощью классической модели разделяемых строк (Community Strings) для ранних версий протокола (SNMPv1/v2c), а также строить сквозные защищенные туннели администрирования на базе продвинутой ролевой модели USM/VACM в рамках стандарта SNMPv3. Архитектура третьей версии полностью исключает перехват управляющего трафика за счет применения криптографических механизмов обязательной авторизации пользователей и блочного шифрования передаваемых пакетов.

Команда	Описание
Глобальные настройки	
snmp-server no snmp-server	Включить snmp-server (по умолчанию snmp-server включен) Выключить snmp-server
snmp max-milliseconds-to-packets <100-10000>	Максимальное время, которое даётся пакетам snmp для отправки в миллисекундах. Значение по умолчанию: 100.
snmp-server engine-id local <word10-64>	Настройка локального идентификатора engineID для SNMPv3. Строка должна содержать четное число символов в 16-ричном формате (число цифр от 10 до 64). **Ограничение:** Комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы.
SNMP community	
snmp-server community <Security name> <Community secret>|encrypted <Use encrypted community secret>	Создание имени и пароля snmp community. <Security name>: Имя группы безопасности или идентификатор сообщества (до 32 символов). <Community secret>: Пароль (community string) в открытом виде (до 32 символов). encrypted: <Use encrypted community secret> Указывает, что вводимый пароль (от 96 до 160 символов) зашифрован (используется для переноса настроек).
snmp-server community <Security name> ip-range <ipv4_addr> <ipv4_netmask> <Community secret> | encrypted <Use encrypted community secret>	Указание ip-адреса и маски источника при доступе по SNMP <ipv4_addr>: Начальный адрес сети. <ipv4_netmask>: Маска подсети Определяет диапазон разрешенных IPv4-адресов управления. (например, 192.168.1.0 255.255.255.0)
snmp-server community <Security name> ipv6-range <ipv6_addr>/<ipv6_netmask> <Community secret> | encrypted <Use encrypted community secret>	Указание ipv6-адреса и маски источника при доступе по SNMP <ipv6_addr>: Начальный адрес сети. <ipv6_netmask>: Маска подсети Определяет диапазон разрешенных IPv6-адресов управления. (например, 2001:db8::/64)
no snmp-server community <word32>	Удаление указанной записи.
SNMP User Configuration	
snmp-server user <word32>	Создание записи user <word32> - имя пользователя, которому принадлежит данный

engine-id <word10-64> {md5 | sha} <word8- 32 | 40> priv {aes | des} <word8-32>	параметр. Допустимая длина строки 1~32 символов ASCII с 43 номерами в диапазоне от 0x21 до 0x7E. engine-id <word10-64> - идентификатор. В архитектуре SNMPv3 используется модель безопасности на основе пользователя USM (User based Security Model) для обеспечения безопасности сообщений и модель управления доступом на основе вида VACM (View-based Access Control Model) при управлении доступом. Для входа USM ключами входов являются usm User Engine ID и usm User Name. В простом агенте usm User Engine ID всегда совпадает с собственным значением snmp Engine ID агента. В качестве значения также может использоваться значение snmp Engine ID удаленного устройства (SNMP engine), с которым может связываться данный пользователь. Другими словами, если engine ID пользователя равен engine ID системы, то он является локальным пользователем, в противном случае пользователь является удаленным. md5, sha – протоколы аутентификации, если не указывать конкретный протокол – значит протокол отсутствует. При выборе протокола требуется ввести пароль для аутентификации. Aes, des – протоколы конфиденциальности, если протокол не выбран – значит протокол отсутствует. При выборе протокола требуется ввести пароль конфиденциальности.
SNMP Group Configuration	
snmp-server security-to-group model {v1 | v2c | v3} name <word32> group <word32>	Настройка групп SNMP v1 | v2c | v3 – выбор модели безопасности, каждая зарезервирована в соответствии с версией SNMP. name<word32> - назначение имени безопасности group<word32> - назначение имени группы.
no snmp-server security-to-group model {v1 | v2c | v3} name <word32>	Удаление соответствующей группы
SNMP View Configuration	
snmp-server view <word32><word255> {exclude | include}	Настройка области видимости MIB. <word32> – указание имени вида. <word255> – указание OID поддерева. include – поддерево включено в вид. exclude – поддерево исключено из вида. **Правило перекрытия:** если задано exclude, в системе обязательно должно существовать другое правило include, OID которого полностью

	перекрывает данное исключаемое поддерево.
`no snmp-server view <word32><word255>`	Удаление соответствующей записи
SNMP Access Configuration	
`snmp-server access <word32> model {any | v1 | v2c | v3} level {auth | noauth | priv}{read | write} <word32>`	Настройка прав доступа для групп SNMPv3 <word32> - имя группы model – выбор модели безопасности. level – выбор уровня безопасности: • noauth – Аутентификация и конфиденциальность отсутствуют. • auth – Выполняется аутентификация, конфиденциальность (шифрование) отсутствует. • priv – Выполняется аутентификация и обеспечивается конфиденциальность (шифрование). read | write <word32> (второй) – имя вида MIB, определяющего доступ на чтение текущих значений (read) или установку новых значений (write).
`no snmp-server access <word32> model {any | v1 | v2c | v3} level {auth | noauth | priv}`	Удаление настройки прав доступа для указанной группы безопасности с конкретной моделью и уровнем защиты.
Trap Configuration	
`snmp-server host <word32>`	Указывает устройству IP-адрес (IPv4/IPv6) или DNS-имя сервера управления, куда именно отправлять сообщения о критических событиях.
`no snmp-server host <word32>`	Используется для прекращения отправки уведомлений на конкретный адрес.
`shutdown / no shutdown`	Выключение / включение отправки SNMP trap (внутри контекста хоста).
`Version {v1 | v2 | v3} <word63>`	Выбор версии протокола snmp <word63> - trap community (по умолчанию Version v2)
`Host {<domain_name> | <ipv4_ucast> | <ipv6_ucast>} {informs | traps} <1-65535>`	Настройка адреса сервера для отправки SNMP trap/inform. Допустимо указать корректный IP или имя хоста. Выбор режима работы (informs или traps) и указание UDP-порта. **(По умолчанию порт 162)**.
`informs retries<0-255> timeout <0-2147>`	Установка таймера попыток повторения сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 255. Установка таймера сообщений SNMP trap

	inform. Диапазон допустимых значений: от 0 до 2147.
`snmp-server source <ipv4_addr>`	Указывает конкретный IP-адрес источника, с которого будут отправляться сообщения-ловушки (trap) в сеть.
В глобальном режиме настройка snmp trap	
`snmp-server trap <cword>`	Глобально включает генерацию SNMP-трапов для указанного функционального модуля `<cword>`. - `coldStart`: отправляется устройством сразу после перезагрузки. - `warmStart`: отправляется устройством после мягкого перезапуска системы (программный рестарт без прерывания питания чипсета). - `linkUp, linkDown`: уведомления отправляются соответственно при подключении или отключении интерфейса. - `authFail`: уведомление отправляется при неудачной попытке аутентификации SNMP-запроса. - `authOK`: уведомление отправляется при успешной аутентификации SNMP-запроса. - `topologyChange`: отправляется при изменении топологии сети (например, изменение состояния порта). - `newRoot`: уведомление о смене корневого моста в сети. - `alarmTrapStatus`: состояние тревоги устройства. - `sensor1, sensor2`: оповещения о состоянии датчиков открытия двери, переключение питания на аккумулятор (trap для моделей уличных коммутаторов) - `fan`: статус вентиляторов охлаждения. - `dyingGaspsEvent`: событие критического сбоя питания. - `udldPortDisable`: срабатывание UDLD (Unidirectional Link Detection Protocol), отключения порта. - `pmbusPsu1, pmbusPsu2`: уведомления от блока питания (PSU) по протоколу PMbus. - `fallingAlarm, risingAlarm`: изменения пороговых значений сенсоров. - `poeBudgetExceeded`: превышен бюджет PoE (Power over Ethernet). - `entConfigChange`: изменение конфигурации оборудования. - `ipTrapGlobalsMain, ipTrapInterfacesLink`: специальные уведомления IP-подсетей и состояний интерфейсов. - `lldpRemTablesChange`: изменения таблиц

	удаленных устройств LLDP (Link Layer Discovery Protocol).
Привилегированный режим (Диагностика и проверка)	
`show snmp`	Вывод общей статистики работы SNMP-сервера (включая статус режима, локальный Engine ID, а также таблицы сообществ, пользователей, групп, прав доступа и активных видов MIB).
`show snmp access [<word32>]`	Вывод таблицы контроля доступа (VACM). Отображает параметры: Group Name, Security Model, Security Level (NoAuth, NoPriv / Auth / Priv), а также области Read View Name и Write View Name. При указании аргумента `<word32>` фильтрует вывод по имени конкретной группы.
`show snmp community [<word32>]`	Отображение зарегистрированных строк сообществ (Community Strings). Выводит параметры: Community/Security Name, разрешенный диапазон Source IP (где 0.0.0.0/0 – доступ отовсюду) и пароль Community secret. При указании аргумента `<word32>` выводит параметры конкретного сообщества.
`show snmp host [<word32>]`	Вывод параметров серверов назначения для отправки уведомлений. Отображает имя и системный ID хоста, статус активности, ассоциированное Community, IP-адрес (Destination Host), целевой UDP Port, версию протокола (Version) и параметры режима подтверждения (Inform Mode/Timeout/Retry). При указании аргумента `<word32>` фильтрует вывод по имени конфигурации хоста.
`show snmp mib {context | ifmib}`	Просмотр базы данных управления MIB. Опция context отображает доступные контексты MIB; опция ifmib выводит специализированную MIB-информацию и статистику по сетевым интерфейсам коммутатора (включая индексы портов ifIndex).
`show snmp security-to-group [v1 | v2c | v3]`	Отображение таблицы соответствия имен безопасности (Security Names) конкретным группам пользователей. Без аргументов выводит полные данные для всех версий; при указании ключа (v1/v2c/v3) фильтрует вывод по выбранной модели безопасности.
`show snmp trap [<cword>]`	trap [`<cword>`] Просмотр глобального статуса активности отправки трапов. Без аргументов выводит состояние для всех функциональных

	модулей системы; при указании конкретного имени модуля <cword> (например, linkDown, coldStart, DyingaspEvent) отображает статус генерации уведомлений только для этого события.
show snmp user [<word32>]	user [<word32>] Просмотр списка зарегистрированных пользователей SNMPv3. Отображает их локальный или удаленный статус (EngineID), алгоритмы и параметры аутентификации/шифрования. При указании аргумента <word32> фильтрует вывод по имени конкретного пользователя.
show snmp view [<word32>]	Отображение созданных областей видимости MIB (MIB views) с детальным указанием включенных (included) и исключенных (excluded) веток OID. При указании аргумента <word32> фильтрует вывод по имени конкретного вида (например, show snmp view default_view).

Пример настройки SNMPv2c и отправки SNMP-Trap/Inform:

Включает стандартные сообщества чтения/записи и настраивает отправку подтверждаемых уведомлений (informs) на сервер 192.168.10.8 через дефолтный порт 162.

```
#configure  terminal
(config)# snmp-server community private private
(config)# snmp-server community public public
(config)# snmp-server host test
(config-snmps-host)# no shutdown
(config-snmps-host)# host 192.168.10.8 162 informs
(config-snmps-host)# version v2 public
```

Дефолтные параметры (По умолчанию)

Предустановленные заводские параметры системы, активные при отсутствии пользовательской конфигурации:

```
snmp-server
no snmp-server source
snmp-server engine-id local 80009d38031ca0d3433074
no snmp-server contact
no snmp-server location
snmp max-milliseconds-to-packets 100
snmp-server security-to-group model v1 name public group default_ro_group
snmp-server security-to-group model v1 name private group default_rw_group
snmp-server security-to-group model v2c name public group default_ro_group
snmp-server security-to-group model v2c name private group default_rw_group
snmp-server view default_view .1 include
```

```
    snmp-server access default_ro_group model any level noauth
read default_view
    snmp-server access default_rw_group model any level noauth
read default_view write default_view
```

Пример защищенной настройки SNMPv3:

1. Задаем локальный идентификатор (Engine ID) устройства
   `(config)# snmp-server engine-id local 80009d38031ca0d3433074`
2. Создаем пользователя (теперь он физически привязан к текущему engineID)
   `(config)# snmp-server user USM_USER engine-id 80009d38031ca0d3433074 sha AUTH_PASS priv aes PRIV_PASS`
3. Создаем область видимости объектов MIB (View)
   `(config)# snmp-server view MY_VIEW .1 include`
4. Ассоциируем созданного пользователя с группой безопасности
   `(config)# snmp-server security-to-group model v3 name USM_USER group ADMIN_GROUP`
5. Задаем права доступа для этой группы (VACM)
   `(config)# snmp-server access ADMIN_GROUP model v3 level priv read MY_VIEW write MY_VIEW`

4.2.15. RMON

Команда	Описание
Alarm	
`rmonalarm<1-65535> {ifInDiscards | ifInErrors | ifInNUcastPkts |ifInOctets | ifInUcastPkts | ifInUnknownProtos | ifOutDiscards | ifOutErrors | ifOutNUcastPkts | ifOutOctets | ifOutQLen | ifOutUcastPkts} <uint><1-2147483647> {absolute | delta} rising-threshold<-2147483648-2147483647><0-65535> falling-threshold <-2147483648-2147483647><0-65535> {both | falling | rising}`	Настройка аварийных сигналов `<1-65535>` - Индекс `{ifInDiscards | ifInErrors | ifInNUcastPkts |ifInOctets | ifInUcastPkts | ifInUnknownProtos | ifOutDiscards | ifOutErrors | ifOutNUcastPkts | ifOutOctets | ifOutQLen | ifOutUcastPkts}` – выбор переменной `<uint>` – номер интерфейса `<1-2147483647>` - интервал опроса при выборке и сравнении с нижним или верхним пороговым значением. `absolute | delta` –выбор типа. Для указанной переменной тест может быть выполнен для абсолютных значений или их относительного изменения. `rising-threshold<-2147483648-2147483647>` – Включает сигнализацию, когда значение первый раз превысит пороговое значение подъема либо станет меньше, чем пороговое значение спада

	<0-65535> - Индекс подъема для события. falling-threshold <-2147483648-2147483647> - Пороговое значение спада. Если текущее значение станет меньше порогового значения спада и, при этом, последнее значение выборки больше этого порогового значения, то выдается сигнализация. После генерации события спада, другое такое событие не будет сгенерировано до тех пор, пока значение выборки не станет больше порогового 49 значения спада, достигнет порогового значения подъема и снова вернется к пороговому значению спада. <0-65535> - Индекс спада для события {both | falling | rising} - Выбор метода, который будет использоваться для выборки выбранной переменной и вычисления значения, которое сравнивается с пороговыми значениями.
Event	
rmon event <1-65535> {log | trap} description <line127>	Настройка событий. <1-65535>- Индекс {log | trap} – выбор типа log: Когда генерируется событие, генерируется и запись журнала RMON. trap: посылает сообщение trap всем установленным менеджерам сообщений trap. Logtrap: О событии создается запись в журнале, посылается сообщение trap. description <line127>- описание

4.2.16. Port Security

Функция управлением безопасностью порта (Port Security Limit Control) может ограничить число пользователей, которым разрешен доступ к коммутатору на основе MAC-адресов и VLAN ID (выполняется для каждого порта). Как только число пользователей, желающих получить доступ к коммутатору, превысит заданное число, будет немедленно выполнена выбранная операция.

Команда	Описание

Глобальные настройки	
port-security aging	Включить функцию устаревания. Если функция включена, то оценивается «возраст» безопасных MAC-адресов в том смысле, в котором он учитывается параметром Aging Period (Срок устаревания). Когда устаревание включено, с того момента, как конечный хост станет безопасным, запускается таймер. По истечении таймера, коммутатор начинает искать кадры конечного хоста и, если таких кадров не появляется в течение следующего срока устаревания (Aging Period), то предполагается, что конечный хост отключился и на коммутаторе освобождаются соответствующие ресурсы
no port-security aging	Выключить функцию устаревания.
port-security aging time <10-10000000>	Установка срока устаревания. По умолчанию установлен срок устаревания 3600 секунд.
port-security hold time<10-10000000>	Настройка времени удержания, используется для определения того, как долго MAC-адрес хранится в таблице MAC-адресов, если было обнаружено, что он нарушает ограничение. Допустимый диапазон составляет от 10 до 10 000 000 секунд, по умолчанию - 300 секунд.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
port-security	Включение управления ограничением количества хостов порта. Чтобы сделать данную функцию работоспособной, необходимо включить ее как глобально, так и для порта.
no port-security	Выключение управления ограничением количества хостов порта
port-security maximum<0-1023>	Установка максимального числа MAC-адресов, которые могут оставаться безопасными на этом порту. Это число не может превышать 1024.
port-security violation {protect | restrict | shutdown }	Выбор режима при превышении предела MAC-адресов на порту

	Protect – ничего не предпринимать Restrict - Если предел достигнут, последующие MAC-адреса порта будут подсчитаны и отмечены как нарушающие. Такие адреса MAC удаляются из таблицы MAC-адресов по истечении времени удержания. В лучшем случае нарушения предельных значений MAC - адрес может быть помечен как нарушение в любой момент времени. Shutdown- Если предел достигнут, то это приведет к отключению порта. Это означает, что все защищенные MAC-адреса будут удалены из порта и новые адреса не будут изучены.
port-security maximum-violation<1-1023>	Настройка максимального количества MAC-адресов, которые могут быть помечены как нарушающие этот порт. Это число не может превышать 1023. По умолчанию - 4. Он используется только тогда, когда установлен режим restrict
port-security mac-address sticky	Включение прикрепления MAC-адресов к порту. Когда порт находится в режиме sticky, все MAC-адреса, которые в противном случае были бы изучены как динамические, узнаются как закрепленные. Прикрепленные MAC-адреса являются частью рабочей конфигурации и поэтому могут быть сохранены в startup-config. Прикрепленные MAC-адреса сохраняются при изменении ссылок (в отличие от динамических, которые придется запоминать заново). Они также выдерживают перезагрузку, если рабочая конфигурация сохранена в startup-config.
port-security mac-address <mac_ucast> vlan <vlan_id> sticky	добавление статического или закрепленного MAC-адреса, управляемого Port Security. Для добавления статического MAC-адреса ввод sticky опускается.

Пример настройки порта в режиме Restrict:

```
# configure  terminal
(config)#interface GigabitEthernet 1/1
(config-if)# port-security
(config-if)# port-security maximum 20
```

```
(config-if)# port-security violation restrict
(config-if)# port-security maximum-violation 1000
(config-if)# port-security mac-address 00-00-00-00-00-01
```

Пример настройки порта в режиме sticky:

```
# configure  terminal
(config)#interface GigabitEthernet 1/1
(config-if)# port-security
(config-if)# port-security maximum 6
(config-if)# port-security violation restrict
(config-if)# port-security maximum-violation 1000
(config-if)# port-security mac-address sticky
```

4.2.17. NAS (Network Access Server)

Конфигурирование сервера доступа в сеть (Network Access Server) полезно в сетевой среде, в которой желательно аутентифицировать клиентов (supplicants) до того, как они получат доступ к ресурсам защищенной сети. Для эффективного управления доступом для неизвестных клиентов, IEEE разработал стандарт 802.1X, обеспечивающий процедуру аутентификации на порту, предотвращающую несанкционированный доступ к сети по запросам пользователей, впервые предоставляющих учетные данные для целей аутентификации. Коммутатор, соединяющий клиентов и radius-сервер, обычно работает как аутентификатор. Для обмена сообщениями аутентификации между клиентами и удаленным RADIUS-сервером, проверяющим аутентичность пользователя и его права доступа, используется EAPOL (расширенный протокол аутентификации по локальным сетям). На данной странице можно настроить конфигурацию аутентификатора либо глобально, либо для каждого порта отдельно.

Команда	Описание
Глобальные настройки	

`dot1x system-auth-control`
 	
`no dot1x system-auth-control`
	Включение на коммутаторе глобально 802.1X и аутентификацию на основе MAC- адресов.
	
	Выключение на коммутаторе глобально 802.1X и аутентификацию на основе MAC- адресов. Если глобально эти протоколы выключены, передача кадров будет разрешена на всех портах.

`dot1x re-authentication`
 	
`no dot1x re-authentication`
	Включить повторную аутентификацию по истечении интервала времени, заданного в поле "Reauthentication Period" (Интервал повторной аутентификации). Повторную аутентификацию можно использовать для определения того, подключено ли к порту коммутатора новое устройство.

`dot1x authentication timer re-`	Установка интервала времени, по

authenticate <1-3600>	истечении которого подключенное устройство может быть аутентифицировано повторно. По умолчанию установлен интервал повторной аутентификации 3600 секунд. Допустимый диапазон значений от 1 до 3600 секунд.
dot1x timeout tx-period <1-65535>	Установка интервала времени, в течение которого коммутатор будет ожидать ответ от подавшего запрос на доступ к сети устройства в течение сессии аутентификации перед тем, как передать пакет Request Identify (Запрос идентификации) EAPOL. По умолчанию задано 30 секунд. Допустимый диапазон значений от 1 до 65535 секунд.
dot1x authentication timer inactivity <10-1000000>	Установка интервала времени, определяющего допустимое время доступа клиента к коммутатору для аутентификации по 802.1X и MAC-адресу. По умолчанию составляет 300 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд.
dot1x timeout quiet-period <10-1000000>	Установка времени, по истечении которого индицируется отказ EAP, либо превышение интервала ожидания RADIUS, из-за чего клиент не получил доступ. Эта настройка применяется к портам, работающим при аутентификации Single 802.1X, Multi 802.1X или на основе MAC - адресов. По умолчанию время удерживания составляет 10 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд.
dot1x feature radius-qos	Включение QoS, назначенного RADIUS.
dot1x feature radius-vlan	Включение VLAN, назначенного RADIUS.
dot1x feature guest-vlan	Включение гостевого VLAN является специальной VLAN, типичным назначением которой является предоставление ограниченного доступа к сети. Когда функция включена, дубликаты настроек индивидуального порта определяют, может ли порт быть перемещен в гостевую VLAN. Когда функция выключена, возможность перемещения порта в гостевую VLAN отключена на всех портах.
dot1x guest-vlan <1-4095>	Установка номера гостевого vlan, работает только в том случае, когда гостевая VLAN включена. VLAN ID

	представляет собой значение, присваиваемое порту, если порт перемещается в гостевую VLAN. Диапазон значений: от 1 до 4095.
dot1x max-reauth-req<1-255>	Установка максимального числа повторных аутентификаций. Максимальное число передач коммутатором кадра запроса идентификации EAPOL, остающихся без ответа перед тем, как порт будет добавлен в гостевую VLAN. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально. Диапазон 1~255.
dot1x guest-vlan supplicant	Разрешение гостевого VLAN, если виден EAPOL. Коммутатор помнит, был ли принят кадр EAPOL в течение времени жизни порта. Когда коммутатор принимает решение о входе в гостевую VLAN, он сначала проверяет, включена или выключена эта опция. Если она выключена (флаг в поле снят – значение по умолчанию), коммутатор войдет в гостевую VLAN только в том случае, если кадр EAPOL не был принят на порту в течение времени жизни порта. Если опция включена (флаг в поле установлен), коммутатор войдет в гостевую VLAN, даже если кадр EAPOL был принят на порту в течение времени жизни порта. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
dot1x port-control {auto | force-authorized | force-unauthorized | mac-based | multi | single}	Выбирает режим аутентификации порта. Данная настройка работает только в том случае, когда глобально включен NAS. Режимы работы: Auto – В этом режиме работы требуется, чтобы сервером аутентификации был авторизован dot1x-совместимый клиент. Клиентам, не обладающим dot1x-совместимостью, доступ будет запрещен. force-authorized – В этом режиме работы коммутатор отправит один кадр успешной (аутентификации) EAPOL, если осуществляется подключение к порту, при этом любому клиенту на

	порту будет разрешен доступ к сети без аутентификации `force-unauthorized` – В этом режиме работы коммутатор отправит один кадр отказа (аутентификации) EAPOL, если будет осуществляется подключение к порту, при этом любому клиенту на порту будет запрещен доступ к сети. `mac-based` – авторизация на основе MAC – адресов. Не принимаются и не передаются кадры EAPOL. При аутентификации на основе MAC - адресов, для половины клиентов коммутатор работает, как клиентское устройство, пославшее запрос на доступ к ресурсам сети. Начальный кадр (любого типа), отправленный клиентом, анализируется коммутатором, который, в свою очередь, использует MAC - адрес клиента в качестве имени пользователя и пароля в последующем обмене данными с RADIUS-сервером по EAP. 6-байтный MAC - адрес преобразуется в строку вида "xx-xx-xx-xx-xx-xx", где тире (-) используется в качестве символа-разделителя между шестнадцатеричными цифрами (записанными символами нижнего регистра). `Multi` – В режиме работы Multi 802.1X, одно или более клиентских устройств могут быть аутентифицированы на одном и том же порту в одно и то же время. Каждое клиентское устройство аутентифицируется индивидуально; его безопасность в таблице MAC - адресов обеспечивает модуль “Port Security” (Безопасность порта). `Single` – В режиме работы Single 802.1X, аутентифицироваться на порту будет преимущественно одно клиентское устройство, отправившее запрос на доступ к ресурсам сети. Для связи между клиентским устройством и коммутатором используются нормальные кадры EAPOL. Если к порту подключено более одного клиентского устройства, первым из них будет считаться то, которое появилось раньше всех остальных в тот период, когда порт был включен. Если такое клиентское

	устройство не отправило правильной учетной информации в течение заданного времени, шанс получит другое клиентское устройство. Как только клиентское устройство будет успешно аутентифицировано, только ему будет разрешен доступ. Этот режим работы является наиболее безопасным из всех поддерживаемых режимов. В этом режиме для обеспечения безопасности MAC - адреса клиентского устройства используется модуль “Port Security” (Безопасность порта) (после того, как устройство будет успешно аутентифицировано).
`dot1x radius-qos`	включение RADIUS-Assigned QoS на порту
`dot1x radius-vlan`	включение RADIUS-Assigned VLAN на порту
`dot1x guest-vlan`	включение гостевого VLAN на порту
`dot1x re-authenticate`	Рестарт процесса аутентификации

4.2.18. ACL. Списки доступа

ACL является последовательным списком, используемым для разрешения или запрета доступа пользователей к информации или к выполнению задач по сети. В данном коммутаторе пользователи могут задать правила, применяемые к номерам портов для разрешения или запрета операций, или ограничения предельной скорости.

Команда	Описание
Глобальные настройки	
`access-list rate-limiter <1-16> {100kbps | 100pps | pps}`	Настройка ограничения скорости: <1-16> - идентификатор правила {100kbps | 100pps | pps} – выбор единиц измерения, после ввода единиц измерения требуется ввести пороговое значение, при превышении которого пакеты будут отбрасываться.

`access-list ace <1-128>`
 	
`no access-list ace <1-128>`
	Создание правила фильтрации для политики доступа – для определенного порта или для всех портов
	
	Удаление правила

`access-list ace <1-128> ingress {any | interface}`	Выбор входящего порта.
`access-list ace <1-128> policy<0-63>`	Выбор фильтра политики, чтобы отфильтровать конкретную политику по данному ACE. По умолчанию установлен фильтр не присвоен.

access-listace<1-128>frame-type {any | arp | etype | ipv4 | ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp}	Выбор типа кадра. По умолчанию можно использовать любой тип кадра.
access-list ace <1-128> action {deny | filter | permit}	Выбор операции с кадром, который попадает в этот ACE Deny – кадр, попавший в этот ACE, отбрасывается. Permit – кадру, который попадает в этот ACE, предоставляется разрешение на операцию ACE. Filter – кадры, соответствующие ACE, фильтруются.
access-list ace <1-128> rate-limiter <1-16> access-list ace <1-128> rate-limiter disable	Включение ограничения скорости. Выключение ограничения скорости.
access-list ace <1-128> mirror access-list ace <1-128> mirror disable	Включение функции зеркала Выключение функции зеркала
access-list ace <1-128> logging access-list ace <1-128> logging disable	Включение регистрации в системном журнале. Выключение регистрации в системном журнале.
access-list ace <1-128> shutdown access-list ace <1-128> shutdown disable	Включить функцию отключения порта Выключить функцию отключения порта
access-list ace <1-128> tag {any | tagged | untagged}	Выбор кадров в соответствии с тегами 802.1Q. Any – допускается любое значение Tagged– Только кадр с тегами. Untagged – Только кадры без тегов. Значение по умолчанию - Any
access-list ace 1 vid {<1-4095> | any}	Выбор vlanid для данного ACE Any – фильтр не задан
access-list ace 1 tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <0-7> | any}	Выбор значения User Priority (Приоритет пользователя), найденного в теге VLAN
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
access-listpolicy<0-63>	Установка идентификатора правил списка доступа определенному порту. Порт может использовать только один

	идентификатор правил списка доступа, однако, идентификатор правил списка доступа может быть применен ко многим портам. По умолчанию идентификатор имеет значение 0.
access-list action {deny | permit}	Разрешает или запрещает кадр на основе того, согласуется ли он с правилом из присвоенной группы правил.
access-list rate-limiter <1-16>	Установка идентификатора ограничителя скорости, применяемого к порту. Правило ограничения скорости может быть задано в режиме глобальной конфигурации, командой access-list rate-limiter <1-16> {100kbps | 100pps | pps}
access-list redirect interface GigabitEthernet <port_type_list>	Выбор порта, на который перенаправляются согласующиеся кадры.
access-list mirror No access-list mirror	Включение функции зеркалирования. Когда функция зеркалирования включена, копии согласованных кадров будут зеркалироваться в порт назначения. Этим параметром задается зеркалирование порта на основе ACL, а порт зеркалирования задается на общей странице настройки зеркала, реализованной независимо. Выключение функции зеркалирования
access-list logging no access-list logging	Включение регистрации согласующихся кадров в системном журнале. Выключение регистрации
access-list shutdown no access-list shutdown	Выключение порта, когда согласующиеся кадры появляются на порту. Отмена команды
access-list port-state no access-list port-state	Изменение состояния порта. Повторное включение порта, который был выключен правилом acl Изменение состояния порта. Выключение
Настройка Time-base	Описание
time-range <word32>	Команда используется для создания или изменения диапазона времени на коммутаторе. Используется в списках доступа (ACL) для управления доступом к сети в определенные периоды времени.

no time-range [<word32>]	<word32> – это уникальное имя, которое вы даете диапазону времени. Оно может содержать до 32 символов. Команда используется для удаления диапазона времени, который был ранее создан на коммутаторе.
Подрежим настройки time-range	Описание
absolute [start <hhmm><date>] [end <hhmm><date>]	Установка абсолютного времени начала или конца диапазона времени. Время задается в формате часов и минут (HH:MM), а дата – в формате года, месяца и дня (YYYY/MM/DD)
no absolute	Отмена настройки абсолютного времени.
periodic {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday|daily|weekdays|weekend} <hhmm> to [Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday] <hhmm>	Установка периодического времени. Можно указать дни недели (пятница, понедельник, суббота, воскресенье, четверг, вторник, среда) или типы периодов (ежедневно, еженедельно, выходные). Время задается в формате часов и минут (HH:MM).
no periodic {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday|daily|weekdays|weekend} <hhmm> to [Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday] <hhmm>	Отмена настройки периодического времени.
Настройка ACL Time-base	Описание
access-list ace <1-1024> action {permit|deny|filter {switchport <1~53>|interface <port_type_list>}} [time-range {<word>|disable}]	Создание списка доступа (ACL) с указанием номера (от 1 до 1024), действия (разрешить, запретить или фильтровать), порта коммутатора или интерфейса, с диапазоном времени.
Просмотр информации Time-base	
show time-range [<word32>]	Команда используется для отображения информации о диапазоне времени, который был создан на коммутаторе. Эта команда позволяет просмотреть настройки времени, связанные с определенным именем диапазона, или все созданные диапазоны времени.

4.2.19. IP Source Guard. Защита IP-адреса источника

Функция IP Source Guard в Ethernet-коммутаторах предназначена для обеспечения дополнительной защиты от несанкционированных действий пользователей.

4.2.20. IP Source Guard

Команда	Описание
Глобальные настройки	

`ip verify source`
 	
`no ip verify source`
	Включение защиты IP-адреса источника
	
	Выключение защиты IP-адреса источника

`ip verify source translate`
 	
`no ip verify source translate`
	преобразование динамических записей в статические.
	
	Отмена команды

`ip source binding interface GigabitEthernet <port_type_id><vlan_id><ipv4_ucast><mac_ucast>`	Настройка статических правил. Установка соответствий между IP-адресом, номером порта, MAC-адресом и VLAN ID.
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

`ip verify source`
 	
`no ip verify source`
	Включение защиты IP-адреса источника на порту. Для того, чтобы защита IP-адресов источника работала, функция должна быть включена в глобальном режиме и на порту.
	
	Выключение защиты IP-адреса источника на порту.

`ip verify source limit <0-2>`	Выбор максимального числа динамических клиентов на порту. Возможны следующие варианты: 0, 1, 2 Если включен режим работы порта и максимальное число клиентов равно 0, коммутатор будет только передавать IP-пакеты, которые согласуются со статическими элементами списка (IP-адресами) для данного порта. По умолчанию значение unlimited (неограниченное количество)

4.2.21. IPv6 Source Guard

Команда	Описание
Глобальные настройки	

`ipv6 verify source`
 	
`no ipv6 verify source`
	Включение защиты IP-адреса источника
	
	Выключение защиты IP-адреса источника

ipv6 verify source translate no ipv6 verify source translate	преобразование динамических записей в статические. Отмена команды
ipv6 source binding interface GigabitEthernet <port_type_id> {<ipv6_ucast> | vlan}	Настройка статических правил. Установка соответствий между IP-адресом, номером порта, MAC-адресом и VLAN ID.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ipv6 verify source No ipv6 verify source	Включение защиты IP-адреса источника на порту. Для того, чтобы защита IP-адресов источника работала, функция должна быть включена в глобальном режиме и на порту. Выключение защиты IP-адреса источника на порту.
ipv6 verify source limit<0-2>	Выбор максимального числа динамических клиентов на порту. Возможны следующие варианты: 0, 1, 2 Если включен режим работы порта и максимальное число клиентов равно 0, коммутатор будет только передавать IP-пакеты, которые согласуются со статическими элементами списка (IP-адресами) для данного порта. По умолчанию значение unlimited (неограниченное количество)

4.2.22. ARP inspection. Инспекция ARP

Инспекция ARP-пакетов используется для отфильтровывания несанкционированных пакетов ARP. Это позволяет предотвратить многие виды атак класса «man-in-the-middle» (атака «человек посередине»). При обнаружении коммутатором несанкционированного ARP-пакета им автоматически создается фильтр MAC-адресов, блокирующий трафик от MAC-адреса и сети VLAN, от которых поступил несанкционированный ARP-пакет. Период активности фильтра MAC-адресов на коммутаторе можно настраивать.

Команда	Описание
Глобальные настройки	
ip arp inspection no ip arp inspection	Включение функции инспекции ARP-пакетов Выключение функции инспекции ARP-пакетов
ip arp inspection vlan <vlan_list> logging {all | deny | permit}	Выбор VLAN на которых будет включена функция инспекции ARP-пакетов. А также настройка типа записей, передаваемых в журнал.
ip arp inspection entry	Настройка статической записи

interface GigabitEthernet <port_type_id><vlan_id><mac_ucast><ipv4_ucast>	<port_type_id> – номер порта <vlan_id> – номер vlan <vlan_id> – mac-адрес <ipv4_ucast> – ip-адрес
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
no ip arp inspection trust ip arp inspection trust	Включение функции инспекции ARP-пакетов на порту. Выключение функции инспекции ARP-пакетов на порту.
ip arp inspection check-vlan no ip arp inspection check-vlan	Включение проверки VLAN. Выключение проверки VLAN.
ip arp inspection logging {all | deny | permit} no ip arp inspection logging	deny - В журнал помещаются запрещенные записи. permit - В журнал помещаются разрешенные записи. All – В журнал помещаются все записи В журнал ничего не записывается.

4.2.23. Настройка Gratuitous ARP

Gratuitous ARP (GARPs) – это специальный вид пакетов ARP, отправляемых устройством даже тогда, когда оно не запрашивало MAC-адрес другого устройства. Эти пакеты используются для обновления таблиц ARP на соседних устройствах, позволяя своевременно обновлять записи в таблице ARP.

Настройка Gratuitous ARP полезна в ситуациях, когда устройство перемещается внутри сети или изменяется IP-адрес, чтобы быстро обновить таблицы ARP соседей и избежать задержек связи.

Команда	Описание
Настройка интерфейса L3	
ip gratuitous-arp tx-interval <5-200>	Включить периодическую отправку gratuitous-arp кадров (сразу request и reply) с интерфейса L3.
no ip gratuitous-arp	Отключает периодическую отправку gratuitous-arp кадров с L3 интерфейса.
ip gratuitous arp {deny |	Запретить или разрешить получение gratuitous-arp кадров на L3 интерфейсе.

permit}	

Пример:

```
!
interface vlan 10
 ip address 192.168.10.18 255.255.255.0
 ip gratuitous-arp tx-interval 5
ip gratuitous-arp deny
!
```

4.2.24. ARP Proxy

ARP Proxy (Proxy ARP) – это механизм, который позволяет коммутатору отвечать на ARP-запросы, предназначенные для устройств, которые находятся за ним, но не в той же подсети. Это полезно в сетях с несколькими подсетями, где требуется обеспечить взаимодействие между устройствами, находящимися в разных подсетях.

Принцип работы ARP Proxy

Когда устройство отправляет ARP-запрос для IP-адреса, который находится в другой подсети, коммутатор с включенным ARP Proxy отвечает на этот запрос, используя свой MAC-адрес. Это позволяет устройству, отправившему запрос, установить связь с устройством в другой подсети через коммутатор.

Команда	Описание
Команда в глобальном режиме	
ip arp proxy no ip arp proxy	Включает режим проксирования ARP-запросов для коммутатора Отключает режим проксирования ARP-запросов для коммутатора
ip arp timeout <1-4294967295> | default	Настройка времени ожидания ARP-записей в глобальной конфигурации коммутатора. - Параметр <1-4294967295> указывает на диапазон значений времени ожидания. - default – значение по умолчанию 60000 секунд.
Настройка в режиме конфигурирования L3 интерфейса	Описание
ip arp proxy no ip arp proxy	Включает режим проксирования ARP-запросов для конкретного L3 интерфейса. Отключает режим проксирования ARP-запросов для конкретного L3 интерфейса.
ip arp timeout <1-4294967295> | default	Настройка времени ожидания в режиме конфигурирования L3 интерфейса. - Параметр <1-4294967295> указывает на диапазон значений времени ожидания. - default – значение по умолчанию 60000

	секунд.
Команды просмотра информации.	
`show ip arp configuration`	Команда просмотра информации о конфигурации ARP.
`show ip arp`	Команда просмотра информации о ARP.

Пример конфигурации:

SW1

```
hostnameSW1
!
vlan 2-4
!
ip arp proxy
ip arp timeout 60
!
interface GigabitEthernet 1/1
 switchport mode trunk
 switchport trunk allowed vlan 2,3
 description Connect_SW2
!
interface GigabitEthernet 1/2
 switchport access vlan 2
 description Client_A
!
interface VLAN 2
 ip address 192.168.2.1 255.255.255.0
 no ip arp proxy
!
interface VLAN 3
 ip address 192.168.3.1 255.255.255.0
 no ip arp proxy
!
interface VLAN 4
 ip address 192.168.4.1 255.255.255.0
```

SW2

```
hostname SW2
!
vlan 1-4
!
ip arp proxy
ip arp timeout 60
!
interface GigabitEthernet 1/1
 switchport mode trunk
 switchport trunk allowed vlan 2,3
 description Connect_SW1
!
interface GigabitEthernet 1/2
```

```
 switchport access vlan 3
 description Client_B
!
interface VLAN 2
 ip address 192.168.2.2 255.255.255.0
 no ip arp proxy
!
interface VLAN 3
 ip address 192.168.3.2 255.255.255.0
 no ip arp proxy
!
interface VLAN 4
 ip address 192.168.4.2 255.255.255.0
```

4.2.25. Radius

Команда	Описание
Глобальные настройки	
radius-server timeout<1-1000>	Настройка времени ожидания ответа от сервера аутентификации перед тем, как повторить запрос.
radius-server retransmit<1-1000>	Настройка числа повторной передачи запросов на сервер аутентификации.
radius-server deadtime<1-1440>	Настройка времени отсутствия сервера (время, в течении которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос)
radius-server key (unencrypted | encrypted) <line1-63>	Ввод ключа длиной не более 64 символов.
radius-server attribute 4 <ipv4_ucast>	Настройка ipv4-адреса, в качестве атрибута 4 в пакетах запроса доступа RADIUS. По умолчанию используется ip-адрес исходящего интерфейса.
radius-server attribute 95 <ipv6_ucast>	Настройка ipv6-адреса, в качестве атрибута 4 в пакетах запроса доступа RADIUS. По умолчанию используется ip-адрес исходящего интерфейса.
radius-server attribute 32 <line1-253>	Идентификатор длиной не более 256 символов, используемый в качестве атрибута 32 в пакетах запроса доступа RADIUS.
Настройка сервера	
radius-server host<word1-255>	Настройка имени хоста RADIUS сервера или его ip-адрес
radius-server host <имя или ip-адрес> auth-port <0-65535>	Настройка порта UDP, используемого для аутентификации на RADIUS-сервере.
radius-server host <имя или ip-адрес> acct-port <0-65535>	Настройка порта UDP, используемого для аккаутинга.

radius-server host <имя или ip-адрес> timeout <1-1000>	Настройка время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, команду вводить не нужно.
radius-server host <имя или ip-адрес> retransmit <1-1000>	Настройка времени повторной передачи, оно будет использовано вместо глобального значения времени повторной передачи. Если желательно использовать глобальное значение, команду вводить не нужно.
radius-server host <имя или ip-адрес> key (unencrypted | encrypted) <line1-63>	Настройка ключа, оно будет использовано вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, команду вводить не нужно.

Примечание: передать все параметры сервера можно одной строкой, указывая значения параметров последовательно. Сервер, указанный раньше в конфигурации считается основным.

4.2.26. Настройка TACACS+

Команда	Описание
Глобальные настройки	
tacacs-server primary-mode	Включение функционала выбора серверов для опроса, начиная с первого, как они указаны в настройках
tacacs-server timeout<1-1000>	Настройка времени ожидания ответа от сервера аутентификации перед тем, как повторить запрос.
tacacs-server deadtime<1-1440>	Настройка времени отсутствия сервера (время, в течении которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос) Работает только с включенным функционалом tacacs-server primary-mode
tacacs-server key (unencrypted | encrypted) <line1-63>	Ввод ключа длиной не более 64 символов.
Настройка сервера	
tacacs-server host<word1-255>	Настройка имени хоста TACACS+ сервера или его ip-адрес
tacacs-server host <имя или ip-адрес> port <0-65535>	Настройка порта TCP, используемого для аутентификации на сервереTACACS+.
tacacs -server host <имя или ip-адрес> timeout <1-1000>	Настройка время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, команду вводить не нужно.
tacacs-server host <имя или	Настройка ключа, оно будет использовано

ip-адрес> key (unencrypted | encrypted) <line1-63>	вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, команду вводить не нужно.

Примечание: передать все параметры сервера можно одной строкой, указывая значения параметров последовательно. Сервер, указанный раньше в конфигурации считается основным.

4.2.27. LAG

Команда	Описание
aggregation mode (smac|dmac|ip|port) no aggregation mode	Настройка режима работы для расчета линейного порта, через который будет передаваться кадр. smac - используется MAC-адрес источника dmac - используется MAC-адрес назначения ip – используется ip-адрес port - используются порты TCP/UDP назначения и источника. Возможно включение нескольких режимов работы. вернуть стандартное значение
Настройка группы агрегирования	
interface GigabitEthernet <port_type_list>	Выбор интерфейсов для объединения в группу
aggregation group <1-32> mode {active|on|passive}	Назначение id группы и включение режима агрегации On - статическая агрегация Active – режим активной агрегации LACP Passive- режим пассивной агрегации LACP

4.2.28. LACP

LACP (Link Aggregation Control Protocol) – это протокол управления агрегацией каналов, подкомпонент стандарта IEEE 802.3ad.

Он позволяет объединить несколько физических каналов между сетевыми устройствами в один логический канал. В результате каналы, поддерживающие протокол LACP, могут увеличить логическую полосу пропускания и надёжность сети без изменения какой-либо сетевой инфраструктуры.

Кроме того, даже если одна ссылка выходит из строя, в режиме LACP другие доступные члены ссылки в той же группе LACP будут балансировать нагрузку.

LACP использует LACPDU сообщения для обмена информацией с соседней стороной. После включения LACP порт посылает LACPDU, уведомляя ответную сторону о приоритете и MAC-адресе системы, приоритете и адресе порта, и ключе операции. Когда ответный порт получает эту информацию, он сравнивает её с информацией о своих портах, настроенных на агрегацию. Таким образом обе стороны достигают соглашения о включении или исключении порта из динамической группы агрегации.

Команда	Описание

Глобальные настройки	
`lacp system-priority<1-65535>`	Настройка значения `system-priority`. По умолчанию - 32768
Настройки портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`lacp port-priority <1-65535>`	Чем меньше это целое число, тем больше приоритет. Это значение приоритета определяет, какой порт будет активен, а какой – будет играть роль резервного.
`lacp timeout (fast | slow)`	Параметр Timeout (Время ожидания) определяет период времени между передачами BPDU. Когда параметр имеет значение Fast (Быстро), пакеты LACP будут передаваться каждую секунду; когда параметр имеет значение Slow (Медленно), перед отправкой пакета LACP будет выдержан интервал 30 секунд.

Пример настройки портов в режиме LACP:

```
# configure  terminal
(config)#interface GigabitEthernet 1/1-2
(config-if)# aggregation group 1 mode active
```

4.2.29. Настройка loop-protect (Loop Protection)

Функция Loop Protection предназначена для обнаружения петляния трафика на L2-уровне и предотвращения широковещательных штормов. Механизм работает путем отправки специальных служебных кадров (PDU) и отслеживания их возврата на коммутатор.

В текущей версии программного обеспечения поддерживается два режима работы:

– **Port-based (по умолчанию):** При обнаружении петли коммутатор выполняет настроенное действие над физическим портом.
– **Vlan-based:** Защита блокирует передачу трафика только в рамках конкретных VLAN, на которых была обнаружена петля, сохраняя при этом общую работоспособность физического порта для других незатронутых VLAN.

Команда	Описание
Глобальные настройки	

`loop-protect`
 	
`no loop-protect`
	Включение функции защиты от петель.
	
	Выключение функции защиты от петель.

`loop-protect mode {port-based | vlan-based}`	Выбор операционного режима защиты. По умолчанию используется port-based.

`loop-protect shutdown-time <0-604800>`
 	
`no loop-protect shutdown-time`
	Период времени (в секундах), на который порт/VLAN выключается при обнаружении петли. Значение 0 означает, что объект останется выключенным до перезагрузки устройства.
	
	Выставление значения времени блокировки по умолчанию (180 сек).

`loop-protect transmit-time <1-10>`	Интервал между отправками пакетов PDU защиты от петель на каждом порту (допустимые значения: от 1 до 10 секунд).
`no loop-protect transmit-time`	Выставление интервала отправки пакетов по умолчанию (5 сек).
`loop-protect with-stp`	Активация механизма защиты от петель совместно с протоколом Spanning Tree Protocol (STP). **Примечание: команда работает только в режиме port-based.**
`no loop-protect with-stp`	Отключение механизма защиты от петель совместно с протоколом Spanning Tree Protocol (STP).
`loop-protect vlan <vlan_list>`	Включение функции loop-protect на выбранных VLAN (список ID, например: 1,3-5,7) для работы в режиме vlan-based.
`no loop-protect vlan <vlan_list>  <cr>`	Отключение функции loop-protect на выбранных VLAN или на всех VLAN сразу.
Режим конфигурации физического интерфейса	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров.
`loop-protect / no loop-protect`	Включение или выключение функции защиты от петель на выбранных портах. (по умолчанию включено на всех портах)
`loop-protect action {log | log shutdown | shutdown}`	Настройка операции при обнаружении петли на порту: • log – События регистрируются в журнале, но порт остается включенным. • log shutdown – Порт отключается на период времени, заданный в глобальных настройках, и события регистрируются в журнале. • shutdown – Порт отключается на период времени, заданный в глобальных настройках.
`loop-protect tx-mode`	Включение генерации пакетов защиты от петель PDU (активно по умолчанию).
`no loop-protect tx-mode`	Выключение генерации пакетов защиты от петель PDU.
Привилегированный режим (exec)	
`loop-protect unblocking interface <port_type_list>`	Принудительное ручное разблокирование указанных физических портов, отключенных функцией защиты.
`loop-protect unblocking vlan <vlan_list>`	Принудительное ручное разблокирование трафика в указанных VLAN, заблокированных функцией защиты.
`show loop-protect`	Отображение глобальных параметров

	конфигурации и краткой информации по всем физическим интерфейсам системы.
`show loop-protect interface [<port_type_list>]`	Отображение детальной информации и текущего статуса функции на указанных физических интерфейсах (или на конкретном порту).
`show loop-protect vlan-based`	Отображение глобальной конфигурации и общего списка защищаемых VLAN (или сообщения об их отсутствии).
`show loop-protect vlan-based vlan [<vlan_list>]`	Отображение детальной таблицы статуса защиты, счетчиков петель и времени последнего инцидента для указанных VLAN.

Примеры настройки:

1) Настройка защиты на уровне физических портов (Port-based) с отключением STP

Этот вариант используется на абонентских портах (Edge-портах) или стыках, где протокол Spanning Tree не должен работать. Чтобы пакеты защиты от петель корректно обрабатывались, на самом интерфейсе GigabitEthernet 1/1 протокол Spanning Tree принудительно деактивируется. Действие при обнаружении петли переводится в режим log shutdown.

```
# configure terminal
! Включение функции защиты глобально (на портах она активна по умолчанию)
(config)# loop-protect
!
! Настройка физического интерфейса
(config)# interface GigabitEthernet 1/1
(config-if)# no spanning-tree
(config-if)# loop-protect action log shutdown
(config-if)# exit
```

2) Настройка защиты на основе VLAN (Vlan-based)

Этот вариант применяется на магистральных портах (Trunk), где требуется изолированная защита от петель внутри конкретных VLAN (например, VLAN 100). При петле в VLAN 100 блокируется передача данных исключительно внутри этого VLAN, в то время как сам физический интерфейс и трафик остальных VLAN (например, VLAN 200) продолжают работать в штатном режиме. На портах функция активна по умолчанию.

```
# configure terminal
! Включение защиты глобально, выбор режима VLAN и указание защищаемого списка VLAN
(config)# loop-protect
(config)# loop-protect mode vlan-based
(config)# loop-protect vlan 100
!
! Настройка магистрального порта
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 100,200
(config-if)# exit
```

4.2.30. IPMC Profile

PMC профили используются для обеспечения контроля доступа к IP мультикаст потокам. Существует возможность создать 64 профиля с 128 правилами в каждом.

Команда	Описание
Глобальные настройки	
`ipmc profile` `no ipmc profile`	Включение функции ipmc profile Выключение функции ipmc profile

`ipmc profile <word16>`
 	
`no ipmc profile <word16>`
	Назначение имени профиля, при вводе команды осуществляется переход в режим конфигурации профиля.
	
	Удаление соответствующего профиля.

`Ipmc range <word16> (<ipv4_mcast> | <ipv6_mcast>)`	Создание и назначение имени диапазону ip-адресов, а также указание диапазона ipv4 или ipv6 мультикастовых адресов для многоадресной рассылки.
Настройка профиля IPMC	
`Description <line64>`	Настройка описания профиля
`range <word16> (deny | permit)`	Команда разрешает или запрещает правило для профиля.

Пример настройки `ipmc`:

```
# configure  terminal
(config)# ipmc range 1 233.3.2.1 233.3.22.1
(config)# ipmc range 2 233.3.23.1 233.3.44.1
(config)# ipmc range 3 233.3.45.1 233.3.66.1
(config)# ipmc range 4 233.3.67.1 233.3.88.1
(config)# ipmc profile
(config)# ipmc profile 1
(config-ipmc-profile)#  description 1
(config-ipmc-profile)#  range 1 permit
(config-ipmc-profile)#  range 2 permit
(config-ipmc-profile)#  range 3 permit
(config-ipmc-profile)#  range 4 permit
(config-ipmc-profile)# ipmc profile 2
(config-ipmc-profile)#  description 2
(config-ipmc-profile)# ipmc profile 3
(config-ipmc-profile)#  description 3
(config-ipmc-profile)# ipmc profile 4
(config-ipmc-profile)#  description 4
```

4.2.31. MVR

Протокол MVR - регистрация многоадресных VLAN (Multicast VLAN Registration) позволяет медиасерверу передавать многоадресный поток по одной многоадресной VLAN, при этом клиенты, принимающие поток многоадресной VLAN, могут оставаться в различных сетях VLAN. Клиенты различных VLAN, намеревающиеся вступить в

многоадресную группу или выйти из нее, отправляют в порт приемника сообщение IGMP Join (Вступить в группу) либо IGMP Leave (Покинуть группу). Порт приемника, принадлежащий одной из многоадресных групп, может принимать многоадресный поток от медиасервера. Далее, MVR изолирует пользователей, не намеревающихся принимать многоадресный трафик и, следовательно, обеспечивать безопасность данных за счет сегрегации VLAN, допускающей только многоадресный трафик в другие сети VLAN, к одной из которых принадлежит абонент. Несмотря на то, что общий многоадресный трафик проходит от MVR VLAN в VLAN различных групп, пользователи различных VLAN IEEE 802.1Q или частных VLAN не могут обмениваться какой-либо информацией (за исключением услуг маршрутизации верхнего уровня).

Команда	Описание
Привилегированный режим	
`mvr` `no mvr`	Включение / выключение функции MVR на коммутаторе.
`mvr proxy` `no mvr proxy`	Включение / выключение режима MVR Proxy (проксирование отчетов IGMP/MLD от абонентов в сторону портов-источников).
`mvr vlan <vlan_list>` `no mvr vlan <vlan_list>`	Создание / удаление многоадресного VLAN (MVR VLAN) по его числовому идентификатору.
`mvr vlan <vlan_list> name <word16>`	Назначение символьного имени (до 16 символов) для указанного многоадресного VLAN. (Удаляется только при удалении самого MVR VLAN командой no mvr vlan <vlan_list>).
`mvr name <word16> <параметр>` `no mvr name <word16> <параметр>`	Обращение к существующему MVR VLAN по его символьному имени (вместо числового ID) для настройки или сброса параметров (channel, election, frame, igmp-address, igmp-proxy-source-zero, last-member-query-interval, mode).
`mvr {vlan <vlan_list> | name <word16>} igmp-address <ipv4_ucast>` `no mvr {vlan <vlan_list> | name <word16>} igmp-address`	Назначение / сброс IPv4-адреса, используемого в качестве адреса источника в заголовке IP кадров управления IGMP.
`mvr {vlan <vlan_list> | name <word16>} igmp-proxy-source-zero` `no mvr {vlan <vlan_list> | name <word16>} igmp-proxy-source-zero`	Включение / отключение использования нулевого IP-адреса (0.0.0.0) в качестве адреса источника только для проксируемых сообщений IGMP Report и Leave.
`mvr {vlan <vlan_list> | name <word16>} election` `no mvr {vlan <vlan_list> | name <word16>} election`	Включение / отключение функции IGMP Querier для участия коммутатора в выборах Querier-маршрутизатора в данном MVR VLAN.
`mvr {vlan <vlan_list> | name <word16>} mode {compatible | dynamic}` `no mvr {vlan <vlan_list> | name <word16>} mode`	Выбор режима работы MVR: • dynamic — MVR разрешает динамически отправлять сообщения о членстве на порты источника (режим по умолчанию); • compatible — отправка сообщений MVR о членстве на порты источника запрещена.

	Команда no возвращает режим по умолчанию (dynamic).
mvr {vlan <vlan_list> | name <word16>} frame priority <0-7> no mvr {vlan <vlan_list> | name <word16>} frame priority	Настройка приоритета передачи (CoS) кадров управления IGMP/MLD (допустимые значения: 0–7). Команда no сбрасывает приоритет к значению по умолчанию (0).
mvr {vlan <vlan_list> | name <word16>} frame tagged no mvr {vlan <vlan_list> | name <word16>} frame tagged	Включение / отключение тегирования (802.1Q) исходящих кадров управления IGMP/MLD.
mvr {vlan <vlan_list> | name <word16>} channel <word16> no mvr {vlan <vlan_list> | name <word16>} channel	Привязка / отмена привязки профиля фильтрации каналов IPMC по его имени (настройка профиля описана в п. 4.2.30).
mvr {vlan <vlan_list> | name <word16>} last-member-query-interval <0-31744> no mvr {vlan <vlan_list> | name <word16>} last-member-query-interval	Настройка максимального времени ожидания сообщения о членстве IGMP/MLD на порту приемника до удаления порта из многоадресной группы (LLQI, в десятых долях секунды, диапазон: 0–31744). Команда no возвращает значение по умолчанию (5, т.е. 0,5 секунды).
Настройка порта	
interface GigabitEthernet <port_type_list> interface 10GigabitEthernet <port_type_list> interface 25GigabitEthernet <port_type_list> interface Port-channel<port_type_list>	Переход в режим настройки параметров порта.
mvr immediate-leave no mvr immediate-leave	Включение / выключение функции немедленного выхода абонента из мультикаст-группы (Fast Leave) без ожидания таймаута.
mvr max-groups <1-10> no mvr max-groups	Ограничение максимального количества мультикаст-групп (каналов MVR), которые могут одновременно приниматься на данном порту (диапазон значений: от 1 до 10).
mvr {vlan <vlan_list> | name <word16>} type {receiver | source}	name <word16>} type {receiver | source}Назначение роли порта в указанном MVR VLAN (по номеру VLAN или его имени): • source — порт источника (аплинк), через который поступает многоадресный трафик. Абоненты не могут быть напрямую подключены к портам источника;

	• receiver — абонентский порт приемника, на котором обрабатываются запросы IGMP/MLD для подключения к мультикаст-группам.

Мониторинг и диагностика MVR

Команда	Описание
Привилегированный режим	
`show mvr`	Отображение общего статуса функции MVR (включена/выключена), параметров настроенных MVR VLAN (имя, режим работы, CoS-приоритет, тегирование, статус Querier) и ролей портов (source / receiver).
`show mvr detail`	Вывод расширенной информации и статистики по работе MVR (счетчики принятых и отправленных сообщений IGMP/MLD Report, Query, Leave и ошибок).
`show mvr {vlan <vlan_list> | name <word16>} [detail]`	Просмотр статуса и статистики MVR с фильтрацией по конкретному идентификатору VLAN или его символьному имени.
`show mvr group-database [detail]`	Вывод таблицы активных многоадресных групп (каналов MVR), зарегистрированных в базе данных коммутатора, с указанием портов-участников.
`show mvr group-database interface <type> <port_list>`	interface <type> <port_list>Просмотр списка активных мультикаст-групп MVR, привязанных к конкретным интерфейсам (*, GigabitEthernet, 10GigabitEthernet, Port-channel).
`show mvr group-database {vlan <vlan_list> | name <word16>}`	Фильтрация базы данных активных мультикаст-групп MVR по номеру VLAN или его символьному имени.
`show mvr group-database sfm-information [vlan <vlan_list> | name <word16> | interface <type> <port_list>]`	Вывод информации о фильтрации источников многоадресной рассылки (SFM — Source-Filtered Multicast, актуально для IGMPv3/MLDv2: режимы INCLUDE/EXCLUDE и список IP-адресов источников).

Пример настройки MVR:

```
# configure terminal
(config)# vlan 2000-2001
(config-vlan)# exit

! Создание диапазона мультикаст-адресов и профиля фильтрации
IPMC
(config)# ipmc profile
(config)# ipmc range 1 225.0.0.1 225.0.255.255
(config)# ipmc profile TV_PROFILE
(config-ipmc-profile)# range 1 permit
(config-ipmc-profile)# exit

! Глобальная настройка MVR
```

```
(config)# mvr
(config)# mvr vlan 2000 name IPTV_VLAN
(config)# mvr name IPTV_VLAN frame priority 6
(config)# no mvr name IPTV_VLAN frame tagged
(config)# mvr name IPTV_VLAN channel TV_PROFILE

! Настройка магистрального порта источника (source)
(config)# interface 10GigabitEthernet 1/3
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan all
(config-if)# mvr name IPTV_VLAN type source
(config-if)# exit

! Настройка абонентского порта приемника (receiver)
(config)# interface GigabitEthernet 2/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 2001
(config-if)# mvr immediate-leave
(config-if)# mvr name IPTV_VLAN type receiver
(config-if)# end
#
```

4.2.32. IPMC

4.2.33. IGMP Snooping

Протокол управления группами интернета IGMP (Internet Group Management Protocol) обеспечивает управление участием в многоадресных IP-группах. IGMP используется IP-хостами и соседними многоадресными маршрутизаторами для установления принадлежности к многоадресной группе. Он может использоваться наиболее эффективно при поддержке таких услуг, как потоковое онлайн-видео и игры. IGMP Snooping – это процесс слушания трафика IGMP. Как следует из названия, IGMP snooping представляет собой функцию, позволяющую коммутатору «прослушивать» обмен данными между хостами и маршрутизаторами, обрабатывая пакеты 3-го уровня (пакеты IGMP, посылаемые по многоадресной сети). Когда на коммутаторе включен IGMP snooping, он анализирует все пакеты, передаваемые между хостами, подключенными к коммутатору и многоадресными маршрутизаторами в сети. Когда коммутатор принимает отчет IGMP для данной многоадресной группы от хоста, коммутатор добавляет номер порта хоста к многоадресному списку для этой группы. Когда коммутатор обнаруживает сообщение IGMP Leave (Покинуть группу IGMP), он удаляет порт хоста из ячейки таблицы. IGMP snooping позволяет эффективно снижать многоадресный трафик при стриминге и других экстенсивно расходующих полосу пропускания IP приложениях. Коммутатор, использующий IGMP snooping, в этом трафике будет передавать хостам только многоадресный трафик. Снижение многоадресного трафика уменьшает число пакетов, обрабатываемых коммутатором (однако при этом требуется увеличение оперативной памяти для обработки многоадресных таблиц) и снижает нагрузку на оконечные хосты, так как их сетевые карты (или операционные системы) не будут принимать и фильтровать весь многоадресный трафик, генерируемый сетью.

Команда	Описание
Глобальные настройки	

ip igmp snooping no ip igmp snooping	Включение функции igmp snooping Выключение функции igmp snooping
ip igmp unknown-flooding no ip igmp unknown-flooding	включение режима передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика. выключение режима передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика.
ip igmp ssm-range <ipv4_mcast>	Назначение диапазона многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяет поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов.
ip igmp host-proxy leave-proxy	Подавляет сообщения о выходе из группы, отличающиеся от принятых, от последнего порта участника группы. Прокси-сервер сообщений о выходе из группы подавляет все не являющиеся необходимыми сообщения IGMP о выходе из группы таким образом, что коммутатор, не являющийся querier, передает пакет выхода из группы только тогда, когда последний динамический порт-участник покидает многоадресную группу
ip igmp host-proxy no ip igmp host-proxy	Включение прокси-сервера Выключение прокси-сервера
Настройка порта	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ip igmp snooping mrouter	Назначение порта портом маршрутизатора
ip igmp snooping immediate-leave	Включение функции быстрого выхода из группы. Когда принят пакет выхода из группы, коммутатор немедленно удаляет порт из многоадресной услуги, не посылая специфичный для группы запрос IGMP GS на этот интерфейс.
ip igmp snooping max-groups	Назначение максимального числа многоадресных групп, в которые порт может вступить одновременно. Когда для порта будет достигнуто максимальное число групп, новые сообщения с отчетами IGMP о вступлении в группу будут отбрасываться. По умолчанию выбрано неограниченное число групп (unlimited). Допустимый диапазон значений от 1 до 10.
ip igmp snooping filter <word16>	Настройка фильтра на порту для многоадресных групп. Когда определенная многоадресная группа выбрана на порту, сообщения IGMP join reports (отчеты о вступлении в группу) на порту отбрасываются.

Пример настройки igmp snooping:

```
# configure  terminal
(config)# vlan 10
(config-vlan)# exit
(config)# ip igmp snooping
(config)# no ip igmp unknown-flooding
(config)# interface GigabitEthernet 1/1
(config-if)#  switchport mode access
(config-if)#  switchport access vlan 10
(config-if)#  ip igmp snooping immediate-leave
(config-if)# interface GigabitEthernet 1/3
(config-if)#  switchport mode trunk
(config-if)# interface vlan 10
(config-if-vlan)# ip igmp snooping
(config-if-vlan)# ip igmp snooping compatibility v2
(config-if-vlan)# ip igmp snooping query-max-response-time 10
(config-if-vlan)# ip igmp snooping query-interval 45
```

Примечание. IP IGMP SNOOPING начиная с версии ПО 2020.12v1.18.6 и далее иммигрировал с L3 в L2, ниже новое описание команд.

Команда	Описание
В глобальном режиме	

`ip igmp snooping`
 	
`no ip igmp snooping`
	Включение функции igmp snooping
	
	Выключение функции igmp snooping

`ip igmp snooping vlan <vlan_list>`
 	
`no ip igmp snooping vlan <vlan_list>`
	Эта команда включает поддержку IGMP Snooping для указанных VLAN'ов (<vlan_list> перечисляются влан через запятую, пример: 20, 30, 40). Когда эта команда применяется, коммутатор отслеживает запросы IGMP от устройств конечных узлов и фильтрует широковещательные пакеты multicast-трафика таким образом, чтобы отправлять их только активным участникам группы.
	
	Эта команда отключает поддержку IGMP Snooping для указанных VLAN'ов. После отключения данная технология больше не будет отслеживать IGMP-запросы клиентов и передавать multicast трафик в пределах указанных VLAN'ов, используя механизм "flooding" (широковещательная рассылка пакетов).

`ip igmp unknown-flooding`	Включение режима передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика. выключение режима передачи незарегистрированного (не принадлежащего группам) многоадресного IP трафика.

no ip igmp unknown-flooding	Отключает передачу незарегистрированных (не принадлежащих известным группам) многоадресных IP-пакетов. Без этого параметра коммутаторы будут ограничивать распространение multicast-трафика лишь теми устройствами, которые официально подтвердили своё участие в группе через механизм IGMP. Использование этой команды предотвращает избыточную передачу ненужного трафика и улучшает общую производительность сети.
ip igmp ssm-range <ipv4_mcast> no ip igmp ssm-range <ipv4_mcast>	Назначение диапазона многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяет поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов. Команда отменяет настройку диапазонов SSM.
ip igmp host-proxy leave-proxy no ip igmp host-proxy leave-proxy	Подавляет сообщения о выходе из группы, отличающиеся от принятых, от последнего порта участника группы. Прокси-сервер сообщений о выходе из группы подавляет все не являющиеся необходимыми сообщения IGMP о выходе из группы таким образом, что коммутатор, не являющийся querier, передает пакет выхода из группы только тогда, когда последний динамический порт-участник покидает многоадресную группу. Отключает параметр, восстанавливая стандартное поведение отправки сообщений о выходе всеми участниками группы. В результате каждый узел сети будет регулярно отсылать собственное сообщение о выходе, независимо от статуса других членов группы.
ip igmp host-proxy	Включение прокси-сервера. Когда эта функция включена, коммутатор действует как посредник между клиентами (host) и

	маршрутизатором, осуществляя обработку IGMP-запросов и действий, направленных на поддержание списков мультикаст-групп.
no ip igmp host-proxy	Выключение прокси-сервера.
ip igmp snooping vlan <vlan_list> mrouter interface <port_type_list>	фиксирует статически определенный интерфейс, через который принимаются multicast-packets от маршрутизатора (mrouter). То есть вручную задаётся интерфейс, на котором ожидается поступление multicast-трафика.
no ip igmp snooping vlan <vlan_list> mrouter interface <port_type_list>	снимает данное статическое назначение, возвращая процесс обнаружения mrouter обратно в автоматический (динамический) режим. В этом случае коммутатор автоматически обнаруживает и выбирает подходящий интерфейс для приёма multicast-трафика от маршрутизатора.
ip igmp snooping vlan <vlan_list> compatibility [auto|v1|v2|v3]	Команда используется для настройки совместимости протокола IGMP (Internet Group Management Protocol) с различными версиями протокола на уровне VLAN. Параметры: - <vlan_list> – список номеров VLAN, разделенных пробелами или диапазоном (например, 1, 1-5, 1,3,5). Это номера VLAN, для которых настраивается совместимость. - [auto|v1|v2|v3] – режим совместимости: - auto – автоматическое определение версии IGMP на основе трафика (рекомендуемый вариант); - v1 – принудительное использование версии IGMPv1; - v2 – принудительное использование версии IGMPv2; - v3 – принудительное использование версии IGMPv3.
no ip igmp snooping vlan <vlan_list> compatibility	Команда отменяет ранее настроенную совместимость версий IGMP для указанных VLAN, ставит режим auto
ip igmp snooping vlan <vlan_list> last-member-query-interval <0-31744>	Команда устанавливает интервал отправки последнего запроса члена группы (Last Member Query Interval) для указанного списка VLAN. Интервал определяет временной промежуток, в течение которого коммутатор ожидает подтверждения наличия членов группы перед удалением записи группы из таблицы групповых адресов. Параметры:

	- <vlan_list> – Список номеров VLAN, разделённых пробелами или диапазонами. Например, 1-5, 1,3,5. - <0-31744> – Значение интервала в миллисекундах. Диапазон значений от 0 до 31744 мс
`no ip igmp snooping vlan <vlan_list> last-member-query-interval`	Удаляет установленное значение интервала Last Member Query для указанного списка VLAN и возвращает его к значению по умолчанию.
`ip igmp snooping vlan <vlan_list> priority <0-7>`	Команда предназначена для установки приоритета порта коммутации для управления многоадресным трафиком IGMP (Internet Group Management Protocol) внутри заданных VLAN. Параметры: - <vlan_list> – перечень номеров VLAN, для которых устанавливается приоритет (можно указывать диапазон, например, 1-10 или отдельные VLAN, перечисленные через запятую или пробел, например, 1,3,5). - <0-7> – уровень приоритета порта (целое число от 0 до 7, где 0 является наивысшим приоритетом, а 7 – наименьшим).
`no ip igmp snooping vlan <vlan_list> priority`	Команда используется для удаления установленной конфигурации приоритета порта для заданных VLAN и восстановления параметра по умолчанию.
`ip igmp snooping vlan <vlan_list> querier election`	Команда активирует механизм выборов мастера запросов (querier) среди устройств, подключенных к указанным VLAN, для протокола IGMP (Internet Group Management Protocol). Когда включена эта функция, устройства обмениваются сообщениями, определяющими одно устройство в качестве основного отправителя запросов IGMP, которое управляет многоадресной рассылкой в сети. Параметры: - <vlan_list> – список номеров VLAN, разделенных пробелами или диапазоном (например, 1, 1-5, 1,3,5). Эти VLAN будут участвовать в выборах мастер-запрашивающего устройства.
`no ip igmp snooping vlan <vlan_list> querier election`	Команда отключает процедуру выборов master-querier для указанных VLAN. После её выполнения, каждое устройство

	самостоятельно отправляет запросы IGMP независимо друг от друга, без участия централизованного координирующего устройства.
ip igmp snooping vlan <vlan_list> querier address <ipv4_ucast>	Команда задает IP-адрес интерфейса, используемого устройством для отправки запросов IGMP (Internet Group Management Protocol) в пределах определенных VLAN. Устройство, назначенное мастером-запрашивающим (querier), инициирует периодические запросы, необходимые для поддержания актуальности таблиц multicast-групп. Параметры: - <vlan_list> – Список номеров VLAN, разделенных пробелами или диапазоном (например, 1, 1-5, 1,3,5), для которых указывается IP-адрес запрашивающего устройства. - <ipv4_ucast> – Уникальный IPv4-адрес, используемый устройством для отправки запросов IGMP.
no ip igmp snooping vlan <vlan_list> querier address	Команда отменяет указанную вручную конфигурацию адреса запросчика для соответствующих VLAN и восстанавливает настройку по умолчанию.
ip igmp snooping vlan <vlan_list> query-interval <0-31744>	Команда устанавливает интервал отправки общих запросов (General Queries) протокола IGMP (Internet Group Management Protocol) для определённого набора VLAN. Запросы используются для обновления списков участников мультикаст-группы и поддержания состояния группового членства. Параметры: - <vlan_list> – Перечень номеров VLAN, для которых изменяется интервал запросов. Можно задать одиночные VLAN (1) или диапазон (1-5, 1,3,5). - <0-31744> – Периодичность отправки общего запроса в миллисекундах (ms). Допустимый диапазон значений от 0 до 31744 ms.
no ip igmp snooping vlan <vlan_list> query-interval	Команда отменяет изменение интервала отправки запросов и восстанавливает значение по умолчанию для указанных VLAN.
ip igmp snooping vlan <vlan_list> query-max-response-time <0-31744>	Команда задает максимальное время отклика на общий запрос (general query) протокола IGMP (Internet Group

	Management Protocol) для указанных VLAN. Этот таймаут определяет максимальный срок, в течение которого хосты должны подтвердить свое участие в группе, иначе они будут исключены из группы. Параметры: - <vlan_list> – Список номеров VLAN, разделенных пробелами или диапазоном (например, 1, 1-5, 1,3,5). Для этих VLAN меняется время максимального отклика. - <0-31744> – Время ожидания в миллисекундах (мс), диапазон от 0 до 31744 мс.
`no ip igmp snooping vlan <vlan_list> query-max-response-time`	Команда отменяет ручную установку максимального времени отклика и возвращает значение по умолчанию для указанных VLAN.
`ip igmp snooping vlan <vlan_list> report-suppression`	Команда включает подавление отчетов (reports suppression) в протоколе IGMP (Internet Group Management Protocol) для указанных VLAN. Эта функция предотвращает передачу повторяющихся отчётов от разных хостов одной и той же подгруппы, уменьшая объём трафика в сети. Если один хост отправил отчёт о принадлежности к группе, остальные хосты в той же VLAN могут воздерживаться от повторной отправки аналогичных отчётов. Параметры: - <vlan_list> – Список номеров VLAN, разделённых пробелами или диапазоном (например, 1, 1-5, 1,3,5). Подавление отчётов включается именно для этих VLAN. Подавление отчетов улучшает эффективность обработки многоадресного трафика, особенно в больших сетях с большим количеством клиентов.
`no ip igmp snooping vlan <vlan_list> report-suppression`	Команда отключает подавление отчетов IGMP для указанных VLAN. Каждый клиент снова начнёт отправлять собственные отчёты независимо от действий других хостов.
`ip igmp snooping vlan <vlan_list> robustness-variable <1-255>`	команда устанавливает коэффициент устойчивости (robustness variable) для протокола IGMP (Internet Group Management Protocol) в указанных VLAN. Коэффициент устойчивости представляет собой множитель, который применяется к

	временным интервалам протокола IGMP для повышения надёжности работы системы в условиях нестабильной связи или большого количества устройств. Чем больше значение коэффициента, тем дольше сохраняется запись в таблице группы даже при отсутствии активных членов группы, что снижает вероятность потери важных сведений о группах. Параметры: - <vlan_list> – Перечень номеров VLAN, разделённый пробелами или диапазоном (например, 1, 1-5, 1,3,5). Именно для этих VLAN изменится коэффициент устойчивости. - <1-255> – Целочисленное значение коэффициента устойчивости, принимающее значения от 1 до 255.
`no ip igmp snooping vlan <vlan_list> robustness-variable`	Команда отменяет установленные вручную значения коэффициента устойчивости и возвращает стандартные настройки для указанных VLAN.
`ip igmp snooping vlan <vlan_list> static <ipv4_mcast>`	Команда позволяет создать статическую группу многоадресной рассылки (Multicast group) для определенного набора VLAN. Статически сконфигурированная группа означает, что устройства автоматически включаются в нее, даже если они сами не присылают запросы на присоединение к группе. Параметры: - <vlan_list> – Перечисленный список номеров VLAN, разделенный пробелами или диапазоном (например, 1, 1-5, 1,3,5). Все указанные VLAN получают доступ к указанной группе. - <ipv4_mcast> – Адрес многоадресной группы IPv4 (например, 224.0.0.1). Это адрес, на который производится рассылка пакетов.
`no ip igmp snooping vlan <vlan_list> static <ipv4_mcast>`	Команда удаляет ранее созданные статические группы многоадресной рассылки для указанных VLAN и соответствующего адреса группы.
`ip igmp snooping vlan <vlan_list> unsolicited-report-interval <0-31744>`	Команда Определяет интервал отправки несвоевременных (unsolicited) отчетов протокола IGMP (Internet Group Management Protocol) для указанных VLAN. Несвоевременные отчеты отправляются устройствами сразу после

	присоединения к группе, минуя обычный цикл регулярных запросов от мастеру-запрашивающему (querier). Параметры: - <vlan_list> – Списки номеров VLAN, разделённые пробелами или диапазоном (например, 1, 1-5, 1,3,5). Изменения применяются к данным VLAN. - <0-31744> – Временной интервал в миллисекундах (мс), в диапазоне от 0 до 31744 мс. Определяет минимальный интервал времени между отправками таких отчетов. Установка меньшего интервала повышает отзывчивость сети, позволяя быстро добавлять новые члены в группы, но также увеличивает нагрузку на сеть.
`no ip igmp snooping vlan <vlan_list> unsolicited-report-interval`	Команда отменяет предыдущие настройки интервала отправки несвоевременных отчетов и возвращает значение по умолчанию для указанных VLAN.
В режиме настройки порта коммутатора	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров
`ip igmp snooping immediate-leave`	Включение функции быстрого выхода из группы. Когда принят пакет выхода из группы, коммутатор немедленно удаляет порт из многоадресной услуги, не посылая специфичный для группы запрос IGMP GS на этот интерфейс.
`no ip igmp snooping immediate-leave`	Возвращает обычное поведение, при котором записи сохраняются до конца текущего цикла опроса.
`ip igmp snooping max-groups <1-10>`	Назначение максимального числа многоадресных групп, в которые порт может вступить одновременно. Когда для порта будет достигнуто максимальное число групп, новые сообщения с отчетами IGMP о вступлении в группу будут отбрасываться. Допустимый диапазон значений от 1 до 10.
`no ip igmp snooping max-groups`	Отменяет предыдущее ограничение и применяет настройки

	по умолчанию неограниченное число групп (unlimited).
ip igmp snooping filter <word16>	Настройка фильтра на порту для многоадресных групп. Когда определенная многоадресная группа выбрана на порту, сообщения IGMP join reports (отчеты о вступлении в группу) на порту отбрасываются
no igmp snooping filter	Отменяет предварительно установленный фильтр группы и возвращает стандартное поведение.
Команды просмотра информации	
show ip igmp snooping [detail|<cr>]	- show ip igmp snooping: выводит базовую информацию о настройках и состоянии IGMP snooping. - show ip igmp snooping detail: отображает подробную информацию, включая дополнительные сведения о каждом интерфейсе, состояние фильтров, максимальную продолжительность удержания записей и другие детальные параметры.
show ip igmp snooping group-database [detail|interface <port_type_list>|vlan <vlan_list>|<cr>]	- show ip igmp snooping group-database: выводит обобщённую информацию обо всех активных группах. - show ip igmp snooping group-database detail: показывает расширенные сведения о каждой группе, включая дополнительную статистику и временные метки. - show ip igmp snooping group-database interface <port_type_list>: отображает информацию только для выбранных типов интерфейсов. - show ip igmp snooping group-database vlan <vlan_list>: выводит информацию только для указанных VLAN.
show ip igmp snooping group-database sfm-information [detail|interface <port_type_list>|vlan <vlan_list>|<cr>]	- show ip igmp snooping group-database sfm-information: выводит общие сведения о группе и источниках, участвующих в фильтрации. - show ip igmp snooping group-database sfm-information detail: отображает расширенные подробности о каждой группе, включая статистические данные и списки активных источников. - show ip igmp snooping group-database sfm-information interface <port_type_list>: выводит информацию только для указанных типов интерфейсов.

	- show ip igmp snooping group-database sfm-information vlan <vlan_list>: отображает данные только для выбранных VLAN.
show ip igmp snooping mrouter [detail|<cr>]	- show ip igmp snooping mrouter: выводит основную информацию о зарегистрированных mrouters. - show ip igmp snooping mrouter detail: предоставляет более детальные сведения, включая статус и статистические данные по каждому интерфейсу.
show ip igmp snooping vlan <vlan_list>	Предназначена для просмотра состояния и настроек механизма IGMP snooping для отдельных VLAN. IGMP snooping используется для оптимизации трафика многоадресной рассылки (multicast) в сетях Ethernet, контролируя процесс присоединения и ухода узлов из многоадресных групп и устраняя нежелательное широковещание.

Пример настройки igmp snooping:

```
(config)# vlan 100,2036
(config-vlan)# exit
(config)# no ip igmp unknown-flooding
(config)# ip igmp snooping
(config)# ip igmp snooping vlan 2036
(config)# ip  igmp snooping vlan 2036 querier election
(config)# ip  igmp snooping vlan 2036 querier address 2.2.2.2
(config)# ip  igmp snooping vlan 2036 report-suppression
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 100,2036
(config-if)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 2036
```

4.2.34. MLD Snooping

MLD – Multicast Listener Discovery Protocol - протокол определения получателей многоадресных потоков, использующийся в IPv6. Аналогичную роль в IPv4 выполняет протокол IGMP.

Команда	Описание
Глобальные настройки	
ipv6 mld snooping no ipv6 mld snooping	Включение функции mld snooping, включено по умолчанию Выключение функции mld snooping
ipv6 mld unknown-flooding no ipv6 mld unknown-	Включение функции рассылки незарегистрированного трафика Отключение функции рассылки незарегистрированного

flooding	трафика. Управление лавинной рассылкой вступает в силу только тогда, когда включена функция mld snooping. Когда MLD Snooping отключен, незарегистрированный трафик IPMCv6 всегда активен, несмотря на этот параметр.
ipv6 mld ssm-range <ipv6_mcast>	Настройка диапазона SSM (многоадресная рассылка с учетом источника) позволяет узлам и маршрутизаторам, поддерживающим SSM, запускать модель службы SSM для групп в диапазоне адресов.
ipv6 mld host-proxy no ipv6 mld host-proxy	Включение прокси-сервера. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений о присоединении и оставить сообщения на стороне маршрутизатора. Отключение прокси-сервера
ipv6 mld host-proxy leave-proxy no ipv6 mld host-proxy leave-proxy	Включение MLD Leave Proxy. Эту функцию можно использовать, чтобы избежать пересылки ненужных сообщений о выходе на сторону маршрутизатора. Выключение MLD Leave Proxy.
ipv6 mld snooping vlan <vlan_list>	

MLD Snooping VLAN Configuration	
interface vlan<vlan_list>	Создание интерфейса
ipv6 mld snooping no ipv6 mld snooping	Включение функции mldsnooping для VLAN Выключение функции mldsnooping для VLAN
ipv6 mld snooping querier election no ipv6 mld snooping querier election	Включение выбора MLD Querier в VLAN Выключение выбора MLD Querier в VLAN
ipv6 mld snooping compatibility {auto | v1 | v2}	Настройка совместимости. Значение совместимости по умолчанию - MLD-Auto.
ipv6 mld snooping priority <0-7>	Приоритет интерфейса. Он указывает уровень приоритета управляющего кадра MLD, сгенерированный системой. Эти значения можно использовать для определения приоритетов различных классов трафика. Значение приоритета интерфейса по умолчанию - 0.
ipv6 mld snooping robustness-variable <1-255>	Настройка переменной устойчивости. Переменная устойчивости позволяет

	настроить ожидаемую потерю пакетов в канале. Допустимый диапазон**1** к **255**, значение переменной устойчивости по умолчанию - 2.
ipv6 mld snooping query-interval <1-31744>	Настройка интервала запроса. Интервал запроса - это интервал между общими запросами, отправляемыми запросчиком. Допустимый диапазон <1-31744>секунд, интервал запроса по умолчанию составляет 125 секунд.
ipv6 mld snooping query-max-response-time <0-31744>	Настройка интервала ответа на запрос. Максимальная задержка ответа, используемая для расчета максимального кода ответа, вставляемого в периодические общие запросы. Допустимый диапазон <0-31744> Интервал ответа на запрос по умолчанию составляет 100 в десятых долях секунды (10 секунд).
ipv6 mld snooping last-member-query-interval <0-31744>	Настройка максимальной задержки ответа, Допустимый диапазон <0-31744> в десятых долях секунды, интервал по умолчанию составляет 10 в десятых долей секунды (1 секунда).
ipv6 mld snooping unsolicited-report-interval <0-31744>	Настройка интервала незапрашиваемого отчета – это время между повторениями первоначального отчета узла, представляющего интерес, в многоадресном адресе. Допустимый диапазон <0-31744> в десятых долях секунды, интервал по умолчанию - 1 секунда
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
ipv6 mld snooping mrouter no ipv6 mld snooping mrouter	Настройка порта в качестве порта маршрутизатора Отмена команды
ipv6 mld snooping immediate-leave No ipv6 mld snooping immediate-leave	Включение функции немедленного отключения. Система удалит запись группы и прекратит пересылку данных после получения сообщения о выходе из MLDv1, не отправляя сообщения запроса последнего участника. Выключение функции немедленного отключения.

ipv6 mld snooping max-groups <1-10>	Ограничение количества групп многоадресной рассылки, к которым может принадлежать порт коммутатора.
ipv6 mld snooping filter <word16>	Настройка контроля доступа при регистрации групп многоадресной рассылки <word16> - профиль IPMC в качестве условия фильтрации для конкретного порта

4.2.35. LLDP

Протокол LLDP (Link Layer Discovery Protocol) является протоколом канального уровня, на котором сетевые устройства обмениваются информацией о себе с другими устройствами, напрямую соединенными через сеть. Используя LLDP, два устройства, на которых функционируют сетевые протоколы разных уровней, могут обучаться информации друг друга. Для обнаружения соседних устройств используется набор атрибутов, ссылающийся на TLV. Устройство может передавать и принимать такую детальную информацию, как описание порта, описание системы и ее возможностей, адрес управления.

Команда	Описание
Глобальные настройки	
lldp timer<5-32768>	Настройка интервала между кадрами LLDP, отправляемыми соседям данного устройства для обновления информации о данном устройстве. Допустимые значения: от 5 до 32768 секунд. По умолчанию задано 30 секунд.
lldp holdtime <2-10>	Данная настройка определяет, как долго кадры LLDP будут считаться правильными и используется для вычисления TTL. Диапазон допустимых значений: 2~10 раз. По умолчанию задано 4.
lldp transmission-delay <1-8192>	Настройка задержки между кадрами LLDP, содержащими изменения конфигурации. Допустимые значения: от 1 до 8192 секунд.
lldp reinit <1-10>	Настройка задержки между кадром отключения и новой инициализацией LLDP. Допустимые значения: от 1 до 10 секунд
Настройка порта	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
lldp transmit	Режим работы: только передача. Коммутатор будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, принятую от соседних устройств.

`no lldp transmit`	Выключат режим

`lldp receive`
 	
`no lldp receive`
	Режим работы: только прием. Коммутатор будет анализировать информацию LLDP, принятую от соседних устройств.
	
	Выключат режим

`lldp cdp-aware`	Операция CDP aware (Распознавание CDP) используется для декодирования входящих кадров CDP (Cisco Discovery Protocol). Если эта опция включена, CDP TLVs, которые могут быть отображены в соответствующее поле таблицы соседних устройств LLDP будут декодированы, в противном случае эти кадры будут отброшены. CDP TLVs отображаются в поле таблицы соседних устройств LLDP

`lldp tlv-select (management-address vid| port-description | system-capabilities | system-description | system-name)`
 	
`no lldp tlv-select (management-address vid| port-description | system-capabilities | system-description | system-name)`
	Настройка атрибутов для обнаружения соседних устройств. Эти атрибуты содержат описания типа, длины и значений и ссылаются на TLVs. Данное устройство может передавать такую детальную информацию, как описание порта, имя и описание системы и ее возможностей, адрес управления.
	
	Отключение соответствующего атрибута. Соседние устройства не будут получать соответствующую информацию об устройстве.

4.2.36. LLDP MED

Протокол LLDP для конечных медиа-устройств LLDP-MED (LLDP for Media Endpoint Devices) является расширением LLDP и работает между конечными устройствами, такими как IP-телефоны и сетевыми устройствами (например, коммутаторами). Протокол LLDP-MED обеспечивает поддержку приложений передачи голоса по IP (VoIP) и дополнительные TLVs для обнаружения, обеспечения политики сети, функции Power over Ethernet, управления реестром и информации о местоположении.

Команда	Описание
Глобальные настройки	
`lldp med fast <1-10>`	Настройка параметра Fast start repeat count (Число повторов быстрого старта) позволяет задать, сколько раз будет повторен быстрый старт передачи. Рекомендуемое значение (4 раза) означает, что с интервалом 1 секунда будут переданы 4 кадра LLDP, если принят кадр LLDP с новой информацией. Следует отметить, что LLDP-MED и

	механизм LLDP-MED Fast Start 100 предназначены только для работы на линиях между устройствами соединения по сети, поддерживающими LLDP-MED и конечными устройствами и неприменимы к линиям между элементами инфраструктуры LAN, включая и устройства соединения по сети или линии другого типа.
`lldp holdtime <2-10>`	Данная настройка определяет, как долго кадры LLDP будут считаться правильными и используется для вычисления TTL. Диапазон допустимых значений: 2~10 раз. По умолчанию задано 4.
`lldp transmission-delay <1-8192>`	Настройка задержки между кадрами LLDP, содержащими изменения конфигурации. Допустимые значения: от 1 до 8192 секунд.
`lldp reinit <1-10>`	Настройка задержки между кадром отключения и новой инициализацией LLDP. Допустимые значения: от 1 до 10 секунд
Настройки местоположения	
`lldp med location-tlv latitude (north south) <word8>`	Задание широты. Широта должна быть приведена в диапазоне 0-90 градусов и содержать не более 4 цифр. Можно задать экваториальное положение либо на север от экватора (North) либо на юг (South) от экватора.
`lldp med location-tlv longitude (east west) <word9>`	Задание долготы. Долгота должна быть приведена в диапазоне 0-180 градусов и содержать не более 4 цифр. Можно указать направление – либо на восток от нулевого меридиана (East) либо на запад от нулевого меридиана (West).
`lldp med location-tlv (floors meters) <word11>`	Задание высоты. Высота должна быть приведена в диапазоне от - 32767 до 32767 и содержать не более 4 цифр. Можно выбрать единицы измерения высоты – либо в метрах, либо в этажах.
`lldp med datum (nad83-mllw nad83-navd88 wgs84)`	Выбор системы координат: • WGS84: (Географические, трехмерные) – Всемирная геодезическая система 1984, CRS Code 4327, нулевой меридиан: гринвичский. • NAD83/NAVD88: Североамериканская система координат 1983, CRS Code 4269, нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - North American Vertical

	Datum of 1988 (NAVD88). Эта пара систем координат используется для указания местоположения на земле, на водных пространствах, подверженных приливам и отливам (для которых можно использовать систему координат NAD83/MLLW). • NAD83/MLLW: Североамериканская система координат 1983, CRS Code 4269, нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - Mean Lower Low Water (MLLW). Эта пара связанных систем координат используется при указании местоположения в океане, на морях и на 101 других водных пространствах. Опция включена, CDP TLVs, которые могут быть отображены в соответствующее поле таблицы соседних устройств LLDP будут декодированы, в противном случае эти кадры будут отброшены. CDP TLVs отображаются в поле таблицы соседних устройств LLDP
`lldp med location-tlv civic-addr (additional-code | additional-info | apartment | block | building | city | country | county | district | floor | house-no | house-no-suffix | landmark | leading-street-direction | name | p-o-box | place-type | postal-community-name | room-number | state | street | street-suffix | trailing-street-suffix | zip-code)`	Указание адреса `additional-code` – Добавочный код `additional-info` – Дополнительная информация о местоположении. `Apartment` – Апартамент, номер. `Block` – Квартал, блок. `Building` – Строение. `City` – Город, поселок. `Country` – Код страны по стандарту ISO 3166, состоящий из двух прописных букв ASCII. `County` – Округ. `District` – Район города, округ города, административный район города. `Floor` – Этаж `house-no` – Номер дома `house-no-suffix` - Суффикс номера дома. `Landmark` – Адрес какого-либо заметного объекта на местности. `leading-street-direction` – Направление главной улицы. `Name` – ФИО резидента или лица, арендующего офис. `p-o-box` – Номер абонентского ящика `place-type` – Тип площади `postal-community-name` – ФИО

	почтового адресата `room-number` - Номер комнаты`state` - Единица административно-территориального деления (штат, кантон, регион, провинция, префектура). `Street` - Улица. `street-suffix` – Суффикс улицы `trailing-street-suffix` – Навигационный суффикс улицы `zip-code` - Почтовый код
Создание правил	
`lldp med media-vlan-policy <0-31> (guest-voice guest-voice-signaling softphone-voice streaming-video video-conferencing video-signaling voice voice-signaling) (tagged untagged) <vlan_id> (dscp l2-priority)`	Типы приложений, в том числе: “Voice” (Голосовой вызов), “Voice Signalling” (Сигнализация голосового вызова), “Guest Voice” (Гостевой голосовой вызов), “Guest Voice Signalling” (Сигнализация гостевого голосового вызова), “Softphone Voice” (Голосовой вызов по софтофону), “Video Conferencing” (Видеоконференция), “Streaming” (Потоковая передача), “Video Signalling” (Сигнализация видеопотока). `l2-priority` – выбор одного из восьми уровней приоритета `dscp` – одно из значений 64-точечного кода

4.2.37. Таблица mac –адресов

Таблица MAC-адресов – это таблица соответствий между MAC-адресами устройств назначения и портами коммутатора. MAC-адреса могут быть статические и динамические. Статические MAC-адреса настраиваются пользователем вручную, имеют наивысший приоритет, хранятся постоянно и не могут быть перезаписаны динамическими MAC-адресами. MAC-адреса – это записи, полученные коммутатором в пересылке кадров данных, и хранятся в течение ограниченного периода времени. Когда коммутатор получает кадр данных для дальнейшей передачи, он сохраняет MAC-адрес кадра данных вместе с соответствующим ему портом назначения. Когда MAC-таблица опрашивается для поиска MAC-адреса назначения, при нахождении нужного адреса кадр данных отправляется на соответствующий порт, иначе коммутатор отправляет кадр на широковещательный домен. Если динамический MAC-адрес не встречается в принятых кадрах данных длительное время, запись о нем будет удалена из MAC-таблицы коммутатора.

Команда	Описание
`mac address-table aging-time <0,10-1000000>`	Настройка срока устаревания для MAC - адресов, полученных обучением, которые будут присутствовать в таблице MAC - адресов. Диапазон допустимых значений:

	от 10 до 1000000 секунд
mac address-table learning vlan <vlan_list>	Включение изучения MAC-адресов в заданном vlan
mac address-table static <mac_addr> vlan <vlan_id> interface GigabitEthernet <port_type_list>	Настройка статических MAC-адресов

4.2.38. Privatevlan

Частные VLAN основаны на маске порта источника и не соединяются с обычными VLAN. Это означает, что номера VLAN ID обычных VLAN и номера VLAN ID частных VLAN могут быть одинаковыми. Чтобы была возможна передача пакетов, порт должен принадлежать и обычной, и частной VLAN. По умолчанию, все порты не поддерживают VLAN и являются членами VLAN 1, и Private VLAN 1.

Порт, не поддерживающий VLAN, может быть членом только одной VLAN, но может быть членом нескольких частных VLAN.

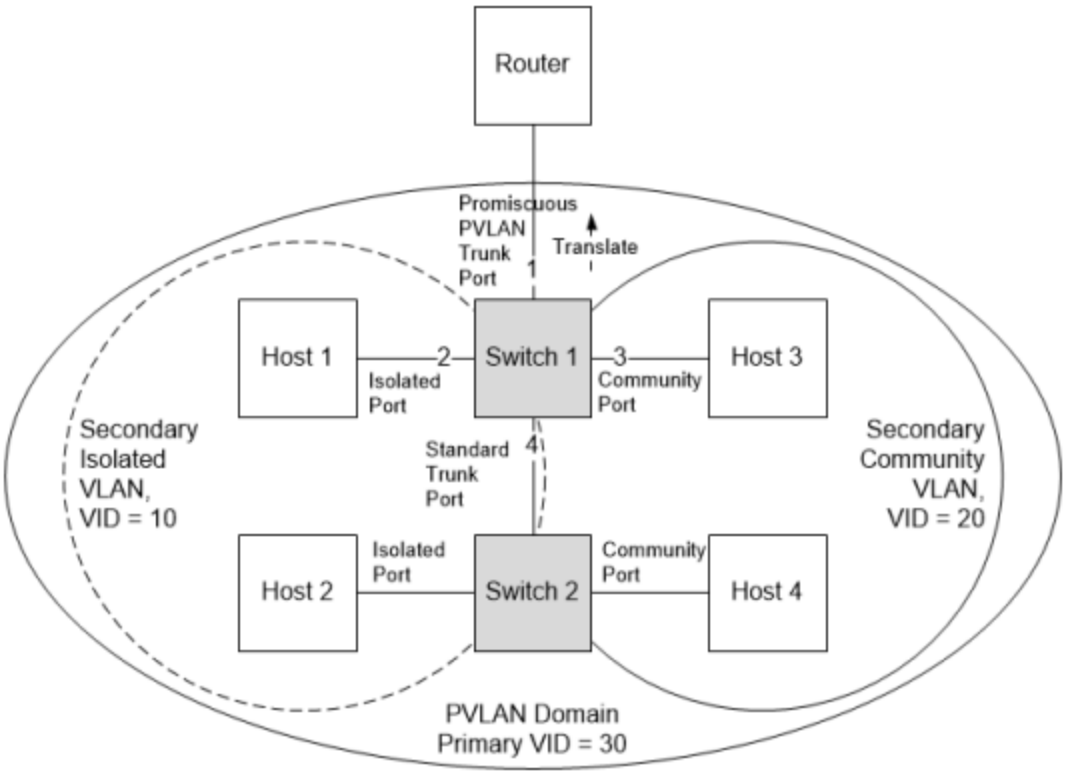
Частные VLAN используются для группировки портов с целью предотвращения связи внутри PVLAN. Изоляция порта используется для предотвращения связи между портами клиентов в одной и той же VLAN или частной VLAN. Порт, который изолирован от остальных портов не может передавать какой-либо одноадресный, многоадресный или широковещательный трафик в любые другие порты той же самой VLAN или PVLAN.

Команда	Описание
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов для настройки параметров
pvlan <range_list> no pvlan <range_list>	Создание Private VLAN Удаление Private VLAN
pvlan isolation no pvlan isolation	Команда выполнение которой приведет к изоляции выбранных портов от остальных. Отмена команды

Пример настройки Port Isolation :

```
# configure  terminal
(config)# interface GigabitEthernet 1/1
(config-if)# pvlan 1-2
(config-if)# pvlan isolation
(config-if)# interface GigabitEthernet ½
(config-if)# pvlan 3-4
(config-if)# pvlan isolation
```

Пример настройки PVLAN для группы коммутаторов:




```
Swith_1(config)# hostname Swith_1
Swith_1(config)# vlan 10
swith_1(config-vlan)# name Isolated VLAN
swith_1(config-vlan)# exit
Swith_1(config)# vlan 20
swith_1(config-vlan)# name Community VLAN
swith_1(config-vlan)# exit
Swith_1(config)# vlan 30
swith_1(config-vlan)# name Primary VLAN
swith_1(config-vlan)# exit
Swith_1(config)# svl fid 30 vlan 10,20,30
Swith_1(config)# switchport vlan mapping 1 egress 10 30
Swith_1(config)# switchport vlan mapping 1 egress 20 30
Swith_1(config)# interface GigabitEthernet 1/1
Swith_1(config-if)# description to_Router
Swith_1(config-if)# switchport mode trunk
Swith_1(config-if)# switchport trunk allowed vlan 10,20,30
Swith_1(config-if)# exit
Swith_1(config)# interface GigabitEthernet 1/2
Swith_1(config-if)# description Isolate_port
Swith_1(config-if)# switchport mode hybrid
Swith_1(config-if)# switchport hybrid native vlan 10
Swith_1(config-if)# switchport hybrid allowed vlan 30
Swith_1(config-if)# no switchport hybrid ingress-filtering
Swith_1(config-if)# switchport hybrid egress-tag none
Swith_1(config-if)# exit
Swith_1(config)# interface GigabitEthernet 1/3
Swith_1(config-if)# description Community_port_1
```

```
Swith_1(config-if)# switchport mode hybrid
Swith_1(config-if)# switchport hybrid native vlan 20
Swith_1(config-if)# switchport hybrid allowed vlan 20,30
Swith_1(config-if)# no switchport hybrid ingress-filtering
Swith_1(config-if)# switchport hybrid egress-tag none
Swith_1(config-if)# exit
Swith_1(config)# interface GigabitEthernet 1/4
Swith_1(config-if)# description to_Swith_2
Swith_1(config-if)# switchport mode trunk
Swith_1(config-if)# switchport trunk allowed vlan 10,20,30
Swith_1(config-if)# end
```

В примере интерфейс GigabitEthernet 1/1 служит для подключения маршрутизатора, он может обмениваться данными с хостами 1-4 и Switch 1 и 2.

Хосты 1 и 2 могут обмениваться данными с только маршрутизатором (Isolated VLAN 10).

Хосты 3 и 4 могу обмениваться данными с маршрутизатором и между собой (Community VLAN 20).

4.2.39. Изоляция портов (Protected ports)

Функция, которая позволяет предотвращать обмен данными между определёнными портами, позволяя им взаимодействовать только с назначенными uplink-портами.

Команда	Описание
Команда в режиме настройки интерфейса (группы интерфейсов)	

`switchport protected-port`
 	
`no switchport protected-port`
	Перевести порт (группу портов) в режим изоляции.
	
	Восстановить значение по умолчанию.

Команда просмотра информации	
`show switchport protected-port [ interface <port_type_list> ]`	Показать информацию о функции изоляции на интерфейсах (группы интерфейсов).

4.2.40. VCL

MAC-based VLAN -назначение номера VLAN в соответствии с мак-адресом хоста.

Команда	Описание
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

`switchport vlan mac <mac_ucast> vlan <vlan_id>`
 	
`no switchport vlan mac <mac_ucast> vlan <vlan_id>`
	Настройка привязки mac-адреса к vlan
	
	Удаление привязки.

Protocol-based VLAN – назначение номера VLAN в зависимости от используемого протокола.

Команда	Описание
Глобальные настройки	

`vlan protocol eth2 <0x600-0xffff> group <word16>`
 	
`vlan protocol snap 0x00E02B 0x0001 group <word16>`
 	
`vlan protocol llc 0xff 0xff group <word16>`
	Выбор соответствующего протокола
	
	0x00E02B – OUL (0x000000 - 0XFFFFFF)
	0x0001 – PID(0x0 - 0xFFFF)
	
	0xff – DSAP(0x00 - 0xFF)
	0xff - SSAP(0x00 - 0xFF)

Настройка группы	
`interface GigabitEthernet <port_type_list>`	Выбор портов для объединения в группу

`switchport vlan protocol group <word16> vlan <vlan_id>`
 	
`no switchport vlan protocol group <word16>`
	Команда, выполнение которой приведет к объединению портов в одну группу и назначение ей VLAN.
	
	Удаление соответствующей группы

IP Subnet-based VLAN - назначение номера VLAN в зависимости от ip-адреса

Команда	Описание
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов для настройки параметров

`switchport vlan ip-subnet <ipv4_subnet><vlan_id>`
 	
`no switchport vlan ip-subnet <ipv4_subnet><vlan_id>`
	Настройка привязки ip-адресов к vlan
	
	Удаление привязки.

4.2.41. Voice VLAN

Функция голосовой VLAN позволяет пересылать голосовой трафик в голосовой VLAN, после чего коммутатор может классифицировать и планировать сетевой трафик. Рекомендуется, чтобы на порту было две сети VLAN - одна для голоса, другая для данных.

Команда	Описание
Глобальные настройки	
`voice vlan`	Включение функции voice vlan Примечание. Перед активацией голосового VLAN на коммутаторах: NTS-1080, NTS-1024, NTS-15040, NTS-15080, NTS-1080P, NTS-1024P, NTS-15040P, NTS-15080P,

no voice vlan	NTS-4G2S-AT, NTS-8G2S-AT, NTS-4G2S-BT, NTS-8G2S-BT. Отключите протокол MSTP, чтобы предотвратить возможные конфликты. На остальных устройствах серии MSTP совместим с функцией Voice VLAN. Выключение функции voice vlan
voice vlan vid	Назначение номера vlan
voicevlanaging-time<10-10000000>	Настройка времени безопасного обучения. Допустимый диапазон составляет от 10 до 10000000 секунд. По умолчанию – 86400сек.
voice vlan class <0-7>	Указывает класс трафика. Весь трафик в Voice VLAN будет иметь этот класс. По умолчанию установлен 7 класс.
voice vlan oui <oui> description <line32> no vlan oui <oui>	Создание записи в таблице OUI Oui – это глобальный уникальный идентификатор, присвоенный IEEE. Он должен состоять из 6 символов, формат ввода - «xx-xx-xx» (x - шестнадцатеричная цифра). Description – Описание адреса OUI Удаление соответствующей записи.
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов
switchport voice vlan mode {auto | disable | force}	Настройка режима Auto – автоматическое определение Disable – отключен Force – принудительное включен
switchport voice vlan security no switchport voice vlan security	Включение режима безопасности. Когда эта функция включена, все нетелефонные MAC-адреса в VLAN будут заблокированы на 10 секунд. Выключение режима безопасности. Когда эта функция включена, все нетелефонные MAC-адреса в VLAN будут заблокированы на 10 секунд.
switchport voice vlan discovery-protocol { both | lldp | oui}	Настройка протокола обнаружения порта. Работает только при режиме «Auto». Возможные протоколы обнаружения: Both- OUI и LLDP Lldp- обнаружение телефонного устройства по LLDP Oui- обнаружение телефонного устройства по адресу OUI

Пример настройки voice vlan:

```
# configure  terminal
(config)# vlan 184,220
(config-vlan)# exit
(config-vlan)# voice vlan
(config)# voice vlan vid 184
(config)# voice vlan oui 24-9A-D8 description YearLink
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid allowed vlan 184,220
(config-if)# switchport hybrid untagged vlan add 184,220
(config-if)# switchport hybrid native vlan 220
(config-if)# switchport hybrid ingress-filtering
(config-if)# switchport voice vlan mode auto
```

4.2.42. QoS (Качество обслуживания)

Сетевой трафик всегда непредсказуем, поэтому основным фактором обеспечения качества является предоставление наилучшего способа доставки. Для преодоления этой проблемы используется понятие качества обслуживания (Quality of Service (QoS)) применяемое ко всей сети. Гарантируется, что сетевой трафик будет приоритезирован в соответствии с заданным критерием, и прием будет производиться с использованием обработки по приоритетам. 115 QoS позволяет назначить различные классы сетевых услуг различным типам трафика, например, мультимедийному, видео, трафику конкретного протокола, критичному по времени трафику, трафику резервного копирования файлов. Чтобы задать приоритеты пакетов на данном коммутаторе, перейдите на страницу “Port Classification” (Классификация порта FIFO,PQ).

Команда	Описание
Глобальные настройки	
DSCP-Based QoS Ingress Classification	
`qos map dscp-cos <0-63> cos <0-7> dpl <0-1>`	настройка основных QoS DSCP на основе параметров QoS Ingress классификации. `dscp-cos<0-63>`- Значение DSCP входящего пакета. <0-7> - значение cos `dpl<0-1>` – Выбор приоритета отбрасывания DPL для соответствующего значения DSCP для обработки входящих кадров. По умолчанию задано 0. Значение “1” дает более высокий приоритет отбрасывания.
DSCP Translation	
`qos map dscp-ingress-translation <0-63><0-63>`	Преобразование DSCP на входящей стороне в любое из <0-63> значений DSCP.
`qos map dscp-classify <0-63>`	Включение классификации на входящей стороне, как определено в таблице настройки DSCP QoS на порту
`qos map dscp-egress-translation <0-63><0-1> to <0-`	Настройки для исходящей стороны. Заново отображает значение DP в выбранное

63>	значение DSCP. <0-1> 0- Управляет перераспределением кадров с уровнем DP 0. 1- Управляет перераспределением кадров с DP уровня 1. В любом случае после выбора требуется ввести значение, на которое будет переназначен DSCP
DSCP Classification	
qosmapcos-dscp<0~7>dpl<0~1>dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af3 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va }	Настройка сопоставления CoS и DPL со значением DSCP <0~7> - класс обслуживания <0~1> - уровни приоритета отбрасывания, для которого необходимо выбрать значение dscp
QoS Control List Configuration	
qos qce <1-256>	Создание записи QCE
qos qce <1-256> interface GigabitEthernet <port_type_list>	Выбор портов, настроенных с помощью этого QCE
qos qce <1-256> dmac {<mac_addr> | any | broadcast | multicast | unicast}	Настройка MAC-адреса назначения. Возможны следующие значения: any(Любой), broadcast(Широковещательный), multicast(Многоадресный), unicast(Одноадресный).
qos qce <1-256> smac {<mac_addr> | any}	Настройка MAC-адреса источника. Возможно указать конкретный MAC или выбрать любой.
qos qce <1-256> tag type {any | c-tagged | s-tagged | tagged | untagged}	Указание тип тега. Возможные значения: any: Сопоставление кадров с тегами и без тегов. untagged: Соответствие немаркированным кадрам. tagged: Сопоставление кадров с тегами. c-tagged: Соответствие фреймов с C-тегами. s-tagged: Соответствие фреймов с S-тегами. Значение по умолчанию - «Любой».
qosqce<1-256>tagvid {<vcap_vr> | any}	Указание диапазона VLAN или любой VLAN
qosqce<1-256>tagpcp {<pcp> | any}	Указание значения PCP, возможно указать конкретное значение, диапазон или выбрать вариант “любой”. Допустимые значения 0-7.
qos qce <1-256> tag dei {<0-1> | any}	Указание значения DEI. Может быть “0”,

	“1” или “любое”
qos qce <1-256> inner-tag type {any | c-tagged | s-tagged | tagged | untagged}	Указание типа внутреннего тега.
qos qce <1-256> inner-tag vid {<vcap_vr> | any}	
qos qce <1-256> inner-tag pcp {<pcp> | any}	
qos qce <1-256> inner-tag dei {<0-1> | any}	
qos qce <1-256> frame-type {any | etype |ipv4 | ipv6 | llc | snap}	Указание типа кадра, используемого при просмотре входящих кадров. Возможны следующие типы кадров: Any - QCE будет соответствовать всем типам кадров. Etype – Будут разрешены только кадры Ethernet (с типом EtherType 0x600-0xFFFF) llc – Будут разрешены только кадры LLC. snap -Будут разрешены только кадры SNAP. ipv4–QCE будет соответствовать только кадрам IPV4. ipv6–QCE будет соответствовать только кадрам IPV6.
qos qce <1-256> action {cos | dpl | dscp | pcp-dei | policy | vid}	Настройка операции, выполняемой на входящих кадрах, когда настройки параметров согласуются с содержимым кадра. Cos– значения (0-7) или «По умолчанию» Dpl– значения (0- 1) или «По умолчанию». Dscp- (0-63, BE, CS1-CS7, EF или AF11-AF43) или «По умолчанию». pcp-dei– значения pcp(0-7) или «По умолчанию», dei - (0-1) или «По умолчанию» policy– номер acl политики или «По умолчанию» vid - значение vlan «По умолчанию» означает, что классифицированное значение по умолчанию не изменяется этим QCE.
Global Storm Policer Configuration	
qos storm {broadcast | multicast | unicast} <1-1024000> {fps | kfps}	Настройка управления широковещательным штормом broadcast | multicast | unicast – выбор типа пакетов <1-1024000> – пороговое значение в пакетах в секунду. Принятые пакеты, при которых превышено выбранное значение, будут отброшены.

	fps | kfps- единицы измерения
Weighted Random Early Detection Configuration	
qos wred queue <0~7> min-fl <1-100> max <1-100> fill-level	Настройка управления переполнением очередей <0~7>- номер очереди min-fl<1-100>- нижний пороговый уровень заполнения. Если уровень заполнения очереди ниже этого порога, вероятность отбрасывания равна нулю. Значение 0–100%. max<1-100>- Управляет верхней вероятностью отбрасывания или пороговым значением уровня заполнения для кадров, помеченных как уровень приоритета отбрасывания > 0. Значение 1–100%. fill-level- max управляет уровнем заполнения, при котором вероятность выпадения достигает 100%. Эта конфигурация позволяет зарезервировать часть очереди исключительно для кадров, отмеченных уровнем приоритета отбрасывания 0 (зеленые кадры). Зарезервированная часть рассчитывается как (100 - Макс) %. По умолчанию - max управляет вероятностью выпадения, когда уровень заполнения чуть ниже 100%.
Настройка порта	
interface GigabitEthernet <port_type_list>	Выбор портов
QoS Port DSCP Configuration	
qos dscp-translate	Включение трансляцию значений DSCP на основе установленного метода классификации
qos dscp-classify {any | selected | zero} No qos dscp-classify	Выбор метода классификации Zero – Классификация выполняется, если DSCP входящих кадров равен 0. Selected- классифицируются только DSCP, для которых включена классификация в таблице трансляции DSCP. any – классифицируются все поля DSCP. Классификация DSCP входящих кадров не выполняется
qos dscp-remark {remap | remap-dp | rewrite}	Настройка перезаписи значений DSCP исходящих кадров. rewrite - Перезапись значений DSCP исходящих кадров включена, но

	отображение после перезаписи не выполняется. remap - Кадр с DSCP, поступивший от анализатора, снова отображается и помечается новым значением DSCP. В зависимости от уровня DP кадра, новое значение DSCP берется из таблицы трансляции DSCP из поля Egress Remap DP0 или DP1. remap-dp – Кадр с DSCP, поступивший от анализатора снова отображается и помечается новым значением DSCP. Новое значение DSCP всегда берется из таблицы трансляции DSCP из поля Egress Remap DP0
No qos dscp-remark	Перезапись значений DSCP исходящего трафика выключена
QoS Egress Port Tag Remarking	
qos tag-remark {mapped | pcp <0-7> dei <0-1>}	Выбор режима изменения тегов на порту Mapped – Используется отображение значений классов QoS и уровней DP в значения PCP/DEI. pcp<0-7>dei<0-1> – Используются значения PCP/DEI. По умолчанию - PCP:0; DEI:0.
QoS Egress Port Shapers	
qos wrr <1-100>	Установка режима работы с очередями – взвешенный, должен быть задан вес в каждой очереди. По умолчанию режим работы с очередями - строгий. В этом режиме кадры из выходных очередей с более высокими приоритетами будут передаваться первыми (по сравнению с кадрами, находящимися в очередях с низкими приоритетами).
No qos wrr	Выключение взвешенного режима работы с очередями
Ingress Queue Policers	
qos queue-policer queue <0~7><1-3276700> {kbps | mbps}	Настройка скорости в очередях <0~7> – номер очереди <1-3276700> – Скорость, до которой будет ограничена скорость в очереди. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон

	значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с. {kbps | mbps} – Единицы измерения ограничения скорости очереди входящих кадров.
Ingress Port Policers	
qos policer <1-3276700> {fps | kbps | kfps | mbps} flowcontrol	Настройка и включение функции ограничения скорости на порту <1-3276700>- скорость, до которой будет ограничена скорость на порту. По умолчанию задано 500 кбит/с. Допустимый диапазон для kbps (кбит/с) и fps (кадров/с): от 100 до 1000000. Допустимый диапазон для Mbps (Мбит/с) и kfps (кадров/с): от 1 до 3300 Мбит/с. {fps | kbps | kfps | mbps} – Единицы измерения ограничения скорости Flowcontrol – включение функции управления потоком. Если управление потоком включено и порт работает в режиме управления потоком, то будут отправляться кадры pause, вместо отбрасывания входящих кадров.
Port Classification	
qoscos<0-7>	Настройка класса QoS, выбираемый по умолчанию. Класс QoS с номером 0 имеет наименьший приоритет. По умолчанию задано 0.
qos dpl<0-1>	Настройка приоритета отбрасывания: 0: Подтвержденные кадры. 1: Кадры, которые могут быть отброшены
qos pcp<0-7>	Настройка значения пользовательского приоритета (Priority Code Point) для не тегированных кадров.
qos dei<0-1>	Настройка значения индикатора отбрасывания по критерию (Drop Eligible Indicator) для не тегированных кадров.
qos trust tag No qos trust tag	режим классификации для тегированных кадров на данном порту: • Enabled (Включен): Для тегированных кадров используется значение PCP и DEI из таблицы (PCP, DEI) to (QoS class, DP level) Mapping. • Disabled (Выключен): Для тегированных кадров используется класс QoS и уровень DP по умолчанию.
qos trust dscp	включение QoS на основе DSCP (входящий порт).
qos qce key {double-tag | ip-	Выбор типа определяющего ключа,

addr | mac-ip-addr | normal}	сгенерированный для кадров, полученных через порт. Допустимые значения: Normal – соответствует внешнему тегу, SMAC/DMAC, IP-протоколу, DSCP, SIP/DIP, SPORT и DPORT. double-tag – четверть ключа, соответствует внутреннему и внешнему тегу. ip-addr - половина ключа, совпадение внутреннего и внешнего тега, SIP и DIP. Для кадров, не относящихся к IP, используйте только внешний тег. mac-ip-addr – Полный ключ, совпадающий внутренний и внешний тег, SMAC, DMAC, SIP и DIP.
qos qce addr {destination | source}	Выбор режима IP/MAC-адреса, определяющего, должна ли классификация QCL основываться на адресах источника (SMAC/SIP) или назначения (DMAC/DIP) на этом порту. Этот параметр используется только в том случае, если тип ключа Normal. Допустимыми значениями являются: source – Позволяет сопоставлять SMAC/SIP. Destination – Позволяет сопоставлять DMAC/DIP.
Настройка Storm Policer Configuration на интерфейсе	
interface GigabitEthernet <port_type_list>	Выбор портов
qosstorm{broadcast| multicast | unicast| unknown } <1-13128147> { fps | kbps| kfps| mbps | shutdown| <cr> } { shutdown } <cr>	Команды QoS Storm Control предназначены для защиты сетей от широковещательного шторма (storm control) путём ограничения скорости трафика определённого типа на интерфейсе устройства. Эти команды позволяют задать пороговую скорость, превышение которой вызывает определённое действие, такое как снижение пропускной способности или блокировка порта. тип ограничиваемого трафика: – Broadcast – широковещательные пакеты. – Multicast – многоадресные пакеты. – Unicast – одноадресные пакеты. – Unknown – неизвестные MAC-адреса. Может задаваться в единицах измерения: – fps – кадры в секунду. – kbps – килобиты в секунду. – kfps – тысячи кадров в секунду.

	– mbps – мегабит в секунду. {shutdown} – дополнительная опция, при выборе которой интерфейс временно отключится при достижении установленного порога. Примечание. Команда `errdisable storm-control interval <int>` предназначена для установки интервала времени восстановления состояния интерфейса после автоматического отключения (err-disable) вследствие достижения лимита пакета определенного типа (штормового трафика). Для возврата к значению по умолчанию (300 секунд) применить команду: no err disable storm – control interval
`no qos storm {broadcast| multicast | unicast| unknown }`	Команда отменяет ранее установленную защиту от шторма на указанном интерфейсе.

4.2.43. Mirroring (Зеркалирование)

Зеркалирование портов– технология дублирования пакетов одного порта сетевого коммутатора (или отдельной VLAN) на другом.

Зеркалирование портов используется на сетевом коммутаторе для отправки копии сетевых пакетов, видимых на указанных портах (исходный порт), на другие указанные порты (порт назначения). При включенном зеркалировании портов пакеты можно отслеживать и анализировать. Зеркалирование портов применяется широко, например, сетевые инженеры могут использовать зеркалирование портов для анализа и отладки данных или диагностики ошибок в своих сетях, без влияния на возможности обработки пакетов сетевых устройств.

Команда	Описание
Глобальные настройки	

`monitor session <1-5>`
 	
`no monitor session <1-5>`
	Включение функции зеркального отображения (всего возможно создать до пяти сеансов)
	
	Выключение функции зеркального отображения или дистанционного зеркалирования

`monitor session <1-5> source interface` <port_type_list> { both | rx | tx}	Выбор порта источника и типа трафика Both - На зеркальный порт будут переданы кадры, принятые и переданные данным портом Rx - На зеркальный порт будут направлены только кадры, принятые данным портом. Tx - На зеркальный порт будут направлены только кадры, переданные данным портом.

monitor session <1-5> destination interface <port_type_list>	Выбор порта назначения, который получает копию трафика из исходного порта.
monitor session <1-5> source remote vlan <vlan_id>	Включение режима RMirrorSource и назначение vlan куда будет скопирован пакет. Коммутатор является исходным узлом для отслеживания потока. Порт источника расположены на этом коммутаторе.
monitor session <1-5> destination remote vlan <vlan_id>	Включение режима RMirror Destination и назначение vlan куда будет скопирован пакет. Коммутатор является конечным узлом для отслеживания потока. Порт назначения расположен на этом коммутаторе.
monitor session <1-5> source vlan <vlan_list>	Настройка функции зеркалирования на основе VLAN. Если вы хотите контролировать некоторые VLAN на коммутаторе, вы можете установить выбранные VLAN. Сеанс зеркалирования должен иметь в качестве источников либо порты, либо сети VLAN, но не то и другое вместе.

4.2.44. UPnP

Команда	Описание
Глобальные настройки	
Upnp	Включение функции UPnP. При включении автоматически создается два правила списка доступа (ACE) для перенаправления соответствующих UPnP пакетов к процессору.
No Upnp	Выключает функцию UPnP. При выключении правила автоматически удаляются.
upnp advertising-duration<100-86400>	Настройка параметра продолжительности. Этот параметр определяет, насколько часто могут посылаться уведомления UPnP. Длительность переносится пакетами протокола SSDP (Simple 129 Service Discover Protocol), которые информируют пункт управления о том, насколько часто следует принимать сообщения с уведомлениями SSDP от коммутатора. По

	умолчанию установлена длительность уведомления 100 секунд. Однако, вследствие ненадежности протокола UDP рекомендуется уменьшать длительность, так как чем она меньше, тем быстрее обновляется состояние UPnP.
`upnp ip-addressing-mode {dynamic | static}`	Режим ip-адресации `dynamic` - режим по умолчанию. Модуль UPnP помогает пользователям выбрать IP-адрес коммутатора. Он находит первый доступный системный IP-адрес. `static` - Пользователь указывает IP-интерфейс VLAN для выбора IP-адреса коммутирующего устройства.
`upnp static interface vlan <vlan_id>`	Настройка VLAN id для режима статической ip адресации.

4.2.45. GVRP

GVRP (GenecicVLANRegistrationProtocol) является одним из приложений GARP (GenericAttributeRegistrationProtocol, Протокол регистрации общих атрибутов). GARP используется в сетевых мостах, сетевых коммутаторах, или других аналогичных устройствах с возможностью регистрации и перерегистрации специальных атрибутов, таких как идентификаторы VLANи членство в мультикастовых группах в больших локальных сетях. GVRP- приложение GARP, которое отвечает за обмен информацией о VLANи позволяет коммутаторам регистрировать VLANдинамически.

Команда	Описание
Глобальные настройки	
`gvrp`	Включение протокола GVRP глобально

`gvrp time join-time <1-20>`
 	
`gvrp time leave-time <60-300>`
 	
`gvrp time leave-all-time <1000-5000>`
	Настройка таймеров. Таймеры на обоих концах сети должны быть одинаковы, иначе GVRP не сможет работать нормально.

`gvrp max-vlans<1-4094>`	Настройка максимального количества VLAN, которыми GVRP может управлять.
Настройка порта	
`interface GigabitEthernet <port_type_list>`	Выбор портов
`gvrp`	Включение функции gvrp Рекомендуется избегать использования функций GVRP и RSTPодновременно на коммутаторе. Если необходимо включить GVRP, сначала необходимо отключить функцию RSTP для портов

4.2.46. sFlow

sFlow – это технология системы измерения сетевого трафика общего назначения. sFlow предназначен для встраивания в любое сетевое устройство и обеспечения непрерывной статистики по любому протоколу (L2, L3, L4 и вплоть до L7), так что весь трафик в сети может быть точно охарактеризован и отслежен. Эти статистические данные важны для контроля перегрузки, устранения неполадок, наблюдения за безопасностью, планирования сети и т. Д. Они также могут использоваться для целей учета IP.

Команда	Описание
Глобальные настройки	
`sflowagent-ip {ipv4 | ipv6} {<ipv4_addr> | <ipv6_addr>}`	Настройка IP-адреса, используемого в качестве IP-адреса агента в sFlow. Он служит уникальным ключом, который будет идентифицировать агента в течение длительных периодов времени. Поддерживаются адреса IPv4 и IPv6
`sflow collector-address {<domain_name> | <ipv4_addr> | <ipv6_ucast>}`	Настройка IP-адреса или имя хоста приемника sFlow
`sflow collector-port <1-65535>`	Настройка просматриваемого UDP порта
`sflow max-datagram-size <200-1468>`	Настройка максимального количество байтов данных, которое может быть отправлено в одной тестовой датаграмме
`sflow timeout <0-2147483647>`	Настройка таймаута
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов
`sflow`	Включает функцию sflow на порту.
`sflow sampling-rate <1-4096>`	Настройка статической частоты дискретизации.
`sflow max-sampling-size <14-200>`	Максимальное количество байтов, которое должно быть скопировано из пакета, выбранного для выборки, в дейтаграмму sFlow.
`sflow counter-poll-interval<1-3600>`	Интервал опроса. Допустимый диапазон: от 1 до 3600 секунд

4.2.47. UDLD

Обнаружение однонаправленного соединения (UDLD) – это уровень канала передачи данных протокол для контроля физической конфигурации кабелей и обнаружения однонаправленных каналов. UDLD дополняет протокол связующего дерева, который используется для устранения петли переключения.

Чтобы обнаружить однонаправленные каналы до создания петли пересылки, UDLD работает путем обмена пакетами протокола между соседними устройствами.

Для работы UDLD оба коммутирующих устройства в канале должны поддерживать UDLD и иметь его включенным на соответствующих портах.

Команда	Описание
Глобальные настройки	
`Udld enable`	Включение UDLD на всех оптоволоконных портах.
`Udld aggressive`	Включение UDLD в агрессивном режиме на всех оптоволоконных портах.
`udld message time-interval<7-90>`	Настройка интервал сообщений `<7-90>`
`udld unblocking`	Ручное включение заблокированных портов.

4.2.48. DDMI (интерфейс цифрового диагностического мониторинга)

Усовершенствованный цифровой интерфейс позволяет установить связь в реальном времени между коммутатором и трансивером SFP. Это позволяет коммутатору получать доступ к рабочим параметрам в оптоволоконном канале.

DDMI контролирует:

- температуру
- напряжение питания
- передаваемый ток смещения.
- Передаваемая мощность
- Полученная мощность

Команда	Описание
Глобальные настройки	
`ddmi`	Включение функции DDMI. Функция DDMI включена по умолчанию.
`no ddmi`	Выключение функции DDMI

4.2.49. MRP и MVRP

Multiple Registration Protocol (MRP) – это общая структура, рекомендованная IEEE для использования в сетевых мостах, сетевых коммутаторах, или других аналогичных устройствах с возможностью регистрации и перерегистрации специальных атрибутов, таких как идентификаторы VLAN и членство в мультикастовых группах в больших локальных сетях LAN.

Протокол множественных регистраций VLAN Multiple VLAN Registration Protocol (MVRP) является сетевым протоколом второго уровня для автоматической конфигурации информации VLAN в коммутаторах. Он был определён приложением 802.1ak к рекомендациям IEEE 802.1Q-2005.

В пределах второго уровня сетевой модели OSI MVRP обеспечивает динамический обмен информации о VLAN и конфигурацию необходимых VLAN. Например, поставлена задача добавить определённый порт коммутатора в VLAN, или сетевое устройство,

поддерживающее VLAN и подключённое в порт коммутатора требует переконфигурации, и все необходимые транки динамически созданы на других коммутаторах, поддерживающих MVRP. Для выполнения этой задачи без возможностей MVRP потребуется ручная конфигурация VLAN или какой-либо проприетарный метод производителя. Если же выполнять эту задачу средствами MVRP, который использует динамические значения VLAN в фильтруемой базе данных. Если коротко – MVRP помогает динамически поддерживать конфигурации VLAN в статических конфигурациях сетей.

802.1Q даёт возможность:

- Динамически конфигурировать и распределять информацию о принадлежности VLAN через механизмы MVRP.
- Статически конфигурировать информацию о принадлежности VLAN посредством механизмов менеджмента, которые позволяют управлять регистрационными данными о статических записях регистраций VLAN.
- Поддерживать комбинированные статические и динамические конфигурации, при которых некоторые VLAN конфигурируются посредством механизмов менеджмента, а для других VLAN сохраняется возможность динамической конфигурации средствами MVRP.

Команда	Описание
Глобальные настройки	

`mvrp`
 	
`no mvrp`
	Включение функции MVPR.
	
	Выключение функции MVRP

`mvrp managed vlan {<vlan_list> | add | all | except | none | remove}`	Настройка списка VLAN, управляемых MVRP `<vlan_list>`- создание нового списка `Add`– добавить VLAN к существующему списку `All`– все VLAN `Except`– Добавить все VLAN, кроме следующих `None`–пустой список `Remove`– удалить VLAN из текущего списка
Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов
`Mvrp` `No mvrp`	Включение функции MVRP на порту Выключение функции MVRP на порту.

`mrp periodic`
 	
`no mrp periodic`
	Включение функции Periodic Transmission для всех приложений MRP на порту
	
	Выключение функции Periodic Transmission
	на порту

`mrp timers {default | join-time | leave-all-time | leave-time}`	Настройка таймеров `Default`- Установка всех таймеров MRP по умолчанию

	join-time–таймер присоединения. Значения от 1-20сс. По умолчанию значение 20сс. leave-all-time– таймер отключения от всех мультикастовых групп. Значения 1000-5000сс. По умолчанию – 1000сс leave-time– таймер отключения. Значения от 60-300сс. По умолчанию значение 60сс

4.2.50. Link OAM

Команда	Описание
Настройка портов	
interface GigabitEthernet <port_type_list>	Выбор портов
link-oam no link-oam	Включение Link OAM на порту коммутатора. Включение Link OAM дает операторам сети возможность отслеживать состояние сети и быстро определять местоположение неисправных каналов или неисправных состояний. Выключение Link OAM на порту
link-oam mode {active | passive}	Настройка режима OAM как активный или пассивный. По умолчанию установлен пассивный режим. active- DTE, настроенные в активном режиме, инициируют обмен информационными OAMPDU, как определено в процессе обнаружения. После завершения процесса обнаружения активным DTE разрешается отправлять любые OAMPDU при подключении к удаленному одноранговому объекту OAM в активном режиме. Активные DTE работают в ограниченном отношении, если удаленный объект OAM работает в пассивном режиме. Активные устройства не должны отвечать на команды удаленной обратной связи OAM и запросы переменных от пассивного однорангового узла. passive- DTE, настроенные в пассивном режиме, не инициируют процесс обнаружения. Пассивные DTE реагируют на инициирование процесса обнаружения удаленным DTE. Это

	исключает возможность перехода от пассивных к пассивным ссылкам. Пассивные DTE не должны отправлять запросы переменных или OAMPDU управления шлейфом.

`link-oam remote-loopback supported`
 	
`no link-oam remote-loopback supported`
	Включение функции удаленной петли. Может использоваться для локализации неисправностей и тестирования производительности связи.
	
	Выключение функции удаленной петли.

`link-oam link-monitor supported`
 	
`no link-oam link-monitor supported`
	Включение функции мониторинга на порту.
	
	Выключение функции мониторинга на порту.

`link-oam mib-retrieval supported`
 	
`no link-oam mib-retrieval supported`
	Включение поддержки MIB на порту коммутатора
	
	Выключение поддержки MIB на порту коммутатора

Настройка событий	
`link-oam link-monitor frame {threshold | window}`	Событие "Ошибочный кадр" подсчитывает количество ошибочных кадров, обнаруженных в течение указанного периода. Период задается временным интервалом (`window`). Это событие генерируется, если количество ошибочных кадров равно или превышает заданный порог для этого периода (`threshold`). `Window` – окно ошибки должно иметь целое значение от 1 до 60, а его значение по умолчанию равно "1". `Threshold` – порог ошибки должен находиться в диапазоне 0-4294967295, а его значение по умолчанию равно "1".
`link-oam link-monitor symbol-period {threshold | window}`	Событие подсчитывает количество ошибок символа, произошедших в течение указанного периода. Период определяется количеством символов, которые могут быть получены за определенный промежуток времени на базовом физическом уровне. Это событие генерируется, если количество ошибок символа равно или превышает заданный порог для этого периода. `window` - окно ошибки должно иметь целое значение от 1 до 60, а его значение

	по умолчанию равно "1". `threshold` - порог ошибки должен находиться в диапазоне 0-4294967295, а его значение по умолчанию равно "1".
`link-oam link-monitor frame-seconds {threshold | window}`	Событие подсчитывает количество секунд с ошибками, произошедших в течение указанного периода. Период определяется временным интервалом. Это событие генерируется, если количество секунд с ошибками в кадре равно или превышает заданный порог для этого периода. `Window` – окно ошибки должно иметь целое значение в диапазоне от 10 до 900, а его значение по умолчанию равно "60". `threshold` - порог ошибки должен находиться в диапазоне 0-65535, а его значение по умолчанию равно "1".

4.2.51. CFM

CFM (Connectivity Fault Management), IEEE 802.1 ag – предоставляет функции наблюдения, поиска и устранения неисправностей в сетях Ethernet, позволяя контролировать соединение, изолировать проблемные участки сети и идентифицировать клиентов, к которым применялись ограничения в сети.

Команда	Описание
Глобальные настройки	
`cfm sender-id-tlv {chassis | chassis-management | disable | management}`	Выбор идентификатора tlv `Chassis`– идентификатор шасси (MAC-адрес) `chassis-management`- идентификатор шасси (MAC-адрес) и адрес управления (IPv4-адрес) `management`- адрес управления (IPv4-адрес) `disable`– исключить идентификатор tlv
`cfm port-status-tlv {disable enable}`	Включение или выключение tlv для статуса порта
`cfm interface-status-tlv {disable enable}`	Включение или выключение tlv для статуса интерфейса
`cfm organization-specific-tlv disable`	Исключить TLV для конкретной организации
`cfm organization-specific-tlv enable oui <oui> subtype <0-255> value <string63>`	Включить TLV для конкретной организации `<oui>` – Это трехбайтовый OUI, передаваемый с TLV, зависящим от организации.

	<0-255> – Это подтип, передаваемый с TLV для конкретной организации. Может быть любым значением в диапазоне [0; 255] <string63> – Это значение, передаваемое в TLV для конкретной организации. Значение представляет собой печатаемую строку символов длиной 0-63.
CFM Domain Configuration	
cfm domain <kword1-15>	Создание имени домена
Format {none | string}	Выбор формата имени MD. Чтобы имитировать идентификаторы MEG Y.1731, используйте тип None.
Level <0-7>	Уровень MD / MEG этого домена. Допустимые значения ограничены до 0–7.
sender-id-tlv {chassis | chassis-management | defer | disable | management }	Выбор идентификатора tlv Chassis– идентификатор шасси (MAC-адрес) chassis-management- идентификатор шасси (MAC-адрес) и адрес управления (IPv4-адрес) management- адрес управления (IPv4-адрес) disable– исключить идентификатор tlv defer – применяются настройки глобальной конфигурации
port-status-tlv {defer | disable | enable}	Включение или выключение tlv для статуса порта Defer– применяются настройки глобальной конфигурации
interface-status-tlv {defer | disable | enable}	Включение или выключение tlv для статуса интерфейса Defer – применяются настройки глобальной конфигурации
organization-specific-tlv {defer | disable}	disable - исключить TLV для конкретной организации Defer – применяются настройки глобальной конфигурации
Service<kword1-15>	Переход в режим конфигурации CFM Service
CFM Service Configuration	
Format {integer primary-vid string }	Выбор формата имени службы. Это решает, как будет интерпретироваться значение параметра Name. Возможные значения: integer primary-vid

	string
type {port | vlan<1-4095>}	Выбор MEP в сервисе Основной VID MA. VLAN, равный 0, означает, что все MEP, созданные в этом MA, будут созданы как MEP порта (интерфейсные MEP). На каждом интерфейсе может быть только одна портовая MEP. MEP данного порта может быть создана с тегами, если VLAN этой MEP не равна нулю.
continuity-check interval {100ms | 10ms | 1s | 3.3ms}	Настройка скорости CCM всех MEP, привязанных к этой услуге
sender-id-tlv {chassis | chassis-management | defer | disable | management}	Выбор идентификатора tlv Chassis– идентификатор шасси (MAC-адрес) chassis-management- идентификатор шасси (MAC-адрес) и адрес управления (IPv4-адрес) management- адрес управления (IPv4-адрес) disable– исключить идентификатор tlv defer – применяются настройки глобальной конфигурации
port-status-tlv {defer | disable | enable}	Включение или выключение tlv для статуса порта Defer– применяются настройки глобальной конфигурации
interface-status-tlv {defer | disable | enable}	Включение или выключение tlv для статуса интерфейса Defer – применяются настройки глобальной конфигурации
organization-specific-tlv {defer | disable}	disable - исключить TLV для конкретной организации Defer – применяются настройки глобальной конфигурации
Mep<1-8191>	Переход в режим конфигурации CFM Mep
CFM Mep Configuration	
interface GigabitEthernet <port_type_id>	Указание порта на котором находится эта MEP
Vlan{1-4095 | inherit}	Указание идентификатора VLAN. inherit- используется для обозначения не тегированного трафика (подразумевается MEP порта).
Pcp <0-7>	Выбор значения PCP в теге VLAN PDU. Не используется без тегов.
Smac <mac_ucast>	Настройка MAC-адреса источника,

	который будет использоваться в блоках PDU CCM, исходящих от этой MEP. Адрес должен быть одноадресным. Формат: XX: XX: XX: XX: XX: XX. Если все нули, вместо него будет использоваться MAC-адрес порта коммутатора.
`alarm-level <1-6>`	Установка уровня сигнализации. Если обнаружен дефект с приоритетом выше этого уровня, будет сгенерировано уведомление о неисправности. Допустимый диапазон: [1; 6], где 1 указывает, что любой дефект вызывает аварийный сигнал, а 6 означает, что никакой дефект не может вызвать аварийный сигнал.
`alarm-time-present <2500-10000>`	Установка времени в миллисекундах, в течение которого должны присутствовать дефекты, прежде чем будет выдано уведомление о неисправности. По умолчанию 2500 мс.
`alarm-time-absent <2500-10000>`	Установка времени в миллисекундах, в течение которого дефекты должны отсутствовать до сброса уведомления о неисправности. По умолчанию 10000 мс.
`continuity-check` `no continuity-check`	включение генерации сообщений проверки целостности (CCM) отключение генерации сообщений проверки целостности
`admin-state {disable | enable}`	включить или отключить эту MEP. Когда эта MEP включена, она проверяет полученные / отсутствующие CCM и может вызывать дефекты.
`remote mep<1-8191>`	Установка удаленной MEP, от которой эта MEP, как ожидается, будет получать PDU CCM.

4.2.52. APS

APS сетевой протокол канального уровня, предназначен для поддержки топологии, исключающей зацикливание трафика, и её перестроение в случае нарушений в кольцевых сетях Ethernet на первом-втором уровне сетевой модели OSI.

Команда	Описание
Глобальные настройки	
`Aps <1-10>`	Создание экземпляра APS
`working interface GigabitEthernet <port_type_id>`	Назначение интерфейса в качестве рабочего порта
`working sf-trigger link`	Выбор триггера для сигнала ошибки В качестве триггера используется состояние порта

working sf-trigger mep domain <kword1-15> service <kword1-15> mep-id <1-8191>	В качестве триггера используется mep. Требуется ввод domain service mep - id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
protect interface GigabitEthernet <port_type_id>	Назначение интерфейса в качестве защищенного порта
protect sf-trigger link	Выбор триггера для сигнала ошибки В качестве триггера используется состояние порта
protect sf-trigger mep domain <kword1-15> service <kword1-15> mep-id <1-8191>	В качестве триггера используется mep. Требуется ввод domainservicemep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
Mode {1-for-1 | bidirectional-1-plus-1 | unidirectional-1-plus-1}	1-for-1 - В линейной архитектуре защитной коммутации 1: 1 защитный транспортный объект выделен рабочему транспортному объекту. Однако нормальный трафик транспортируется либо на рабочем транспортном объекте, либо на защитном транспортном объекте, используя мост селектора в источнике защищенного домена. Селектор в приемнике защищенного домена выбирает объект, который несет нормальный трафик bidirectional-1-plus-1 - В линейной архитектуре защитной коммутации 1 + 1 для каждого рабочего транспортного объекта выделен защитный транспортный объект. Обычный трафик копируется и направляется как рабочим, так и защитным транспортным объектам с постоянным мостом в источнике защищенного домена. Трафик на рабочих и защитных транспортных объектах передается одновременно в приемник защищенного домена, где выбор между рабочим и защитным транспортными объектами осуществляется на основе некоторых заранее определенных критериев, таких как индикация неисправности сервера. unidirectional-1-plus-1 – однонаправленный APS. Команда mode unidirectional-1-plus-1 tx-apsвключает передачу

	блоков APS PDUs. PS даже в однонаправленном режиме 1+1. Прием APS PDU в этом режиме используются только в информационных целях.
`Level<0-7>`	Установка уровня MD / MEG, используемый в L-APS PDU. По умолчанию 0.
`Vlan<vlan_id>`	Установка идентификатора VLAN, используемого в L-APS PDU. Команда `vlan untagged`– не вставлять тег VLAN в PDU LAPS
`vlan <vlan_id> pcp <0-7>`	Настройка PCP (приоритет) (по умолчанию 7). Значение PCP, используемое в теге VLAN, если L-APS PDU не является немаркированным. Должно быть значение в диапазоне 0–7.
`Smac <mac_ucast>`	Установка MAC-адреса источника, используемый в PDU L-APS. Адрес должен быть одноадресным. Если все нули, будет использоваться MAC-адрес порта коммутатора.

`Revertive`
 	
`no revertive`
	Включение реверсивного режима, то есть трафик переключается обратно на рабочий порт после устранения условий, вызывающих переключение. В случае сброса команды (например, принудительное переключение) это происходит немедленно. В случае устранения дефекта это обычно происходит по истечении таймера WTR (ожидания восстановления).
	
	Режим восстановления порта не является реверсивным, и трафику разрешается оставаться на защищенном порте после устранения причины переключения.

`wait-to-restore <1-720>`	Настройка ожидания перед восстановлением рабочего порта после устранения неисправности. Допустимый диапазон 1–720
`hold-off-time <0-10000>`	Установка таймера задержки. Когда возникает новый (или более серьезный) дефект, запускается таймер задержки, и о событии будет сообщено после истечения таймера. Время удержания измеряется в миллисекундах, а допустимые значения находятся в диапазоне от 0 до 10000. По умолчанию 0, что означает немедленное сообщение о дефекте.
`admin-state {disable | enable}`	Изменение состояния экземпляра APS

	(выключено/включено)

4.2.53. ERPS

ERPS -сетевой протокол, использующийся для исключения образования колец в топологии. Может быть заменой семейству протоколов **STP**.

Команда	Описание
Глобальные настройки	
`Erps <1-64>`	Создание экземпляра ERPS
`rpl {neighbor | owner} {port0 | port1}`	Выбор режима кольцевой защиты и кольцевого порта
`Version {v1 | v2}`	Выбор версии протокола ERPS
`ring-type {interconnected-sub-ring | major | sub-ring}`	Выбор типа кольца.
`ring-type sub-ring`	Выбор режима `sub-ring` При вводе дополнительной команды `virtual-channel` – включает виртуальный канал R-APS, то есть PDU R-APS не пересылаются между кольцевым портом, если один конец заблокирован
`ring-type interconnected-sub-ring connected-ring <1-64>`	Выбор режима взаимосвязанного `sub-ring`, которое имеет только один кольцевой порт (порт 0), но подключается к главному кольцу. `<1-64>` – Номер экземпляра ERPS подключенного кольца Дополнительная команда `propagate-topology-change` – Управляет тем, должно ли кольцо, на которое ссылается экземпляр Interconnect, распространять R-APS для PDU всякий раз, когда изменяется топология этого под-кольца. При вводе команды `virtual-channel` – PDU R-APS передаются по подключенному кольцу, к которому подключается это под-кольцо
`{port0 | port1} interface GigabitEthernet <port_type_id>`	Назначение интерфейса кольцевому порту 0
`{port0 | port1} sf-trigger link`	Установка в качестве триггера сбоя сигнала состояние соединения
`{port0 | port1} sf-trigger mep domain <kword1-15> service <kword1-15> mep-id <1-8191>`	В качестве триггера используется mep. Требуется ввод domain service mep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
`ring-id <1-239>`	Настройка идентификатора кольца. Идентификатор кольца используется - вместе с управляющей VLAN - для

	идентификации блоков PDU R-APS как принадлежащих определенному кольцу.
node-id <mac_ucast>	Настройка идентификатора узла. Идентификатор узла используется внутри конкретного PDU R-APS для уникальной идентификации этого узла (коммутатора) в кольце.
Level <0-7>	Установка уровня MD / MEG
control-vlan <vlan_id>	Установка VLAN, по которой блоки PDU R-APS передаются и принимаются на кольцевых портах.
control-vlan <vlan_id> pcp <0-7>	Установка значения PCP, используемое в теге VLAN PDU R-APS.
revertive	Включение режима возврата. Восстановление значений по умолчанию после истечения таймера ожидания восстановления.
guard-time<0-2000>	Установка таймера защиты.
wait-to-restore<1-720>	Установка времени ожидания восстановления в секундах. Допустимый диапазон 1–720 сек. Используется только в реверсивном режиме
hold-off-time<0-10000>	Установка таймера задержки. Когда возникает новый (или более серьезный) дефект, запускается таймер задержки, и о событии будет сообщено после истечения таймера. Время удержания измеряется в миллисекундах, а допустимые значения находятся в диапазоне от 0 до 10000. По умолчанию 0, что означает немедленное сообщение о дефекте.
admin-state {disable | enable}	Изменение состояния экземпляра ERPS (выключено/включено)
protected-vlans<vlan_list>	Указание VLAN, защищенные этим экземпляром кольца. По крайней мере, одна VLAN должна быть защищена.
rpl {neighbor | owner} {port0 | port1}	Настройка режима rpl Neighbor - этот коммутатор является соседом RPL Owner - этот коммутатор является владельцем RPL В обоих режимах требуется указать кольцевой порт.

4.2.54. Настройка Spanning Tree

Протоколы семейства **Spanning Tree Protocol (STP/RSTP/MSTP/PVST/Rapid-PVST)** предназначены для обеспечения отказоустойчивости L2-сетей путем

автоматического блокирования избыточных (петлевых) физических связей и их динамического включения в случае аварии на основных маршрутах.

На коммутаторах серии NTS протокол Spanning Tree **включен по умолчанию** глобально и на всех интерфейсах в режиме **MSTP (Multiple Spanning Tree Protocol)**. По умолчанию все настроенные на коммутаторе VLAN автоматически привязываются к базовому инстансу **Instance 0.**

Команда	Описание
Глобальные настройки	

`spanning-tree`
 	
`no spanning-tree`
	Глобальное включение протокола Spanning Tree на коммутаторе. (По умолчанию включено)
	
	Глобальное отключение протокола Spanning Tree на коммутаторе.

`spanning-tree mode {mstp | pvst | rapid-pvst | rstp | stp}`
 	
`no spanning-tree mode`
	Выбор операционного режима работы протокола:
	• **mstp** – Режим Multiple Spanning Tree (стандарт IEEE 802.1s), включен по умолчанию.
	• **pvst** – Режим Per-Vlan Spanning Tree (по-VLAN-овое связующее дерево).
	• **rapid-pvst** – Режим Rapid Per-Vlan Spanning Tree (быстрое по-VLAN-овое связующее дерево).
	• **rstp** – Режим Rapid Spanning Tree (стандарт IEEE 802.1w).
	• **stp** – Классический режим 802.1D Spanning Tree.
	
	Сброс режима работы протокола на значение по умолчанию (mstp).

`spanning-tree mst <0-64> priority <0-61440>`	Настройка приоритета коммутатора (Bridge Priority) для указанного инстанса MSTP. Значение должно быть кратно 4096. Для базовой топологии используется `<instance_id>` равный 0. По умолчанию: 32768.
`spanning-tree mst <0-64> vlan <vlan_list>`	Прямая привязка списка или диапазона VLAN к выбранному инстансу MSTP из глобального режима конфигурации.
`no spanning-tree mst <0-64>`	Сброс настроек конкретного инстанса MSTP (удаление маппинга VLAN и возврат приоритета по умолчанию).
`spanning-tree mst name <word32> revision <0-65535>`	Одновременное задание текстового имени (до 32 символов) и номера ревизии для MST-региона. Важно: для корректной работы MSTP параметры имени и ревизии должны полностью совпадать на всех коммутаторах в рамках одного региона.
`spanning-tree edge bpdu-guard`	Глобальное включение функции защиты BPDU Guard для всех граничных портов. Если на любой

	Edge-порт придет пакет BPDU, интерфейс автоматически заблокируется.
no spanning-tree edge bpdu-guard	Глобальное отключение функции защиты BPDU Guard для всех граничных портов.
spanning-tree edge bpdu-filter	Глобальная активация фильтрации пакетов BPDU для всех граничных портов. Коммутатор перестает отправлять и обрабатывать входящие BPDU на Edge-интерфейсах.
no spanning-tree edge bpdu-filter	Глобальное отключение фильтрации пакетов BPDU для граничных портов.
spanning-tree recovery interval <30-86400>	Настройка интервала автоматического восстановления (в секундах) для портов, заблокированных защитными механизмами (например, BPDU Guard).
no spanning-tree recovery interval	Отключение автоматического восстановления заблокированных портов.
spanning-tree vlans <vlan_list>	Указание списка VLAN, внутри которых разрешена работа протоколов PVST/Rapid-PVST.
no spanning-tree vlans <vlan_list>	Исключение указанных VLAN из обработки протоколами PVST/Rapid-PVST (полное отключение STP для данных VLAN).
spanning-tree vlan <vlan_list> priority <0-61440>	Настройка приоритета коммутатора для конкретных экземпляров VLAN (в режимах pvst и rapid-pvst). Значение должно быть кратно 4096
spanning-tree vlan <vlan_list> hello-time <1-10>	Настройка интервала генерации конфигурационных пакетов BPDU (в секундах) индивидуально для указанных VLAN.
spanning-tree vlan <vlan_list> forward-time <4-30>	Время нахождения портов в промежуточных состояниях Listening и Learning (в секундах) индивидуально для указанных VLAN.
spanning-tree vlan <vlan_list> max-age <6-40>	Максимальное время ожидания служебных пакетов BPDU (в секундах) индивидуально для указанных VLAN.
no spanning-tree vlan <vlan_list>	Сброс всех индивидуальных параметров и приоритета, выбранного VLAN на значения по умолчанию
Подрежим конфигурации агрегированных каналов.	
spanning-tree aggregation	Переход в подрежим групповой настройки параметров Spanning Tree для всех агрегированных каналов (LAG/Port-Channel).
spanning-tree auto-edge / no spanning-tree auto-edge	Управление автоматическим определением статуса граничного порта.

spanning-tree bpdu-guard / no spanning-tree bpdu-guard	Включение, выключение защиты BPDU Guard.
spanning-tree link-type {auto | point-to-point | shared}   <

spanning-tree restricted-role	
spanning-tree restricted-tcn	Глобальная блокировка распространения уведомлений об изменении топологии (TCN) для всех агрегированных интерфейсов во всех VLAN.
no spanning-tree restricted-tcn	Снятие глобальной блокировки TCN для агрегированных интерфейсов.
spanning-tree restricted-tcn vlan <vlan_id>	Выборочная блокировка уведомлений TCN на агрегированных каналах только внутри указанного VLAN.
no spanning-tree restricted-tcn vlan <vlan_id>	Снятие блокировки уведомлений TCN на агрегированных каналах для указанного VLAN.
spanning-tree vlan <vlan_id> cost {<1-200000000> | auto}	Настройка стоимости пути (Path Cost) для всех агрегированных каналов в рамках выбранного VLAN (применяется в режимах pvst / rapid-pvst). Ключевое слово auto возвращает дефолтный расчет стоимости.
no spanning-tree vlan <vlan_id> cost	Сброс стоимости пути, указанного VLAN для агрегированных интерфейсов.
spanning-tree vlan <vlan_id> port-priority <0-240>	Настройка приоритета агрегированных каналов для выбранного VLAN (в режимах pvst / rapid-pvst). Значение должно быть кратно 16. По умолчанию: 128
no spanning-tree vlan <vlan_id> port-priority	Сброс приоритета, указанного VLAN для агрегированных интерфейсов к дефолтному значению 128
Режим конфигурации физического интерфейса	
interface GigabitEthernet <port_type_list>	Переход в режим настройки указанных портов.
spanning-tree / no spanning-tree	Индивидуальное включение или принудительное деактивирование работы STP на выбранном физическом интерфейсе.
spanning-tree portfast / no spanning-tree portfast	Управление быстрым переходом порта в состояние Forwarding.
spanning-tree edge / no spanning-tree edge	Назначение конкретного порта граничным (Edge) или сброс данной роли.
spanning-tree bpdu-guard / no spanning-tree bpdu-guard	Включение или выключение защиты BPDU Guard индивидуально на выбранном порту.
panning-tree bpdu-filter / no spanning-tree bpdu-filter	Включение или выключение фильтрации пакетов BPDU индивидуально на выбранном порту.

spanning-tree restricted-role / no spanning-tree restricted-role	Включение или отключение Root Guard (запрет подключенному устройству становиться Root Bridge).
spanning-tree restricted-tcn no spanning-tree restricted-tcn	Глобальная блокировка распространения уведомлений об изменении топологии (TCN) с данного физического интерфейса во всех VLAN. Снятие глобальной блокировки уведомлений TCN с данного интерфейса.
spanning-tree restricted-tcn vlan <vlan_id> no spanning-tree restricted-tcn vlan <vlan_id>	– Выборочная блокировка уведомлений TCN на физическом интерфейсе только внутри указанного VLAN. Снятие блокировки уведомлений TCN на физическом интерфейсе для указанного VLAN.
spanning-tree link-type {auto | point-to-point | shared} no spanning-tree link-type	Настройка типа связи (L2-среды) для физического интерфейса: – point-to-point (Точка-точка) – Интерфейс напрямую соединен ровно с одним соседним коммутатором. Включает механизм Proposal/Agreement**,** позволяя порту переходить в состояние передачи (Forwarding) мгновенно (за доли секунды) без ожидания таймеров. – shared (Общая среда) – К порту через полудуплекс (Half-Duplex) или старый хаб подключено несколько L2-устройств. Мгновенная сходимость невозможна, порт переходит в Forwarding медленно через стадии Listening/Learning с задержкой по таймеру (до 30 сек), чтобы избежать петель. – auto (Автоопределение, по умолчанию) – Коммутатор сам выставляет тип связи на основе дуплекса порта. Если порт поднялся в Full-Duplex**,** включается point-to-point. Если в Half-Duplex, принудительно выставляется shared. Сброс настройки типа связи интерфейса на значение по умолчанию
spanning-tree auto-edge / no spanning-tree auto-edge	Включение или отключение функции автоматического определения граничного порта.
spanning-tree mst <0-64> cost {<1-200000000> | auto}	Настройка стоимости пути конкретного физического интерфейса для выбранного инстанса MSTP (для базовой топологии используется инстанс 0).

no spanning-tree mst <0-64> cost	Сброс стоимости пути указанного инстанса на физическом порту (возврат к auto).
spanning-tree mst <0-64> port-priority <0-240> no spanning-tree mst <0-64> port-priority	Настройка приоритета физического интерфейса для выбранного инстанса MSTP (значение должно быть кратно 16, по умолчанию 128) Сброс приоритета выбранного инстанса на физическом порту к дефолтному значению 128.
spanning-tree vlan <vlan_id> cost {<1-200000000> | auto} no spanning-tree vlan <vlan_id> cost	Настройка стоимости пути физического интерфейса для выбранного VLAN (в режимах pvst / rapid-pvst) Сброс стоимости пути указанного VLAN на физическом интерфейсе.
spanning-tree vlan <vlan_id> port-priority <0-240> no spanning-tree vlan <vlan_id> port-priority	Настройка приоритета физического интерфейса для выбранного VLAN (в режимах pvst / rapid-pvst) Сброс приоритета, выбранного VLAN на физическом интерфейсе к значению 128.
Привилегированный режим (exec)	
show spanning-tree	Отображение глобального статуса протокола, параметров корневого моста и таблиц состояний портов последовательно по всем активным инстансам MSTP.
show spanning-tree active	Вывод детальной таблицы состояний исключительно по активным (находящимся в работе up) интерфейсам коммутатора, отсекая выключенные порты.
show spanning-tree summary	Краткая сводка о глобальном состоянии STP, используемой версии протокола, текущих значениях глобальных таймеров и статусе защитных механизмов.
show spanning-tree interface <port_type_list>	Отображение краткого статуса STP и метрик для конкретно указанного интерфейса или группы портов.
show spanning-tree mst configuration	Вывод параметров MST-региона: текущего имени конфигурации (Configuration Name), номера ревизии (Configuration Revision), а также карты распределения VLAN по инстансам (MSTI).
show spanning-tree mst <0-64>	Вывод топологии, параметров собственного и корневого мостов, а также таблицы состояний портов строго для выбранного инстанса MSTP.
show spanning-tree mst <0-64> interface <port_type_list>	Просмотр состояния и метрик конкретного физического или логического порта строго в контексте выбранного инстанса MSTP.
show spanning-tree detailed	Вывод сводной таблицы счетчиков полученных и отправленных BP-пакетов по всем интерфейсам коммутатора.
show spanning-tree detailed interface	Вывод таблицы счетчиков пакетов для конкретного физического порта (GigabitEthernet /

<interface_type> <port_id>	10GigabitEthernet) или логического агрегированного канала (Port-channel).
show spanning-tree detailed vlan <vlan_list>	Просмотр детальных счетчиков пакетов для конкретных VLAN. Примечание: данная команда доступна только в по-VLAN-овых режимах работы (PVST/RPVST).
show spanning-tree vlan	Отображение топологии для выбранного VLAN (доступно только в режимах pvst и rapid-pvst).

Примеры настройки:

1. Балансировка трафика в режиме MSTP

Задача: Обеспечить отказоустойчивость и распределение сетевой нагрузки между коммутаторами **NTS1** и **NTS2**, соединенными по топологии «точка-точка» через интерфейсы GigabitEthernet 1/24. Сеть содержит VLAN 10, 20, 30, 40. Нагрузка распределяется следующим образом: коммутатор NTS1 назначается корневым мостом (Root Bridge) для VLAN 10 и 20 (MSTI 1), а коммутатор NTS2 – для VLAN 30 и 40 (MSTI 2).

Настройка коммутатора NTS1:

1. Создание идентификаторов VLAN в локальной базе данных
```
vlan 10,20,30,40
exit
```
2. Конфигурирование параметров региона MSTP одной строкой
```
spanning-tree mst name NTS_REGION revision 1
```
3. Ассоциация (маппинг) VLAN с соответствующими инстансами MSTP
```
spanning-tree mst 1 vlan 10,20
spanning-tree mst 2 vlan 30,40
```
4. Настройка приоритетов коммутатора для распределения ролей Root Bridge
```
spanning-tree mst 1 priority 4096
spanning-tree mst 2 priority 28672
```
5. Глобальная активация защитных механизмов на абонентском периметре
```
spanning-tree edge bpdu-guard
spanning-tree recovery interval 300
```
6. Конфигурирование магистрального интерфейса (Trunk) для связи с NTS2
```
interface GigabitEthernet 1/24
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
exit
```
7. Настройка абонентского порта доступа (интерфейс подключения ПК в VLAN 10)
```
interface GigabitEthernet 1/1
switchport mode access
switchport access vlan 10
```
– Перевод интерфейса в категорию граничных портов (Edge) для оптимизации времени сходимости
```
spanning-tree edge
```
– Подавление генерации уведомлений об изменении топологии (TCN) при нестабильности линка на абонентской стороне
```
spanning-tree restricted-tcn
exit
```

Настройка коммутатора NTS2:

1. Создание идентификаторов VLAN в локальной базе данных
```
vlan 10,20,30,40
exit
```
2. Конфигурирование параметров региона MSTP (значения должны быть идентичны NTS1)
```
spanning-tree mst name NTS_REGION revision 1
```
3. Ассоциация VLAN с инстансами MSTP
```
spanning-tree mst 1 vlan 10,20
spanning-tree mst 2 vlan 30,40
```
4. Настройка приоритетов коммутатора (зеркальное распределение ролей)
```
spanning-tree mst 1 priority 28672
spanning-tree mst 2 priority 4096
```
5. Глобальная активация защитных механизмов на абонентском периметре
```
spanning-tree edge bpdu-guard
spanning-tree recovery interval 300
```
6. Конфигурирование магистрального интерфейса (Trunk) для связи с NTS1
```
interface GigabitEthernet 1/24
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40
exit
```
7. Настройка абонентского порта доступа (интерфейс подключения ПК в VLAN 30)
```
interface GigabitEthernet 1/1
switchport mode access
switchport access vlan 30
spanning-tree edge
spanning-tree restricted-tcn
exit
```

Пример вывода в режиме MSTP:

```
NTS1# show  spanning-tree
MSTI0 Bridge STP Status
Bridge ID    : 32768.1C-A0-D3-42-71-FF
Root ID      : 32768.1C-A0-D3-42-71-FF
Root Port    : -
Root PathCost: 0
Regional Root: 32768.1C-A0-D3-42-71-FF
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 25
TC Last      : 0d 00:01:09
Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
---------  --------------  ----------  ---  --------  ----  -
--  -------------
Gi 1/1     DesignatedPort  Forwarding  128     20000  Yes   Yes
0d 00:01:16
Gi 1/24    DesignatedPort  Forwarding  128     20000  No    Yes
0d 00:02:35
MSTI1 Bridge STP Status
```

```
    Bridge ID    : 4097.1C-A0-D3-42-71-FF
    Root ID      : 4097.1C-A0-D3-42-71-FF
    Root Port    : -
    Root PathCost: 0
    TC Flag      : Steady
    TC Count     : 16
    TC Last      : 0d 00:01:09
    Port        Port Role        State        Pri  PathCost  Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/1     DesignatedPort  Forwarding  128     20000  Yes   Yes
0d 00:01:17
    Gi 1/24    DesignatedPort  Forwarding  128     20000  No    Yes
0d 00:01:39
    MSTI2 Bridge STP Status
    Bridge ID    : 28674.1C-A0-D3-42-71-FF
    Root ID      : 4098.1C-A0-D3-43-AB-49
    Root Port    : GigabitEthernet 1/24
    Root PathCost: 20000
    TC Flag      : Steady
    TC Count     : 16
    TC Last      : 0d 00:01:10
    Port        Port Role        State        Pri  PathCost  Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/1     DesignatedPort  Forwarding  128     20000  Yes   Yes
0d 00:01:17
    Gi 1/24    RootPort        Forwarding  128     20000  No    Yes
0d 00:01:39

    NTS2#  show  spanning-tree
    MSTI0 Bridge STP Status
    Bridge ID    : 32768.1C-A0-D3-43-AB-49
    Root ID      : 32768.1C-A0-D3-42-71-FF
    Root Port    : GigabitEthernet 1/24
    Root PathCost: 0
    Regional Root: 32768.1C-A0-D3-42-71-FF
    Int. PathCost: 20000
    Max Hops     : 20
    TC Flag      : Steady
    TC Count     : 4
    TC Last      : 0d 00:01:47
    Port        Port Role        State        Pri  PathCost  Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/1     DesignatedPort  Forwarding  128    200000  Yes   Yes
0d 00:01:50
    Gi 1/24      RootPort          Forwarding  128      20000  No
Yes  0d 00:01:50
    MSTI1 Bridge STP Status
```

```
    Bridge ID    : 28673.1C-A0-D3-43-AB-49
    Root ID      : 4097.1C-A0-D3-42-71-FF
    Root Port    : GigabitEthernet 1/24
    Root PathCost: 20000
    TC Flag      : Steady
    TC Count     : 9
    TC Last      : 0d 00:01:17
    Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/1     DesignatedPort  Forwarding  128    200000  Yes   Yes
0d 00:01:20
    Gi 1/24      RootPort          Forwarding  128      20000   No
Yes  0d 00:01:20
    MSTI2 Bridge STP Status
    Bridge ID    : 4098.1C-A0-D3-43-AB-49
    Root ID      : 4098.1C-A0-D3-43-AB-49
    Root Port    : -
    Root PathCost: 0
    TC Flag      : Steady
    TC Count     : 8
    TC Last      : 0d 00:01:17
    Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/1     DesignatedPort  Forwarding  128    200000  Yes   Yes
0d 00:01:20
    Gi 1/24      DesignatedPort   Forwarding  128      20000   No
Yes  0d 00:01:20
```

2. По-VLAN балансировка трафика в режиме Rapid-PVST

Задача: Перевести коммутаторы в режим по-VLAN-ового связующего дерева (без использования регионов). Коммутатор NTS1 должен функционировать в качестве Root Bridge для VLAN 100 (с ускоренными таймерами), а коммутатор NTS2 – в качестве Root Bridge для VLAN 200. Магистральное соединение организовано через интерфейс GigabitEthernet 1/20 на NTS1 и интерфейс GigabitEthernet 1/4 на NTS2.

Настройка коммутатора NTS1:

1. Создание локальных идентификаторов VLAN
   ```
   vlan 100,200
   exit
   ```
2. Изменение глобального режима функционирования Spanning Tree на Rapid-PVST
   ```
   spanning-tree mode rapid-pvst
   ```
3. Активация процессов связующего дерева для указанных VLAN
   ```
   spanning-tree vlans 100,200
   ```
4. Конфигурирование приоритета и временных параметров для VLAN 100 (Основной корень)
   ```
   spanning-tree vlan 100 priority 4096
   ```

```
spanning-tree vlan 100 hello-time 2
```

– Порядок строго выверен: сначала снижаем max-age, затем forward-time для прохождения проверки ядра

```
spanning-tree vlan 100 max-age 15
spanning-tree vlan 100 forward-time 10
```

5. Конфигурирование приоритета и временных параметров для VLAN 200 (Резервный мост)

```
spanning-tree vlan 200 priority 28672
spanning-tree vlan 200 hello-time 2
spanning-tree vlan 200 max-age 20
spanning-tree vlan 200 forward-time 15
```

6. Настройка параметров безопасности абонентского сегмента

```
spanning-tree edge bpdu-guard
spanning-tree recovery interval 300
```

7. Конфигурирование магистрального интерфейса связи с NTS2

```
interface GigabitEthernet 1/20
switchport mode trunk
switchport trunk allowed vlan 100,200
```

– Активация выборочной фильтрации TCN-уведомлений, поступающих из транка, в рамках VLAN 200

```
spanning-tree restricted-tcn vlan 200
```

– Оптимизация метрики стоимости пути для трафика VLAN 100

```
spanning-tree vlan 100 cost 500
exit
```

8. Настройка абонентского порта доступа (например, ПК в VLAN 100)

```
interface GigabitEthernet 1/1
switchport mode access
switchport access vlan 100
spanning-tree edge
spanning-tree restricted-tcn
exit
```

Настройка коммутатора NTS2:

1. Создание локальных идентификаторов VLAN

```
vlan 100,200
exit
```

2. Изменение глобального режима функционирования Spanning Tree на Rapid-PVST

```
spanning-tree mode rapid-pvst
```

3. Активация процессов связующего дерева для указанных VLAN

```
spanning-tree vlans 100,200
```

4. Конфигурирование приоритета и временных параметров для VLAN 100 (Резервный мост)

```
spanning-tree vlan 100 priority 28672
spanning-tree vlan 100 hello-time 2
spanning-tree vlan 100 max-age 15
spanning-tree vlan 100 forward-time 10
```

5. Конфигурирование приоритета и временных параметров для VLAN 200 (Основной корень)

```
spanning-tree vlan 200 priority 4096
spanning-tree vlan 200 hello-time 2
spanning-tree vlan 200 max-age 20
```

```
spanning-tree vlan 200 forward-time 15
```

6. Настройка параметров безопасности абонентского сегмента
```
spanning-tree edge bpdu-guard
spanning-tree recovery interval 300
```
7. Конфигурирование фактического магистрального интерфейса связи с NTS1
```
interface GigabitEthernet 1/4
switchport mode trunk
switchport trunk allowed vlan 100,200
```
– Активация выборочной фильтрации TCN-уведомлений в рамках VLAN 100
```
spanning-tree restricted-tcn vlan 100
```
– Оптимизация метрики стоимости пути для трафика VLAN 200
```
spanning-tree vlan 200 cost 500
exit
```
8. Настройка абонентского порта доступа (например, ПК в VLAN 200)
```
interface GigabitEthernet 1/1
switchport mode access
switchport access vlan 200
spanning-tree edge
spanning-tree restricted-tcn
exit
```

Пример вывода в режиме Rapid-PVST:

```
NTS1# show  spanning-tree
VLAN 1 bridge RPVST status
Bridge ID    : 32769.1C-A0-D3-42-71-FF
Root ID      : 32769.1C-A0-D3-42-71-FF
Root Port    : -
Root PathCost: 0
Regional Root: 32769.1C-A0-D3-42-71-FF
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 6
TC Last      : 0d 00:00:59
Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
---------  --------------  ----------  ---  --------  ----  -
--  -------------

VLAN 100 bridge RPVST status
Bridge ID    : 4196.1C-A0-D3-42-71-FF
Root ID      : 4196.1C-A0-D3-42-71-FF
Root Port    : -
Root PathCost: 0
Regional Root: 4196.1C-A0-D3-42-71-FF
Int. PathCost: 0
Max Hops     : 20
TC Flag      : Steady
TC Count     : 4
TC Last      : 0d 00:00:03
```

```
    Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/1     DesignatedPort  Forwarding  128     20000  Yes   Yes
0d 00:03:50
    Gi 1/20    DesignatedPort  Forwarding  128       500  No    Yes
0d 00:00:07

    VLAN 200 bridge RPVST status
    Bridge ID    : 28872.1C-A0-D3-42-71-FF
    Root ID      : 4296.1C-A0-D3-43-AB-49
    Root Port    : GigabitEthernet 1/20
    Root PathCost: 20000
    Regional Root: 28872.1C-A0-D3-42-71-FF
    Int. PathCost: 0
    Max Hops     : 20
    TC Flag      : Steady
    TC Count     : 6
    TC Last      : 0d 00:00:05
    Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/20    RootPort        Forwarding  128     20000  No    Yes
0d 00:00:07

    NTS2#  show  spanning-tree
    VLAN 1 bridge RPVST status
    Bridge ID    : 32769.1C-A0-D3-43-AB-49
    Root ID      : 32769.1C-A0-D3-42-71-FF
    Root Port    : GigabitEthernet 1/4
    Root PathCost: 20000
    Regional Root: 32769.1C-A0-D3-43-AB-49
    Int. PathCost: 0
    Max Hops     : 20
    TC Flag      : Steady
    TC Count     : 27
    TC Last      : 0d 00:01:41
    Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
    ---------  --------------  ----------  ---  --------  ----  -
--  -------------

    VLAN 100 bridge RPVST status
    Bridge ID    : 28772.1C-A0-D3-43-AB-49
    Root ID      : 4196.1C-A0-D3-42-71-FF
    Root Port    : GigabitEthernet 1/4
    Root PathCost: 20000
    Regional Root: 28772.1C-A0-D3-43-AB-49
    Int. PathCost: 0
    Max Hops     : 20
    TC Flag      : Steady
```

```
    TC Count     : 5
    TC Last      : 0d 00:00:49
    Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
    ---------  -------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/4     RootPort       Forwarding  128     20000  No    Yes
0d 00:00:52

    VLAN 200 bridge RPVST status
    Bridge ID    : 4296.1C-A0-D3-43-AB-49
    Root ID      : 4296.1C-A0-D3-43-AB-49
    Root Port    : -
    Root PathCost: 0
    Regional Root: 4296.1C-A0-D3-43-AB-49
    Int. PathCost: 0
    Max Hops     : 20
    TC Flag      : Steady
    TC Count     : 6
    TC Last      : 0d 00:00:50
    Port        Port Role        State        Pri   PathCost   Edge
P2P         Uptime
    ---------  -------------  ----------  ---  --------  ----  -
--  -------------
    Gi 1/1     DesignatedPort  Forwarding  128    200000  Yes   Yes
0d 00:01:38
    Gi 1/4     DesignatedPort  Forwarding  128       500  No    Yes
0d 00:00:52
```

4.2.55. POE

Power over Ethernet (PoE) – технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet. Данная технология предназначается для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Команда	Описание
Глобальные настройки	
`poe supply <0-460>`	Настройка максимальной мощности, которую может обеспечить источник питания.

`poe capacitor-detect`
 	
`no poe capacitor-detect`
	Включение функции `capacitor-detect`
	
	Выключение функции `capacitor-detect`

Настройка портов	
`interface GigabitEthernet <port_type_list>`	Выбор портов
`poe mode{plus | standard}`	Выбор режима poe для порта

no poe mode	Plus – включает PoE PoE IEEE 802.3at с поддержкой IEEE 802.3af Standard – включает режим соответствия PoE IEEE 802.3af отключает poe на порту
poe priority {critical | high | low}	Установка приоритета. Существует три уровня приоритета мощности: низкий, высокий и критический. Приоритет используется в том случае, когда удаленным устройствам требуется больше энергии, чем может обеспечить источник питания. В этом случае порт с самым низким приоритетом будет отключен, начиная с порта с самым высоким номером порта.
poe lldp no poe lldp	Включение обработки параметров PoE, полученных через LLDP. Отключение обработки протокол LLDP настраивается отдельно, а передачу информации PoE через LLDP можно настроить командой lldp med transmit-tlv poe.

Включение poe на коммутаторе задается настройкой максимальной мощности, которую может обеспечить источник питания:

```
# configure  terminal
(config)# poe supply 180
```

4.2.56. Selective QinQ и Double QinQ

Selective QinQ – функции, позволяющая тегировать пакеты разным внешним тэгом VLAN в зависимости от разного внутреннего тэга VLAN в соответствии с требованиями пользователя.

Double QinQ – это технология двойного тегирования трафика.

Команда настройки интерфейса	Описание
evc ingress selective-qinq inner-vlan <vlan_list> add outer-vlan <vlan_id>	Создание записи, где: inner-vlan <vlan_list> – значения клиентских vlan во фреймах приходящем на UNI порт (порт, к которому подключается пользовательское оборудование). outer-vlan <vlan_id> - новое значение vlan для фреймов, которое будет добавлено при отсылке через NNI порт (порт в

no evc ingress selective-qinq inner-vlan <vlan_list>	направлении ядра сети). Удаление соответствующей записи
evc ingress double-qinq untagged-vlan native add outer-vlan <vlan_id> no evc ingress double-qinq untagged-vlan native	Запись для добавления внешней метки VLAN (outer-vlan <vlan_id>) к обычному входящему пакету без меток, который приходит с клиентского устройства и добавление 2-й метки (native). Удаление соответствующей записи
evc egress vlan <vlan_id> action inner-vlan <vlan_id> no evc egress vlan <vlan_id>	Запись для исходящего трафика (egress), которая указывает коммутатору добавлять внутренний тег inner-vlan <vlan_id> для пакетов, уходящих в vlan <vlan_id>. Удаление соответствующей записи
evc egress vlan <vlan_id> action outer-vlan <vlan_id> no evc egress vlan <vlan_id>	Запись для исходящего трафика (egress), которая указывает коммутатору заменять тег vlan <vlan_id> на значение outer-vlan <vlan_id>. Удаление соответствующей записи
Команда просмотра информации	Описание
show evc interface GigabitEthernet <port_type_list> | 10GigabitEthernet <port_type_list>	Просмотр информации по созданным на интерфейсах коммутатора записей ingress/egress

4.2.57. Динамическая маршрутизация

4.2.57.1. OSPF

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры. Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы

Команда	Описание
Глобальные настройки	
router ospf | router ospf6	Режим конфигурации протокола OSPF
area <id> authentication | nssa | range | stub | virtual-link	Идентификатор области OSPF может быть указан адрес IPv4 формат (A.B.C.D) или десятичное значение от 0 до 4294967295 authentication Включить

	аутентификацию nssa Зона типа NSSA (Not so stubby area) - no-summary не принимать информацию о суммированных внешних маршрутах внутрь NSSA-зоны - translate type7 <always/candidate/never> функционирование режима транслятора (Из Type7 в Type5): в принудительном режим/в режиме выборов/не участвует - range <ipv4_addr><ipv4_netmask> суммировать маршруты, соответствующие диапазону адресов (только для границы зоны) - advertise cost <0-16777215> анонсировать созданный суммарный маршрут с выбранным показателем - not-advertise не анонсировать суммарный маршрут - stub Настройка зоны в режиме stub -no-summary не отправлять информацию о суммированных внешних маршрутах - virtual-link <ipv4_addr> настройка идентификатора виртуального канала до удаленного маршрутизатора - authentication Включить аутентификацию - message-digest Использовать аутентификацию с шифрованием MD5 - null Использовать пустое значение аутентификации - authentication-key <encrypted/unencrypted> настройка простой аутентификации по паролю - dead-interval <1-65535> интервал времени, по истечении которого сосед объявляется неработающим - hello-interval <1-65535> время между пакетами HELLO - retransmit-interval <3-65535> время между повторной передачей объявлений о состоянии потерянного канала

	- message-digest-key <1-255> md5 <encrypted/unencrypted> настройка аутентификации с шифрованием md5
default-metric <0-16777214>	Установить метрику маршрута
distance <1-255>	Административное расстояние (по умолчанию 110)
max-metric router-lsa administrative | on-shutdown <5-100> | on-startup <5-86400>	Анонс собственный Router-LSA с максимальной метрикой - administrative настраивает режим тупикового маршрутизатора OSPF, применяемый административно, на неопределенный период - on-shutdown <5-100> настраивает OSPF для объявления максимальной метрики во время завершения работы в течение настроенного периода времени. Устройство объявляет максимальную метрику, когда режим маршрутизатора OSPF отключен - on-startup <5-86400> настраивает OSPF для объявления максимальной метрики во время запуска в течение настроенного периода времени
network <ipv4_addr><ipv4_wildcard-mask> area <area_id>	Настройка маршрутизации в сети IPv4
passive-interface	Запрет обновления маршрутизации на интерфейсе
redistribute connected metric <0-16777214> metric-type <1-2> | rip metric <0-16777214> metric-type <1-2> | static metric <0-16777214> metric-type <1-2>	Анонсирование маршрутов connected metric <0-16777214> metric-type <1-2> разрешить анонсирование connected-маршрутов, metric – значение метрики для импортируемых маршрутов, metric-type – пометка OSPF external rip metric <0-16777214> metric-type <1-2> разрешить анонсирование rip-маршрутов, metric – значение метрики для импортируемых маршрутов, metric-type – пометка OSPF external - static metric <0-16777214> metric-type <1-2>разрешить анонсирование static-маршрутов, metric – значение метрики для импортируемых маршрутов, metric-type – пометка OSPF external
router-id <ipv4_addr>	Идентификатор маршрутизатора для

	процесса OSPF, адрес IPv4 формат (A.B.C.D)
Настройка интерфейса	
ip ospf authentication | authentication-key | cost | dead-interval | hello-interval | message-digest-key | priority | retransmit-interval	- authentication включить аутентификацию в OSPF и определить ее тип - message-digest аутентификация с использование шифрования MD5 - null не использовать аутентификацию - authentication-key <encrypted/unencrypted> назначить пароль для аутентификации соседей - cost <1-65535> установите метрику состояния канала OSPF для интерфейса. Он используется для расчета кратчайшего пути - dead-interval <1-65535/minimal> установите значение dead-интервала - hello-interval <1-65535> установите значение интервала приветствия для конкретного интерфейса - message-digest-key <1-255><encrypted/unencrypted> Настройка аутентификация с шифрованием MD5 - priority <0-255> Установите приоритет маршрутизатора OSPF для конкретного интерфейса - retransmit-interval <3-65535> Установите значение интервала повторной передачи для конкретного интерфейса. Это интервал времени перед повторной передачей пакета описания базы данных или запроса состояния канала, если он не был подтвержден
Команды просмотра информации о OSPF	
show ip ospf	Отобразить конфигурацию OSPF.
show ip ospf database	Отобразить состояние базы данных протокола OSPF.
show ip ospf neighbor	Отобразить информацию об OSPF-соседях.
show ip ospf interface	Отобразить конфигурацию всех OSPF-интерфейсов.
show ip ospf route	Отобразить все OSPF-маршруты

Пример настройки.

```
(config)#vlan 1-10
```

```
(config)#ip routing
(config)#interface vlan 1
(config-if-vlan)#ip address 192.168.2.120 255.255.255.0
(config-if-vlan)#ipv6 address 2::6/32
(config)#interface vlan 2
(config-if-vlan)#ip address 100.101.105.1 255.255.255.0
(config-if-vlan)#ipv6 address 3:1::6/32
(config)#interface vlan 3
ip address 100.101.106.1 255.255.255.0
ipv6 address 4:1::6/32
(config)#router ospf
(config-router)#router-id 192.168.2.120
(config-router)#redistribute connected
(config-router)#redistribute static
(config-router)#network 192.168.0.0 0.0.255.255 area 0.0.0.0
(config)#router ospf6
(config-router)#area 0.0.0.0 range 2::/32
(config-router)#redistribute connected
(config-router)#redistribute static
(config-router)#interface vlan 1 area 0.0.0.0
```

4.2.57.2. RIP

RIP (Routing Information Protocol) – это протокол динамической маршрутизации, использующий алгоритм Distance Vector (расстояние-вектор). Протокол распространяет информацию о сетях среди маршрутизаторов, позволяя автоматически строить таблицы маршрутизации.

Основные особенности RIP:

- Метрикой маршрута служит число переходов (hop count); максимальное значение метрики – 15 (сети с большим числом переходов игнорируются).
- Существует две версии RIP:
  - RIPv1: классовый (classful), широковещательные обновления.
  - RIPv2: поддерживает CIDR, multicast, аутентификацию.

Команда	Описание
Глобальные настройки	
`router rip` `no router rip`	Войти в режим конфигурации RIP Удаляет конфигурацию RIP
`default-information originate`	Сообщает другим устройствам о наличии маршрута по умолчанию. Примечание: По умолчанию включается отправка стандартных маршрутов (если они присутствуют).
`default-metric <1-16>`	Задаваемая вручную метрика для стандартных маршрутов. Формат: Число от 1 до 16 (чем больше число, тем хуже маршрут). Примечание: Стандартная метрика по умолчанию равна 1.

distance <1-255>	Административное расстояние (предпочтительность) для определенного типа маршрутов. Формат: Число от 1 до 255 (меньшие числа означают более предпочтительные маршруты).
redistribute connected metric <1-16>	Перераспределяет локальные подключённые маршруты в RIP. Формат: Значение метрики от 1 до 16. Примечание: использовать осторожно, чтобы избежать петель маршрутизации.
redistribute ospf metric <1-16>	Перераспределяет маршруты из протокола OSPF в RIP. Формат: Значение метрики от 1 до 16. Примечание: важно правильно настраивать фильтры, чтобы избежать конфликтов маршрутов.
redistribute static metric <1-16	Перераспределяет статически заданные маршруты в RIP. Формат: Значение метрики от 1 до 16.
neighbor <ipv4_addr>	Используется для принудительного объявления соседей в ранних версиях RIP. Формат: IPv4 адрес
network <ipv4_addr>	Объявляет сеть, доступную через данный интерфейс. Формат: IPv4 адрес сети.
offset-list <word1-31> in | out <0-16> vlan <vlan_id>	Применяется для задания смещений (метрик) к определенным маршрутам на основании списков доступа. Формат: Имя списка доступа + направление (in/out) + новая метрика + номер VLAN.
passive-interface default | vlan <vlan_list>	Предотвращает распространение RIP-объявлений через указанный интерфейс VLAN. Формат: Тип интерфейса (Vlan) + номера VLAN или ключевое слово default (для всех интерфейсов).
timers basic <5-2147483><5-2147483><5-2147483>	Меняет интервалы обновления, удаления старых записей и очистки мусорных маршрутов.

	Формат: Три временных параметра соответственно: Update Time, Timeout, Garbage Collection. - Примечание: По умолчанию обновление маршрутов идёт каждые 30 сек., очистка удалённых маршрутов начинается спустя 180 сек., полное удаление после дополнительного ожидания в 120 сек.
`version 1 | 2`	Выбирает версию RIP (версия 1 классовая, версия 2 поддерживает CIDR и группы мультикаста). Формат: Цифры 1 или 2.
Настройка интерфейса L3	
`ip rip authentication key-chain <word1-31>`	Указывает цепочку ключей для аутентификации сообщений RIP. Формат: <word1-31> – название цепочки.
`ip rip authentication mode md5 | text`	Определяет метод аутентификации: MD5-хеширование или простой текст. - md5: Использование криптографического хэша MD5 для защиты целостности сообщений. - text: Простой текст без шифрования (менее безопасный вариант).
`ip rip authentication string encrypted <word128>`	Устанавливает зашифрованную строку пароля для аутентификации. Формат: <word128> – пароль длиной до 128 символов.
`ip rip authentication string unencrypted <word1-15>`	Устанавливает незашифрованную строку пароля для аутентификации. Формат: <word1-15> – строка пароля длиной до 15 символов.
`ip rip receive version 1 | 2 | none`	Управляет приёмом версий RIP-пакетов. - 1: только пакеты RIPv1 принимаются. - 2: только пакеты RIPv2 принимаются. - `none`: Пакеты RIP вообще не принимаются.
`ip rip send version 1 | 2`	Управляет отправкой версий RIP-пакетов. - 1: отправляются только пакеты RIPv1. - 2: отправляются только пакеты RIPv2.

`ip rip split-horizon poisoned-reverse`	Включает механизм расщепления горизонта (split horizon) с обратным отравлением (poison reverse). Принцип работы: Маршруты, принятые с интерфейса, обратно на этот же интерфейс не отправляются. Особенности: это помогает предотвращать петли маршрутизации.

Базовый пример настройки RIP для 2 коммутаторов:

Шаг 1: Базовая настройка коммутаторов

1.1 Конфигурация устройства SW1

```
hostname SW1
vlan 1-4
interface GigabitEthernet 1/4
 switchport mode trunk
 switchport trunk allowed vlan 1-4
interface vlan 1
 ip address 192.168.1.10 255.255.255.0
interface vlan 2
 ip address 192.168.2.1 255.255.255.0
interface vlan 3
 ip address 192.168.3.1 255.255.255.0
interface vlan 4
 ip address 192.168.4.1 255.255.255.0
```

1.2 Конфигурация устройства SW2

```
hostname SW2
vlan 1,10-13
interface GigabitEthernet 1/4
 switchport mode trunk
 switchport trunk allowed vlan 1,10-13
interface vlan 1
 ip address 192.168.1.16 255.255.255.0
interface vlan 10
 ip address 192.168.10.1 255.255.255.0
interface vlan 11
 ip address 192.168.11.1 255.255.255.0
interface vlan 12
 ip address 192.168.12.1 255.255.255.0
interface vlan 13
ip address 192.168.13.1 255.255.255.0
```

Шаг 2: Настройка протокола RIP

2.1 На SW1:

```
router rip
 version 2
```

```
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
```

2.2 На SW2:

```
router rip
 version 2
 network 192.168.1.0
 network 192.168.10.0
network 192.168.11.0
 network 192.168.12.0
 network 192.168.13.0
```

Как проверить правильность настройки?

После завершения настроек введите на обоих коммутаторах команду:

show ip route - она отображает таблицу маршрутизации, где можно увидеть маршруты, полученные от второго устройства.

Команды для диагностики RIP:

Команда show ip rip выводит подробную информацию о состоянии и параметрах протокола RIP.

Команда show ip rip database предназначена для отображения базы данных маршрутов протокола RIP.

4.2.57.3. IS-IS

IS-IS (intermediate system to intermediate system) – протокол динамической маршрутизации, основанный на состоянии каналов (link-state). Он работает по алгоритму Дейкстры и строит единую базу данных топологии сети, чтобы выбирать оптимальные маршруты для передачи данных. IS-IS представляет собой протокол внутреннего шлюза (IGP). Протокол IS-IS распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

Команда настройки ISIS	Описание
`router isis <word>`	Войти в режим конфигурирования маршрутизатора ISIS.
`area-password [clear|md5] <word>`	Настройка пароля аутентификации области - `clear` – аутентификация открытым текстом; - `md5` – аутентификация MD5.
`domain-password [clear|md5] <word>`	Настройка пароля аутентификации домена - `clear` – аутентификация открытым текстом; - `md5` – аутентификация MD5.
`is-type [level-1| level-1-2| level-2-only]`	Настройка типа маршрутизатора в домене: - `level-1` – все взаимодействия происходят на 1 уровне; - `level-2-only` – все взаимодействия на 2 уровне; - `level-1-2` – устройство поддерживает взаимодействия

	обоих уровней.
log-adjacency-changes	Включение в журнал информации об изменениях в отношениях смежности между маршрутизаторами ISIS.
lsp-gen-interval [<1-120>|level-1|level-2] <1-120>	Настройка минимального нтервала в секундах между повторной генерацией одного и того же LSP - level – уровень, для которого указывается интервал. Если не указывать, интервал применится к обоим уровням.
lsp-refresh-interval [<1-65235>|level-1|level-2] <1-65235>	Настройка максимального интервала в секундах, между генерацией LSP. - level – уровень, для которого указывается интервал. Если не указывать, интервал применится к обоим уровням.
max-lsp-lifetime [<350-65535>|level-1|level-2] <350-65235>	Настройка времени жизни LSP. Значение должно быть хотя бы на 300 секунд больше, чем lsp-refresh-interval. level – уровень, для которого указывается время. Если не указывать, время применится к обоим уровням.
metric-style [narrow|transition|wide]	Настройка стиля метрики. - narrow – поддерживать только стандартную (узкую) метрику. -wide – поддерживать только расширенную метрику. - transition – поддерживать оба стиля метрики.
mpls-te [on|router-address]	Включение функционала MPLS-TE и настройка статического ip-адреса.
mpls-te [on|inter-as] [level-1|level-1-2|level-2-only]	Включение функционала MPLS-TE и настройка уровня для INTER-AS LSP.
net <word>	Назначение NET адрес – уникальный идентификатор маршрутизатора в пределах IS-IS домена. При записи NET используется шестнадцатеричная система счисления.
set-overload-bit	Установка бита перегрузки, который указывает другим маршрутизаторам не использовать данный маршрутизатор как транзитный для передачи данных.
spf-interval [<1-120>|level-1|level-2] <1-120>	Настройка минимального интервала между последовательными расчетами SPF в секундах. - level – уровень, для которого указывается интервал.

	Если не указывать, интервал применится к обоим уровням.
Команда настройки интерфейса vlan	Описание
ip router isis <word>	Включение маршрутизации IS-IS для интерфейса
isis circuit-type [level-1|level-1-2|level-2-only]	Настройка уровня соседства для интерфейса
isis csnp-interval <1-600> [level-1|level-2]	Настройка интервала отправки CSNP в секундах - level – уровень, для которого указывается интервал. Если не указывать, интервал применится к обоим уровням.
isis hello padding	Включение паддинг во всех сообщениях HELLO
isis hello-interval <1-600> [level-1|level-2]	Настройка интервала для HELLO в секундах - level – уровень, для которого указывается интервал. Если не указывать, интервал применится к обоим уровням.
isis hello-multiplier <2-100> [level-1|level-2]	Настройка множителя времени удержания (hold-timemultiplier) для пакетов HELLO
isis metric <0-16777215> [level-1|level-2]	Настройка метрики для данного интерфейса. - level – уровень IS-IS, для которого будет применяться метрика.
isis network point-to-point	Установить тип интерфейса point-to-point.
isis passive	Перевести интерфейс в пассивный режим. В этом режиме интерфейс не отправляет и не принимает HELLOPDU.
isis password [clear|md5] <word>	Настройка пароля аутентификации канала - clear – аутентификация открытым текстом; - md5 – аутентификация MD5.
isis priority <0-127> [level-1|level-2]	Настройка приоритета для выбора назначенного маршрутизатора - level – уровень, для которого указывается приоритет. Если не указывать, приоритет применится к обоим уровням.
isis psnp-interval <0-120> [level-1|level-2]	Настройка интервала отправки пакетов PSNP - level – уровень, для которого указывается интервал. Если не указывать, интервал применится к обоим уровням.
isis three-way-handshake	Включить трехстороннее рукопожатие
Команда просмотра информации о ISIS	Описание
show isis database	Отобразить базу данных топологии

[<word>|detail]	протокола IS-IS. - detail – отображение подробной информации о TLV; - <word> – отображение информации по выбранной LSPID
show isis hostname	Отобразить известные ISIS Hostname
show isis interface [<vlan-id>|detail]	- vlan-id – отобразить информацию об интерфейсе vlan, участвующем в IS-IS - detail – отобразить информацию о всех интерфейсах vlan, участвующих в IS-IS.
show isis mpls-te interface [<vlan_id>|router]	Отобразить параметры управления трафиком MPLS для всех или указанного интерфейса.
show isis neighbor [<word>|detail]	Отобразить информацию о всех или указанном соседях. - detail – отобразить детальную информацию о соседях.
show isis spf-delay-ietf	Отобразить информацию о задержке IS-ISSPF
show isis summary	Отобразить краткую информацию о состоянии IS-IS
show isis topology [level-1|level-2]	Отобразить топологию путей IS-IS к промежуточным системам глобально или для указанного уровня

Пример настройки.

```
# configure terminal
(config)# vlan 20-21
(config)# ip routing
(config)# interface GigabitEthernet 1/2
(config-if)#s witchport mode trunk
(config-if)# switchport trunk allowed vlan all
(config)# interface vlan 1
(config-if-vlan)# ip address 192.168.1.240 255.255.255.0
(config)# interface vlan 20
(config-if-vlan)# ip address 192.168.20.240 255.255.255.0
(config-if-vlan)# ip router isis 1
(config)# interface vlan 21
(config-if-vlan)# ip address 192.168.21.240 255.255.255.0
(config)# router isis 1
(config-router)# net 49.0001.0000.0000.0240.00
```

4.2.57.4. BGP

BGP (Border Gateway Protocol – протокол граничного шлюза) является протоколом маршрутизации между автономными системами (AS). Протокол BGP предназначен для обмена информацией о достижимости подсетей между AS, то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов

внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие AS.

Команда	Описание
Глобальные настройки	
`router bgp <1-4294967295>`	Включить маршрутизацию по протоколу BGP. Задать идентификатор AS и войти в режим его конфигурирования.
Настройки конфигурирования маршрутизатора BGP	
`aggregate-address [{<ipv4_subnet>|<ipv6_subnet>} ] [{as-set|summary-only}]`	Включить агрегацию специфичных маршрутов
`bgp always-compare-med`	Включить сравнение метрики (MED) при выборе маршрута.

`bgp bestpath compare-routerid`
 	
`as-path confed`
 	
`multipath-relax`
	Используется для указания маршрутизатору, что при выборе наилучшего маршрута, если два маршрута имеют одинаковые значения других атрибутов, то маршрут с меньшим Router ID должен быть предпочтительнее.
	
	- Используется для указания маршрутизатору игнорировать атрибут AS_PATH при выборе лучшего маршрута, если этот путь проходит через конфигурацию Confederations.
	
	- Настраивает протокол пограничного шлюза (BGP) для обработки двух маршрутов BGP как равноценных, даже если их AS-пути различаются, при условии, что длина их AS-путей и другие соответствующие атрибуты одинаковы.

`bgp cluster-id <ipv4_addr>`	Задать идентификатор кластера
`bgp dampening <1-45> Half-life time <1-20000> Reuse-limit <1-20000> Value to start suppressing a route <1-255> Maximum Suppress-time`	Настройка механизма защиты от нестабильности маршрутов
`bgp deterministic-med`	Изменяет процесс выбора лучшего пути. После включения команды, значение атрибута MED будет проверяться сразу после проверки AS-path.
`bgp ebgp-requires-policy`	Используется для требования применения политики маршрутизации при установлении сеанса eBGP
`bgp listen range [{<ipv4_subnet>|<ipv4_subnet>`	Конфигурация динамического соседства BGP (peerings) на основе заданного

peer-group <word>}]	диапазона IP-адресов.
bgp route-reflector allow-outbound-policy	Настройка отправки анонсов маршрутов, полученные от клиента, другим клиентам, даже если эти маршруты не были получены от самого Route Reflector напрямую.
bgp router-id [{<ipv4_addr>	Установить идентификатор маршрутизатора BGP
distance [{<1-255>|bgp	Установить значения административного расстояния
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] activate	Задать IPv4- или IPv6-адрес для BGP-соседа и включение поддержки address family.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] addpath-tx-all-paths	Включение отправки всех доступных путей (path)
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] addpath-tx-bestpath-per-AS	Включение отправки только лучшего маршрута, рассчитанного на уровне AS
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] advertisement-interval <0-600>	Настройка интервала, с которым соседний маршрутизатор будет отправлять сообщения об обновлениях маршрутизации
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] [{<1-10>|origin}]	Настройка принимать входящие маршруты с AS-путем, содержащим номер AS с тем же значением, что и у текущей системной AS. Параметр (1-10) указывает количество допустимых вхождений номера AS системы в AS-пути. Параметр origin указывает на прием только маршрутов, созданных с тем же номером AS, что и у системы.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] as-override	Настройка переопределения номера AS при анонсе маршрутов этому соседу.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] attribute-unchanged [{as-path|med|next-hop}]	Включает атрибуты, которые следует оставить без изменений для анонсов, отправляемых одноранговому узлу.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] bfd [{<2-255>|check-control-plane-failure|multihop|singlehop}]	Настройка протокола BFD на BGP-соседстве.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] capability dynamic	Включает динамическую согласованность возможностей BGP.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] extended-nexthop	Включает поддержка расширенных next-hop адресов.
neighbor [{<ipv4_addr>|<ipv6_addr>|<wor	Настройка фильтрация исходящих маршрутов.

d>}] capability orf [{both|receive|send}]	
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] default-originate	Анонсировать маршрута по умолчанию.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] description <line80>	Описание соседства.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] disable-connected-check	Отключение проверки физического подключения соседа.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] distribute-list <word> [{in|out}]	Настройка фильтрации анонсов маршрутов.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] dont-capability-negotiate	Отключение переговоров о возможностях (capabilities) BGP с соседом.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] ebgp-multihop	Включение установки сессии с соседом, используя протокол EBGP
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] enforce-first-as	Включает проверку соответствия что первый AS-номер в пути AS, полученном от соседа, соответствует ожидаемому AS-номеру этого соседа.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] enforce-multihop	Включает ожидание, что пакеты BGP, отправляемые этому соседу, могут пройти через несколько промежуточных маршрутизаторов, а не только напрямую.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] filter-list <word> [{in|out}]	Настройка применения фильтра маршрутов, который определен списком фильтров.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] local-as <1-4294967295> no-prepend replace-as	Настройка альтернативной AS для этого процесса BGP - Если указан атрибут no-prepend, то предоставленный local-as не добавляется к полученному AS_PATH. - Если указан атрибут replace-as, то при передаче обновлений локальных маршрутов этому одноранговому узлу к AS_PATH добавляется только предоставленный local-as.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] maximum-prefix <uint>	Настройка ограничения на количество префиксов, которые маршрутизатор примет от соседа.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] next-hop-self all	Включает изменение атрибута next-hop для маршрутов, полученных от указанного соседа на свой. - атрибут all указывает, что команда next-

	hop-self применяется ко всем маршрутам, полученным от указанного соседа.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] override-capability	Отключает проверку наличия определенной capability у соседа.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] passive	Отключает инициацию соединения с соседом.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] password	Установить пароль.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] peer-group <word>	Включение соседства в группе.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] prefix-list <word> [{in|out}]	Настройка применения списка префиксов.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] remote-as [{<1-4294967295>|external|internal}]	Настройка номера AS для соседа или определение к какой AS он принадлежит.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] remove-private-AS [all|replace-AS]	Удаление частных номеров автономных систем (ASN) в исходящих обновлениях
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] route-map <word> [export|import|in|out]	Указание маршрутной карты, представляющей политику импорта или экспорта однорангового узла, настроенного как RS-клиент
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] route-reflector-client	Установить этот узел как RR
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] route-server-client	Установить этот узел как RS
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] send-community	Включение отправки BGP Community
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] shutdown	Отключение соседа без удаления конфигурации для него
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] soft-reconfiguration inbound	Включает применение новых политик и маршрутной информации без переустановки сеанса
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] solo	Эта команда используется для указания того, что маршруты, объявленные одноранговым узлом, не должны отражаться обратно
neighbor	Настройка строгого сравнения удалённых и

[{<ipv4_addr>|<ipv6_addr>|<word>}] strict-capability-match	локальных возможностей. Если возможности различаются, отправляется ошибка «Неподдерживаемая возможность» и соединение сбрасывается.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] timers [<0-65535>|connect] <1-65535>	Установить таймеры connect, keepalive и hold для соседа.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] ttl-security hops <uint>	Определение количества переходов, при котором будет разрешено стать соседями. Эта команда является взаимоисключающей с ebgp-multihop.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] unsuppress-map <word>	Политика фильтрации, которая отменяет ранее установленное ограничение на анонс определенных маршрутов.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] update-source [{<ipv4_addr>|<ipv6_addr>|<word>}]	Указание исходного адреса для сеанса BGP с этим соседом.
neighbor [{<ipv4_addr>|<ipv6_addr>|<word>}] weight <0-65535>	Установить атрибут weight для этого соседа
network [<ipv4_addr>|<ipv4_subnet>|<ipv6_subnet>] [backdoor|label-index|mask|route-map]	Указание сетей для анонса и настройка атрибутов и политик для них
redistribute [connected|kernel|ospf|rip|static|vpn]	Включает импорт и экспорт маршрутов, соответствующих выбранному параметру
table-map <word>	Настройка карты маршрутов
update-delay <uint><uint>	Включает режим «только чтение» на указанное время при перезапуске процесса BGP
Настройка одноадресной и многоадресной маршрутизации в MBGP	
address-family [ipv4|ipv6] multicast	Вход в надстройку MBGP для настройки многоадресной маршрутизации.
address-family [ipv4|ipv6] unicast	Вход в надстройку MBGP для настройки одноадресной маршрутизации.
Команды просмотра информации о BGP	
show bgp [<ipv4_addr>|<ipv6_addr>|<ipv4_subnet>|<ipv6_subnet>] [bestpath|multipath|longer-prefixes]	Вывод информации об оптимальных маршрутах и объявлениях более специфичных префиксов для выбранной подсети
show bgp attribute-info	Используется для просмотра подробной информации об атрибутах пути BGP
show bgp cidr-only	Используется для просмотра маршрутной таблицы BGP и отображения только CIDR-блоков (сетей) в таблице

show bgp community	Показывает информацию об атрибутах BGPCommunity, примененных к маршрутам.
show bgp community-info	Используется для просмотра информации о BGP-сообществах (BGP communities)
show bgp community-list	Показывает список настроенных на маршрутизаторе BGP-сообществ и правил фильтрации, которые используются для управления маршрутами и трафиком в BGP-сетях
show bgp dampening [dampened-paths|flap-statistics|parameters]	Просмотр маршрутов, которые были временно подавлены (заблокированы), статистике по нестабильности маршрутов и настроенные параметры механизма BGP Route Dampening
show bgp detail	Отображение подробной информации о состоянии протокола BGP
show bgp filter-list <word>	Показывает информацию по фильтру
show bgp import-check-table detail	Показывает подробную информацию о конфликтах при импорте маршрутов в BGP-таблицу из локальных данных (например, из OSPF или статических маршрутов).
show bgp l2vpn evpn [all|neighbors|rd|statistics|update-groups]	Используется для отображения информации о BGP в контексте Ethernet VPN (EVPN).
show bgp large-community [<0-65535>|exact-match]	Выводит список всех BGP large-community атрибутов, которые были настроены, с указанием их типа и идентификатора сети.
show bgp large-community-info	Отображает информацию о том, как обрабатываются и передаются BGP large communities между пирами.
show bgp large-community-list [<1-500>|<word>] exact-match	Используется для отображения, указанного BGP large community, который было настроено и применяется в сети
show bgp memory	Используется для просмотра подробной информации об использовании динамической памяти протоколом BGP
show bgp multicast paths	Используется для отображения информации о мультикастовых маршрутах, которые были переданы через Multicast BGP (MBGP)
show bgp neighbors [<ipv4_addr>|<ipv6_addr>|<word>] [advertised-routes|dampened-routes|filtered-routes|flap-statistics|prefix-counts|received|received-routes|routes]	Используется для отображения маршрутов, которые были анонсированы, подавленных маршрутов из-за их нестабильности, отфильтрованных маршрутов согласно заданным правилам, статистики нестабильного соединения, количество анонсируемых префиксов и принятых маршрутов
show bgp nexthop detail	Используется для отображения информации о следующем узле для BGP-

	маршрутов
`show bgp paths`	Используется для просмотра информации о маршрутах BGP
`show bgp peer-group <word>`	Используется для отображения информации о группе BGP-соседей
`show bgp prefix-list <word>`	Отображение содержимого списка префиксов, который используется для фильтрации и управления маршрутной информацией
`show bgp regexp <word>`	Используется для отображения информации о BGP-соседях и маршрутах, которые соответствуют регулярному выражению
`show bgp route-leak`	Используется для отображения информации о перенаправлении трафика через сторонние AS
`show bgp route-map <word>`	Используется для отображения конфигурации и правил маршрутного списка
`show bgp statistics [-all]`	Отображает статистические данные о работе протокола BGP
`show bgp summary`	Отображение краткой информации о состоянии сессий BGP с соседними маршрутизаторами, включая IP-адреса, состояния пиров и счетчик сообщений
`show bgp summary failed`	Отображает сводку по ошибкам или неудачным попыткам установить соединение с BGP-соседом
`show bgp`	Используется для отображения таблицы BGP, показывающей все известные BGP маршруты без каких-либо меток или дополнительных данных, используемых в других технологиях, таких как MPLS
`show bgp [<word>|advertise-queue|advertised-routes|packet-queue|statistics]`	Отображает очередь обновлений о префиксах для отправки/получения и просмотра статистики по группам обновлений BGP
`show bgp view [<word>|all|default]`	Используется для просмотра всей информации о протоколе BGP, включая таблицы маршрутизации, информацию о соседях и таблицы с маршрутами по умолчанию, которая содержит маршруты, используемые, когда для пакета не найден более конкретный маршрут в таблице маршрутизации
`show bgp vpn paths`	Используется для отображения информации о маршрутах, полученных по протоколу BGP для VPN
`show bgp vrfs`	Показывает информацию о таблицах маршрутизации BGP для каждой VRF

Пример настройки.

```
# configure terminal
(config)# vlan 2-3,100
(config)# ip routing
(config)# interface GigabitEthernet 1/24
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 100
(config)# interface vlan 2
(config-if-vlan)# ip address 192.168.102.1 255.255.255.0
(config)# interface vlan 3
(config-if-vlan)# ip address 192.168.103.1 255.255.255.0
(config)# interface vlan 100
(config-if-vlan)# ip address 192.168.101.1 255.255.255.252
(config)# router bgp 100
(config-router)# bgp router-id 192.168.101.1
(config-router)# neighbor 192.168.101.2 remote-as 200
(config-router)# network 192.168.102.0/24
(config-router)# network 192.168.103.0/24
```

4.2.57.5. BFD

Протокол BFD (Bidirectional Forwarding Detection) позволяет быстро обнаружить неисправности линков. BFD может работать как со статическими маршрутами, так и с протоколами динамической маршрутизации RIP, OSPF, BGP.

Команда	Описание
Команда в глобальном режиме	
`bfd`	Включение BFD
`peer <A.B.C.D|X:X::X:X> [{multihop|local-address <A.B.C.D|X:X::X:X>|interface IFNAME|vrf NAME}]`	Создает и настраивает нового партнера BFD для прослушивания и обмена данными. - `multihop` сообщает, что следует ожидать пакеты с TTL менее 254 (поскольку потребуется более одного перехода), и прослушивать порт многоадресного режима (4784). При использовании многоадресного режима режим эха не будет работать. - `local-address` предоставляет локальный адрес, к которому мы должны привязать наш прослушиватель, и адрес, который мы должны использовать для отправки пакетов. Этот параметр обязателен для IPv6. - `interface` выбирает, какой интерфейс нам следует использовать. - `vrf` выбирает, какой домен мы хотим

	использовать.
Команда в режиме конфигурирования BFD партнера	Описание
`detect-multiplier <2-255>`	Настраивает множитель обнаружения потери пакетов. Пример: если локальная система имеет множитель обнаружения 3, а удаленная система имеет интервал передачи 300, локальная система обнаружит сбои только через 900 миллисекунд без получения пакетов.
`echo-interval <10-60000>`	Задаёт минимальный интервал для передачи системой эхо-пакетов BFD в миллисекундах (с учётом джиттера). Значение по умолчанию – 50 мс.
`echo-mode`	Включает режим передачи эха.
`receive-interval <10-60000>`	Задаёт минимальный интервал для получения системой управляющих пакетов в миллисекундах. Значение по умолчанию – 300 мс.
`transmit-interval <10-60000>`	Задаёт минимальный интервал для передачи системой управляющих пакетов в миллисекундах (с учётом джиттера). Значение по умолчанию – 300 мс.
`shutdown`	Отключает одноранговый узел.
Команды просмотра информации о стеке	
`show bfd [vrf NAME] peer [<WORD>|<A.B.C.D|X:X::X:X> [{counters|multihop|local-address <A.B.C.D|X:X::X:X>|interface IFNAME}]`	Показать статус определенного узла BFD.
`show bfd peers`	Показать статус всех узлов BFD.
`show bfd [vrf NAME] peers brief|counters`	Отобразить краткую информацию обо всех настроенных узлах BFD и их текущем статусе.

Пример настройки.

```
# configure terminal
(config)# vlan 11
(config-vlan)# exit
(config)# interface vlan 11
(config-if-vlan)#  ip address 192.168.1.1 255.255.255.0
(config-if-vlan)# exit
(config)# bfd
(config)# peer 192.168.1.1 local-address 192.168.1.2 interface
(config)# peer 192.168.1.1 local-address 192.168.1.2 interface
11
(config-bfd-peer)# no shutdown
```

4.2.57.6. PIM

PIM (Protocol Independent Multicast) – это протокол многоадресной передачи, обеспечивающий эффективную доставку мультимедийных потоков группе клиентов одновременно. Протокол позволяет устройствам обмениваться информацией о группах и источниках передач и строить эффективные пути доставки данных.

1. Основные настройки

```
conf t
vlan 2-3
exit
```

- Здесь создаются два VLAN'а с номерами 2 и 3. Эти VLAN'ы будут использоваться для разделения сегментов сети и организации многоадресной передачи.

2. Активация IP-маршрутизации

ip routing

Команда активирует возможность построения таблицы маршрутизации на устройстве. Без нее невозможна передача трафика между различными сегментами сети.

3. Интерфейсы Loopback

```
interface loopback 1
ip address 2.2.2.2 255.255.255.255
ip pim
ip igmp
exit
```

Создается виртуальный интерфейс loopback с адресом 2.2.2.2. Этот интерфейс необходим для стабильности и идентификации устройства в маршрутизации. Параметры ip pim и ip igmp разрешают использование PIM и IGMP на данном интерфейсе.

4. Статическое назначение RP (Rendezvous Point)

```
ip pim rp 2.2.2.2 224.0.0.0/4
```

Назначается узел с адресом 2.2.2.2 в качестве RP для всех групп IPv4 мультикастинга. Группы охватывают диапазон от 224.0.0.0 до 239.255.255.255.

5. Физические интерфейсы Ethernet

```
interface GigabitEthernet 1/1
switchport access vlan 3
exit
interface GigabitEthernet 1/2
switchport access vlan 2
exit
```

Оба физических интерфейса работают в режиме свитч-порта, привязаны к разным VLAN'ам (VLAN 2 и VLAN 3 соответственно).

6. Настройка L3 интерфейсов (vlan)

```
interface vlan 2
ip address 10.0.12.1 255.255.255.0
ip igmp snooping
ip pim
ip igmp
exit
interface vlan 3
ip address 10.0.13.1 255.255.255.0
ip igmp snooping
ip pim
ip igmp
exit
```

Создаются логические интерфейсы для каждого VLAN с присвоением IP-адресов и разрешением работы PIM и IGMP. Команда ip igmp snooping обеспечивает фильтрацию и предотвращение широковещательных штормов.

Настройка OSPF

```
router ospf
router-id 2.2.2.2
redistribute connected
network 2.2.2.2 0.0.0.0 area 0.0.0.0
network 10.0.12.0 0.0.0.255 area 0.0.0.0
network 10.0.13.0 0.0.0.255 area 0.0.0.0
exit
```

OSPF запускается с уникальным идентификатором роутера, соответствующим loopback-интерфейсу. Подключаемые сети анонсируются в область 0.0.0.0, позволяя другим устройствам находить маршруты к ним.

Данная конфигурация создает базовую инфраструктуру для взаимодействия устройств в среде с поддержкой PIM и IGMP. Она полезна в ситуациях, когда требуется передавать видеостримы, аудиопередачи или другие мультимедиа-данные через сетевую среду с возможностью масштабируемого распределения.

Если потребуется дополнительное управление или мониторинг работы PIM и IGMP, полезно применять такие команды диагностики, как:

Команда	Описание
`show ip route`	Команда используется для просмотра активных маршрутов многоадресной рассылки (multicast). Показывает информацию о потоках multicast-трафика, источник группы, состояние маршрута и интерфейсы, принимающие трафик.
`show ip mroute`	Отображает список соседей протокола PIM (Protocol Independent Multicast). Эта команда полезна для проверки соединения между устройствами, участвующими в процессе распространения группового трафика.

`show ip pim neighbor`	Показывает активное членство устройств в группах PIM. Информация включает интерфейс, группу, удалённого соседа и таймеры присоединения.
`show ip pim join`	Эта команда выводит информацию о группах IGMP (Internet Group Management Protocol), включённых устройствах и их интерфейсах. Используется для проверки принадлежности узлов сети к определенным multicast-группам.
`show ip igmp groups`	Информация о источниках multicast-трафика, зарегистрированных протоколом IGMP. Отображаются адреса источников и группы, к которым они принадлежат.
`show ip igmp sources`	Эта команда показывает информацию о назначенных маршрутах репликаторов (RP – rendezvous point). Роли и статус устройства RP критичны для правильной работы PIM Sparse Mode (режима разрежённой многоточечной рассылки).
`show ip pim rp-info`	спользуется для отображения информации о назначенных маршрутах протоколов многоадресной передачи PIM (Protocol Independent Multicast)

Это позволит быстро выявить проблемы и диагностировать возможные неисправности.

4.2.57.7. PBR

Политика-Based Routing (PBR) – это технология маршрутизации, позволяющая назначать маршруты и обрабатывать трафик на основании заранее заданных правил политики, игнорируя стандартные таблицы маршрутизации. Она широко применяется для приоритезации определённых потоков данных, разделения нагрузки между провайдерами или направления специфического трафика по отдельным маршрутам.

Процесс настройки включает три основных этапа:

Этап 1. Определение группы next-hop (следующих шагов)

Группа next-hop – это набор IP-адресов промежуточных узлов, на которые отправляются пакеты согласно политике маршрутизации. Для примера рассмотрим два сценария: один для главного шлюза, второй – для резервного шлюза.

Конфигурационные команды:

```
configure terminal
pbr nexthop-group main-gateway
nexthop 10.0.0.1
exit
pbr nexthop-group backup-gateway
nexthop 10.0.0.2
```

```
exit
```

Эти команды создают две группы следующим узлам: первую группу ("main-gateway") с одним основным IP-адресом (10.0.0.1) и вторую группу ("backup-gateway") с резервным IP-адресом (10.0.0.2).

Этап 2. Настройка PBR-карты (правила политики маршрутизации)

Следующий этап – создание самих правил маршрутизации (карты PBR), которые определяют условия сопоставления трафика и дальнейшие действия (назначение маршрута).

Рассмотрим пример двух простых правил:

1. Правило №1: Пакеты с источников внутреннего сегмента сети будут направлены на главный шлюз.

```
pbr-map traffic-routing seq 100
match src-ip 192.168.1.0/24
set nexthop-group main-gateway
exit
```

2. Правило №2: Весь прочий трафик, идущий на удалённую сеть, перенаправляется на резервный шлюз.

```
pbr-map traffic-routing seq 200
match dst-ip  10.10.10.0/24
set nexthop-group backup-gateway
exit
```

Первая карта (traffic-routing) определяет, что весь трафик с внутренних сетей (192.168.1.0/24) отправляется на основной шлюз. Вторая карта отправляет весь остальной трафик, направленный на подсеть (10.10.10.0/24), на резервный шлюз.

параметр seq – это порядок исполнения правил. Меньшее значение seq означает, что соответствующее правило проверяется и исполняется раньше остальных.

Этап 3. Применение PBR на интерфейсах

Чтобы применить созданные правила маршрутизации на конкретном интерфейсе, выполните следующую команду:

```
interface VLAN 2
pbr-policy traffic-routing
exit
```

Этот код назначает политику маршрутизации traffic-routing для всего трафика, проходящего через интерфейс VLAN 2.

Команды просмотра конфигурации и статуса PBR

`show pbr map` - Показывает список всех созданных карт PBR с указанием последовательности (sequence number), критериев выбора (match criteria) и действий (actions).

`show pbr map detail` - Предоставляет подробную информацию обо всех картах PBR, включая критерии сопоставления, выбранные маршруты и количество совпадающих пакетов.

`show pbr map traffic-routing` - Отображает конкретные карты PBR с именем traffic-routing. Полезно, если вам нужно увидеть именно определенную карту маршрутизации.

`show pbr interface 2` - Показывает состояние и применённые политики PBR на указанном интерфейсе (например, VLAN 2). Здесь можно увидеть активные правила PBR и статистику по ним

`show pbr nexthop-groups` - Список всех существующих групп следующего шага (next-hop groups), включающих имена групп и соответствующие IP-адреса следующих точек назначения.

`show pbr nexthop-groups main-gateway` - Подробная информация о конкретной группе следующего шага, указанной в команде (например, main-gateway). Включает список членов группы и статистические данные о трафике.

4.2.58. VRF

VRF (Virtual Routing and Forwarding) – это технология, позволяющая создать на одном физическом устройстве несколько независимых виртуальных маршрутизаторов, каждый из которых обладает собственной таблицей маршрутизации. Это обеспечивает изоляцию трафика разных клиентов или подразделений, позволяя использовать одинаковые IP-адреса и различающиеся схемы маршрутизации, а также предотвращает смешивание трафика между VRF-группами.

Команда	Описание
Глобальные настройки	
`vrf <word> | default`	Создаёт новую виртуальную доменную таблицу маршрутизации (VRF) с именем `<word>`. `default` – указывает на использование основной области таблицы маршрутизации, не принадлежащей к какому-либо VRF.
`no vrf <word> | default`	Удаляет созданную ранее виртуальную доменную таблицу маршрутизации (VRF) с именем `<word> | default`
`ip route <ipv4_addr>/ <ipv4_subnet> | <ipv4_netmask> | <ipv4_ucast> vrf <word>`	команда предназначена для добавления статического маршрута в таблице маршрутизации устройства с поддержкой виртуального маршрутизатора (VRF). - `<ipv4_addr>/<ipv4_subnet>` или `<ipv4_netmask>` – обозначают целевой IPv4 адрес сети и её маску. - `<ipv4_ucast>` – это адрес следующего транзитного узла (хоста или шлюз), куда будут отправляться пакеты,

	предназначенные для указанной сети. - vrf <word> – указывает, что маршрут создается в рамках конкретного виртуального маршрутизатора (VRF), обозначенного именем <word>.
no ip route <ipv4_addr>/<ipv4_subnet> | <ipv4_netmask> | <ipv4_ucast> vrf <word>	Удаляет статический маршрут, созданный ранее с использованием конкретного VRF
Настройка интерфейса L3	
ip vrf forwarding <word64>	Команда используется на интерфейсах уровня 3 (L3-интерфейсах) устройств для связывания интерфейса с определенным виртуальным маршрутом (VRF). Применение этой команды позволяет разделить логически разные таблицы маршрутизации на одном устройстве, создавая отдельные пространства имен и гарантируя изоляцию трафика разных клиентов или сервисов друг от друга. <имя_VRF> – уникальное название виртуальной маршрутизационной области (обычно слово длиной до 64 символов).
no vrf forwarding	Удаляет конфигурацию VRF (Virtual Routing and Forwarding) с определенного интерфейса L3.

Пример:

Допустим, у нас есть две автономные сети (два клиента), каждая из которых нуждается в своей собственной маршрутизации и полном отделении друг от друга. Эту проблему идеально решает VRF.

Порядок настройки VRF

1. Основные настройки (для обоих коммутаторов)

Выполняем базовые настройки устройства:

```
hostname PE1
!
vlan 2-4
```

Аналогичным образом для PE2:

```
hostname PE2
!
vlan 2-4
```

Где:

VLAN 2 и VLAN 3 – сети клиентов (раздельные),
VLAN 4 – служебный VLAN для связи между PE1 и PE2.

2. Настройка IP-адресов и статических маршрутов

Пример для PE1:

```
interface loopback 1
ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet 1/47
switchport access vlan 2
description Interface to Client_A
!
interface GigabitEthernet 1/48
switchport access vlan 4
description Interface to PE2
!
vrf VRF_A
!
vrf VRF_B
!
interface vlan 2
ip vrf forwarding VRF_A
ip address 192.168.1.2 255.255.255.0
!
interface vlan 3
ip vrf forwarding VRF_B
ip address 192.168.2.1 255.255.255.0
!
interface vlan 4
ip address 10.0.0.1 255.255.255.0
!
ip route 192.168.1.0 255.255.255.0 192.168.1.3 vrf VRF_A
ip route 192.168.2.0 255.255.255.0 192.168.2.2 vrf VRF_B
```

Пример для PE2:

```
interface loopback 1
ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet 1/23
switchport access vlan 3
description Interface to Client_B
!
interface GigabitEthernet 1/24
switchport access vlan 4
description Interface to PE1
!
vrf VRF_A
```

```
!
vrf VRF_B
!
interface vlan 2
ip vrf forwarding VRF_A
ip address 192.168.1.3 255.255.255.0
!
interface vlan 3
ip vrf forwarding VRF_B
ip address 192.168.2.2 255.255.255.0
!
interface vlan 4
ip address 10.0.0.2 255.255.255.0
!
ip route 192.168.1.0 255.255.255.0 192.168.1.2 vrf VRF_A
ip route 192.168.2.0 255.255.255.0 192.168.2.1 vrf VRF_B
```

3. Настройка протокола OSPF (опционально)

Если хотите обмениваться маршрутами между устройствами, используйте протокол OSPF:

Пример для PE1:

```
router ospf
router-id 1.1.1.1
redistribute connected
network 10.0.0.0 0.0.0.255 area 0.0.0.0
network 192.168.1.0 0.0.0.255 area 0.0.0.0
network 192.168.2.0 0.0.0.255 area 0.0.0.0
```

Пример для PE2:

```
router ospf
router-id 2.2.2.2
redistribute connected
network 10.0.0.0 0.0.0.255 area 0.0.0.0
network 192.168.1.0 0.0.0.255 area 0.0.0.0
network 192.168.2.0 0.0.0.255 area 0.0.0.0
```

Диагностика и контроль

Чтобы убедиться, что наша конфигурация работает корректно, воспользуйтесь этими командами:

Посмотрите активные маршруты:

```
show ip route vrf all
show ip route vrf VRF_A
show ip route vrf VRF_B
```

Посмотреть таблицу arp:

```
show ip arp
```

4.2.59. Настройка протокола VRRP

VRRP (Virtual Router Redundancy Protocol) – это сетевой протокол, который объединяет несколько физических устройств в одну логическую группу для создания резервного шлюза по умолчанию. Это позволяет избежать сбоев в сети: если основной роутер (Master) становится недоступным, резервный (Backup) берет его функции на себя, обеспечивая бесперебойную работу.

Команда настройки VRRP	
Команда настройки интерфейса vlan	Описание
`vrrp <1-255>`	Выбор VRID (идентификатор виртуального маршрутизатора)
`vrrp <1-255> advertisement-interval <10-40950>`	Настройка интервала (в миллисекундах) между отправками анонсов, которые маршрутизатор-мастер рассылает другим устройствам в группе для подтверждения своей работоспособности
`vrrp <1-255> ip <ipv4_addr>`	Настройка виртуального IP-адреса Примечание: IP не должен совпадать с настроенными IP-адресами на interface vlan в группе
`vrrp <1-255> preempt`	Включение функции, которая разрешает резервному устройству (Backup) перехватить статус главного (Master), если он стал недоступен.
`vrrp <1-255> priority <1-254>`	Настройка приоритета - определяет роль устройства (от 1 до 254). Маршрутизатор с наибольшим приоритетом становится Master-ом (основным активным шлюзом)
`vrrp <1-255> shutdown`	Выключение VRID без удаления настроек
`vrrp <1-255> version <2-3>`	Выбор версии протокола VRRP
Команда просмотра информации	Описание
`show vrrp`	Просмотр информации о всех настроенных экземплярах VRRP на коммутаторе
`show vrrp <1-255> interface vlan <vlan_list>`	Просмотр информации о всех настроенных экземплярах VRRP на одном интерфейсе
`show vrrp <1-255> summary`	Просмотр сводной информации о всех настроенных экземплярах VRRP

Пример настройки:

```
# configure terminal
(config)# interface vlan 10
(config-if-vlan)# ip address 192.168.10.1 255.255.255.0
(config-if-vlan)# vrrp 10 ip 192.168.10.10
(config-if-vlan)# vrrp 1 advertisement-interval 10000
(config-if-vlan)# no vrrp 10 preempt
(config-if-vlan)# exit
```

```
(config)# interface vlan 20
(config-if-vlan)# ip address 192.168.20.1 255.255.255.0
(config-if-vlan)# vrrp 20 ip 192.168.20.10
(config-if-vlan)# vrrp 20 priority 254
```

4.2.60. Стекирование

Стек работает как единое устройство и может объединять до 8 коммутаторов (опционально до 12) одной и той же модели. Стекирование достигается через специальный стековый протокол, который обеспечивает взаимодействие между коммутаторами, формируя цепочку или кольцо.

Команда	Описание
`switch stack enable`	Включить стекирование на коммутаторе;
`switch stack disable`	Выключить стекирование на коммутаторе;
`switch stack interface GigabitEthernet|10GigabitEthernet <port_type_list>`	Выбор портов для стека, можно указать два интерфейса для стекирования (либо GigabitEthernet, либо 10GigabitEthernet);
`switch stack priority <1-12>|local <1-4>`	Выбор приоритета для стекируемого коммутатора: - <1-12> - ID коммутатора в стеке; - local – коммутатор, который является мастером в данный момент; - <1-4> - значение приоритета для выбранного коммутатора;
`switch stack swap <1-12>|local`	Изменение номера юнита в стеке: - <1-12> - ID коммутатора в стеке; - local – коммутатор, который является мастером в данный момент;
`switch stack set <1-12> mac <mac_addr>`	Настройка номера юнита для подключаемого коммутатора в стеке по MAC адресу;
`no switch stack <1-12>`	Исключении информации о коммутаторе, выбывшем из стека.
Команды просмотра информации о стеке	
`show switch stack`	Краткая информация по коммутаторам в стеке
`show switch stack details`	Расширенная информация по коммутаторам в стеке

Примечание 1. При стекировании коммутаторов через порты GigabitEthernet нельзя использовать порт GigabitEthernet 1/1

Примечание 2. При необходимости перезагрузки определенного коммутатора в стеке можно воспользоваться командой

```
reload cold switch <1-12>
```

где <1-12> - ID коммутатора в стеке.

Пример настройки.

Настроить коммутатор для стекирования, выбрать в качестве стекирующих интерфейсов порты 10GigabitEthernet 1 и 2, выбрать для этого коммутатора юнит №5 в стеке.

```
# configure terminal
(config)# switch stack enable
Change will take effect upon next reboot
(config)# switch stack interface 10GigabitEthernet 1/1-2
Change will take effect upon next reboot
(config)# switch stack swap 1 5
Change will take effect upon next reboot
# exit
     # reload cold
```

4.2.61. Обновление ПО и автоматическая конфигурация

Коммутатор имеет возможность автоматической конфигурации и обновления ПО через DHCP (66,67 опции)

Коммутатор загрузит конфигурацию или образ ПО только в том случае если `startup` и `running config` будут равны `default config.`

Важно, в 67 опции передается имя файла конфигурации или имя файла прошивки. Имена файлов конфигурации и прошивки в обязательном порядке должны начинаться с `config_` и `image_` соответственно. Имя файла прошивки необходимо указывать с расширением, например «`image_istax.itb`»

Пример настройки DHCP-сервера:

```
# ip dhcp server
# ip dhcp excluded-address 192.168.102.1 192.168.102.20
# ip dhcp pool name-pool
#  network 192.168.102.0 255.255.255.0
#  default-router 192.168.102.1
#  lease 0 0 5
#  tftp-server 192.168.102.5 (option 66)
#  bootfile-name config_nts.cfg (option 67)
# interface vlan 1
#  ip dhcp server
```

4.2.62. Конфигурация PPPoE Intermediate Agent

Команда	Описание
Глобальные настройки	
`pppoe intermediate-agent`	Включить функцию PPPoE Intermediate Agent
`no pppoe intermediate-agent`	Отключить функцию PPPoE Intermediate Agent
`pppoe intermediate-agent delimiter <word5>`	Задать разделитель

pppoe intermediate-agent type self-defined circuit-id <line64>	Задать собственный формат circuit-id
pppoe intermediate-agent type self-defined remote-id <line64> / raw-mac	Задать собственный формат remote-id или передавать mac
pppoe intermediate-agent type tr-101 circuit-id identifier-string <word32> option (pv sp spv sv) delimiter <word5>	Настроить добавляемые поля circuit-id формата tr-101. pv - порт и vlan, sp - слот и порт, spv - слот порт и vlan, sv - слот и vlan. Задать разделитель
Настройка портов	
pppoe intermediate-agent no pppoe intermediate-agent	Включить функцию PPPoE Intermediate Agent Отключить функцию PPPoE Intermediate Agent,
pppoe intermediate-agent trust no pppoe intermediate-agent trust	Назначить порт в качестве доверенного Назначить порт в качестве недоверенного
pppoe intermediate-agent vendor-tag strip no pppoe intermediate-agent vendor-tag strip	Включить функцию снятия тега вендора на порту Отключить функцию снятия тега вендора на порту
pppoe intermediate-agent circuit-id <line64>	Задать строку circuit-id, для добавления на порту
pppoe intermediate-agent remote-id <line64> raw-mac	Задать строку или mac remote-id, для добавления на порту

4.2.63. Настройка bpdu-tunnel-protocol (l2pt/BPDU Tunneling)

Функция Layer 2 Protocol Tunneling (L2PT / BPDU Tunneling) предназначена для прозрачной передачи служебного управляющего L2-трафика клиентских сетей через транзитную инфраструктуру оператора связи. Данный механизм позволяет объединять разрозненные сегменты сетей клиентов, обеспечивая корректное функционирование их внутренних протоколов управления без изменения сетевой топологии оператора.

Система позволяет перехватывать кадры управления на входящем порт-интерфейсе, и осуществлять подмену оригинального Destination MAC-адреса протокола на туннельный мультикаст-адрес.

По умолчанию для инкапсуляции кадров всех поддерживаемых протоколов задано значение DMAC 01:00:0C:CD:00:02. При необходимости данные значения могут быть изменены.

Ограничение: На интерфейсах, участвующих в процессе туннелирования L2PT, включенные протоколы Spanning Tree и LLDP препятствуют корректной работе функции. Локальный процессор коммутатора будет перехватывать эти кадры для собственных нужд, что может отрицательно сказаться на его работе.

Перед активацией функции на конкретном интерфейсе в обязательном порядке требуется деактивировать Spanning Tree, а также отключить прием и передачу сообщений LLDP

Команда	Описание
Глобальные настройки	
`bpdu-tunnel-protocol <protocol> default-group-mac [vid <vlan_list>]`	Включение туннелирования для указанного протокола с назначением группового MAC-адреса по умолчанию (01:00:0C:CD:00:02) в заданных VLAN. Если параметр vid опущен, задается VLAN 1.
`bpdu-tunnel-protocol <protocol> group-mac <mac_addr> [vid <vlan_list>]`	Включение туннелирования для указанного протокола с назначением нестандартного группового MAC-адреса туннелирования в заданном списке VLAN.
`no bpdu-tunnel-protocol <protocol>`	Отключение туннелирования для выбранного протокола.
Аргумент <protocol> во всех типах команд принимает одно из 17 фиксированных значений: cdp, dot1x, dtp, gvrp, isis-l1, isis-l2, lacp, lldp, oam, ospf, pagp, pvst, rip, stp, udld, vrrp, vtp.	
Режим конфигурации физического интерфейса	
`no spanning-tree`	Деактивация протокола Spanning Tree на интерфейсе. Обязательное условие для активации туннелирования.
`no lldp receive`	Отключение приема пакетов LLDP локальным процессором на интерфейсе.
`no lldp transmit`	Отключение генерации пакетов LLDP локальным процессором на интерфейсе.

`bpdu-tunnel-protocol <protocol>`
 	
`no bpdu-tunnel-protocol <protocol>`
	Активация аппаратной обработки (инкапсуляции и декапсуляции) кадров указанного протокола на данном интерфейсе.
	
	Отключение обработки туннелирования выбранного протокола на данном интерфейсе

Привилегированный режим (exec)	
`show bpdu-tunnel-protocol`	Отображение суммарной таблицы счетчиков инкапсулированных, декапсулированных, перенаправленных и отброшенных пакетов (Rx/Tx Encap/Decap, Redirect, Drops) по всем интерфейсам системы.
`show bpdu-tunnel-protocol interface <port_type_list>`	Отображение детальной таблицы статистики BPDU Tunneling для указанных физического интерфейсов.

Примеры настройки:

1) Настройка туннелирования протокола STP с использованием группового MAC-адреса по умолчанию в VLAN 100:

```
# configure terminal
```

```
(config)# vlan 100
(config-vlan)# exit
(config)#
(config)# bpdu-tunnel-protocol stp default-group-mac vid 100
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid native vlan 100
(config-if)# switchport hybrid allowed vlan all
(config-if)# switchport hybrid untagged vlan add 1,100
(config-if)# no spanning-tree
(config-if)# bpdu-tunnel-protocol stp
```

2) Настройка туннелирования протоколов CDP и LLDP с использованием кастомного группового MAC-адреса в VLAN 100:

```
(config)# bpdu-tunnel-protocol cdp group-mac 01:00:0c:cd:cd:04
vid 100
(config)#      bpdu-tunnel-protocol      lldp      group-mac
01:00:0c:cd:cd:04 vid 100
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode hybrid
(config-if)# switchport hybrid native vlan 100
(config-if)# switchport hybrid allowed vlan all
(config-if)# switchport hybrid untagged vlan add 1,100
(config-if)# no spanning-tree
(config-if)# no lldp receive
(config-if)# no lldp transmit
(config-if)# bpdu-tunnel-protocol cdp
(config-if)# bpdu-tunnel-protocol lldp
```

Команды проверки работоспособности

Для вывода статистических данных по работе туннелирования протоколов используется команда `show bpdu-tunnel-protocol`.

Пример вывода общей таблицы статистики:

show bpdu-tunnel-protocol

Port	Protocol	Rx Encap	Rx Decap	Tx Encap	Tx Decap	Rx redir	Tx redir	Drops

Пример вывода детальной статистики для конкретного интерфейса:

show bpdu-tunnel-protocol interface GigabitEthernet 1/1

Port	Protocol	Rx Encap	Rx Decap	Tx Encap	Tx Decap	Rx redir	Tx redir	Drops
Gi 1/1	stp	142	0	0	139	0	0	0
Gi 1/1	cdp	45	0	0	42	0	0	0
Gi 1/1	lldp	78	0	0	75	0	0	0

Ниже приведена рабочая конфигурация для организации сквозного прохождения трафика.

Интерфейс первого устройства настраивается как абонентский стык с активацией необходимых протоколов. Интерфейс второго устройства выступает в роли транзитной магистрали в сторону сети оператора связи.

```
vlan 1,100
exit
!
bpdu-tunnel-protocol stp default-group-mac vid 100
bpdu-tunnel-protocol cdp default-group-mac vid 100
bpdu-tunnel-protocol udld default-group-mac vid 100
bpdu-tunnel-protocol oam default-group-mac vid 100
bpdu-tunnel-protocol lacp default-group-mac vid 100
bpdu-tunnel-protocol lldp default-group-mac vid 100
bpdu-tunnel-protocol gvrp default-group-mac vid 100
bpdu-tunnel-protocol dot1x default-group-mac vid 100
bpdu-tunnel-protocol isis-l1 default-group-mac vid 100
bpdu-tunnel-protocol isis-l2 default-group-mac vid 100
bpdu-tunnel-protocol pvst default-group-mac vid 100
bpdu-tunnel-protocol dtp default-group-mac vid 100
bpdu-tunnel-protocol vtp default-group-mac vid 100
bpdu-tunnel-protocol pagp default-group-mac vid 100
bpdu-tunnel-protocol rip default-group-mac vid 100
bpdu-tunnel-protocol ospf default-group-mac vid 100
bpdu-tunnel-protocol vrrp default-group-mac vid 100
!
interface GigabitEthernet 1/1
 description CLIENT_PORT_INTERFACE
 switchport mode hybrid
 switchport hybrid native vlan 100
 switchport hybrid allowed vlan all
 switchport hybrid untagged vlan add 1,100
 no lldp receive
 no lldp transmit
 no spanning-tree
 bpdu-tunnel-protocol stp
 bpdu-tunnel-protocol cdp
 bpdu-tunnel-protocol lacp
 bpdu-tunnel-protocol lldp
 bpdu-tunnel-protocol dot1x
 bpdu-tunnel-protocol gvrp
 bpdu-tunnel-protocol dtp
 bpdu-tunnel-protocol isis-l1
 bpdu-tunnel-protocol isis-l2
 bpdu-tunnel-protocol oam
 bpdu-tunnel-protocol ospf
 bpdu-tunnel-protocol pagp
 bpdu-tunnel-protocol pvst
 bpdu-tunnel-protocol rip
 bpdu-tunnel-protocol udld
 bpdu-tunnel-protocol vrrp
 bpdu-tunnel-protocol vtp
```

```
exit
!
interface GigabitEthernet 1/2
 description MAGISTRAL_PORT_INTERFACE
 switchport mode trunk
 switchport trunk allowed vlan 1,100
 no lldp receive
 no lldp transmit
 no spanning-tree
exit
```

Логика и условия срабатывания механизмов инкапсуляции и декапсуляции

–Режим инкапсуляции (Замена DMAC протокола на DMAC группы)**:** Аппаратный механизм подмены адресов на данной конфигурации срабатывает при выполнении следующих условий:

1. Кадр управляющего протокола от клиентского оборудования поступает на порт Gigabit Ethernet 1/1.
2. В заголовке входящего кадра содержится оригинальный Destination MAC-адрес (например, 01:80:C2:00:00:21 для протокола GVRP).
3. Данный протокол явно активирован в конфигурации интерфейса (bpdu-tunnel-protocol gvrp), а сам интерфейс предварительно изолирован от локальных процессов обработки управляющего программного обеспечения (no spanning-tree, no lldp receive/transmit).

Результат: Коммутатор отправляет пакет в VLAN 100 и принудительно перезаписывает его DMAC на групповой адрес q по умолчанию (01:00:0C:CD:00:02). В таком виде кадр беспрепятственно передается между устройствами и выходит в сеть оператора связи через магистральный порт GigabitEthernet 1/2.

4. ВНИМАНИЕ: если кадр с DMAC протокола придет на порт с включенным bpdu-tunnel-protocol данного протокола – он выйдет с VLAN других портов с включенным bpdu-tunnel-protocol этого протокола без изменения DMAC. DMAC будет изменен на DMAC группы только при выходе с порта с выключенным bpdu-tunnel-protocol.

–Режим декапсуляции (Замена DMAC группы на DMAC протокола): Обратный аппаратный механизм восстановления структуры кадра срабатывает при выполнении следующих условий:

1. Инкапсулированный тегированный VLAN 100 кадр со стороны магистрали оператора связи поступает на порт GigabitEthernet 1/2.
2. DMAC кадра - групповой туннельный адрес (01:00:0C:CD:00:02).
3. Метаданные кадра, за исключением DMAC, соответсвуют включенному протоколу (etype, subtype, PID, LLC SSAP, ipproto, и т.д.)
4. Кадр коммутируется внутри системы на абонентский порт GigabitEthernet 1/1, на котором для данного типа трафика активирована команда bpdu-tunnel-protocol протокола с обнаруженными метаданными.

Результат*:* при прохождении кадра через порт GigabitEthernet 1/1 на выход аппаратная логика интерфейса считывает правила привязки протоколов. Коммутатор возвращает оригинальный клиентский MAC-адрес протокола (например, 01:80:C2:00:00:21). Клиент за портом получает исходный L2-пакет

5. ВНИМАНИЕ: если кадр с групповым DMAC придет на порт, где включен протокол с таким DMAC группы – кадр отбросится. Декапсуляция происходит только если кадр приходит на порт с выключенным протоколом.

4.2.64. Control Plane Policing (CoPP)

CoPP – это механизм сетевой безопасности, который защищает процессор (CPU) от перегрузки. Он фильтрует и ограничивает скорость трафика, предотвращая сбои из-за DoS-атак или ошибок в топологии сети.

Команда настройки CoPP	
Команда настройки из режимма глобальной конфигурации	Описание

`Control-plane-policing ['ARP' 'Everything' 'HTTP' 'HTTPS' 'ICMP' 'IGMP' 'IPv4' 'IPv4-Link-Local' 'IPv6' 'IPv6-Link-Local' 'L2CP-Cisco' 'L2CP-Ethernet' 'L2CP-LLC' 'PVST' 'SNMP' 'SSH' 'STP' 'Slow-protocols' 'TCP' 'Telnet' 'UDP']`
 	
`no control-plane-policing ['ARP' 'Everything' 'HTTP' 'HTTPS' 'ICMP' 'IGMP' 'IPv4' 'IPv4-Link-Local' 'IPv6' 'IPv6-Link-Local' 'L2CP-Cisco' 'L2CP-Ethernet' 'L2CP-LLC' 'PVST' 'SNMP' 'SSH' 'STP' 'Slow-protocols' 'TCP' 'Telnet' 'UDP']`
	Включение механизма ограничения для выбранного типа данных. По умолчанию включено
	
	Выключение механизма ограничения для выбранного типа данных.

`control-plane-policing rate ['ARP' 'Everything' 'HTTP' 'HTTPS' 'ICMP' 'IGMP' 'IPv4' 'IPv4-Link-Local' 'IPv6' 'IPv6-Link-Local' 'L2CP-Cisco' 'L2CP-Ethernet' 'L2CP-LLC' 'PVST' 'SNMP' 'SSH' 'STP' 'Slow-protocols' 'TCP' 'Telnet' 'UDP'] fps <10-100000> burst-size <16-4096>`	Указание значения fps и burst-size для всех или выбранного типа данных.
Команда просмотра информации	Описание
`show control-plane-policing ['ARP' 'Everything' 'HTTP' 'HTTPS' 'ICMP' 'IGMP' 'IPv4' 'IPv4-Link-Local' 'IPv6' 'IPv6-Link-Local' 'L2CP-Cisco' 'L2CP-Ethernet' 'L2CP-LLC' 'PVST' 'SNMP' 'SSH' 'STP' 'Slow-protocols' 'TCP' 'Telnet' 'UDP']`	Просмотр значений fps и burst-size для всех или выбранного типа данных.

4.2.65. Green Ethernet (Настройка энергосбережения)

Функционал Green Ethernet позволяет снизить энергопотребление коммутатора за счет управления режимами работы физического уровня (PHY), скоростью вращения вентиляторов охлаждения и яркостью светодиодной индикации портов.

Команда	Описание
Глобальные настройки	
`green-ethernet eee optimize-for-power` `no green-ethernet eee optimize-for-power`	Оптимизация режима энергоэффективного Ethernet (IEEE 802.3az EEE) для минимального энергопотребления. Отмена (команда `no`) возвращает оптимизацию для минимальной задержки передачи трафика.
`green-ethernet fan temp-max <-127..127> [temp-on <-127..127>]`	Настройка температурного режима системы охлаждения: • temp-max — температура (°C), при достижении которой вентиляторы работают на максимальной скорости; • temp-on — температура (°C), при которой вентиляторы включаются на минимальной скорости. Примечание. По умолчанию значения temp-on 75°C и temp-max 100°C.
`green-ethernet led interval <0-24>-<0-24> intensity <0-100>` `no green-ethernet led interval <0-24>-<0-24>`	Настройка яркости светодиодных индикаторов портов в заданный период времени: • `<0-24>-<0-24>` — временной интервал в часах в формате `начало-конец` (например, `22-6` — с 22:00 до 06:00, `0-24` — круглосуточно; `0` обозначает начало суток, `24` — конец суток); • `intensity <0-100>` — уровень яркости индикаторов в процентах (от 0% — полное отключение до 100% — максимальная яркость).
`green-ethernet led on-event [error] [link-change <0-65535>]` `no green-ethernet led on-event`	Временное повышение яркости светодиодов до `100%` при наступлении системных событий: • `error` — при возникновении ошибок на порту; • `link-change <0-65535>` — при изменении состояния линка на указанное количество секунд.
`green-ethernet eee` `no green-ethernet eee`	Включение / отключение технологии энергоэффективного Ethernet (IEEE 802.3az EEE) на порту, переводящей приемопередатчик в спящий режим при отсутствии трафика.
`green-ethernet energy-detect` `no green-ethernet energy-detect`	Включение / отключение функции определения активности на линии (перевод порта в режим пониженного энергопотребления при отсутствии подключенного устройства).
`green-ethernet short-reach` `no green-ethernet short-`	Включение / отключение режима пониженной мощности передатчика при использовании

`reach`	коротких медных кабелей.

Мониторинг и диагностика

Команда	Описание
Привилегированный режим	
`show green-ethernet`	Вывод сводной таблицы статуса энергосбережения по всем портам коммутатора.
`show green-ethernet interface <type> <port_list>`	Вывод подробного статуса энергосбережения для указанных портов
`show green-ethernet eee [interface <type> <port_list>]`	Отображение статуса поддержки и активности технологии EEE по всем или выбранным портам.
`show green-ethernet energy-detect [interface <type> <port_list>]`	Отображение статуса функции определения наличия сигнала (Energy-Detect) на портах.
`show green-ethernet fan`	Отображение текущей температуры чипа (Chip Temp.) и скорости вращения вентиляторов (Fan Speed в об/мин).

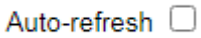
5. Web-интерфейс



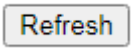
Рис.5.1 – Web-интерфейс

Для удобства навигации все команды разделены на четыре основные группы:
configuration – конфигурация;
monitor – мониторинг;
diagnostics – диагностика;
maintenance – обслуживание.

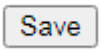
5.1. Основные команды управления настройками



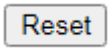
- Включить/выключить автоматическое обновление параметров;



- Обновить параметры;



- Сохранить введенные значения;



- Сбросить введенные значения;


- Update – Обновление прошивки коммутатора;


- Home – Отображает стартовую страницу мониторинга;


- Logout – Смена пользователя;


- Show Help – Показать справку.

5.2. Конфигурация

Вкладка конфигурации (Configuration) сгруппирована по названиям протоколов и используемым настройкам (Рис. 5.2).

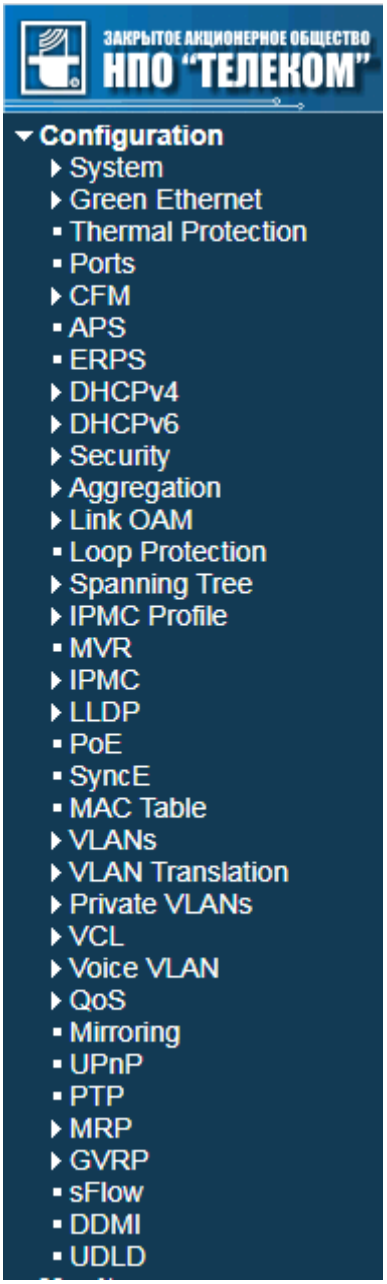


Рис. 5.2 – Вкладка Configuration

5.2.1. System. Системные настройки

Конфигурация системной информации (System Information Configuration) (Рис. 5.2.1.1) (Табл. 5.2.1.1). Позволяет задать информацию о коммутаторе в соответствии с предпочтениями пользователя.

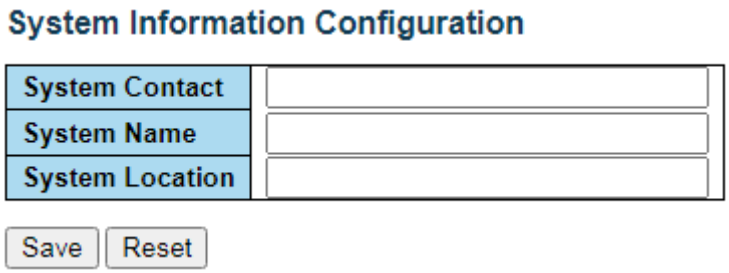


Рис. 5.2.1.1 – Вкладка System Information Configuration

Таблица 5.2.1.1 - Вкладка System Information Configuration

System Contact	Контактная информация. В этом поле можно указать контактную информацию. Имя, фамилия лица, ответственного за систему, адрес электронной почты или другие сведения.
System Name	Имя системы. Имя хоста для данного устройства. Можно использовать (A-Z), (a-z), (0-9), (-). Применение символа «пробел» недопустимо. Первый символ должен быть буквой (прописной или строчной). Первый и последний символы не должны быть знаком минус. Допустимая длина строки 0~255.
System Location	Расположение системы, физическое расположение этого устройства (например: garderob, etazh3 и т.п.). Допустимая длина строки от 0 до 255.

Конфигурация IP (IP Configuration) (Рис. 5.2.1.2) (Табл. 5.2.1.2).

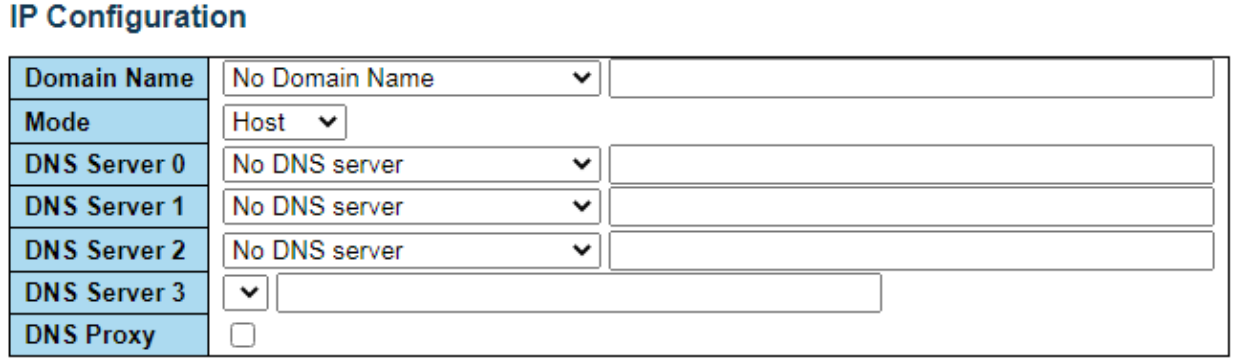


Рис. 5.2.1.2 – IP Configuration

Таблица 5.2.1.2- IP Configuration

Domain Name	Строка имени локального домена, в котором находится устройство. Большинство запросов для имен в этом домене могут использовать короткие имена относительно локального домена. Затем система добавляет доменное имя в качестве суффикса к неквалифицированным именам. Например, если доменное имя задано как «example.com» и вы укажете пункт назначения PING по

	неквалифицированному имени как «test», тогда система определит имя как «test.example.com». Поддерживаются следующие режимы: No Domain Name- Доменное имя использоваться не будет. Configured Domain Name - Явно укажите имя локального домена. Убедитесь, что настроенное доменное имя соответствует домену вашей организации. From any DHCPv6 interfaces - Будет использоваться первое доменное имя, предложенное при аренде DHCPv6 интерфейсу с поддержкой DHCPv6. From this DHCPv6 interface - Укажите, из какого интерфейса с поддержкой DHCPv6 следует отдавать предпочтение предоставленному доменному имени.
Mode	В списке можно выбрать, как будет функционировать стек протоколов IP – как хост или как маршрутизатор. В режиме Host (Хост) IP–трафик между интерфейсами не может быть маршрутизирован. В режиме Router (Маршрутизатор), трафик может маршрутизироваться между всеми интерфейсами. При настройке данного устройства для множества VLAN, следует выбрать режим Router. Режим 21 Host выбран по умолчанию.
DNS Server 0..3	Данная настройка позволяет задать сервер доменных имен (DNS). Режим работы: • From any DHCP interfaces (Из любых интерфейсов DHCP): будет использован IP-адрес первого DNSсервера, полученный от DHCP, при включенной поддержки DHCP на интерфейсе. • No DNS server (Без DNS-сервера): DNS-сервер использоваться не будет. • Configured (Заданный IP-адрес): будет использован IP-адрес DNS-сервера, введенный в десятичном формате с точкой. • From this DHCP interface (Из данного интерфейса DHCP): можно указать из какого интерфейса с активированным DHCP-протоколом предпочтительно выбрать DNS-сервер.

DNS Proxy	Прокси-сервер доменных имен. Когда активирован прокси сервер DNS, система будет отправлять запросы DNS на текущий настроенный DNS-сервер, при этом ответы будут отправляться, как DNS-разрешения клиентским устройствам сети.

IP Интерфейсы (IP Interfaces) (Рис. 5.2.1.3) (Табл. 5.2.1.3).

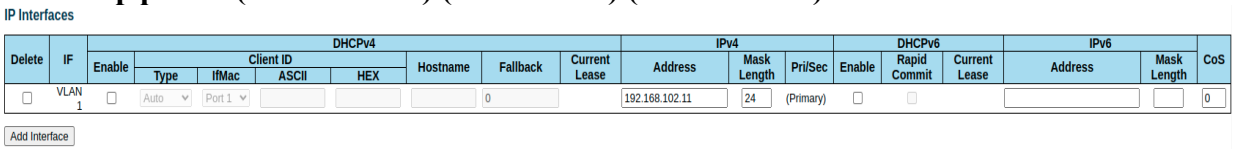


Рис. 5.2.1.3– IP Interfaces

Таблица 5.2.1.3- IP Configuration

Delete			Выберите, чтобы удалить текущий IP-интерфейс.
VLAN			В этом поле указан номер VLAN, ассоциированный с IP-интерфейсом. Доступ к IP-интерфейсу будут иметь только порты с данным номером VLAN. Это поле доступно для ввода только при создании нового интерфейса
DHCPv4	Enable		Включить клиент DHCP. Если этот параметр включен, система настроит адрес IPv4 и маску интерфейса с использованием протокола DHCP. Клиент DHCP объявит сконфигурированное имя системы как имя хоста (hostname), чтобы обеспечить поиск DNS.
	Hostname		Имя хоста DHCP-клиента. Если клиент DHCPv4 включен, настроенное имя хоста будет использоваться в поле DHCP option 12. Если это значение представляет собой пустую строку, в поле используется настроенное имя системы плюс последние три байта системных MAC-адресов в качестве имени хоста.
	Fallback		Опция IPv4 DHCP Fallback определяет как долго (в 22 секундах) коммутатор будет ожидать ответа от DHCPсервера, прежде чем он начнет использовать настроенный статический IP-адрес. Допустимые значения: от 0 до 4294967295 секунд. Нулевое значение отключает механизм резервных действий, таким образом, что коммутатор будет ожидать ответа до тех пор, пока не получит
	Current Lease		Показывает текущий адрес интерфейса, предоставленный сервером DHCP.
	Client ID	Type	Тип идентификатора клиента DHCP IPv4. Выберите, какой из трех типов ниже, то есть IfMac, ASCII или HEX, должен использоваться для идентификатора клиента
		IfMac	Идентификатор клиента DHCP IPv4 IfMac. Когда клиент DHCPv4 включен и тип идентификатора клиента - ifmac, аппаратный MAC-адрес настроенного интерфейса будет использоваться в поле DHCP option 61.
		ASCII	Идентификатор клиента DHCP IPv4 ASCII. Когда

			клиент DHCPv4 включен и тип идентификатора клиента - ascii, строка ASCII будет использоваться в поле DHCP option 61.
		HEX	Идентификатор клиента DHCP IPv4 HEX. Когда клиент DHCPv4 включен и тип идентификатора клиента «HEX», шестнадцатеричное значение будет использоваться в поле DHCP option 61.
IPv4	Address	IP v4-адрес интерфейса. Если DHCP включен, то это поле не используется. Поле может оставаться пустым, если не требуется IP v4.	
	Mask Length	Маска сети IP v4. Если протокол DHCP активирован, это поле не используется. Поле можно оставить пустым.	
	Pri/Sec	Основной/Дополнительный ip адрес	
IPv6	Address	IPv6-адрес интерфейса. Поле можно оставить пустым	
	Mask Length	Маска сети IP v6. Поле можно оставить пустым.	
DHCP v6	Enable	Включить клиент DHCP. Если этот параметр включен, система настроит адрес IP v6 и маску интерфейса с использованием протокола DHCP.	
	Rapid Commit	Позволяет серверу быстро фиксировать контейнер или глобальную группу. По умолчанию эта опция не задана и считается отключенной.	
	Current Lease	Показывает текущий адрес интерфейса, предоставленный сервером DHCP.	
CoS		Позволяет задать маркировку 802.1p исходящего трафика с интерфейса управления.	

IP-маршруты (IP Routers) (Рис. 5.2.1.4) (Табл. 5.2.1.4).

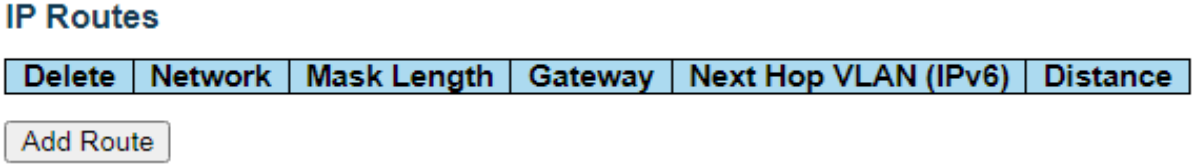


Рис. 5.2.1.4– IP Route

Таблица 5.2.1.4- IP Route

Delete	Удаление текущего маршрута
Network	Адрес сети назначения. Это IP-адрес сети назначения или IP-адрес хоста этого маршрута.
Mask Length	Маска сети. Это маска IP-адреса сети назначения или маска хоста.
Gateway	IP-адрес шлюза. Шлюз и сеть должны быть одного типа.
Next Hop	Идентификатор VLAN (VID) конкретного интерфейса IPv6, связанного со

VLAN	шлюзом. Данный VID находится в диапазоне от 1 до 4094 и будет работать только тогда, когда соответствующий интерфейс IPv6 действителен. Если IP-адрес шлюза IPv6 локальный, он должен указать VLAN следующего перехода для шлюза. Если IP-адрес шлюза IPv6 не локальный, система игнорирует VLAN следующего перехода для шлюза.
Distance	Значение расстояния в записи маршрута используется для предоставления маршрутизаторам информации о приоритете протоколов маршрутизации. Когда задействованы два или более разных протокола маршрутизации и имеют один и тот же пункт назначения, значение расстояния может использоваться для выбора наилучшего пути.

Кнопка 

предназначена для добавления новых маршрутов.

Конфигурация NTP (NTP Configuration) (Рис. 5.2.1.5) (Табл. 5.2.1.5)

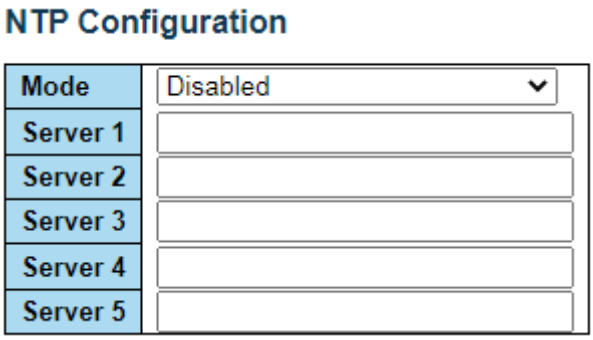


Рис. 5.2.1.5– NTP

Таблица 5.2.1.5- NTP

Mode	Режим работы NTP: включен/выключен
Server 1..5	IPv4 или IPv6-адрес NTP-сервера

Конфигурация часового пояса (Time Zone Configuration) (Рис. 5.2.1.6) (Табл. 5.2.1.6).

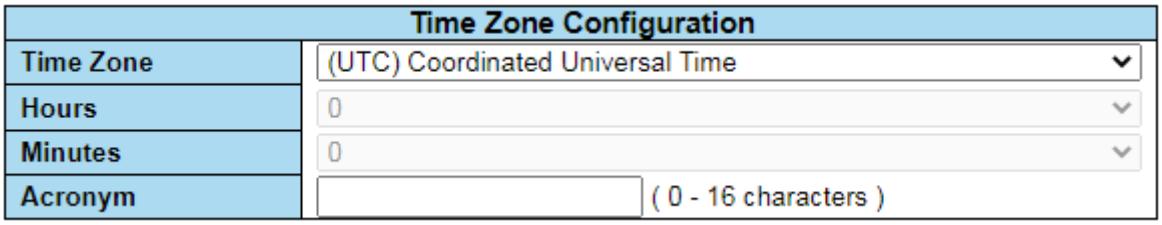


Рис. 5.2.1.6 – Конфигурация часового пояса

Таблица 5.2.1.6 - Конфигурация часового пояса

Time Zone	Выберите соответствующий часовой пояс из раскрывающегося списка
Acronym	Настраиваемый пользователем акроним для определения часового пояса (до 16 символов).

Конфигурация перехода на летнее время (Daylight Saving Time Configuration) (Рис. 5.2.1.7) (Табл. 5.2.1.7).

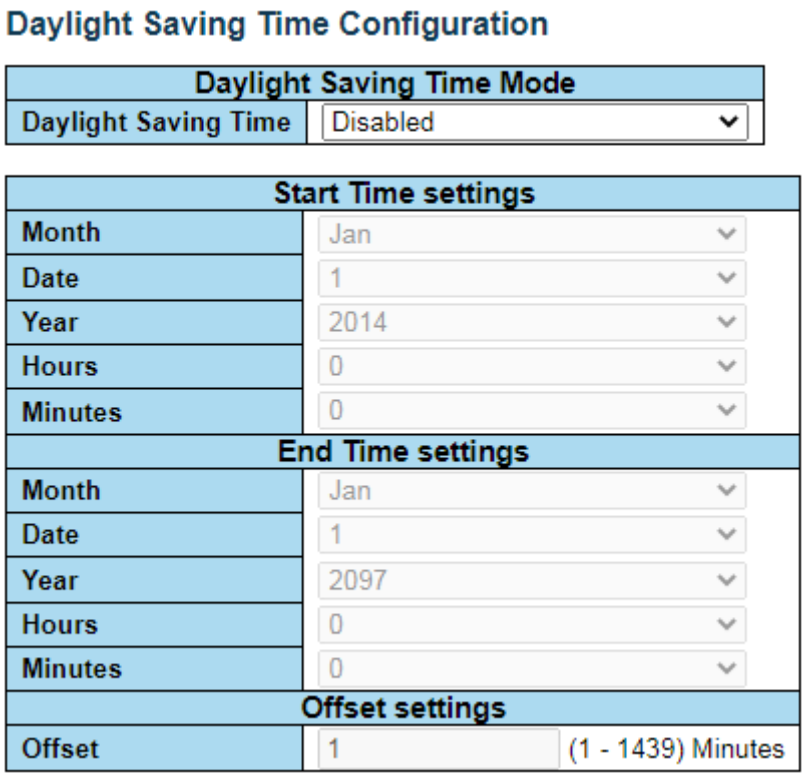


Рис. 5.2.1.7– Конфигурация перехода на летнее время

Таблица 5.2.1.7- Конфигурация часового пояса

Daylight Saving Time		Disabled (Отключено) – переход на летнее время отключен; Recurring (Повторяющийся) – повторять переход на летнее время каждый год; Non-Recurring (Единовременный) - переход на летнее время один раз
Start Time settings (Время начала действия)	Month	Месяц начала
	Date	Дата начала
	Year	Год начала
	Hours	Час начала
	Minutes	Минуты начала
End Time settings (Время окончания действия)	Month	Месяц конца
	Date	Дата конца
	Year	Год конца
	Hours	Час конца
	Minutes	Минуты конца
Offset settings		Введите количество минут для добавления в летнее время. (Диапазон: 1-1440)

Конфигурация журнала системных сообщений (System Log) (Рис. 5.2.1.8) (Табл. 5.2.1.8).

Syslog (системный журнал) – стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP.

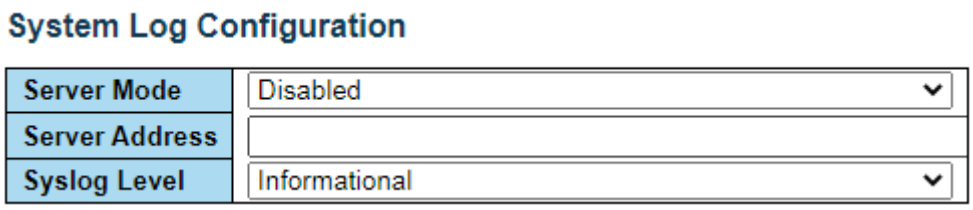


Рис. 5.2.1.8– System Log

Таблица 5.2.1.8- System Log

Server Mode	Режим работы сервера: Включен (Enabled)/Выключен (Disabled);
Server Address	IP v4 – адрес syslog-сервера, также можно указать host name;
Syslog Level	Укажите тип отправляемых сообщений. Возможные режимы: • Error (Ошибка) –отправлять только ошибки; • Warning (Предупреждение) – отправлять предупреждения и ошибки; • Notice (Уведомление) – отправлять уведомления, предупреждения и ошибки; • Informational (Информация) – отправлять информационные сообщения, уведомления, предупреждения и ошибки;

5.2.2. Green Ethernet. Настройка энергосбережения. Настройка энергосбережения.

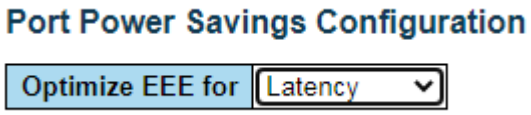


Рис. 5.2.2.1 – Port Power Savings Configuration

Таблица 5.2.2.1 - Port Power Savings Configuration

OptimizeEEEfor	Коммутатор может быть настроен на оптимизацию EEE для наилучшего энергосбережения (Power) или минимальной задержки трафика (Latency).

Конфигурация портов.

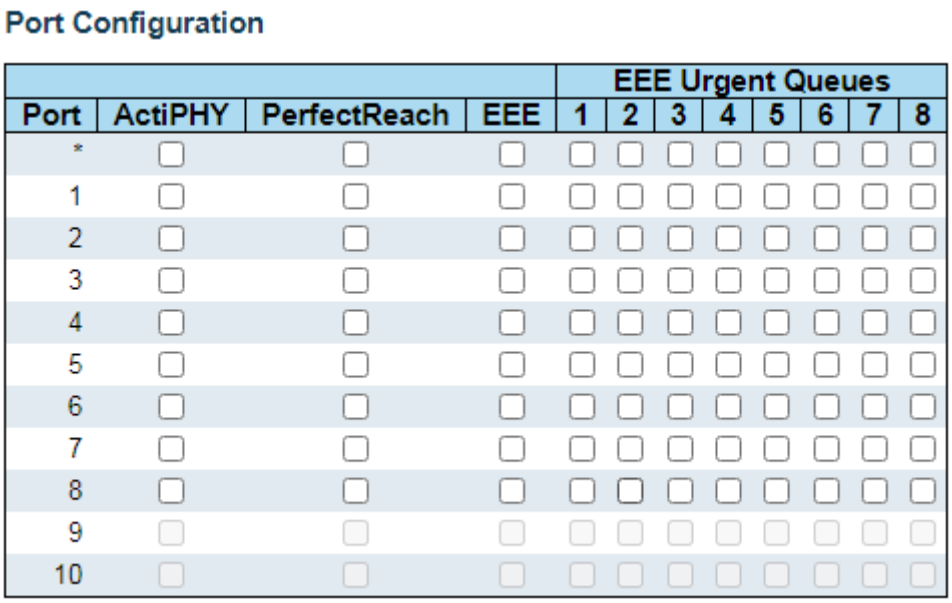


Рис. 5.2.2.2 – Port Configuration

Таблица 5.2.2.2 - Port Configuration

ActiPHY	Включение/выключение функции ActiPHY. ActiPHY снижает мощность порта при отсутствии связи. Порт включается на короткое время, чтобы определить, вставлен ли кабель.
PerfectReach	Включение/выключение функции PerfectReach. PerfectReach работает, определяя длину кабеля и снижая мощность для портов с короткими кабелями.
EEE	Включение/выключение EEE для порта коммутатора. Для максимальной экономии энергии схема не запускается сразу после того, как данные для передачи готовы для порта, а вместо этого ставится в очередь до тех пор, пока пакет данных не будет готов к передаче. Это приведет к некоторой задержке трафика.
EEE Urgent Queues	Настройка очередей. Установленные очереди активируют передачу кадров, как только данные станут доступны. В противном случае очередь отложит передачу до тех пор, пока не будет передана пачка кадров.

5.2.3. Thermal Protection Configuration. Настройка защиты от перегрева.

Эта страница позволяет пользователю проверить и настроить текущую настройку защиты от перегрева.

Когда температура превышает настроенную температуру тепловой защиты, порты отключаются, чтобы снизить энергопотребление. Можно распределить порты по разным группам (Рис 5.2.3.1). Каждой группе может быть задана температура (Рис 5.2.3.2), при которой соответствующие порты должны быть выключены.

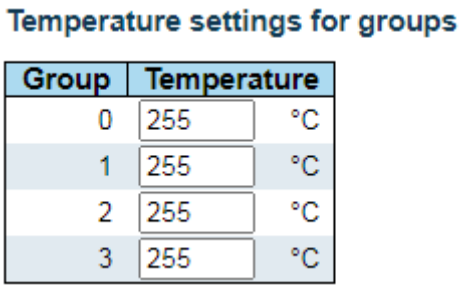


Рис. 5.2.3.1 – Настройка температуры

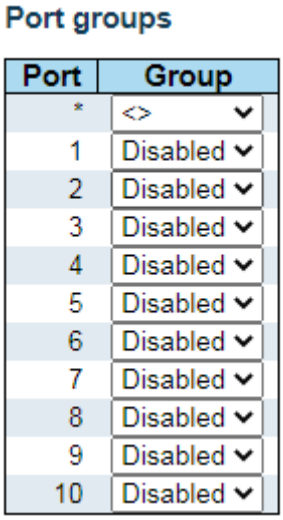


Рис. 5.2.3.2 – Группы портов

5.2.4. Конфигурация портов. Ports

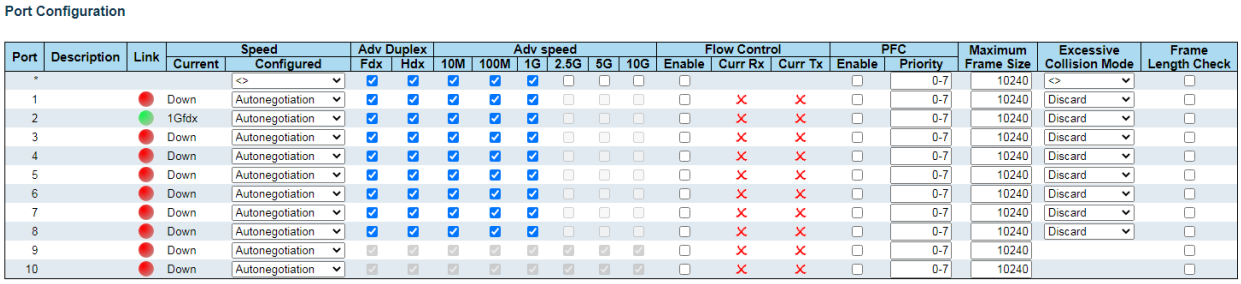


Рис. 5.2.4.1 – Port Configuration

Таблица 5.2.4.1 - Port Configuration

Port		Номер порта
Description		
Link		Текущее состояние (Link):  - наличие;  - отсутствие;
Speed	Current	Отображает текущую скорость соединения;
	Configure	Установка скорости соединения. Отображаются только

	d	поддерживаемые скорости. Возможные варианты: • Disabled - отключить порт коммутатора; • Auto – автоматический режим, выбирается максимальная скорость, которая возможна при текущем соединении; • SFP_Auto_AMS – автоматический режим определения скорости SFP; • Скорости: 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX/1Gbps FDX/ 2.5Gbps FDX/10Gbps FDX/100-FX/100-FX_AMS/1000- X/1000-X_AMS;
Adv Duplex	Fdx Hdx	При установленном режиме автоматического Hdx определения FDX/HDX, порт будет предлагать указанные режимы (FDX дуплекс) и (HDX полудуплекс) в качестве предпочтительных для порта, связанного по этому каналу устройства (если на нем также установлен автоматический режим);
Adv speed	10M 100M 1G 2.5G 5G 10G	При установленном режиме автоматического определения скорости, порт будет предлагать указанные скорости в качестве предпочтительных для порта, связанного по этому каналу устройства (если на нем также установлен автоматический режим);
Flow Control	Enable Curr Rx Curr Tx	Управление потоком. В столбце Current Rx указано, поддерживает ли порт паузы при приеме кадров. В столбце Current Tx указано, поддерживает ли порт паузы при передаче кадров. Настройки Rx и Tx определяются результатами последнего автосогласования параметров. Перед тем, как использовать управление потоком проверьте настройки в этих столбцах. Данная настройка связана также с выбранной скоростью Configured Speed.
PFC	Enable Priority	Установить приоритет (0-7) потока управления;
Maximum Frame Size		Максимальный размер фрейма для порта коммутатора, включая FCS;
Excessive Collision Mode		Режим работы при слишком большом числе столкновений пакетов: Данная настройка конфигурирует порт на установку режима передачи при столкновениях пакетов "Discard" (отбрасывание кадра после 16 столкновений – выбрано по умолчанию),
Frame Length Check		Включение/выключение проверки длины кадра. Если включена «проверка длины кадра», кадры с размером полезной нагрузки менее 1536 байтов отбрасываются, если поле EtherType / Length не соответствует фактической длине полезной нагрузки. Если «проверка длины кадра» отключена, кадры не отбрасываются из-за несоответствия длины кадра. Примечание. Счетчики отбрасывания не подсчитывают количество потерянных кадров из-за несоответствия длины кадра.

5.2.5. CFM Global Configuration

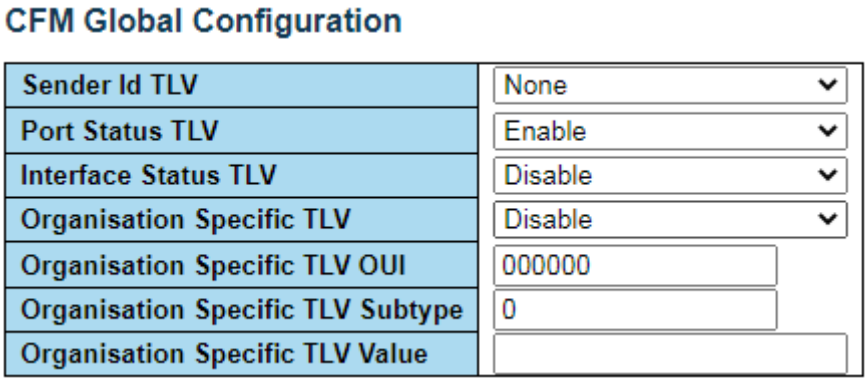


Рис. 5.2.5.1 – CFM Global Configuration

Таблица 5.2.5.1 - Port Configuration

Sender Id TLV	Выбор идентификатора tlv: Chassis – идентификатор шасси (MAC-адрес) chassis-management - идентификатор шасси (MAC-адрес) и адрес управления (IPv4-адрес) management - адрес управления (IPv4-адрес) disable – исключить идентификатор tlv
Port Status TLV	Включение или выключение tlv для статуса порта
Interface Status TLV	Включение или выключение tlv для статуса интерфейса
Organisation Specific TLV	Включение или выключение TLV для конкретной организации
Organisation Specific TLV OUI	трехбайтовый OUI, передаваемый с TLV, зависящим от организации.
Organisation Specific TLV Subtype	подтип, передаваемый с TLV для конкретной организации. Может быть любым значением в диапазоне [0; 255]
Organisation Specific TLV Value	значение, передаваемое в TLV для конкретной организации. Значение представляет собой печатаемую строку символов длиной 0-63.

Настройка домена CFM

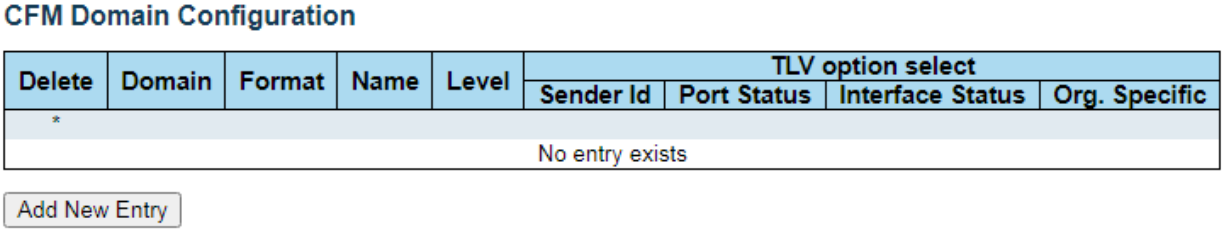


Рис. 5.2.5.2 – настройка домена CFM

Таблица 5.2.5.2 - настройка домена CFM

Delete		Кнопка удаления записи. Запись будет удалена при следующем сохранении.
Domain		Имя домена. Значение – это отдельное слово, начинающееся с буквенной буквы AZ или az длиной от 1 до 15.
Format		Выбор формата имени: None `String`
Name		Содержимое этого параметра зависит от значения параметра формата. Если формат None: Имя не используется, но за кадром будет установлены все нули. Этот формат обычно используется блоками PDU типа Y.1731. Если формат `String`: Имя должно содержать строку от 1 до 43 символов.
Level		Уровень этого домена. Допустимые значения ограничены 0–7.
TLV option select	Sender Id	Выбор идентификатора tlv Chassis – идентификатор шасси (MAC-адрес) chassismanage - идентификатор шасси (MAC-адрес) и адрес управления (IPv4-адрес) management - адрес управления (IPv4-адрес) none – исключить идентификатор tlv defer – применяются настройки глобальной конфигурации
	Port Status	Включение или выключение tlv для статуса порта Defer– применяются настройки глобальной конфигурации
	Interface Status	Включение или выключение tlv для статуса интерфейса Defer – применяются настройки глобальной конфигурации
	Org. Specific	disable - исключить TLV для конкретной организации Defer – применяются настройки глобальной конфигурации

CFM Service Configuration

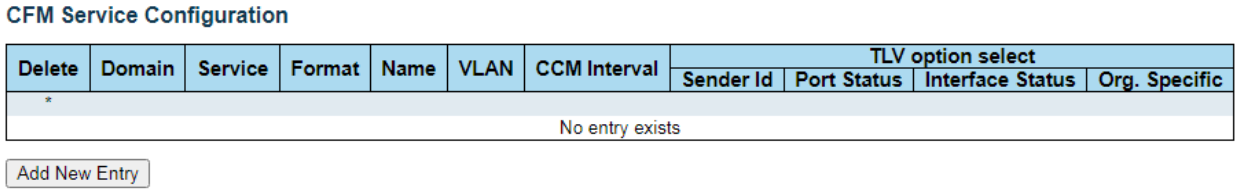


Рис. 5.2.5.3 – CFM Service Configuration

Таблица 5.2.5.3 - CFM Service Configuration

Delete	Кнопка удаления записи. Запись будет удалена при следующем сохранении.
Domain	Имя домена, под которым находится эта Служба.
Service	Название службы. Значение – это отдельное слово, начинающееся с буквенной буквы AZ или az длиной от 1 до 15.

Format		Выбор формата имени службы. Это решает, как будет интерпретироваться значение параметра Name. Возможные значения: String Two Octets Y1731 ICC Y1731 ICC CC
Name		Содержимое этого параметра зависит от значения элемента Format. Помимо ограничений объяснить для каждого из них, применяется следующее в целом: Если формат домена none, размер не может превышать 45 байт. Если формат домена не none, размер не может превышать 44 байта. Если формат String, применяется следующее: длина должна быть в диапазоне [1; 44]. Содержание должно быть в диапазоне [32; 126] Если формат Two Octets, применяется следующее: Имя [0] и Имя [1] будут интерпретироваться как 8-разрядные целые числа без знака (допустим диапазон [0; 255]). Имя [0] будет помещено в PDU перед именем [1]. Оставшиеся доступные байты в имени использоваться не будут. Если формат Y1731 ICC, применяется следующее: длина должна быть 13. Содержимое должно быть в диапазоне [az, AZ, 0-9]. Y.1731 указывает, что это конкатенация ICC (кода оператора связи ITU) и UMC (уникального кода идентификатора MEG): ICC: 1-6 байтов UMC: 7-12 байтов В принципе UMC может принимать любое значение в диапазоне [1; 127], но этот API не позволяет указывать длину ICC, поэтому базовый код не знает, где заканчивается ICC и начинается UMC. Формат домена должен быть none. Если формат Y1731 ICC CC, применяется следующее: длина должна быть 15. Первые 2 символа (CC): должны быть среди [AZ] Следующие 1-6 символов (ICC): должны быть среди [az, AZ, 0-9] Следующие 7-12 символов (UMC): должно быть среди [az, AZ, 0-9]. В имени [3-7] может присутствовать ОДИН (косая черта). Формат домена должен быть none.
VLAN		Выбор MEP в сервисе Основной VID MA. VLAN, равный 0, означает, что все MEP, созданные в этом MA, будут созданы как MEP порта (интерфейсные MEP). На каждом интерфейсе может быть только одна портовая MEP. MEP данного порта может быть создана с тегами, если VLAN этой MEP не равна нулю.
CCM Interval		Настройка скорости CCM всех MEP, привязанных к этой услуге
TLV option select	Sender Id	Выбор идентификатора tlv Chassis – идентификатор шасси (MAC-адрес)

		chassismanage - идентификатор шасси (MAC-адрес) и адрес управления (IPv4-адрес) management - адрес управления (IPv4-адрес) none – исключить идентификатор tlv defer – применяются настройки глобальной конфигурации
	Port Status	Включение или выключение tlv для статуса порта Defer– применяются настройки глобальной конфигурации
	Interface Status	Включение или выключение tlv для статуса интерфейса Defer – применяются настройки глобальной конфигурации
	Org. Specific	disable - исключить TLV для конкретной организации Defer – применяются настройки глобальной конфигурации

CFM Mep Configuration

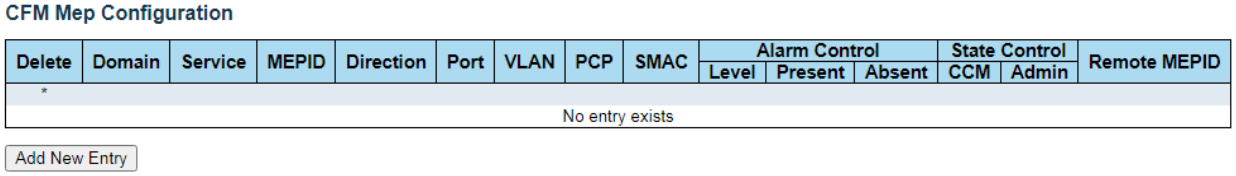


Рис. 5.2.5.4 – CFM Mep Configuration

Таблица 5.2.5.4 - CFM Mep Configuration

Delete		Кнопка удаления записи. Запись будет удалена при следующем сохранении.
Domain		Имя домена, в котором находится эта MEP.
Service		Имя сервиса, под которым находится данный MEP.
MEPID		Идентификатор этого MEP. Должно быть целым числом [1..8091]
Direction		Установите, является ли эта MEP восходящей или нисходящей.
Port		Порт, на котором находится эта MEP.
VLAN		Идентификатор VLAN. Используйте значение 0 для обозначения не тегированного трафика (подразумевается MEP порта).
PCP		Выберите значение PCP в теге VLAN PDU. Не используется без тегов.
SMAC		Установите MAC-адрес источника, который будет использоваться в блоках PDU CCM, исходящих от этой MEP. Адрес должен быть одноадресным. Формат: XX: XX: XX: XX: XX: XX. Если все нули, вместо него будет использоваться MAC-адрес порта коммутатора.
Alarm Control	Level	Установка уровня сигнализации. Если обнаружен дефект с приоритетом выше этого уровня, будет сгенерировано уведомление о неисправности. Допустимый диапазон: [1; 6], где 1 указывает, что любой дефект вызывает аварийный сигнал, а 6 означает, что никакой дефект не

		может вызвать аварийный сигнал.
	Present	Установка времени в миллисекундах, в течение которого должны присутствовать дефекты, прежде чем будет выдано уведомление о неисправности. По умолчанию 2500 мс.
	Absent	Установка времени в миллисекундах, в течение которого дефекты должны отсутствовать до сброса уведомления о неисправности. По умолчанию 10000 мс
State Control	CCM	Включение или отключение генерации сообщений проверки целостности (CCM)
	Admin	включить или отключить эту MEP. Когда эта MEP включена, она проверяет полученные / отсутствующие CCM и может вызывать дефекты.
Remote MEPID		Укажите удаленную MEP, от которой эта MEP, как ожидается, будет получать PDU CCM. Должно быть целым числом [0..8091], где 0 означает неопределенное. Значение Remote MEPID должно отличаться от значения MEPID.

5.2.6. Автоматическое защитное переключение (APS)

APS - сетевой протокол канального уровня, предназначен для поддержки топологии, исключающей зацикливание трафика, и её перестроение в случае нарушений в кольцевых сетях Ethernet на первом-втором уровне сетевой модели OSI.

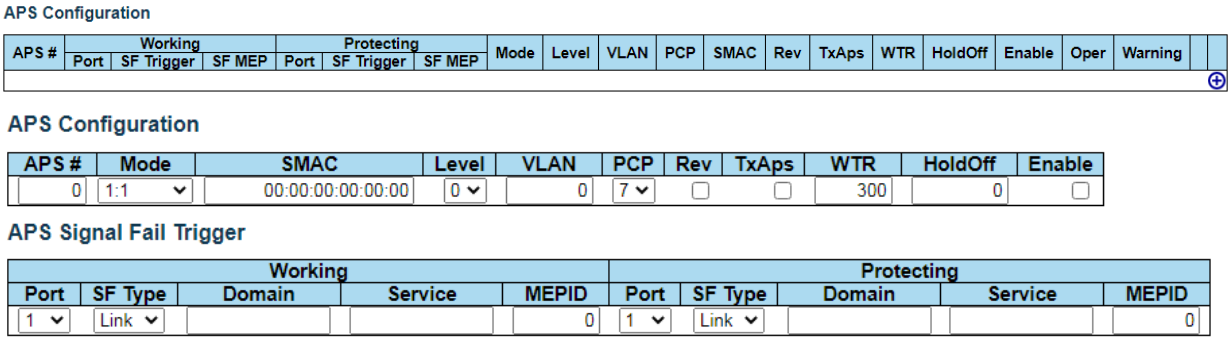


Рис. 5.2.6.1 – настройка автоматического защитного переключения

Таблица 5.2.6.1 - настройка автоматического защитного переключения

APS	Идентификатор APS. Максимальное количество создаваемых экземпляров APS - 10. Щелкните ссылку, чтобы перейти на страницу экземпляра APS, вы можете сбрасывать счетчики и выдавать команды.
Mode	**1: 1** - В линейной архитектуре защитной коммутации 1: 1 защитный транспортный объект выделен рабочему транспортному объекту. Однако нормальный трафик транспортируется либо на рабочем транспортном объекте, либо на защитном транспортном объекте, используя мост селектора в источнике защищенного домена. Селектор в приемнике защищенного домена выбирает объект, который несет нормальный трафик **1 + 1 Bi**– В линейной архитектуре защитной коммутации 1 + 1 для каждого рабочего транспортного объекта выделен защитный транспортный объект. Обычный трафик копируется и направляется как рабочим, так и защитным транспортным

		объектам с постоянным мостом в источнике защищенного домена. Трафик на рабочих и защитных транспортных объектах передается одновременно в приемник защищенного домена, где выбор между рабочим и защитным транспортными объектами осуществляется на основе некоторых заранее определенных критериев, таких как индикация неисправности сервера. **1 + 1 Uni**– однонаправленный APS.
SMAC		MAC-адрес источника, используемый в PDU L-APS. Адрес должен быть одноадресным. Если все нули, будет использоваться MAC-адрес порта коммутатора.
Level		Установка уровня MD / MEG, используемый в L-APS PDU. По умолчанию 0.
VLAN		Установка идентификатора VLAN, используемого в L-APS PDU. При VLAN 0 – не вставлять тег VLAN в PDU LAPS
PCP		Выбор значения PCP в теге VLAN PDU. Не используется без тегов.
Rev		Включение/выключение реверсивного режима, то есть трафик переключается обратно на рабочий порт после устранения условий, вызывающих переключение. В случае сброса команды (например, принудительное переключение) это происходит немедленно. В случае устранения дефекта это обычно происходит по истечении таймера WTR (ожидания восстановления).
TxAps		Выберите, будет ли этот конец передавать блоки PDU APS. Используется только для режима **1 + 1 Uni**– однонаправленный APS
WTR		Настройка ожидания перед восстановлением рабочего порта после устранения неисправности. Допустимый диапазон 1–720
HoldOff		Установка таймера задержки. Когда возникает новый (или более серьезный) дефект, запускается таймер задержки, и о событии будет сообщено после истечения таймера. Время удержания измеряется в миллисекундах, а допустимые значения находятся в диапазоне от 0 до 10000. По умолчанию 0, что означает немедленное сообщение о дефекте.
Enable		Изменение состояния экземпляра APS (включено /выключено)
Working	Port	Выбор интерфейса в качестве рабочего порта
	SF Type	Выбор триггера для сигнала ошибки LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
	Domain	
	Service	
	MEPID	
Protecting	Port	Назначение интерфейса в качестве защищенного порта
	SF Type	Выбор триггера для сигнала ошибки LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP, который должен представлять рабочий поток. Выбранный экземпляр MEP может не существовать при настройке этого APS.
	Domain	
	Service	
	MEPID	

5.2.7. ERPS

ERPS -сетевой протокол, использующийся для исключения образования колец в топологии. Может быть заменой семейству протоколов **STP**.

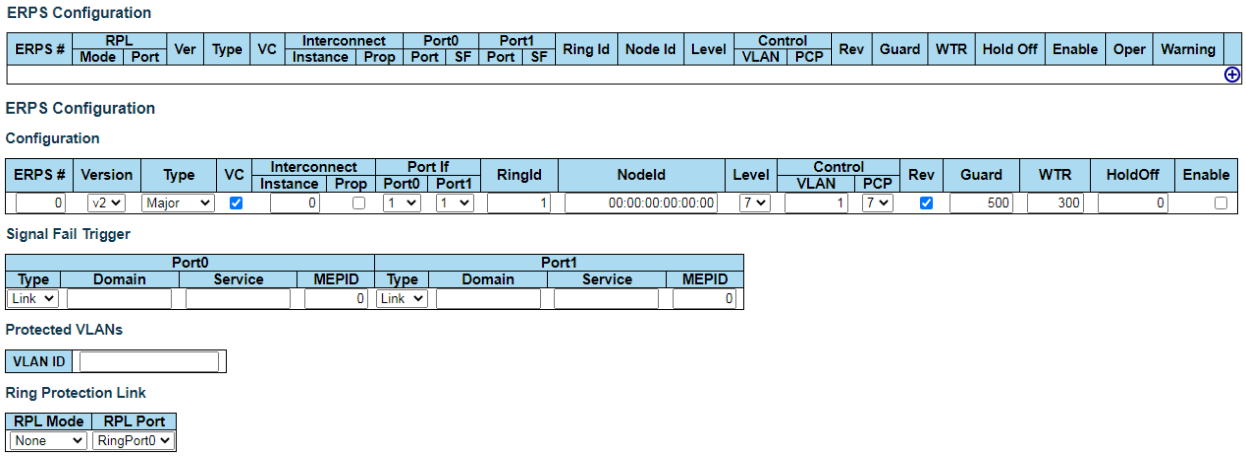


Рис.5.2.7.1 – конфигурация ERPS

Таблица 5.2.7.1 - конфигурация ERPS

ERPS		Идентификатор ERPS. Допустимое значение от 1 до 64 .
Version		Версия протокола ERPS. Поддерживаются версии v1 и v2 .
Type		Тип кольца. Возможные значения: Major: основное кольцо ERPS Sub: Подкольцо ERPS InterSub: подкольцо ERPS на соединительном узле
VC		Включение/выключение виртуального канала R-APS, то есть PDU R-APS не пересылаются между кольцевым портом, если один конец заблокирован
Interconnect	Instance	идентификатор экземпляра кольца, к которому это подкольцо подключено.
	Prop	Определяет, должно ли кольцо, на которое ссылается Interconnect Instance, распространять PDU очистки R-APS всякий раз, когда изменяется топология этого подкольца.
Port If	Port0	Указание интерфейса используемого в качестве порта 0
	Port1	Указание интерфейса используемого в качестве порта 1
RingId		Идентификатор кольца. Используется - вместе с управляющей VLAN - для идентификации блоков PDU R-APS как принадлежащих определенному кольцу.
NodeId		ID узла. Используется внутри конкретного PDU R-APS для уникальной идентификации этого узла (коммутатора) в кольце.
Level		Установка уровня MD / MEG
Control	VLAN	VLAN, по которой блоки PDU R-APS передаются и принимаются на кольцевых портах.
	PCP	Значение PCP, используемое в теге VLAN PDU R-APS
Rev		Включение/выключение режима возврата. Восстановление значений по умолчанию после истечения таймера ожидания восстановления.

Guard		Время защиты в мс. Допустимый диапазон: 10 - 2000 мс.
WTR		Время ожидания восстановления в секундах. Допустимый диапазон 1 - 720 сек.
HoldOff		Время задержки в мс. Значение округляется до точности 100 мс. Допустимый диапазон 0 - 10000 мс.
Enable		Изменение состояния экземпляра ERPS (выключено/включено)
Port0	Type	Настройка триггера сигнализации для порта0. Тип: LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP.
	Domain	
	Service	
	MEPID	
Port1	Type	Настройка триггера сигнализации для порта1. Тип: LINK - В качестве триггера используется состояние порта MEP - В качестве триггера используется mep. Требуется ввод domain, service, mep-id, относящиеся к экземпляру MEP.
	Domain	
	Service	
	MEPID	
VLAN ID		Сети VLAN, защищенные этим экземпляром кольца. По крайней мере, одна VLAN должна быть защищена. Укажите в виде списка номеров vlan или диапазонов vlan, разделенных запятыми. Например: 1,4,7,30-70
RPL Mode		Режим соединения с кольцевой защитой. None: у этого коммутатора нет порта RPL в кольце. Owner: этот коммутатор является владельцем RPL для кольца Neighbor: этот коммутатор является соседом RPL для кольца
RPL Port		Указывает, является ли это портом 0 или 1 каналом защиты кольца. Не используется, если для параметра RPL Mode установлено значение None.

5.2.8. Конфигурирование DHCPv4 сервера

DHCP (протокол динамической настройки узла) – сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации, клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Можно задать диапазон адресов, 28 распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок.

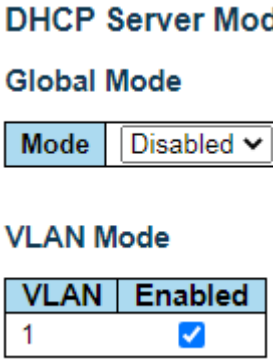


Рис. 5.2.8.1 – DHCP Сервер

Таблица 5.2.8.1 - DHCP Сервер

Mode	Включить/выключить DHCPv4
VLAN	Номер VLAN
Enabled	Включения / отключение DHCP-сервера для соответствующего VLAN.

Исключение групп IP адресов (Рис. 5.2.8.2) (Табл. 5.2.8.2).

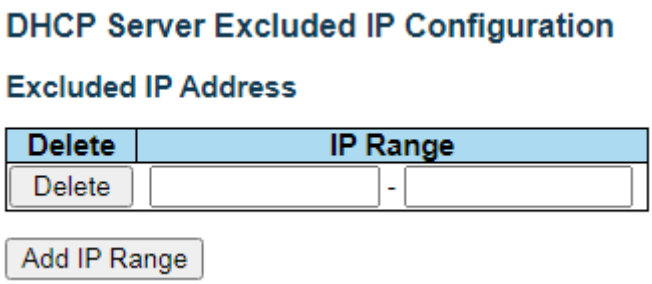


Рис. 5.2.8.2 – Исключение групп IP адресов

Таблица 5.2.8.2 - Исключение групп IP адресов

Delete	Удалить текущий диапазон IP адресов
IP Range	Задать диапазон-группу исключаемых IP адресов. Обычно адреса шлюзов, так как DHCP сервер не должен раздавать адреса шлюзов клиентам
Add IP Range	Добавить диапазон IP адресов

Создание адресных пулов DHCP (Рис. 5.2.8.3) (Табл. 5.2.8.3). При этом методе, DHCP сервер будет выделять IP адрес из пула адресов (иногда называемым диапазоном или областью) на период времени (в аренду), который настраивается.

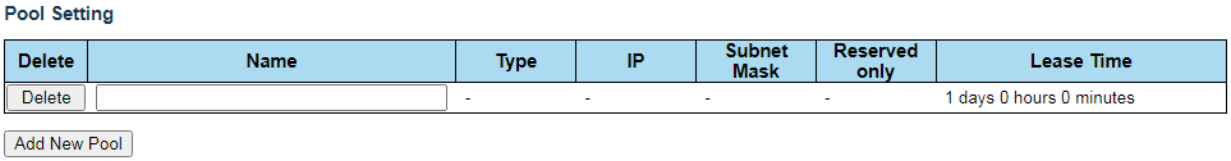


Рис. 5.2.8.3– Адресные пулы DHCP

Таблица 5.2.8.3- Адресные пулы DHCP

Delete	Удалить текущий адресный пул
Name	Имя пула
Type	Тип узла для клиента NetBIOS Node Type. Здесь могут быть следующие значения: b – broadcast, p - peer-to-peer, m – mixed, h – hybrid от этого зависит порядок преобразования имени в IP для клиентов сети Microsoft.
IP	IP адрес, диапазон
Subnet Mask	Маска подсети
Reserved only	Только зарезервированные адреса. Если этот параметр включен, IP-адреса, которые можно выбрать из пула, ограничиваются теми, которые введены в таблицу зарезервированных записей.

Lease Time	Время аренды адреса. По умолчанию время аренды равно 24 часам. Можно выставить свое время аренды.

DHCP snooping (Рис. 5.2.8.4) (Табл. 5.2.8.4). DHCP snooping (Отслеживание DHCP) – защитная функция, позволяющая предотвратить несанкционированное подключение к сети стороннего DHCP сервера с целью перехвата клиентских DHCP запросов. Сущность DHCP snooping заключается в том, чтобы закрыть возможность обработки DHCP запросов на недоверенных портах. Администратор сети должен вручную настроить доверенные порты, - порты, за которыми находится настоящий DHCP сервер.

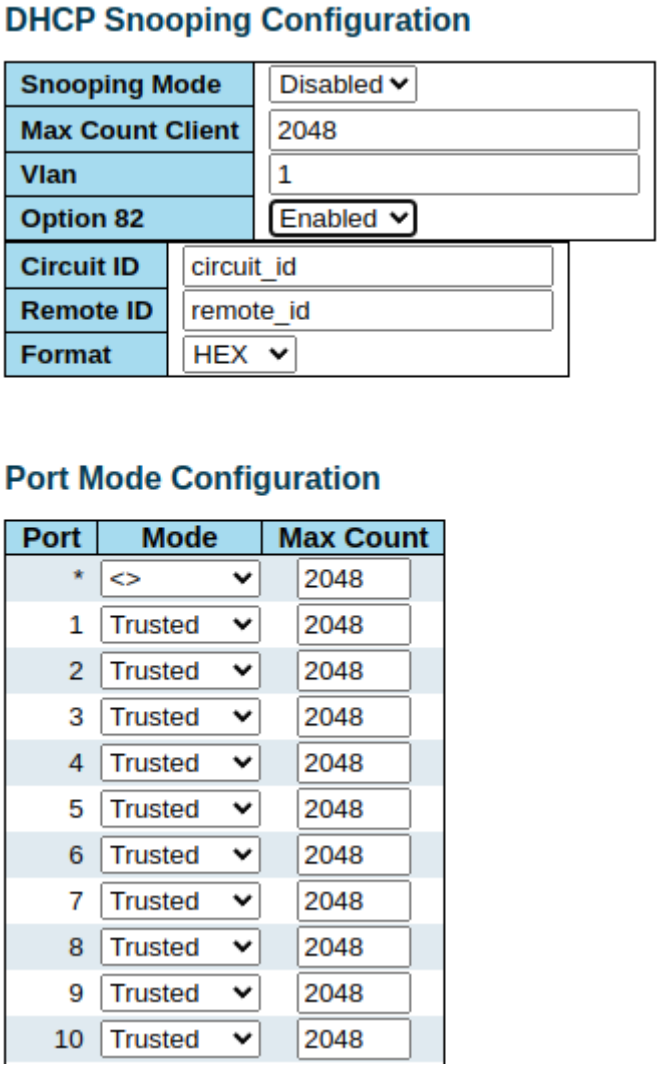


Рис. 5.2.8.4 – DHCP snooping

Таблица 5.2.8.4 - DHCP snooping

Snooping mode	Включение/выключение функции DHCP snooping
Max Count Client	Максимальное количество клиентов
Vlan	Номер vlan
Option 82	Включение/выключение опции 82
Circuit ID	Идентификатор порта коммутатора
Remote ID	Идентификатор коммутатора

Format	Формат опции 82 HEX/ascii
Port	Номер порта
Mode	Режим для порта: • Ненадёжный (Untrusted) – порт, к которому подключен клиент. DHCP-ответы, приходящие с этого порта, отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database). • Доверенный (Trusted) – порт коммутатора, к которому подключен другой коммутатор или DHCPсервер. DHCP-пакеты, полученные с доверенного порта, не отбрасываются.
Max Count	Максимальное количество клиентов

DHCP Relay (Рис. 5.2.8.5) (Табл. 5.2.8.5). Настройка DHCP Relay позволяет коммутатору переадресовывать запросы от DHCP-клиента к другому DHCP серверу (например, старшему в иерархии сети).

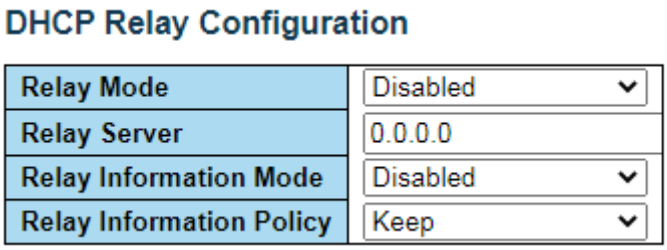


Рис. 5.2.8.5 – DHCP Relay

Таблица 5.2.8.5 - DHCP Relay

Relay Mode	Включение/выключение функции DHCP Relay
Relay Server	Адрес DHCP сервера
Relay Information Mode	Включение/выключение режима выбора действия, которое необходимо выполнить, если пересылаемое сообщение уже содержит информацию о переадресации
Relay Information Policy	Действие: Keep – информация не меняется; Replace – информация перезаписывается. Drop – отбросить пакет.

5.2.9. DHCPv6

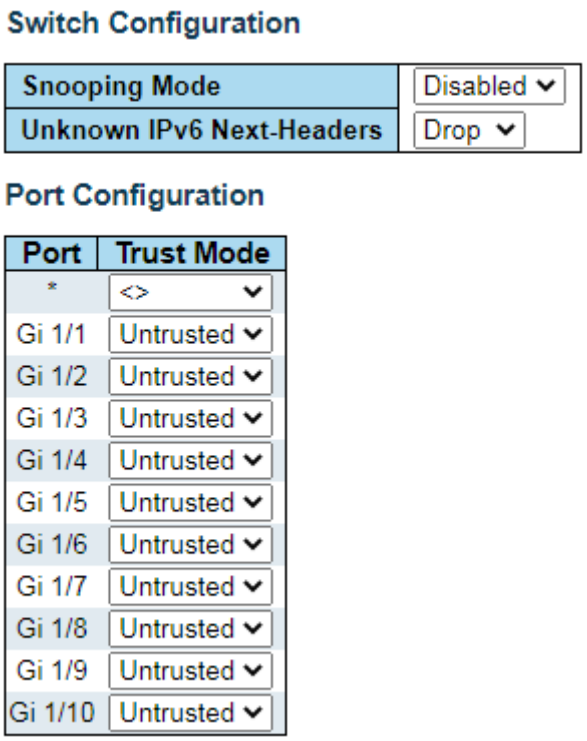


Рис. 5.2.9.1 – DHCPv6

Таблица 5.2.9.1 - DHCPv6

Snooping Mode	Включение/выключение функции DHCPv6 snooping
Unknown IPv6 Next-Headers	Выбор обработки неизвестных значений заголовка IPv6. Коммутатор должен анализировать все пакеты IPv6 для клиента DHCPv6, чтобы определить, действительно ли это сообщение DHCPv6 Возможные варианты: drop- Отбрасывать пакеты с неизвестными заголовками расширения IPv6. Это наиболее безопасный вариант, но он может привести к перебоям в трафике. allow-Разрешить пакеты с неизвестными заголовками расширения IPv6. Это менее безопасный вариант, но он предотвращает перебои в трафике.
Port	Номер порта
Trust Mode	Режим для порта: • Ненадёжный (Untrusted) – порт, к которому подключен клиент. DHCP-ответы, приходящие с этого порта, отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database). • Доверенный (Trusted) – порт коммутатора, к которому подключен другой коммутатор или DHC Pсервер. DHCP-пакеты, полученные с доверенного порта, не отбрасываются.

DHCPv6 Relay (Рис. 5.2.9.2) (Табл. 5.2.9.2). Настройка DHCPv6 Relay для vlan

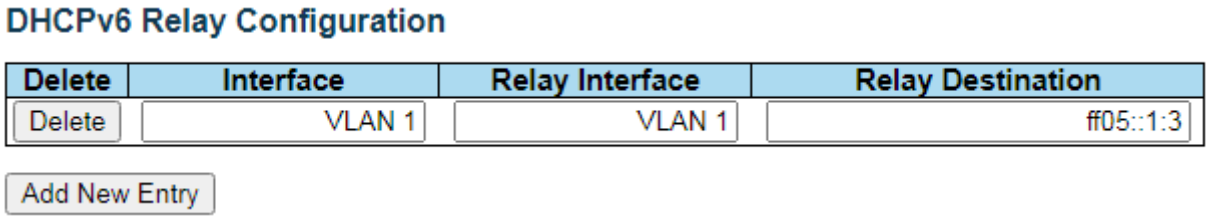


Рис. 5.2.9.2– DHCPv6 Relay

Таблица 5.2.9.2– DHCPv6 Relay

Delete	Удалить текущую запись
Interface	Номер интерфейса
Relay Interface	Номер интерфейса, используемый для ретрансляции.
Relay Destination	Адрес IPv6, представленный в виде удобочитаемого теста, как указано в RFC5952. IPv6-адрес сервера DHCPv6, на который должны быть ретранслированы запросы. Значение по умолчанию «ff05 :: 1: 3» означает «любой DHCP-сервер».

5.2.10. Конфигурация пользователей. Users Configuration.

Для управления учетными записями пользователей необходимо перейти по вкладке Configuration→Security→Switch→Users. На этой странице представлен обзор текущих пользователей (Рис. 5.2.10.1) (Табл. 5.2.10.1).

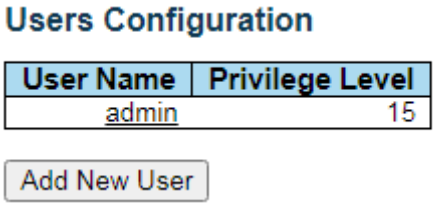


Рис. 5.2.10.1 – Конфигурация пользователей

Таблица 5.2.10.1 – Конфигурация пользователей

User Name	Имя пользователя
Privilege Level	Уровень привилегий пользователя. Допустимый диапазон: от 0 до 15. Как правило, уровень привилегий 15 используется для учетной записи администратора, уровень привилегий 10 для стандартной учетной записи пользователя и уровень привилегий 5 для учетной записи наблюдателя.

Кнопка 

предназначена для добавления новых пользователей (Рис. 5.2.10.2) (Табл. 5.2.10.2).

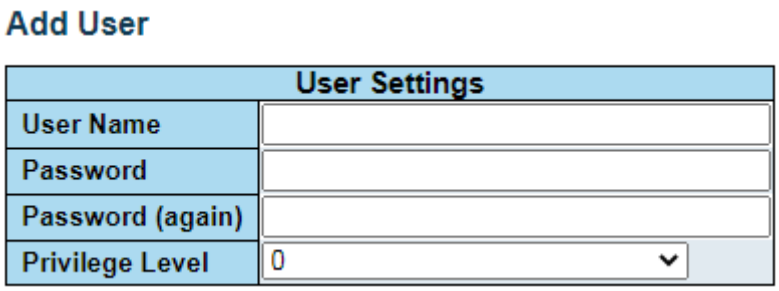


Рис. 5.2.10.2 – Добавление пользователей

Таблица 5.2.10.2 – Добавление пользователей

User Name	Имя пользователя
Password	Пароль
Password (again)	Повтор пароля
Privilege Level	Уровень привилегий пользователя от 0 до 15.

5.2.11. Уровни привилегий. Privilege Levels

Для доступа к настройкам уровней привилегий необходимо перейти по вкладке Configuration→Security→Switch→ Privilege Levels. На этой странице представлен обзор текущих уровней привилегий (Рис. 5.2.11.1) (Табл. 5.2.11.1).

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Alarm	5	10	5	10
APS	5	10	5	10
CFM	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Miscellaneous	15	15	15	15
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
PTP	5	10	5	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UDLD	5	10	5	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Рис. 5.2.11.1 – Уровни привилегий

Таблица 5.2.11.1 – Уровни привилегий

Group Name	Имя, идентифицирующее группу привилегий. В большинстве случаев группа состоит из одного модуля (например, LACP, RSTP или QoS), но

		некоторые содержат более одного. Группы в деталях: -System: Contact, Name, Location, Timezone, Daylight Saving Time, Log; -Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard; -IP: все, кроме ping; -Ports: все, кроме VeriPHY; -Diagnostics: ping и VeriPHY; - Maintenance: CLI - System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web - Users, Privilege Levels и все в Maintenance; -Debug: присутствует только в CLI.	
Privilege Levels	Configuration Read-only	Конфигурация: только чтение	Уровень привилегий группы от 0 до 15. Привилегия пользователя должна быть такой же или больше, чем уровень этой группы, чтобы иметь доступ к этой группе.
	Configuration/Execute Read/write	Конфигурация: чтение и запись	
	Status/Statistics Read-only	Статус/статистика: только чтение	
	Status/Statistics Read/write	Статус/статистика: чтение и запись	

5.2.12. Конфигурация аутентификации, авторизации и учета. Authentication, Authorization, Accounting

Для доступа к настройкам аутентификации, авторизации и учета необходимо перейти по вкладке Configuration→Security→Switch→Auth Method. Authentication (аутентификация) – сопоставление запроса существующей учётной записи в системе безопасности. Authorization (авторизация, проверка уровня доступа) – сопоставление учётной записи в системе (прошедшей аутентификацию) и определённых полномочий. Accounting (учёт) – слежение за потреблением ресурсов пользователем. На этой странице представлен обзор текущих параметров аутентификации, авторизации и учета (Рис. 5.2.12.1) (Табл. 5.2.12.1).

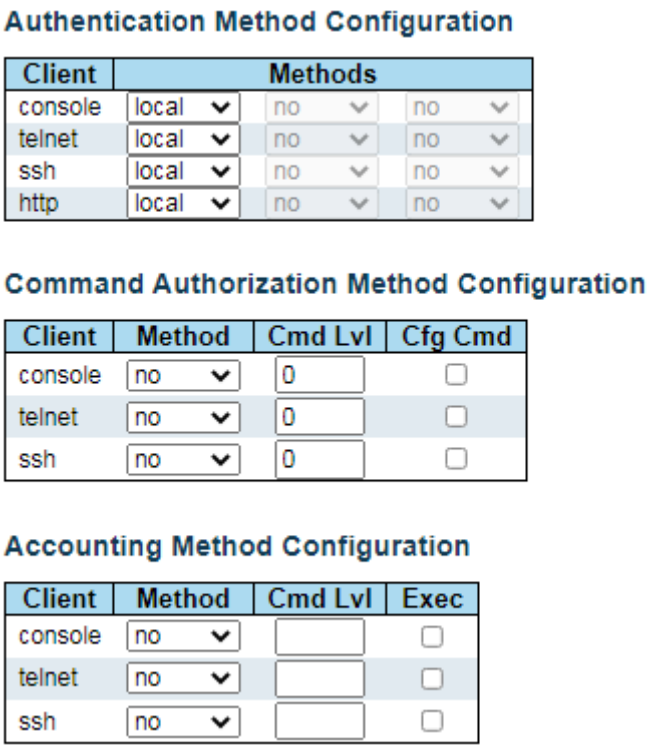


Рис. 5.2.12.1 – Конфигурация аутентификации, авторизации и учета

Таблица 5.2.12.1 – Конфигурация аутентификации, авторизации и учета

Authentication Method Configuration	Client	Клиент: console, telnet, SSH, http
	Methods	- no: аутентификация отключена, и вход в систему невозможен; 35 - local: использовать локальную базу данных на коммутаторе для проверки подлинности; - radius: использовать удаленные серверы RADIUS для аутентификации; - tacacs: использовать удаленные серверы TACACS для аутентификации; Доступность метода проверяется слева направо.
Command Authorization Method Configuration	Client	Клиент: console, telnet, ssh
	Method	- no: авторизация команд отключена. Пользователь получает доступ к командам CLI в соответствии со своим уровнем привилегий. - tacacs: для авторизации команд используется один или несколько удаленных серверов TACACS+. Если все удаленные серверы находятся в автономном режиме, пользователю предоставляется доступ к командам CLI в соответствии с его уровнем привилегий.
	Cmd Lvl	Авторизовать все команды с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15.
	Cfg Cmd	Авторизовать команды конфигурации
Accounting Method Configuration	Client	Клиент: console, telnet, ssh
	Methods	- no: учет отключен; - tacacs: для учета используется один или несколько удаленных серверов TACACS+
	Cmd Lvl	Включает учет всех команд с уровнем привилегий выше или равным этому уровню. Допустимые значения находятся в диапазоне от 0 до 15. Оставьте поле пустым, чтобы отключить учет команд.

	Exec	Режим учета EXEC

5.2.13. Конфигурация SSH

Для доступа к настройкам SSH необходимо перейти по вкладке Configuration→Security→Switch→ SSH. На этой странице представлен обзор текущих параметров SSH. Параметр Mode указывает режим работы SSH.

5.2.14. Конфигурация HTTPS

Для доступа к настройкам HTTPS необходимо перейти по вкладке Configuration→Security→Switch→HTTPS. На этой странице представлен обзор текущих параметров HTTPS (Рис. 5.2.14.1) (Табл. 5.2.14.1).

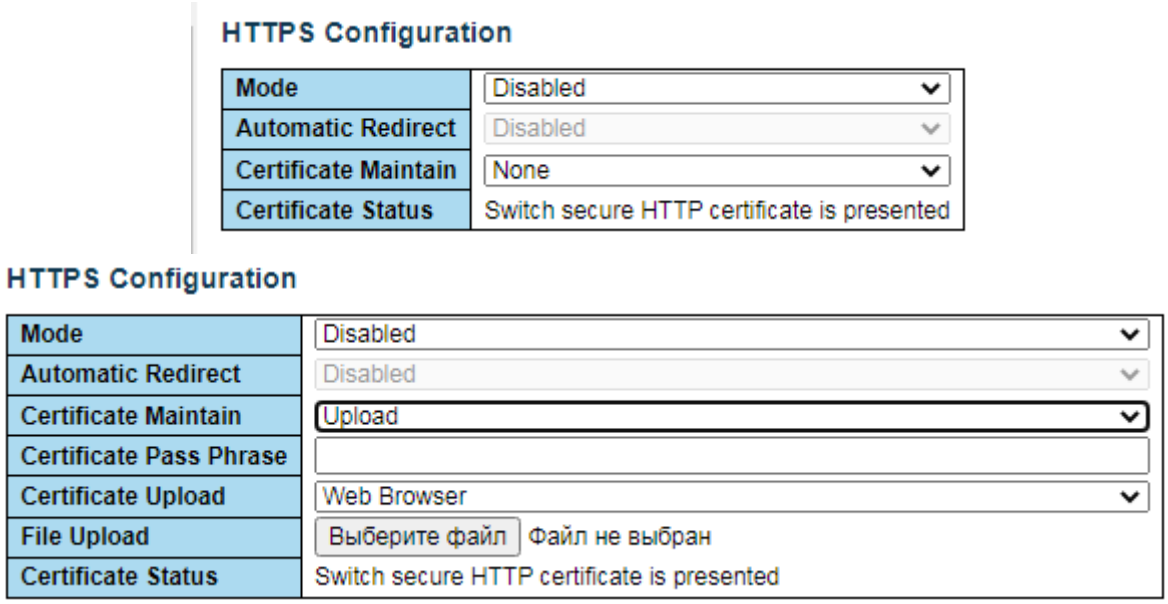


Рис. 5.2.14.1 – Конфигурация HTTPS

Таблица 5.2.14.1 – Конфигурация HTTPS

Mode	Режим работы HTTPS. Когда текущее соединение HTTPS, но HTTPS выключен, web-браузер будет автоматически перенаправляться на соединение HTTP.
Automatic Redirect	Режим работы автоматического перенаправления HTTPS. Применяется только, если для режима работы HTTPS выбрано "Enabled" (Включен). Автоматически направляет HTTP web-браузера на соединение HTTPS, когда включены оба режима работы – HTTPS и Automatic Redirect
Certificate Maintain	Это поле может быть настроено только при отключенном HTTPS. Оно используется для обслуживания сертификации. Возможные действия: - None: никаких действий сертификации; - Delete: удалить сертификат; - Upload: загрузка сертификата, можно выбрать два метода загрузки; - Generate: создание сертификата.
Certificate Algorithm	Алгоритм сертификации. Возможные типы: DSA, RSA.
Certificate Status	Статус сертификации. Возможный статус: 37 - Выдается защищенный сертификат HTTP. Сертификат хранится в базе данных HTTPS; - Сертификат безопасного переключения SSL не представлен: сертификат не хранится в базе данных HTTPS. -

	Выдача защищенного сертификата HTTP. Генерируется сертификат
Pass Phrase	Шаблон для шифровки сертификата
Certificate Upload	Загрузка сертификата. Возможные режимы: - Web Browserr: загрузка сертификата через веб - браузер; - URL: для загрузки сертификата через URL
File Upload	Файл для загрузки

5.2.15. Конфигурация управления доступом. Access Management Configuration

Для доступа к конфигурации управления доступом необходимо перейти по вкладке Configuration→Security→Switch→ Access Management. На этой странице можно настроить таблицу управления доступом (Рис. 5.2.15.1) (Табл. 5.2.15.1). Максимальное число элементов списка 16. Если тип приложения совпадает с одним из типов, имеющимся в списке управления доступом, то доступ к коммутатору будет разрешен.

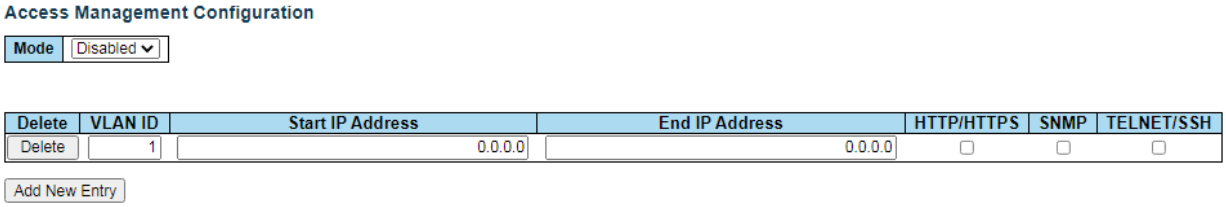


Рис. 5.2.15.1 – Конфигурация управления доступом

Таблица 5.2.15.1 – Конфигурация управления доступом

Mode	Включение/выключение
Delete	Удалить текущую запись
VLAN ID	Номер VLAN для элемента управления доступом
Start IP Address	Начальный IP-адрес для элемента управления доступом
End IP Address	Конечный IP-адрес для элемента управления доступом
SNMP	Если в этом поле установлен флаг, это указывает, что хосту с IP-адресом из указанного диапазона может быть предоставлен доступ к коммутатору по SNMP.
TELNET/SSH	Если в этом поле установлен флаг, это указывает, что хосту с IP-адресом из указанного диапазона может быть предоставлен доступ по TELNET/SSH

Кнопка 

служит для добавления новой записи.

5.2.16. SNMP

Для доступа к конфигурации SNMP необходимо перейти по вкладке Configuration→Security→Switch→ SNMP.

SNMP System Configuration (Системные настройки SNMP) (Рис. 5.2.16.1) (Табл. 5.2.16.1).

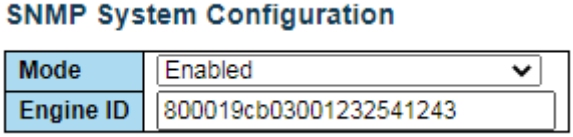


Рис. 5.2.16.1 – Системные настройки SNMP

Таблица 5.2.16.1– Системные настройки SNMP

Mode	Режим работы SNMP
Engine ID	Идентификатор engine ID для SNMPv3. Строка должна содержать четное число (в 16-ном формате), число 39 цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы.

Trap Configuration (Настройки сигнализации) (Рис. 5.2.16.2) (Табл. 5.2.16.2).

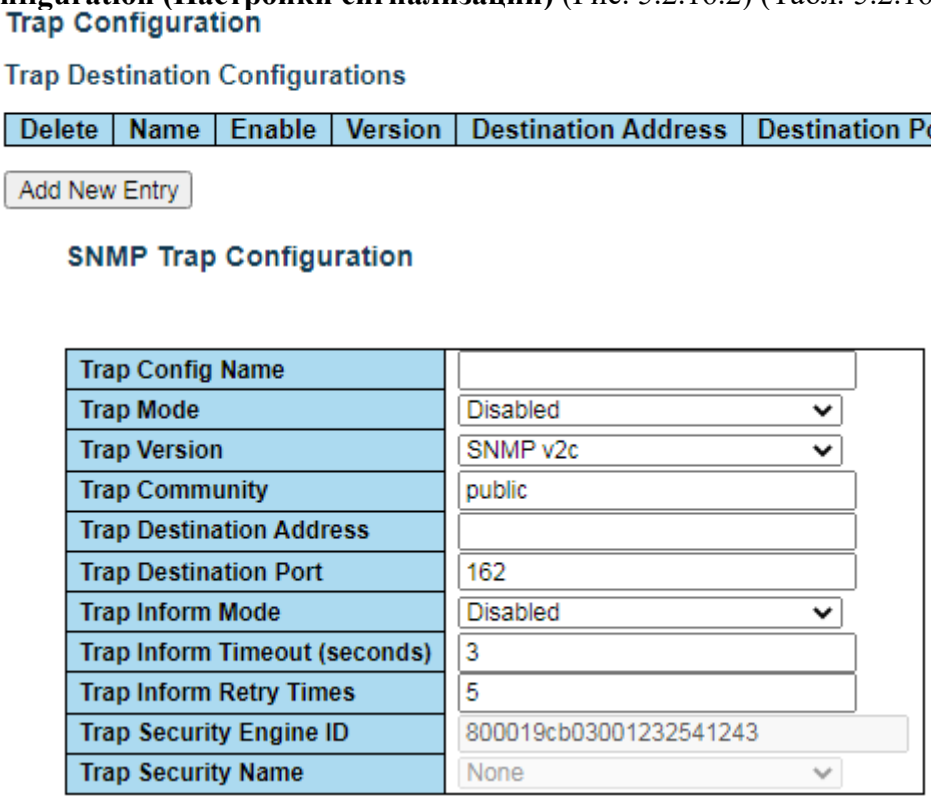


Рис. 5.2.16.2 – Настройки сигнализации

Таблица 5.2.16.2 – Настройки сигнализации

Mode	Включить/выключить отправку SNMP trap
Trap Config Name	Имя конфигурации
Trap Version	Поддерживаемая версия SNMP trap. (SNMP 1/ SNMP v2c/SNMP 3)
Trap Community	Строка доступа community для отправки пакета SNMP trap.
Trap Destination Address	IP-адрес сервера для отправки SNMP trap. Корректный IP-адрес в десятичном формате с точкой. Допустимо также указать корректное имя хоста.
Trap Destination port	Порт назначения SNMP trap. SNMP-агент будет посылать сообщения SNMP на этот порт; диапазон номеров портов 1~65535. По умолчанию порт для сообщений SNMP trap имеет номер 162.
Trap Inform Mode	Включить/выключить режим работы SNMP trap inform
Trap Inform Timeout	Таймер сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 2147.
Trap Inform Retry Times	Таймер попыток повторения сообщений SNMP trap inform. Диапазон допустимых значений: от 0 до 255

Trap Security Engine ID	Режим работы SNMP trap security engine ID. Протокол SNMP v3 посылает сообщения trap и inform, использующие USM для аутентификации и обеспечения конфиденциальности. Сообщениям назначается уникальный идентификатор engine ID и необходимая информация. Если включен режим "Trap Probe Security Engine ID", идентификатор (ID) будет генерироваться автоматически. В противном случае, будет использован ID, указанный в этом поле. Строка должна содержать четное число (в 16-ном формате), число цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы
Trap Security Name	Имя SNMP trap security name. Сообщения SNMP trap и inform SNMP v3 используют USM для аутентификации и обеспечения конфиденциальности. Когда включен режим отправки trap и inform, необходимо задать уникальное имя для обеспечения безопасности.

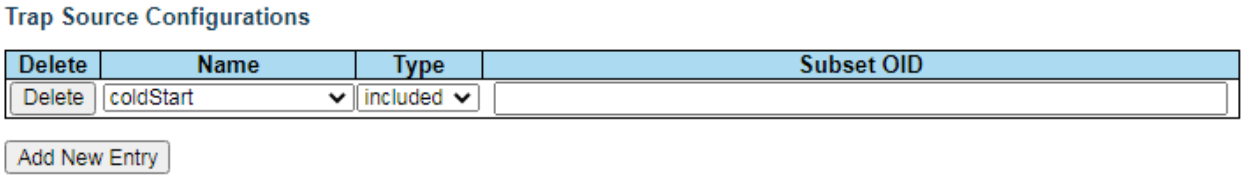


Рис. 5.2.16.3– Trap Source Configurations

Таблица 5.2.16.3– Trap Source Configurations

Delete	Удаление текущей записи.
Name	Указывает имя записи.
Type	Тип фильтра для записи (включить или исключить)
Subset OID	Подмножество OID для записи. Значение должно зависеть от того, какое имя указано в поле Name. Например, ifIdex – это OID подмножества для linkUp и linkDown. Допустимый OID подмножества – это одно или несколько цифровых чисел (0-4294967295) или звездочка (*), разделенных точками (.). Первый символ не должен начинаться со звездочки (*), а максимальное количество OID не должно превышать 128.

SNMPv3 Community Configuration (Настройка SNMPv3Community) (Рис. 5.2.16.4) (Табл. 5.2.16.4).

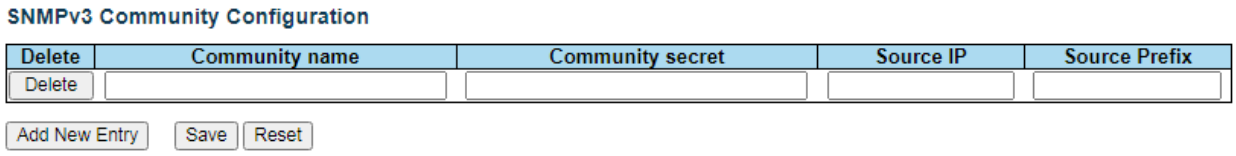


Рис. 5.2.16.4– Настройка SNMP v3 Community

Таблица 5.2.16.4 – Настройка SNMP v3 Community

Delete	Удаление текущей записи.
Community name	Указывает имя безопасности для сопоставления сообщества с конфигурацией групп SNMP. Допустимая длина строки составляет от 1 до 32, а допустимое содержимое - символы ASCII от 33 до 126.
Community secret	Пароль сообщества (строку доступа) для разрешения доступа с

	использованием SNMPv1 и SNMPv2c к агенту SNMP. Допустимая длина строки составляет от 1 до 32, а допустимое содержимое - символы ASCII от 33 до 126.
Source IP	IP-адрес источника при доступе по SNMP
Source Prefix	префикс адреса источника.

Кнопка 

служит для добавления новой записи.

SNMP v3 User Configuration (Пользовательская настройка SNMP v3) (Рис. 5.2.16.5) (Табл. 5.2.16.5).

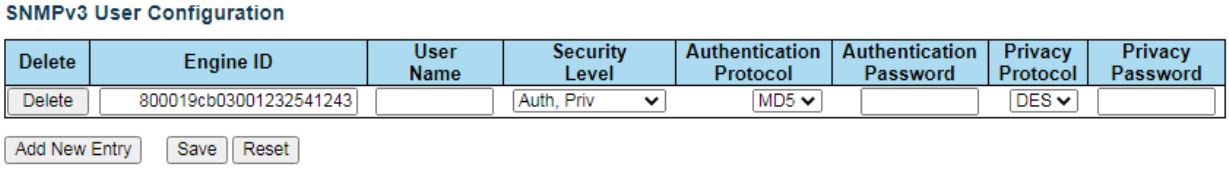


Рис. 5.2.16.5 – Пользовательская настройка SNMP v3

Таблица 5.2.16.5 – Пользовательская настройка SNMP v3

Delete	Удаление текущей записи.
Engine ID	Строка, идентифицирующая engine ID, которому принадлежит этот элемент списка. Строка должна содержать четное число (в 16-чном формате), число цифр от 10 до 64; комбинации цифр, состоящие из одних нулей и из одних «F» недопустимы. В архитектуре SNMPv3 используется модель безопасности на основе пользователя USM (User based Security Model) для обеспечения безопасности сообщений и модель управления доступом на основе вида VACM (View-based Access Control Model) при управлении доступом. Для входа USM ключами входов являются usmUserEngineID и usmUserName. В простом агенте usmUserEngineID всегда совпадает с собственным значением snmpEngineID агента. В качестве значения также может использоваться значение snmpEngineID удаленного устройства (SNMP engine), с которым может связываться данный пользователь. Другими словами, если engine ID пользователя равен engine ID системы, то он является локальным пользователем, в противном случае пользователь является удаленным.
User Name	Строка, идентифицирующая имя пользователя, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с 43 номерами в диапазоне от 0x21 до 0x7E
Security Level	Модель безопасности, которой принадлежит данный параметр. Возможны следующие модели безопасности: • NoAuth, NoPriv: Аутентификация и конфиденциальность отсутствуют. • Auth, NoPriv: выполняется аутентификация, конфиденциальность отсутствует. • Auth, Priv: выполняется аутентификация, обеспечивается конфиденциальность. Если параметр уже существует, значение уровня безопасности изменить невозможно. Это означает, что сначала надо удостовериться, что значение установлено правильно.
Authentication Protocol	Протокол аутентификации, которому принадлежит данный параметр. Возможны следующие протоколы аутентификации: • MD5: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации MD5. • SHA: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации SHA. Если параметр уже существует, значение уровня безопасности изменить невозможно. Это

	означает, что сначала надо удостовериться, что значение установлено правильно.
Authentication Password	Строка, идентифицирующая фразу пароля аутентификации. Допустимая длина строки для протокола аутентификации MD5: от 8 до 32 символов. Допустимая длина строки для протокола аутентификации SHA: от 8 до 40 символов. При записи строки аутентификации могут использоваться символы ASCII с кодами в диапазоне от 0x21 до 0x7E.
Privacy Protocol	Протокол конфиденциальности, которому принадлежит данный вход. Возможны следующие протоколы конфиденциальности: • AES: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации AES. • DES: дополнительный флаг, указывающий, что пользователь использует протокол аутентификации DES.
Privacy Password	Строка, идентифицирующая фразу пароля конфиденциальности. Допустимая длина строки 8~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

Кнопка 

служит для добавления новой записи.

SNMP v3 Group Configuration (Настройки группы SNMP v3) (Рис. 5.2.16.6) (Табл. 5.2.16.6).

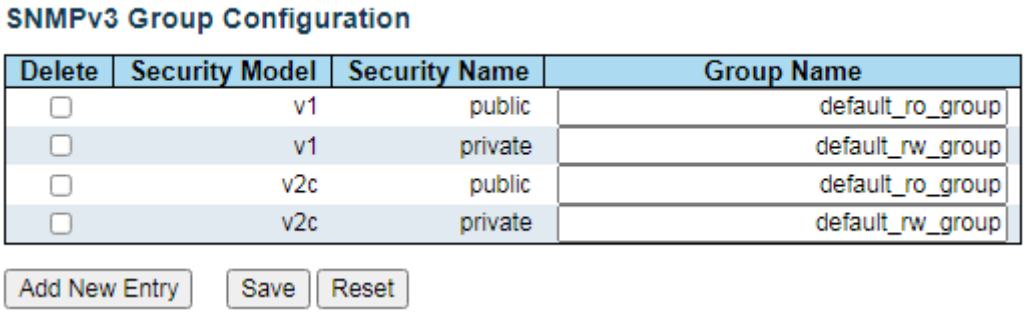


Рис. 5.2.16.6 – Настройки группы SNMP v3

Таблица 5.2.16.6 – Настройки группы SNMP v3

Delete	Удаление текущей записи.
Security Model	Модель безопасности, которой принадлежит данный параметр. Возможны следующие модели безопасности: • v1: зарезервировано для SNMPv1. • v2c: зарезервировано для SNMPv2c. • usm: модель безопасности на основе пользователя USM (User-based Security Model) для SNMPv3.
Security Name	Строка, идентифицирующая безопасное имя, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
Group Name	Строка, идентифицирующая имя группы, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

Кнопка 

служит для добавления новой записи.

SNMPv3 View Configuration (Настройка вида SNMP v3) (Рис. 6.2.16.7) (Табл. 6.2.16.7).

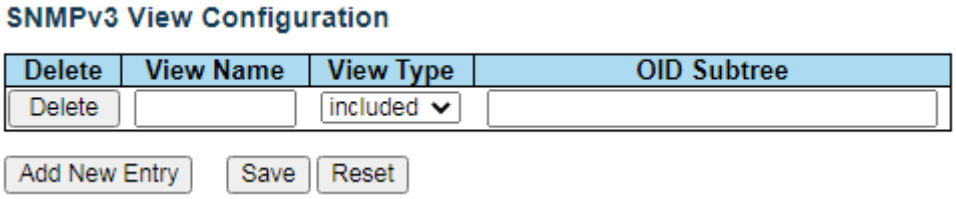


Рис. 5.2.16.7– Настройка вида SNMP v3

Таблица 5.2.16.7 – Настройка вида SNMP v3

Delete	Удаление текущей записи.
View Name	Строка, идентифицирующая имя вида, которому принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
View Type	Тип вида, которому принадлежит данный параметр. Возможны следующие типы видов: • included (поддерево включено): дополнительный флаг, указывающий, что в вид должно быть включено поддерево. • excluded (поддерево исключено): дополнительный флаг, указывающий, что из вида должно быть исключено поддерево. В целом, если для типа вида задано ' excluded ' (поддерево исключено), должен существовать другой вид с типом ' included ' (поддерево включено) и его поддерево OID должно перекрывать поддерево вида с типом ' excluded ' (поддерево исключено).
OID Subtree	OID определяет корень поддерева, добавляемый к именованному виду. Диапазон допустимых значений OID: от 1 до 128. В строке можно указать либо число, состоящее из цифр, либо звездочку (*).

Кнопка 

служит для добавления новой записи.

SNMPv3 Access Configuration (Настройка доступа SNMPv3) (Рис. 5.2.16.8) (Табл. 5.2.16.8).

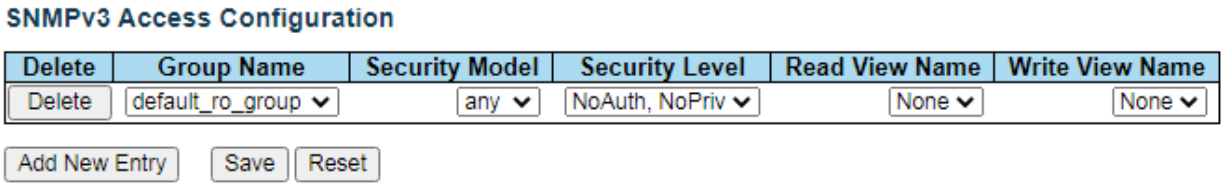


Рис. 5.2.16.8 – Настройка доступа SNMP v3

Таблица 5.2.16.8 – Настройка доступа SNMP v3

Delete	Удаление текущей записи.
Group Name	Строка, идентифицирующая имя группы, которой принадлежит данный параметр. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
Security Model	Модель безопасности, которой принадлежит данный параметр. Возможны следующие модели безопасности: • any (любая): будет принята любая модель безопасности (v1|v2c|usm). • v1: зарезервировано для SNMPv1. • v2c: зарезервировано для SNMPv2c. • usm: модель безопасности на основе пользователя USM (User-based Security Model) для SNMPv3.
Security Level	Уровень безопасности, которому принадлежит данный параметр. Возможны следующие модели безопасности:

	• NoAuth, NoPriv: Аутентификация и конфиденциальность отсутствуют. • Auth, NoPriv: выполняется аутентификация, конфиденциальность отсутствует. • Auth, Priv: выполняется аутентификация, обеспечивается конфиденциальность.
Read View Name	Имя вида при чтении, имя вида MIB, определяющего объекты MIB, для которых данный запрос может быть запросом текущих значений. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.
Write View Name	Имя вида при записи, имя вида MIB, определяющего объекты MIB, для которых данный запрос потенциально может установить новые значения. Допустимая длина строки 1~32 символов ASCII с номерами в диапазоне от 0x21 до 0x7E.

Кнопка 

служит для добавления новой записи.

5.2.17. RMON

Для доступа к конфигурации RMON необходимо перейти по вкладке Configuration→Security→Switch→ RMON.

RMON Statistics Configuration (Настройка статистик RMON) (Рис. 5.2.17.1) (Табл. 5.2.17.1).

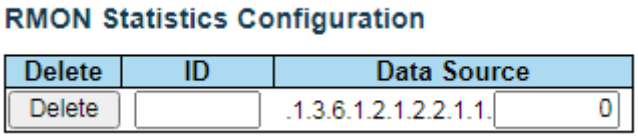


Рис. 5.2.17.1 – Настройка статистик RMON

Таблица 5.2.17.1 – Настройка статистик RMON

Delete	Удаление текущей записи.
ID	Индекс входа. Допустимые значения – от 1 до 65535.
Data Source	ID порта, мониторинг которого требуется осуществлять.

Кнопка 

служит для добавления новой записи.

RMON History Configuration (Настройка журнала RMON) (Рис. 5.2.17.2) (Табл. 5.2.17.2).

На странице RMON History Configuration можно настроить сбор статистики на физическом интерфейсе для мониторинга использования сети, типов пакетов и ошибок. Записи журнала RMON можно использовать при мониторинге спорадически возникающих проблем.

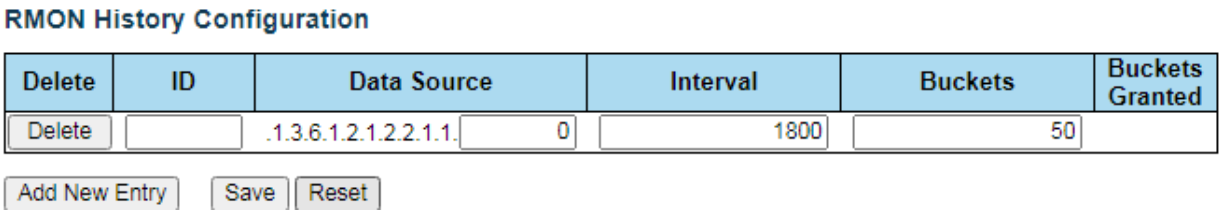


Рис. 5.2.17.2– Настройка журнала RMON

Таблица 5.2.17.2– Настройка журнала RMON

Delete	Удаление текущей записи.
ID	Индекс входа. Допустимые значения – от 1 до 65535.
Data Source	ID порта, мониторинг которого требуется осуществлять.
Interval	Интервал опроса. По умолчанию 1800 секунд. Диапазон допустимых значений: от 1 до 3600 секунд.
Buckets	Число сегментов, требуемых для этого параметра. По умолчанию 50. Диапазон допустимых значений: от 1 до 3600.
Buckets Granted	Предполагаемое число сегментов.

Кнопка 

служит для добавления новой записи.

RMON Alarm Configuration (Настройка сигнализаций RMON) (Рис. 5.2.17.3) (Табл. 5.2.17.3)

На этой странице можно задать конкретный критерий, согласно которому будут генерироваться события. Он может быть установлен для данных теста, собранных за любой указанный интервал времени. Можно контролировать как абсолютные значения, так и их изменения. Можно также задать сигнализации, которые будут выдаваться при превышении пороговых значений либо при снижении ниже пороговых значений.

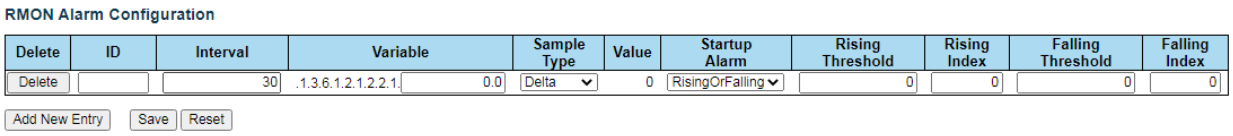


Рис. 5.2.17.3 – Настройка сигнализаций RMON

Таблица 5.2.17.3 – Настройка сигнализаций RMON

Delete	Удаление текущей записи.
ID	Индекс входа. Допустимые значения – от 1 до 65535.
Interval	Интервал опроса при выборке и сравнении с нижним или верхним пороговым значением. Диапазон от 1 до 2^31 секунд.
Variable	Номер объекта переменной MIB, из которой берутся выборки. Выборки могут браться только из переменной ifEntry.n.n . Возможны следующие переменные: InOctets, InUcastPkts, InNUcastPkts, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPkts, OutNUcastPkts, OutDiscards, OutErrors и OutQLen.
Sample type	Тип выборки. Для указанной переменной тест может быть выполнен для абсолютных значений или их относительного изменения.
Value	Статистическое значение в течение последнего периода выборки.
Startup Alarm	Выбирает метод, который будет использоваться для выборки выбранной переменной и вычисления значения, которое сравнивается с пороговыми значениями.
Rising Threshold	Включает сигнализацию, когда значение первый раз превысит пороговое значение подъема либо станет меньше, чем пороговое значение спада.
Rising Index	Индекс подъема для события. Диапазон 1~65535.
Falling Threshold	Пороговое значение спада. Если текущее значение станет меньше порогового значения спада и, при этом, последнее значение выборки больше этого порогового значения, то выдается сигнализация. После генерации события спада, другое такое событие не будет сгенерировано до тех пор, пока значение выборки не станет больше

	порогового значения спада, достигнет порогового значения подъема и снова вернется к пороговому значению спада. (Диапазон: от -2147483647 до 2147483647).
Falling Index	Индекс спада для события. Диапазон 1~65535.

Кнопка Add New Entry служит для добавления новой записи.

RMON Event Configuration (Настройка событий RMON) (Рис. 5.2.17.4) (Табл. 5.2.17.4).
На этой странице можно задать операцию, которая выполняется при выдаче сигнализации.

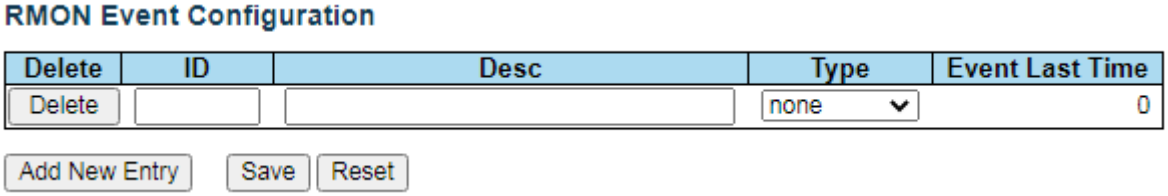


Рис. 5.2.17.4 – Настройка событий RMON

Таблица 5.2.17.4 – Настройка событий RMON

Delete	Удаление текущей записи.
ID	Индекс ID. Диапазон 1~65535.
Desc	Введите в это поле описание для данного входа.
Type	Выберите тип события, которое будет выбираться при срабатывании сигнализации: • None (Нет): Событие сгенерировано не будет. • Log (Журнал): когда генерируется событие, генерируется и запись журнала RMON. • snmptrap: посылает сообщение trap всем установленным менеджерам сообщений trap. • logandtrap: о событии создается запись в журнале, посылается сообщение trap.
Event Last Time	Время последнего события. Значение sysUpTime, когда событие для этого входа было сгенерировано последний раз.

Кнопка Add New Entry служит для добавления новой записи.

5.2.18. Network. Сеть

Port Security Limit Control Configuration. Управление безопасности порта

Функция управлением безопасностью порта (Port Security Limit Control) может ограничить число пользователей, которым разрешен доступ к коммутатору на основе MAC-адресов и VLAN ID (выполняется для каждого порта). Как только число пользователей, желающих получить доступ к коммутатору, превысит заданное число, будет немедленно выполнена выбранная операция.

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ Port Security→Configuration (Рис. 5.2.18.1) (Табл. 5.2.18.1).

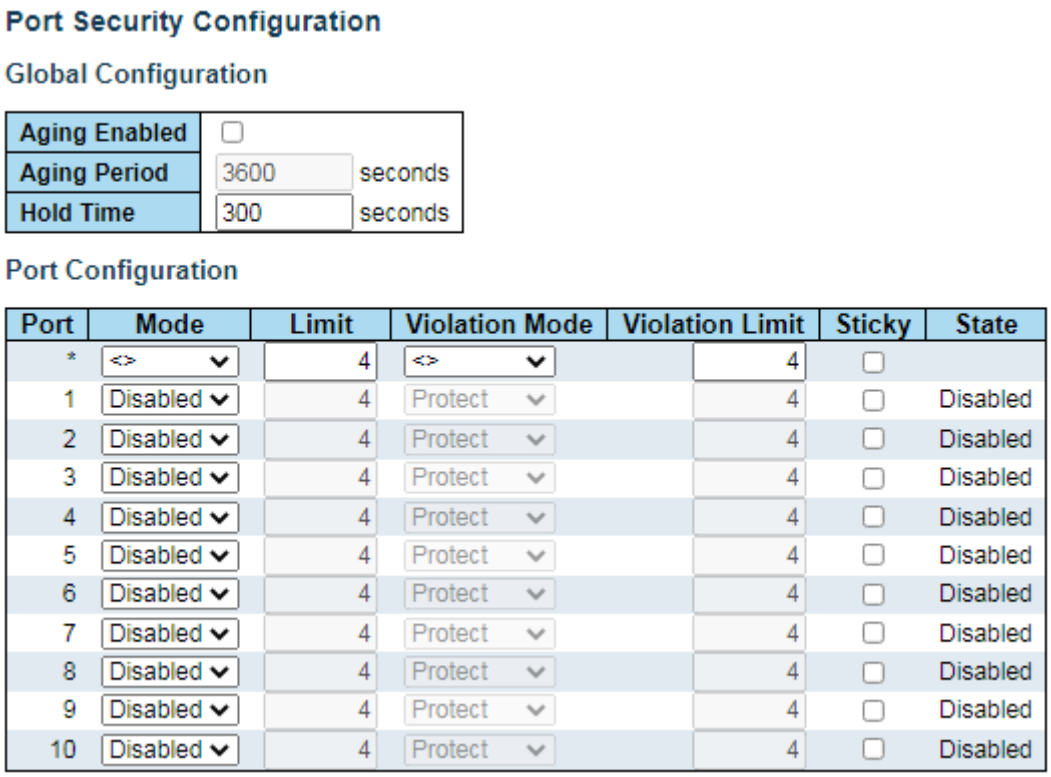


Рис. 5.2.18.1– Управление безопасности порта

Таблица 5.2.18.1– Управление безопасности порта

System Configuration (Настройка системы)	
Aging Enabled	Включить устаревание. Если в этом поле установлен флаг, то оценивается «возраст» безопасных MAC-адресов в том смысле, в котором он учитывается параметром Aging Period (Срок устаревания). Когда устаревание включено, с того момента, как конечный хост станет безопасным, запускается таймер. По истечении таймера, коммутатор начинает искать кадры конечного хоста и, если таких кадров не появляется в течение следующего срока устаревания (Aging Period), то предполагается, что конечный хост отключился и на коммутаторе освобождаются соответствующие ресурсы.
Aging Period	Если в поле Aging Enabled (Устаревание включено) установлен флаг, то становится возможно задать желаемое значение срока устаревания. По умолчанию установлен срок устаревания 3600 секунд. Допустимый диапазон значений от 10 до 10 000 000 секунд.
Hold Time	Время удержания, измеряемое в секундах, используется для определения того, как долго MAC-адрес хранится в таблице MAC-адресов, если было обнаружено, что он нарушает ограничение. Допустимый диапазон составляет от 10 до 10 000 000 секунд, по умолчанию - 300 секунд. Причина сохранения нарушающего MAC-адреса в таблице MAC-адресов заключается в первую очередь в том, чтобы гарантировать, что один и тот же MAC-адрес не вызывает непрерывных уведомлений (если включены уведомления о количестве нарушений).
Port Configuration (Настройка порта)	
Port	Отображается номер порта. “*” означают применение ко всем портам.
Mode	Включает или выключает управление ограничением количества хостов порта (по каждому порту отдельно). Чтобы сделать данную функцию

	работоспособной, необходимо включить ее как глобально, так и для порта.
Limit	Включает или выключает управление ограничением количества хостов порта (по каждому порту отдельно). Чтобы сделать данную функцию работоспособной, необходимо включить ее как глобально, так и для порта.
Violation Mode	Выбор режима при превышении предела MAC-адресов на порту Protect – ничего не предпринимать Restrict - Если предел достигнут, последующие MAC-адреса порта будут подсчитаны и отмечены как нарушающие. Такие адреса MAC удаляются из таблицы MAC-адресов по истечении времени удержания. В лучшем случае нарушения предельных значений MAC - адрес может быть помечен как нарушение в любой момент времени. Shutdown- Если предел достигнут, то это приведет к отключению порта. Это означает, что все защищенные MAC-адреса будут удалены из порта и новые адреса не будут изучены.
Violation Limit	Настройка максимального количества MAC-адресов, которые могут быть помечены как нарушающие этот порт. Это число не может превышать 1023. По умолчанию - 4. Он используется только тогда, когда установлен режим `restrict`
Sticky	Включение прикрепления MAC-адресов к порту. Когда порт находится в режиме `sticky`, все MAC-адреса, которые в противном случае были бы изучены как динамические, узнаются как закрепленные. Прикрепленные MAC-адреса являются частью рабочей конфигурации и поэтому могут быть сохранены в startup-config. Прикрепленные MAC-адреса сохраняются при изменении ссылок (в отличие от динамических, которые придется запоминать заново). Они также выдерживают перезагрузку, если рабочая конфигурация сохранена в startup-config.
State	Отображается текущее состояние порта с точки зрения управления ограничением количества хостов порта.

Port Security Static and Sticky MAC Addresses. Настройка статических и фиксированных MAC-адресов.

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ Port Security→MAC Addresses (Рис. 5.2.18.2) (Табл. 5.2.18.2).

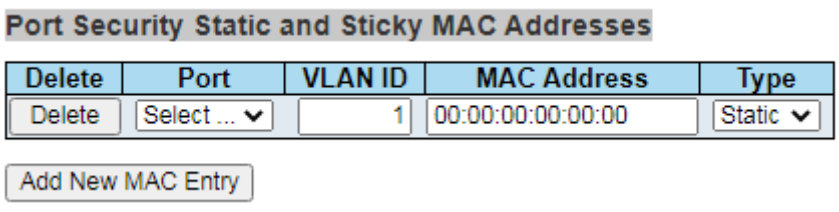


Рис. 5.2.18.2 – Настройка статических и фиксированных MAC-адресов

Таблица 5.2.18.2 – Настройка статических и фиксированных MAC-адресов

Delete	Удалить текущую запись
Port	Номер порта, к которому привязан MAC-адрес.
VLAN ID	Идентификатор VLAN

MAC Address	MAC-адрес
Type	Указывает тип записи и может быть статическим или фиксированным

Кнопка Add New MAC Entry служит для добавления новой записи.

5.2.19. NAS (Network Access Server)

Конфигурирование сервера доступа в сеть (Network Access Server) полезно в сетевой среде, в которой желательно аутентифицировать клиентов (supplicants) до того, как они получат доступ к ресурсам защищенной сети. Для эффективного управления доступом для неизвестных клиентов, IEEE разработал стандарт 802.1X, обеспечивающий процедуру аутентификации на порту, предотвращающую несанкционированный доступ к сети по запросам пользователей, впервые предоставляющих учетные данные для целей аутентификации. Коммутатор, соединяющий клиентов и radius-сервер, обычно работает как аутентификатор. Для обмена сообщениями аутентификации между клиентами и удаленным RADIUS-сервером, проверяющим аутентичность пользователя и его права доступа, используется EAPOL (расширенный протокол аутентификации по локальным сетям). На данной странице можно настроить конфигурацию аутентификатора либо глобально, либо для каждого порта отдельно.

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Network→NAS (Рис. 5.2.19.1) (Табл. 5.2.19.1).

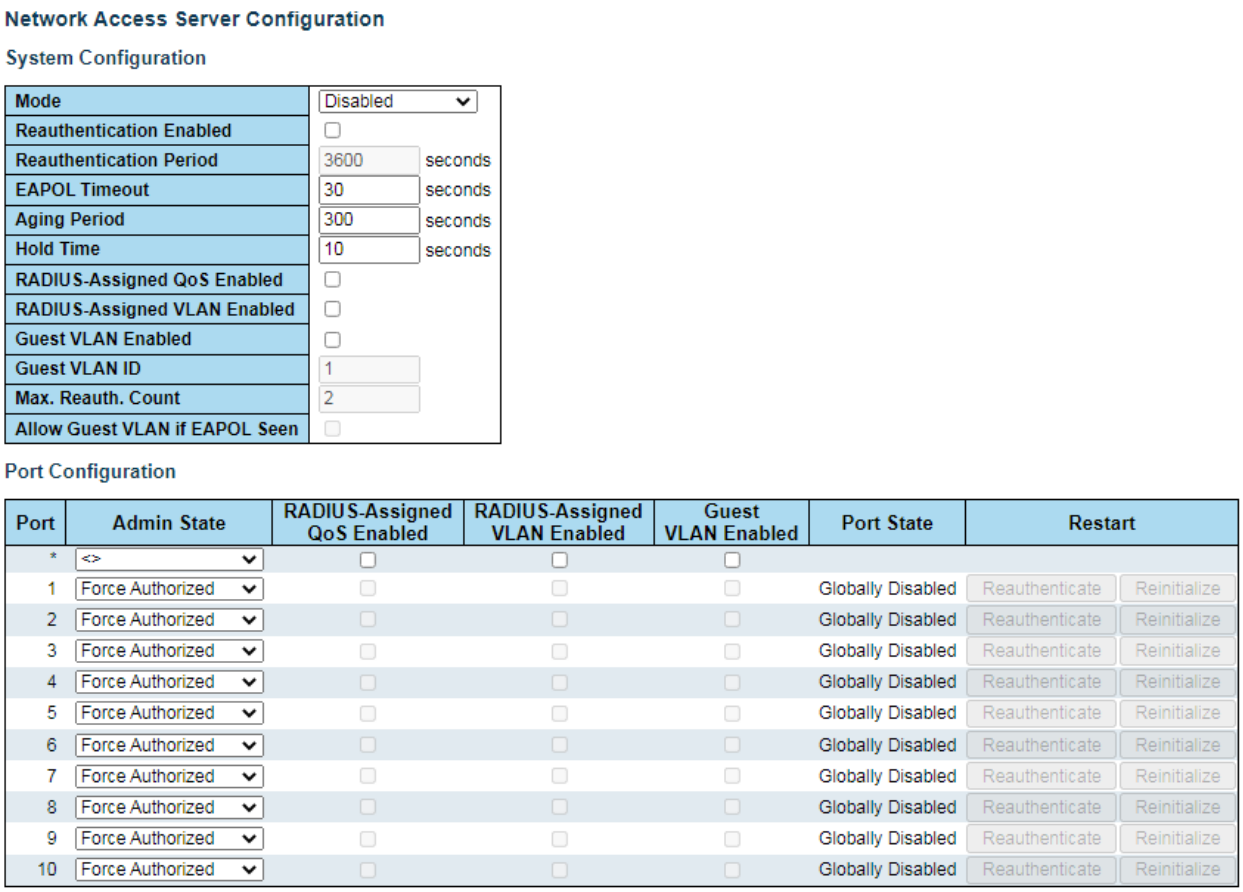


Рис. 5.2.19.1 – Конфигурирование сервера доступа в сеть

Таблица 5.2.19.1 – Конфигурирование сервера доступа в сеть

System Configuration (Настройка системы)	
Mode	Включает на коммутаторе глобально 802.1X и аутентификацию на основе

	MAC- адресов. Если глобально эти протоколы выключены, передача кадров будет разрешена на всех портах.
Reauthentication Enabled	Установите флаг в этом поле, чтобы разрешить клиентам повторную аутентификацию по истечении интервала времени, заданного в поле "Reauthentication Period" (Интервал повторной аутентификации). Повторную аутентификацию можно использовать для определения того, подключено ли к порту коммутатора новое устройство.
Reauthentication Period	Интервал времени, по истечении которого подключенное устройство может быть аутентифицировано повторно. По умолчанию установлен интервал повторной аутентификации 3600 секунд. Допустимый диапазон значений от 1 до 3600 секунд.
EAPOL Timeout	Интервал времени, в течение которого коммутатор будет ожидать ответ от подавшего запрос на доступ к сети устройства в течение сессии аутентификации перед тем, как передать пакет Request Identify (Запрос идентификации) EAPOL. По умолчанию задано 30 секунд. Допустимый диапазон значений от 1 до 65535 секунд.
Aging Period	Интервал времени, определяющий допустимое время доступа клиента к коммутатору для аутентификации по 802.1X и MAC- адресу. По умолчанию составляет 300 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд
Hold Time	Время, по истечении которого индицируется отказ EAP, либо превышение интервала ожидания RADIUS, из-за чего клиент не получил доступ. Эта настройка применяется к портам, работающим при аутентификации Single 802.1X, Multi 802.1X или на основе MAC - адресов. По умолчанию время удерживания составляет 10 секунд. Допустимый диапазон значений от 10 до 1 000 000 секунд.
Radius - Assigned QoS Enabled	Установите флаг в этом поле, чтобы глобально включить QoS, назначаемый RADIUS.
Radius-Assigned VLAN Enabled	Номер VLAN, назначенный RADIUS, обеспечивает средства для централизованного управления VLAN, которому принадлежит успешно аутентифицированное устройство, подключенное к коммутатору. Для VLAN, присвоенному протоколом RADIUS, будет классифицироваться и коммутироваться входящий трафик. RADIUS-сервер должен быть настроен на передачу специальных атрибутов RADIUS для получения преимуществ от этой функции. Установка флага в поле "RADIUSAssigned VLAN Enabled" позволяет быстро (глобально) включить/выключить присвоение RADIUS-сервером меток VLAN. Когда флаг установлен, дубликаты настроек индивидуального порта определяют, включено ли на данном порту присваивание VLAN протоколом RADIUS. Когда флаг в поле снят, присваивание VLAN протоколом RADIUS отключено на всех портах.
Guest VLAN Enabled	Гостевая VLAN является специальной VLAN, типичным назначением которой является предоставление ограниченного доступа к сети. Когда флаг установлен, дубликаты настроек индивидуального порта определяют, может ли порт быть перемещен в гостевую VLAN. Когда флаг в поле снят, возможность перемещения порта в гостевую VLAN отключена на всех портах.
Guest VLAN ID	Номер VLAN ID работает только в том случае, когда гостевая VLAN включена. VLAN ID представляет собой значение, присваиваемое порту, если порт перемещается в гостевую VLAN. Диапазон значений: от 1 до

	4095.
Max. Reauth. Count	Максимальное число повторных аутентификаций. Максимальное число передач коммутатором кадра запроса идентификации EAPOL, остающихся без ответа перед тем, как порт будет добавлен в гостевую VLAN. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально. Диапазон 1~255.
Allow Guest VLAN if EAPOL Seen	Разрешать гостевую VLAN, если виден EAPOL. Коммутатор помнит, был ли принят кадр EAPOL в течение времени жизни порта. Когда коммутатор принимает решение о входе в гостевую VLAN, он сначала проверяет, включена или выключена эта опция. Если она выключена (флаг в поле снят – значение по умолчанию), коммутатор войдет в гостевую VLAN только в том случае, если кадр EAPOL не был принят на порту в течение времени жизни порта. Если опция включена (флаг в поле установлен), коммутатор войдет в гостевую VLAN, даже если кадр EAPOL был принят на порту в течение времени жизни порта. Значение может быть изменено только в том случае, если гостевая VLAN включена глобально.
Port Configuration (Настройка порта)	
Port	Номер порта. “*” означает применение ко всем портам.
Admin State	Выбирает режим аутентификации порта. Данная настройка работает только в том случае, когда глобально включен NAS. Режимы работы: • Force Authorized (Принудительная авторизация): В этом режиме работы 56 коммутатор отправит один кадр успешной (аутентификации) EAPOL, если осуществляется подключение к порту, при этом любому клиенту на порту будет разрешен доступ к сети без аутентификации. • Force Unauthorized (Принудительная не авторизация): В этом режиме работы коммутатор отправит один кадр отказа (аутентификации) EAPOL, если будет осуществляется подключение к порту, при этом любому клиенту на порту будет запрещен доступ к сети. • Port-Based 802.1X (802.1X на основе порта): В этом режиме работы требуется, чтобы сервером аутентификации был авторизован dot1x-совместимый клиент. Клиентам, не обладающим dot1x-совместимостью, доступ будет запрещен. • Single 802.1X (Аутентификация преимущественно одного устройства по 802.1X): В режиме работы Single 802.1X, аутенцифицироваться на порту будет преимущественно одно клиентское устройство, отправившее запрос на доступ к ресурсам сети. Для связи между клиентским устройством и коммутатором используются нормальные кадры EAPOL. Если к порту подключено более одного клиентского устройства, первым из них будет считаться то, которое появилось раньше всех остальных в тот период, когда порт был включен. Если такое клиентское устройство не отправило правильной учетной информации в течение заданного времени, шанс получит другое клиентское устройство. Как только клиентское устройство будет успешно аутентифицировано, только ему будет разрешен доступ. Этот режим работы является наиболее безопасным из всех поддерживаемых режимов. В этом режиме для обеспечения безопасности MAC - адреса клиентского устройства используется модуль “Port Security” (Безопасность порта) (после того, как устройство будет успешно аутентифицировано). • Multi Single 802.1X (Аутентификация многих 57 устройств по 802.1X): В режиме работы Multi 802.1X, одно или более клиентских устройств могут быть аутентифицированы на одном и том же порту в одно и то же время. Каждое клиентское устройство аутентифицируется индивидуально; его

	безопасность в таблице MAC - адресов обеспечивает модуль “Port Security” (Безопасность порта). • MAC-based Auth. (Авторизация на основе MAC - адресов): в отличие от аутентификации 802.1X, при аутентификации на основе MAC - адресов не принимаются и не передаются кадры EAPOL. При аутентификации на основе MAC - адресов, для половины клиентов коммутатор работает, как клиентское устройство, пославшее запрос на доступ к ресурсам сети. Начальный кадр (любого типа), отправленный клиентом, анализируется коммутатором, который, в свою очередь, использует MAC - адрес клиента в качестве имени пользователя и пароля в последующем обмене данными с RADIUS-сервером по EAP. 6-байтный MAC - адрес преобразуется в строку вида "xx-xx-xx-xx-xx-xx", где тире (-) используется в качестве символа-разделителя между шестнадцатеричными цифрами (записанными символами нижнего регистра). Коммутатор поддерживает только метод аутентификации MD5-Challenge, поэтому RADIUSсервер должен быть соответствующим образом сконфигурирован.
Radius-Assigned QoS Enabled	Установите флаг в этом поле, чтобы включить RADIUS-Assigned QoS на порту.
Radius-Assigned VLAN Enabled	Установите флаг в этом поле, чтобы включить RADIUS-Assigned VLAN на порту.
Guest VLAN Enabled	Установите флаг в этом поле, чтобы включить гостевую VLAN на порту.
Port State	Отображается текущее состояние порта (в смысле аутентификации 802.1X). Возможны следующие состояния: • Globally Disabled (Глобально выключен): Аутентификация по 802.1X и аутентификация по MAC-адресам глобально выключены. • Link Down (Порт выключен): Аутентификация по 802.1X и аутентификация по MAC-адресам включены, но к порту ничего не подключено. • Authorized (Авторизован): Порт принудительно переключен в авторизованный режим работы и клиентское устройство успешно авторизовано. • Unauthorized (Не авторизован): Порт принудительно переключен в не авторизованный режим работы, авторизация клиентского устройства RADIUS-сервером была неуспешной. • X Auth/Y Unauth (X авторизовано/Y не авторизовано): Порт работает в режиме с множеством клиентских устройств. X клиентских устройств авторизовано, а Y – не авторизовано.
Restart	При перезапуске аутентификации клиента используется один из методов, описанных ниже. Имейте в виду, что кнопки перезапуска работоспособны только в том случае, когда на коммутаторе глобально включен режим аутентификации (на странице System Configuration (Настройка системы), а Admin State (Административное состояние) порта имеет значение EAPOL-based (на основе EAPOL) или MAC-Based (на основе MAC-адресов). При нажатии кнопок настройки на странице изменены не будут. Reauthenticate (Повторная аутентификация): Повторная аутентификация в том случае, когда истекает период тишины на порту (аутентификация на основе

	EAPOL). При аутентификации на основе MAC-адресов, попытка повторной аутентификации будет предпринята немедленно. Кнопки будут работоспособны, если клиенты успешно аутентифицированы на порту, и не будут работоспособны, если клиенты временно не авторизованы. Reinitialize (Повторная инициализация): выполняется принудительная повторная инициализация клиентов на порту, а затем – немедленная повторная аутентификация. Когда идет повторная аутентификация, клиенты будут переведены в неавторизованное состояние.

5.2.20. ACL. Списки доступа

ACL является последовательным списком, используемым для разрешения или запрета доступа пользователей к информации или к выполнению задач по сети. В данном коммутаторе пользователи могут задать правила, применяемые к номерам портов для разрешения или запрета операций или ограничения предельной скорости. Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ACL.

ACL Ports Configuration (Конфигурирование ACL для портов) (Рис. .2.20.1) (Табл. 5.2.20.1).

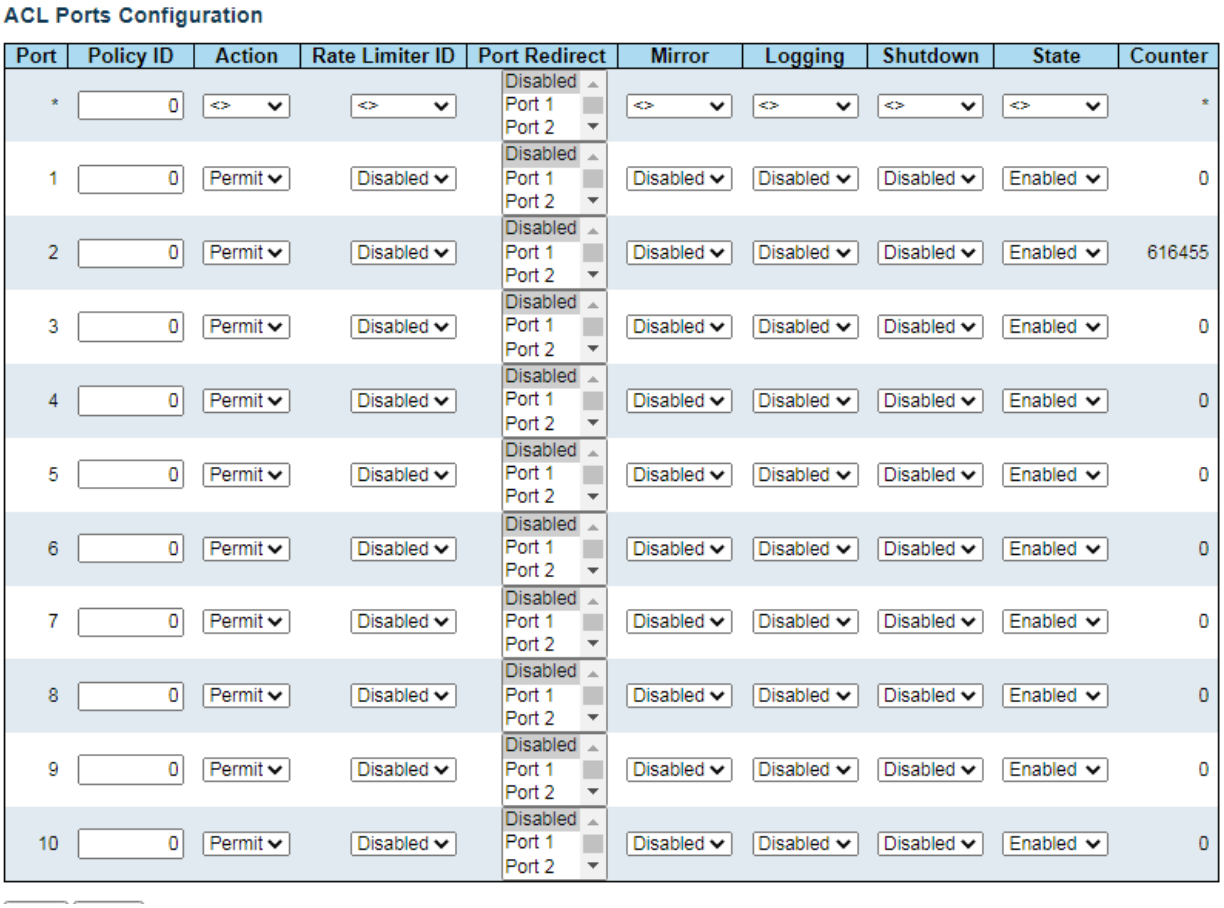


Рис. 5.2.20.1– Конфигурирование ACL для портов

Таблица 5.2.20.1– Конфигурирование ACL для портов

Port	Номер порта
Policy ID	Присваивает идентификатор правил списка доступа определенному порту. Порт может использовать только один идентификатор правил списка доступа, однако, идентификатор правил списка доступа может быть применен ко многим портам. По умолчанию идентификатор

	имеет значение 0. Допустимый диапазон значений 0~255.
Action	Разрешает или запрещает кадр на основе того, согласуется ли он с правилом из присвоенной группы правил
Rate Limiter ID	Выбирает идентификатор ограничителя скорости, применяемого к порту. Правило ограничителя скорости может быть задано на странице настройки “Rate Limiters” (Ограничители скорости).
Port Redirect	Выбор порта, на который перенаправляются согласующиеся кадры.
Mirror	Включает или выключает функцию зеркалирования. Когда функция зеркалирования включена, копии согласованных кадров будут зеркалироваться в порт назначения, заданный на странице настройки “Mirror” (Зеркало). Этим параметром задается зеркалирование порта на основе ACL, а порт зеркалирования задается на общей странице настройки зеркала, реализованной независимо. Для использования зеркалирования на основе ACL включите параметр Mirror (Зеркало) на странице ACL Ports Configuration (Настройка портов ACL). Затем откройте страницу Mirror Configuration (Настройка зеркала), в поле “Port to mirror on” (Порт, в который производится зеркалирование) задайте требуемый порт назначения, поле “Mode” (Режим работы) оставьте Disabled (Выключен).
Logging	Включает регистрацию согласующихся кадров в системном журнале. Для просмотра списка системных событий, войдите в меню System (Система), затем нажмите мышью опцию “System Log Information” (Информация системного журнала).
Shutdown	Это поле позволяет задать, следует ли отключать порт, когда согласующиеся кадры появляются на порту.
State	Выбор состояния порта: • Enabled (Включить): позволяет переоткрыть порт. • Disabled (Выключить): позволяет закрыть порт.
Counters	Число кадров, которые согласуются с правилами, определенными в выбранной группе правил.

Rate Limiters (Ограничители скорости) (Рис. 5.2.20.2) (Табл. 5.2.20.2).

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Рис. 5.2.20.2 – Ограничители скорости

Таблица 5.2.20.2 – Ограничители скорости

Rate Limiter ID	Отображается идентификатор каждого ограничителя скорости
Rate	Указано пороговое значение, при превышении которого пакеты будут отбрасываться. Диапазон допустимых значений 0~3276700 pps (пакетов/сек.) или 1, 100, 200, 300…1000000 кбит/с.
Unit	Выбор единиц измерения скорости

Access Control List (Список доступа) (Рис. 5.2.20.3) (Табл. 5.2.20.3).

Список доступа задает правила фильтрации для политики доступа – для определенного порта или для всех портов. Правила, примененные к порту, начинают действовать немедленно.

Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	

Рис. 5.2.20.3 – Список доступа

Таблица 5.2.20.3 – Список доступа

Ingress Port	Входящий порт элемента списка доступа.
Policy Bitmask	Номер политики и маска битов ACE.
Frame Type	Тип кадра, согласующегося с этим правилом.
Action	Отображается тип операции - permit (разрешить) либо deny (запретить).
Rate Limiter	Отображается, включен или выключен ограничитель скорости, когда найдены согласующиеся кадры
Port Redirect	В этом поле отображается, включено или выключено перенаправление порта.
Mirror	В этом поле отображается, включена или выключена функция

	зеркала.
Counter	В этом поле отображается число кадров, согласующихся с какими-либо правилами, определенными для этого списка доступа.

Чтобы добавить новый элемент списка доступа нажмите мышью на знак плюс (Рис. 5.2.20.4) (Табл. 5.2.20.4).

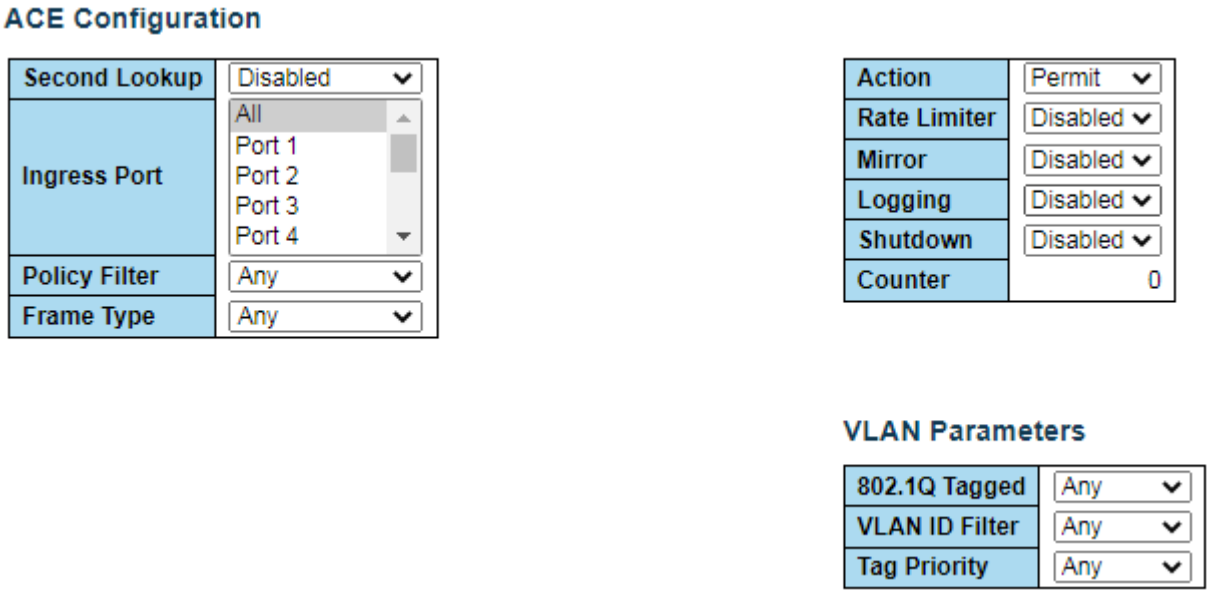


Рис. 5.2.20.4 – Новый элемент списка

Таблица 5.2.20.4– Новый элемент списка

ACE Configuration (Настройка ACE)	
Ingress Port	Выберите входящий порт для элемента списка доступа. Выберите “All” (Все), чтобы применить правило список доступа ко всем портам либо выбрать определенный порт.
Policy Filter	Выбор типа фильтра политики. “Any” (Любой) означает, что этому правилу не присвоено фильтра политики. 63 Выберите “Specific” (Специальный), чтобы отфильтровать конкретную политику по данному ACE.
Frame Type	Выберите согласующийся тип кадра. Доступны следующие типы кадров: Any (Любой), Ethernet, ARP, IPv4. По умолчанию можно использовать любой тип кадра.
Action	Выберите тип операции - permit (разрешить) либо deny (запретить).
Rate Limiter	Позволяет включить или выключить ограничитель скорости, когда найдены согласующиеся кадры.
Mirror	Позволяет включить или выключить функцию зеркала.
Logging	Позволяет включить или выключить регистрацию в системном журнале для согласующихся кадров.
Shutdown	Позволяет включить или выключить отключение порта для согласующихся кадров.
Counter	В этом поле отображается число кадров, согласующихся с какими-либо правилами, определенными для этого списка доступа.
VLAN Parameters (Параметры VLAN)	
802.1Q Tagged	Позволяет выбрать, должны ли кадры содержать теги (то есть быть тегированными).
VLAN ID Filter	Позволяет выбрать фильтр VLAN ID для данного ACE.

	• Any (Любой): фильтр VLAN ID не задан. • Specific (Специальный): позволяет задать номер VLAN ID. Кадр с заданным номером VLAN ID, согласующийся с данным правилом ACE.
Tag Priority	Позволяет выбрать значение User Priority (Приоритет пользователя), найденного в теге VLAN для согласования с данным правилом.

5.2.21. IP Source Guard. Защита IP-адреса источника

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ IP Source Guard. Configuration (Настройка) (Рис. 5.2.21.1) (Табл. 5.2.21.1).

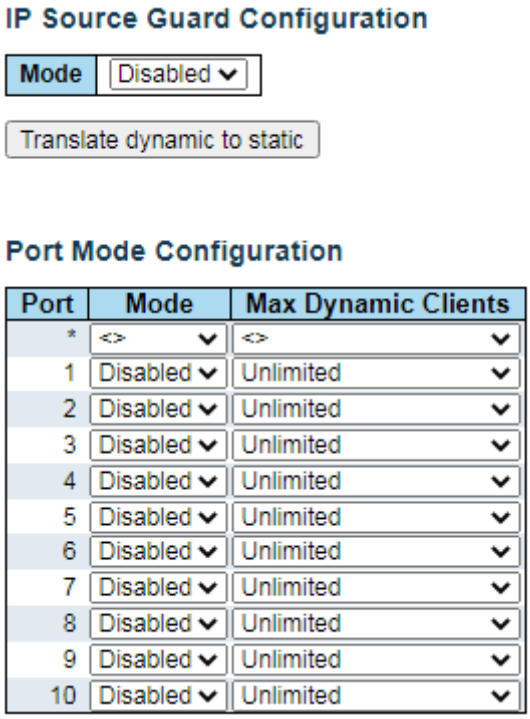


Рис. 5.2.21.1– Настройка

Таблица 5.2.21.1– Настройка

IP Source Guard Configuration (Настройка защиты IP-адреса источника)	
Mode	Включение или выключение защиты IP-адреса источника (глобальное)
Translate dynamic to static	Нажмите на эту кнопку, чтобы преобразовать динамические записи в статические.
Port Mode Configuration (Настройка режима работы порта)	
Port	Номер порта. “*” означает применение ко всем портам.
Mode	Включение или выключение защиты IP-адреса источника на порту. Пожалуйста, имейте в виду, для того чтобы защита IP-адресов источника работала, должны быть включены и глобальный режим работы, и режим работы на порту.
Max Dynamic Clients	Выберите максимальное число динамических клиентов, которые могут быть обучены на порту. Возможны следующие варианты: 0, 1, 2, unlimited (неограниченное количество). Если включен режим работы порта и максимальное число клиентов равно 0, коммутатор будет только передавать IP-пакеты, которые согласуются со статическими элементами списка (IP-адресами) для данного порта.

Static Table (Таблица статических записей) (Рис. 5.2.21.2) (Табл. 5.2.21.2).

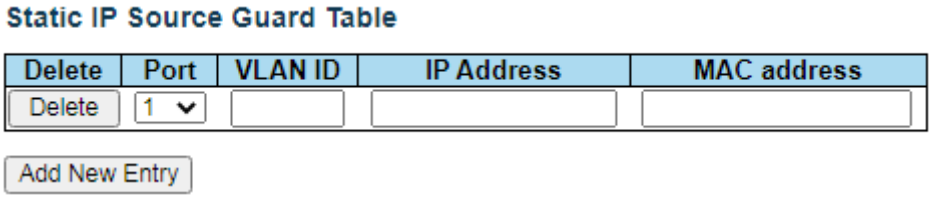


Рис. 5.2.21.2 – Таблица статических записей

Таблица 5.2.21.2 – Таблица статических записей

Delete	Удалить текущую запись
Port	Порт, для которого создается статическая запись.
VLAN ID	Введите ранее сконфигурированный номер VLAN ID.
IP Address	Введите корректный IP-адрес.
MAC Address	Введите корректный MAC-адрес.

Кнопка 

служит для добавления новой записи.

5.2.22. IPv6 Source Guard. Защита IPv6-адреса источника

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ IPv6 Source Guard. Configuration (Настройка) (Рис. 5.2.22.1) (Табл. 5.2.22.1).

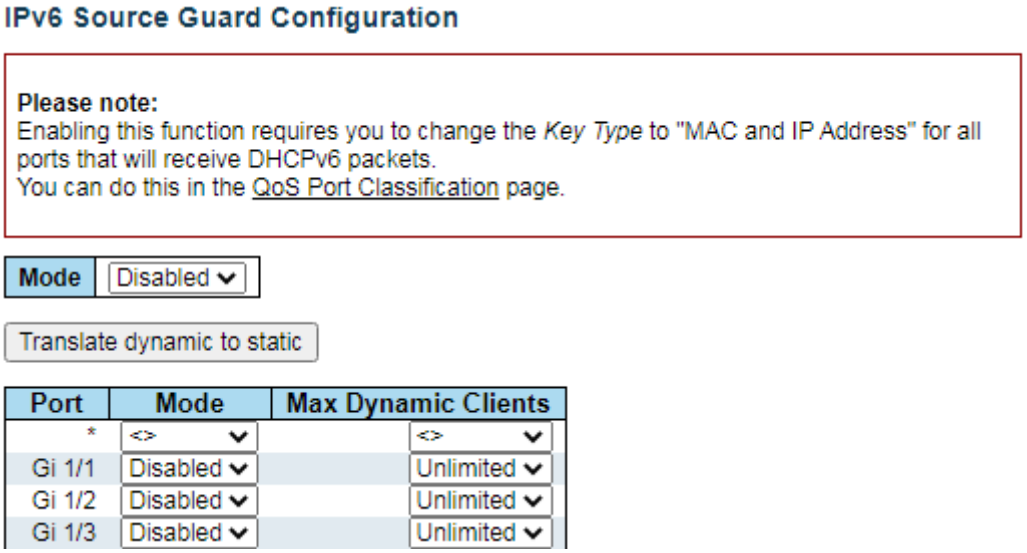


Рис. 5.2.22.1 – Настройка

Таблица 5.2.22.1 – Настройка

IPv6 Source Guard Configuration (Настройка защиты IPv6-адреса источника)	
Mode	Включение или выключение защиты IPv6-адреса источника (глобальное)
Translate dynamic to static	Нажмите на эту кнопку, чтобы преобразовать динамические записи в статические.
Port Mode Configuration (Настройка режима работы порта)	
Port	Номер порта. “*” означает применение ко всем портам.
Mode	IPv6 Source Guard может быть включен / отключен на отдельных портах. IPv6 Source Guard включен только в том случае, если на данном порте включены и глобальный режим, и режим порта.

Max Dynamic Clients	Укажите максимальное количество динамических клиентов, которые могут быть изучены на данном порту. Это значение может быть 0, 1, 2 или неограниченно. Если режим порта включен и значение max dynamic client равно 0, пересылаются только IPv6-пакеты, которые совпадают в статических записях на конкретном порту.

IPv6 Source Guard Static Table (Таблица статических записей ipv6) (Рис. 5.2.22.2**) (Табл.** 5.2.22.2**).**

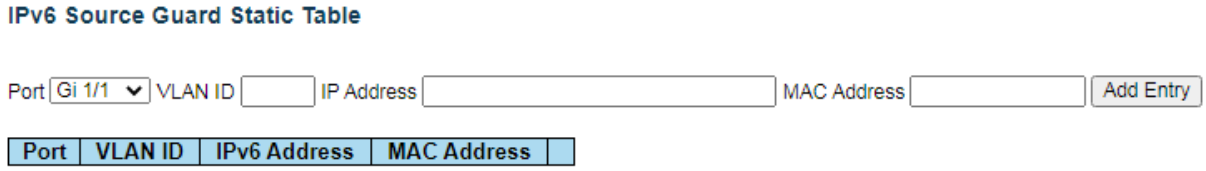
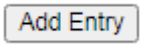


Рис. 5.2.22.2 – Таблица статических записей

Таблица 5.2.22.2 – Таблица статических записей

Port	порт, к которому привязана запись
VLAN ID	Идентификатор VLAN для записи. Если с записью не связан идентификатор VLAN, в этом поле отображается 0.
IPv6 Address	Разрешенный IPv6-адрес.
MAC Address	Разрешенный MAC-адрес.

Чтобы добавить запись нажмите кнопку 

5.2.23. ARP inspection. Инспекция ARP

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→ ARP inspection.

Port Configuration (Настройка порта) (Рис. 5.2.23.1) (Табл. 5.2.23.1).

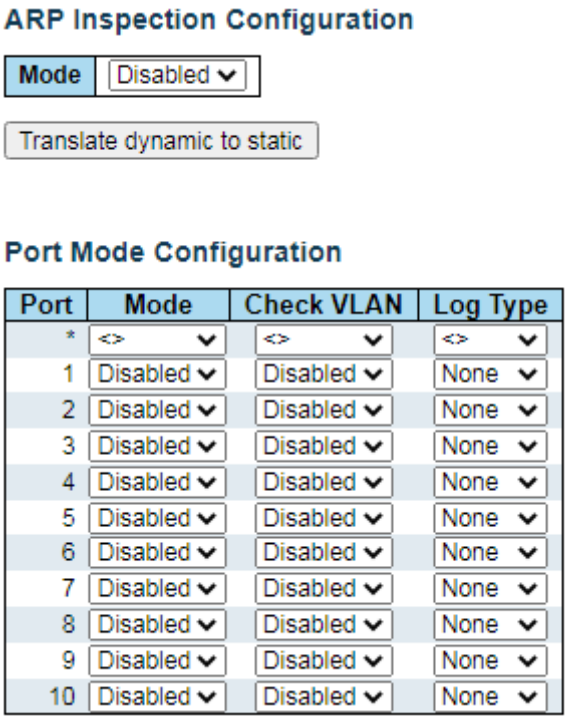


Рис. 5.2.23.1 – Настройка порта

Таблица 5.2.23.1 – Настройка порта

ARP Inspection Configuration (Настройка инспекции ARP)	
Mode	Включает или выключает функцию инспекции ARP глобально.
Port Mode Configuration (Настройка режима работы порта)	
Port	Номер порта. “*” означает применение ко всем портам
Mode	Включает или выключает функцию инспекции ARP на порту. Пожалуйста, имейте в виду, для того чтобы функция инспекции ARP работала, должны быть включены и глобальный режим работы, и режим работы на порту.
Check VLAN	Включает или выключает проверку VLAN.
Log Type	Доступно четыре типа журналов: • None (Нет): Журнала нет. • Deny (Запрещенные): В журнал помещаются запрещенные элементы списка. • Permit (Разрешенные): В журнал помещаются разрешенные элементы списка. • All (Все): В журнал помещаются все элементы списка.

VLAN Configuration (Настройка VLAN) (Рис. 5.2.23.2) (Табл. 5.2.23.2).

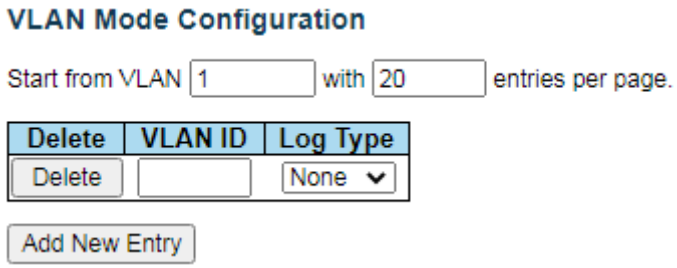


Рис. 5.2.23.2 – Настройка VLAN

Таблица 5.2.23.2 – Настройка VLAN

Delete	Удалить текущую запись
VLAN ID	Позволяет задать, на каких сетях VLAN включена функция инспекции ARP. Во-первых, необходимо включить настройки порта на web-странице Port mode configuration (Настройка режима работы порта). Только тогда, когда для данного порта включены и Global Mode (Глобальный режим работы) и Port Mode (Режим работы порта), функция ARP Inspection включена на данном порту. Во-вторых, на web-странице VLAN mode configuration (Настройка режима VLAN) можно задать, какие VLAN будут проинспектированы. Тип журнала также можно настроить отдельно для каждой VLAN.
Log Type	Доступно четыре типа журналов. • None (Нет): Журнала нет. • Deny (Запрещенные): В журнал помещаются запрещенные элементы. • Permit (Разрешенные): В журнал помещаются разрешенные элементы. • All (Все): В журнал помещаются все элементы.

Кнопка 

служит для добавления новой записи.

Static Table (Таблица статических адресов) (Рис. 5.2.23.3) (Табл. 5.2.23.3).

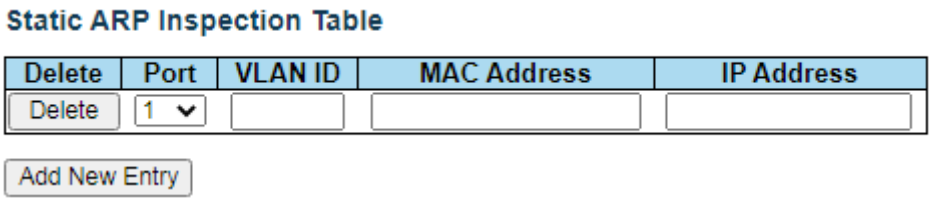


Рис. 5.2.23.3– Таблица статических адресов

Таблица 5.2.23.3– Таблица статических адресов

Delete	Удалить текущую запись
Port	Порт, для которого создается статическая запись.
VLAN ID	Позволяет задать номер VLAN ID.
MAC Address	Укажите допустимый MAC - адрес источника.
IP Address	Укажите допустимый IP-адрес

Кнопка 

служит для добавления новой записи.

Dynamic Table Status (Состояние динамической таблицы) (Рис. 5.2.23.3**) (Табл.** 5.2.23.3**).**

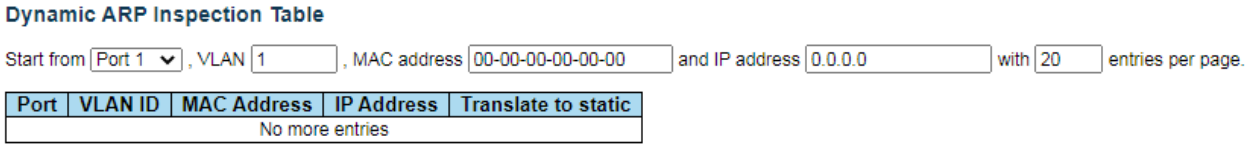


Рис. 5.2.23.3– Состояние динамической таблицы

Таблица 5.2.23.3– Состояние динамической таблицы

Port	Номер порта для данного элемента таблицы.
VLAN ID	Номер сети VLAN ID, в которой разрешен трафик ARP.
MAC Address	Пользовательский MAC - адрес данного элемента таблицы.
IP Address	Пользовательский IP-адрес данного элемента таблицы.

5.2.24. RADIUS

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→AAA→Radius.

Configuration (Настройка) (Рис. 6.2.24.1) (Табл. 6.2.24.1).

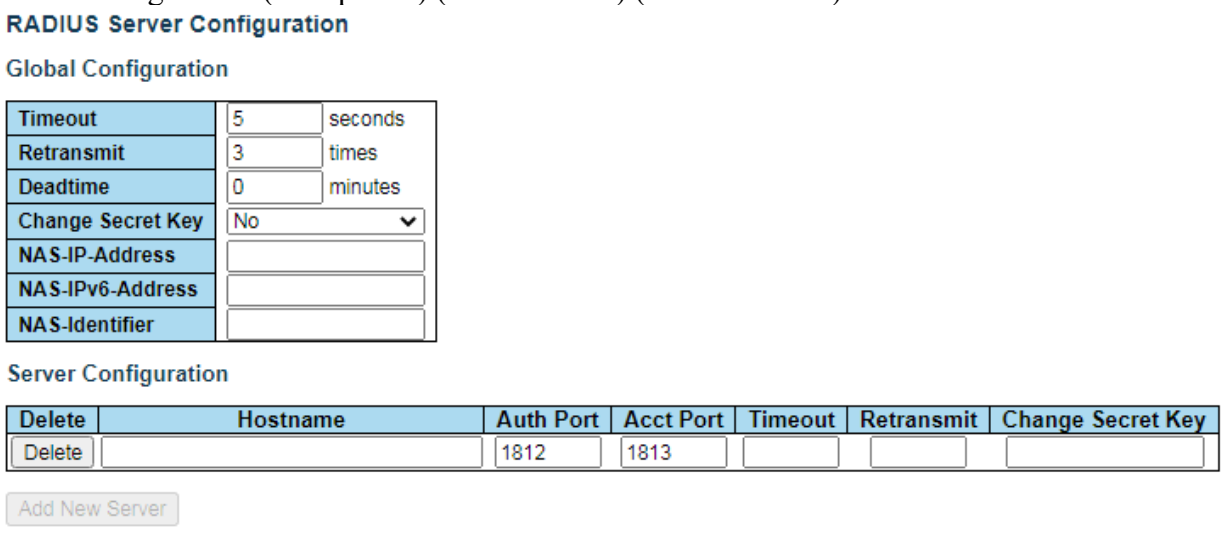
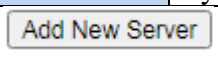


Рис. 5.2.24.1 – Настройка Radius

Таблица 5.2.24.1 – Настройка Radius

Global Configuration (Глобальные настройки)	
Timeout	Время, которое коммутатор ожидает ответа от сервера аутентификации перед тем, как повторить запрос.
Retrasmit	Укажите число раз повторной передачи запросных пакетов на сервер аутентификации, который не отвечает. Если сервер не ответил после последней повторной передачи, коммутатор считает, что сервер аутентификации отсутствует.
Deadtime	Deadtime (Время отсутствия сервера) – это время, в течение которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос. В результате, коммутатор не будет постоянно пытаться установить контакт с сервером, который уже квалифицирован, как отсутствующий. Если присвоить Deadtime значение, большее нуля (0), то эта функция будет включена, но только в том случае, если сконфигурировано более одного сервера. Допустимый диапазон Deadtime: от 0 до 1440 минут.
Change Secret Key	Выбор секретного ключа
Key	Укажите секретный ключ длиной не более 64 символов. Он будет доступен RADIUS-серверу и коммутатору.
NAS-IP- Address	Адрес IPv4, использованный в качестве атрибута 4 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, будет использован IP-адрес исходящего интерфейса.
NAS-IPv6-Address	Адрес IPv6, использованный в качестве атрибута 95 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, будет использован IP-адрес исходящего интерфейса.
NAS Identifer	Идентификатор длиной не более 256 символов, используемый в качестве атрибута 32 в пакетах запроса доступа RADIUS. Если это поле оставить пустым, идентификатор NAS не будет включен в пакет.
Server Configuration (Настройка сервера)	
Hostname	Имя хоста RADIUS-сервера или его IP-адрес.
Auth Port	Порт UDP, используемый на RADIUS-сервере для аутентификации.
Acct Port	Порт UDP, используемый на RADIUS-сервере для аккаунтинга.
Timeout	Если в этом поле указано время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, оставьте это поле пустым.
Retransmit	Если в этом поле указано значение времени повторной передачи, оно будет использовано вместо глобального значения времени повторной передачи. Если желательно использовать глобальное значение, оставьте это поле пустым.
Change Secret Key	Если в этом поле указано значение секретного ключа, оно будет использовано вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, оставьте это поле пустым.

Кнопка 

служит для добавления сервера.

Примечание. Сервер, указанный первым в списке, считается основным.

5.2.25. TACACS+

Для доступа к настройкам необходимо перейти по вкладке Configuration→Security→Switch→Network→AAA→TACACS+.

Configuration (Настройка) (Рис. 5.2.25.1) (Табл. 5.2.25.1)

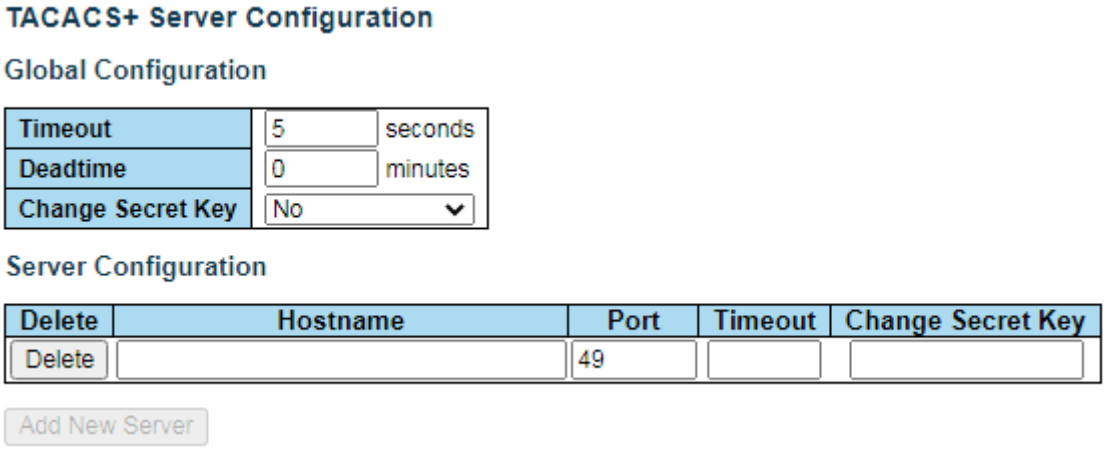
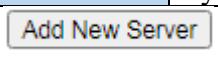


Рис. 5.2.25.1 – Настройка TACACS+

Таблица 5.2.25.1 – Настройка TACACS+

Global Configuration (Глобальные настройки)	
Timeout	Время, которое коммутатор ожидает ответа от сервера TACACS+ перед тем, как повторно передать запрос.
Deadtime	Deadtime (Время отсутствия сервера) – это время, в течение которого коммутатор не будет посылать новые запросы на сервер, который не ответил на предыдущий запрос. В результате, коммутатор не будет постоянно пытаться установить контакт с сервером, который уже квалифицирован, как отсутствующий. Если присвоить Deadtime значение, большее нуля (0), то эта функция будет включена, но только в том случае, если сконфигурировано более одного сервера. Допустимый диапазон Deadtime: от 0 до 1440 минут.
Change Secret Key	Выбор секресного ключа
Key	Укажите секретный ключ длиной не более 63 символов. Он будет доступен серверу TACACS+ и коммутатору
Server Configuration (Настройка сервера)	
Hostname	Имя хоста сервера TACACS+ или его IP-адрес.
Port	Номер порта TCP, используемого на сервере TACACS+ для аутентификации.
Timeout	Если в этом поле указано время ожидания, оно будет использовано вместо глобального времени ожидания. Если желательно использовать глобальное значение, оставьте это поле пустым.
Change Secret Key	Если в этом поле указано значение секретного ключа, оно будет использовано вместо глобального значения секретного ключа. Если желательно использовать глобальное значение, оставьте это поле пустым.

Кнопка 

служит для добавления сервера.

Примечание. Сервер, указанный первым в списке, считается основным.

5.2.26. Aggregation. Агрегирование

При агрегировании линии используется параллельная работа множества портов, в результате чего скорость обмена данными по линии увеличивается. Используется два типа агрегирования: статический и LACP.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Aggregation. **Common Aggregation Configuration (Рис. 5.2.26.1) (Табл. 5.2.26.1).**

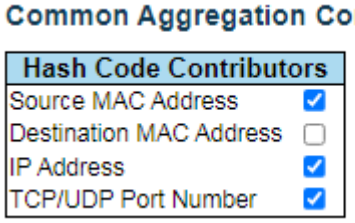


Рис. 5.2.26.1 – Настройка агрегирования

Таблица 5.2.26.1 – Настройка агрегирования

настройка режима работы агрегирования	
Source MAC Address	MAC-адрес источника используется для расчета линейного порта, через который будет передаваться кадр.
Destination MAC Address	MAC-адрес назначения используется для расчета линейного порта, через который будет передаваться кадр.
IP Address	IP-адрес используется для расчета линейного порта, через который будет передаваться кадр.
TCP/UDP Port Number	Порты TCP/UDP назначения и источника используются для расчета линейного порта, через который будет передаваться кадр.

Настройка группы агрегирования (Рис. 5.2.26.2) (Табл. 5.2.26.2).

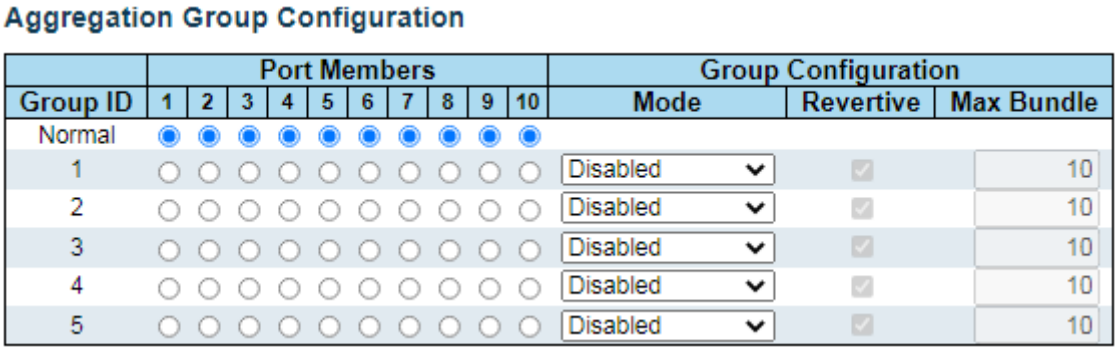


Рис. 5.2.26.2 – Настройка группы агрегирования

Таблица 5.2.26.2 – Настройка группы агрегирования

Настройка группы агрегирования	
Group ID	Номер, идентифицирующий магистраль. “Normal” (Обычный режим работы) означает, что агрегирование не используется. Каждая группа содержит не менее 2 и не более 10 линий (портов). Пожалуйста, имейте в виду, что в каждой группе каждый порт может использоваться только один раз.
Port Members	Выберите порты, принадлежащие магистрали

Mode	Выбор режима для группы агрегации • Disabled: группа отключена. • Static: группа работает в режиме статической агрегации. • LACP (Active): группа работает в режиме активной агрегации • LACP (Passive): группа работает в режиме пассивной агрегации
Revertive	Этот параметр применяется только к группам с включенным LACP. Он определяет, будет ли группа выполнять автоматический (повторный) расчет ссылок, когда становятся доступными ссылки с более высоким приоритетом.
Max Bundle	Этот параметр применяется только к группам с включенным LACP. Он определяет максимальное количество активных объединенных портов LACP, разрешенных в агрегации.

Коммутатор поддерживает протокол LACP (Link Aggregation Control Protocol – протокол управления агрегированием линии), который специфицирован в IEEE 802.3ad. Статические магистрали должны быть сконфигурированы вручную на обоих концах линии. Другими словами, порты, на которых сконфигурирован LACP, могут автоматически согласовывать магистральную линию с портами других устройств, на которых также сконфигурирован LACP. На коммутаторе может быть сконфигурировано любое число портов LACP, однако они не должны при этом быть частью статической магистрали. Если порты на других устройствах также сконфигурированы, как LACP, коммутатор и другие устройства будут согласовывать свои параметры для работы по магистральной линии между ними.

LACP Configuration (Настройка LACP) (Рис. 5.2.26.3) (Табл. 5.2.26.3).

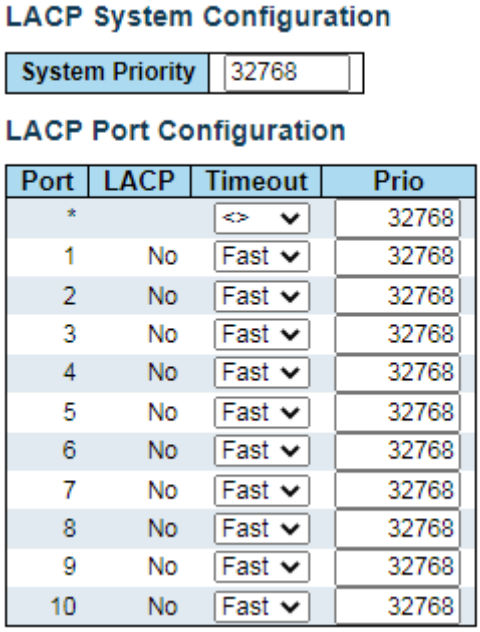


Рис. 5.2.26.3– Настройка LACP

Таблица 5.2.26.3– Настройка LACP

LACP System Configuration	
System Priority	Приоритет системы

LACP Port Configuration	
Port	Номер порта. “*” означает применение ко всем портам.
LACP	Показывает, включен ли LACP в данный момент на этом порту коммутатора.
Timeout	Параметр Timeout (Время ожидания) определяет период времени между передачами BPDU. Когда параметр имеет значение Fast (Быстро), пакеты LACP будут передаваться каждую секунду; когда параметр имеет значение Slow (Медленно), перед отправкой пакета LACP будет выдержан интервал 30 секунд.
Prio	Чем меньше это целое число, тем больше приоритет. Это значение приоритета определяет, какой порт будет активен, а какой – будет играть роль резервного.

5.2.27. Link OAM.

Link OAM дает операторам сети возможность отслеживать состояние сети и быстро определять местоположение неисправных каналов или неисправных состояний.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Link OAM.

Link OAM Port Configuration (Настройка портов) (Рис. 5.2.27.1) (Табл. 5.2.27.1).

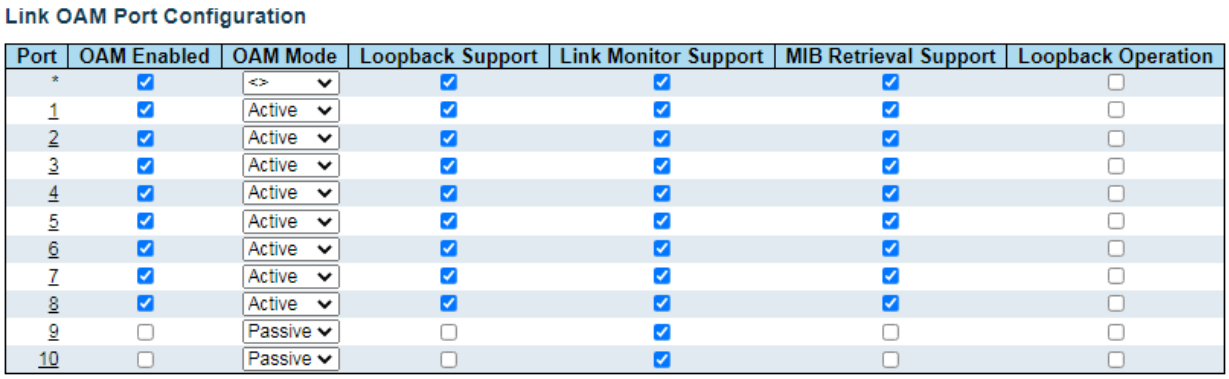


Рис. 5.2.27.1 – Настройка портов

Таблица 5.2.27.1 – Настройка портов

System Priority	Приоритет системы
Port	Номер порта. “*” означает применение ко всем портам.
OAM Enabled	Включение/выключение LinkOAM на порту коммутатора.
OAM Mode	Выбор режима OAM как активный или пассивный. По умолчанию установлен пассивный режим. active - DTE, настроенные в активном режиме, инициируют обмен информационными OAMPDU, как определено в процессе обнаружения. После завершения процесса обнаружения активным DTE разрешается отправлять любые OAMPDU при подключении к удаленному одноранговому объекту OAM в активном режиме. Активные DTE работают в ограниченном отношении, если удаленный объект OAM работает в пассивном режиме. Активные устройства не должны отвечать на команды удаленной обратной связи OAM и запросы переменных от пассивного однорангового узла. passive - DTE, настроенные в пассивном режиме, не инициируют процесс обнаружения. Пассивные DTE реагируют на инициирование процесса обнаружения удаленным DTE. Это

	исключает возможность перехода от пассивных к пассивным ссылкам. Пассивные DTE не должны отправлять запросы переменных или OAMPDU управления шлейфом.
Loopback Support	Включение/выключение функции петли
Link Monitor Support	Включение/выключение функции мониторинга на порту.
MIB Retrieval Support	Включение/выключение поддержки MIB на порту коммутатора
Loopback Operation	Если поддержка обратной связи включена, включение этого поля запустит операцию обратной связи для порта.

Link Event Configuration for Port (настройка событий для порта) (Рис. 5.2.27.2) (Табл. 5.2.27.2).

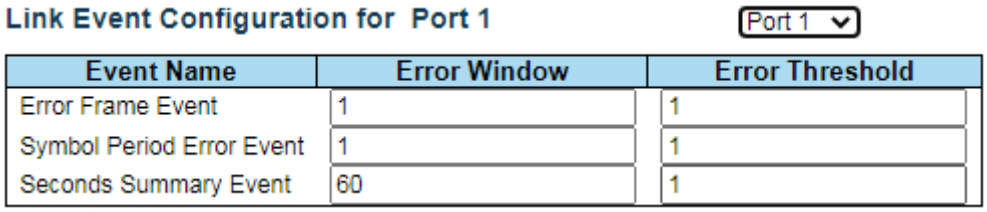


Рис. 5.2.27.2– настройка событий

Таблица 5.2.27.2 – настройка событий

System Priority	Приоритет системы
Port	Номер порта коммутатора.
Event Name	Error Frame Event - Событие ошибочного кадра подсчитывает количество ошибочных кадров, обнаруженных в течение указанного периода. Symbol Period Error Event - Событие периода ошибочного символа подсчитывает количество ошибок символа, произошедших за указанный период. Seconds Summary Event - Событие подсчитывает количество секунд с ошибками, произошедших в течение указанного периода.
Error Window	Представляет период окна порядка 1 секунды для наблюдения за различными событиями связи.
Error Threshold	Представляет пороговое значение для периода окна для соответствующего события связи, чтобы уведомить одноранговый узел об этой ошибке.

5.2.28. Loop protection. Защита от петель

Вследствие неправильного выполнения соединений, проблем с аппаратурой, неправильной настройки протоколов, в сетях иногда возникают петли. В коммутируемых сетях петли потребляют ресурсы коммутатора, в результате чего падает его производительность. Функция Loop Protection (Защита от петель), реализованная в данном коммутаторе, может быть включена глобально либо индивидуально на каждом порту. Использование функции защиты от петель дает возможность коммутатору автоматически обнаруживать петли в сети. При обнаружении петель, порты, принявшие от коммутатора пакет защиты от петель, 74 могут быть отключены либо соответствующие события могут быть зарегистрированы в журнале.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Loop protection. (Рис. 5.2.28.1) (Табл. 5.2.28.1).

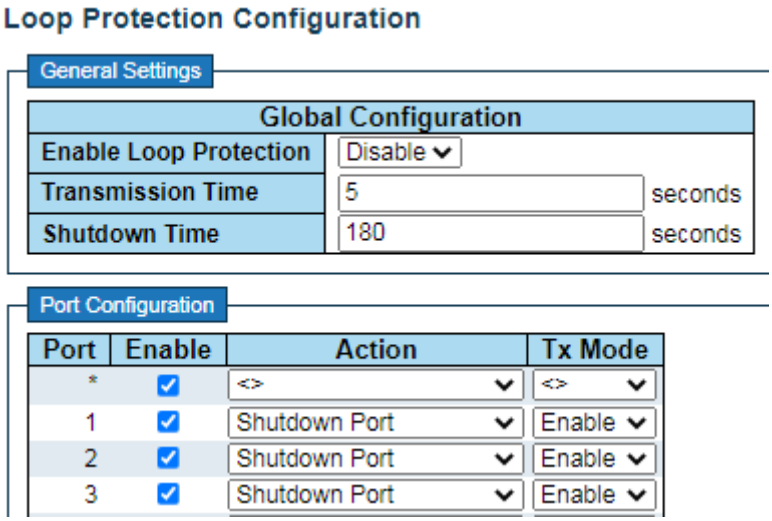


Рис. 5.2.28.1 – Защита от петель

Таблица 5.2.28.1 – Защита от петель

General Settings (Основные настройки)	
Enable Loop protection	Позволяет включить или выключить функцию защиты от петель.
Transmission Time	Интервал между отправкой пакетов защиты от петель PDU на каждом порту. Допустимые значения: от 1 до 10 секунд.
Shutdown Time	Период времени, на который порт будет выключен. Допустимые значения: от 0 до 604800 секунд. 0 означает, что порт будет оставаться выключенным до тех пор, пока устройство не будет перезагружено.
Port Configuration (Настройка порта)	
Port	Список номеров портов. “*” означает применение ко всем портам.
Enable	Позволяет включить или выключить функцию защиты от петель на выбранных портах.
Action	Когда на порту обнаружена петля, функция защиты от петель немедленно выполнит соответствующие операции. Операции могут быть следующими: • Shutdown Port (Отключить порт): Порт, на котором обнаружены петли, отключается на период времени, заданный в поле “Shutdown Time” (Период времени отключения). • Shutdown Port and Log (Выключить порт, но вести регистрацию в журнале): Порт, на котором обнаружены петли, отключается на период времени, заданный в поле “Shutdown Time” (Период времени отключения), но события регистрируются в журнале. • Log Only (Только регистрировать в журнале): События регистрируются в журнале, но порт остается включенным.
Tx Mode	Включает или выключает генерацию пакетов защиты от петель PDU либо осуществляется пассивный поиск PDU, переданных по петле.

5.2.29. Spanning Tree

При некоторых услугах, предоставляемых по сети необходимо, чтобы соединения были всегда включены – это гарантирует конечным пользователям выполнение требующихся им операций в режиме «онлайн», которые не должны прерываться неожиданными разрывами соединений. В таких обстоятельствах, для предотвращения разрывов соединений устанавливается множество активных маршрутов между узлами сети. Однако, наличие множества соединяющихся друг с другом маршрутов увеличивает вероятность образования петель (мостов), которые делают сеть нестабильной, а в наихудшем случае – неработоспособной. Например, таблица MAC-адресов, используемая коммутатором или мостом, может отказать вследствие того, что одни и те же MAC-адреса (и следовательно – одни и те же хосты сети) видны на множестве портов. Во-вторых, может произойти широковещательный шторм. Он обусловлен передачей широковещательных пакетов между коммутаторами по бесконечной петле. Широковещательный шторм может захватить все доступные ресурсы CPU и всю полосу пропускания.

Для решения проблем, связанных с мостами, протокол STP допускает сети, включающие резервные линии, которые обеспечивают автоматические резервные маршруты в том случае, если отказывает активная линия, при этом не возникает опасности образования петель и не требуется вручную включать или отключать резервные линии.

Протокол STP (Spanning Tree Protocol) определен в стандарте IEEE Standard 802.1s. Он позволяет создать топологию в смешанной сети с подключенными мостами 2-го уровня (в типичном случае - Ethernet-коммутаторами) и отключать линии, не являющиеся частью дерева, оставляя один активный маршрут между двумя любыми узлами сети.

Для обеспечения быстрой сходимости после изменения топологии сети, введен протокол, являющийся развитием IEEE Standard 802.1s - RSTP (Rapid Spanning Tree Protocol (IEEE 802.1w)). Протокол RSTP – это улучшенный STP, поэтому эти протоколы имеют сходные основные характеристики. Важно, что создается эффект каскадного соединения – начиная с корневого моста, от которого каждый назначенный (некорневой) мост предлагает своим соседям определить – возможен ли быстрый переход. Это является одним из основных элементов, которые обеспечивают ускоренную сходимость RSTP по сравнению с STP.

Другим расширением RSTP является IEEE 802.1s – MSTP (Multiple Spanning Tree protocol), который позволяет различным сетям VLAN использовать отдельные копии протокола. В отличие от STP и RSTP, MSTP устраняет необходимость иметь различные STP для каждой VLAN. Поэтому в больших сетевых средах, в которых эксплуатируется множество VLAN, MSTP может оказаться полезнее, чем традиционно используемый STP.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Spanning Tree.

Bridge Settings (Настройки моста) (Рис. 5.2.29.1) (Табл. 5.2.29.1).

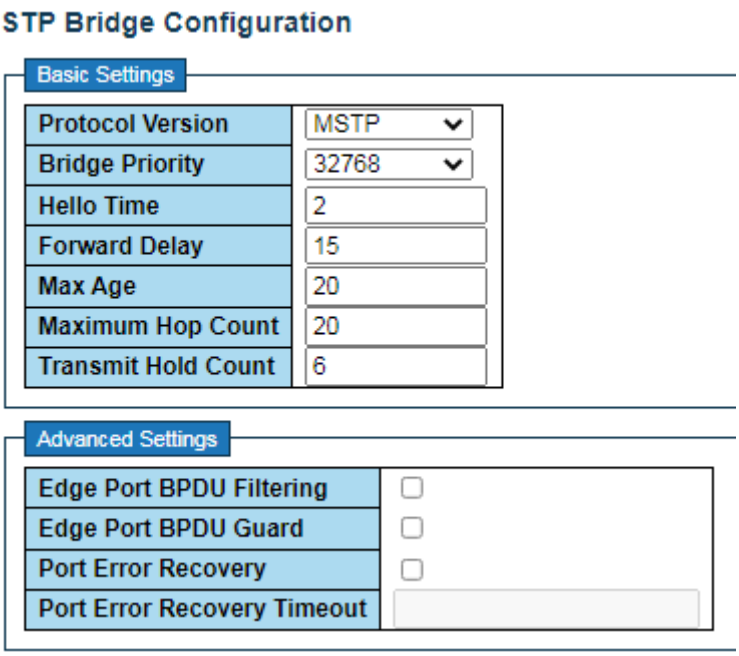


Рис. 5.2.29.1 – Настройки моста

Таблица 5.2.29.1 – Настройки моста

Basic Settings (Основные настройки)	
Protocol Version	Выберите соответствующий протокол. Версии протокола следующие: “STP”, “RSTP” и “MSTP”.
Bridge Priority	Каждый коммутатор имеет относительный приоритет и стоимость пути, которые используются для принятия решения о кратчайшем маршруте для передачи пакетов. Маршрут с наименьшей стоимостью (с наименьшим численным значением) имеет наивысший приоритет и используется всегда, пока не будет выключен. Если имеется множество мостов и интерфейсов, то для получения оптимальной производительности необходимо настроить их приоритеты. При MSTP – это приоритет CIST. В остальных случаях – это приоритет моста STP/RSTP.
Hello Time	Интервал между отправкой пакетов STP BPDU. Допустимые значения находятся в диапазоне от 1 до 10 секунд, по умолчанию - 2 секунды. Примечание. Изменение значения этого параметра по умолчанию не рекомендуется и может иметь неблагоприятные последствия для вашей сети.
Forward Delay	Для мостов STP, Forward Delay – это время, проведенное в каждом из состояний – Listening (Прослушивание) и Learning (Обучение) до перехода в состояние Forwarding (Передача пакетов). Данная задержка возникает, когда в сеть включается новый мост. Допустимые значения: от 4 до 30 секунд.
Max Age	Если другой коммутатор не пошлет конфигурационный пакет в течение заданного периода времени, он считается отключенным. Допустимый диапазон значений: от 6 до 40 секунд, значение Max Age должно быть меньше или равно (Forward Delay-1) *2.
Maximum Hop Count	Максимальное число участков между коммутаторами, после

	прохождения которых, пакет BPDU будет отброшен. При прохождении каждого моста пакетом BPDU, значение счетчика уменьшается на единицу. Когда счетчик участков маршрута станет равным нулю, пакет BPDU будет отброшен. По умолчанию число участков равно 20. Диапазон допустимых значений 6 – 40.
Transmit Hold Count	Число пакетов BPDU, посылаемых портом моста в секунду. Когда это значение превышено, передача следующего пакета BPDU будет задержана. По умолчанию задано 6 секунд. Допустимый диапазон значений: от 1 до 10. Пожалуйста, имейте в виду, что при увеличении этого значения может значительно возрасти загрузка CPU; при уменьшении значения замедляется сходимость алгоритма. Рекомендуется оставить для Transmit Hold Count значение, заданное по умолчанию.
Advanced Settings (Дополнительные настройки)	
Edge Port BPDU Filtering	Фильтрация BPDU на граничном порту. Целью фильтрации пакетов BPDU на порту является предотвращение отправки с коммутатора кадров BPDU на порты, которые подключены к конечным устройствам.
Edge Port BPDU Guard	Защита BPDU на граничном порту. Граничные порты обычно напрямую подключены к ПК, файл-серверам или принтерам. Поэтому граничные порты сконфигурированы таким образом, чтобы обеспечивалось быстрое изменение состояния. В нормальных ситуациях, граничные порты не должны принимать конфигурационные BPDU. Однако, если они принимают их, то вероятно, вследствие атак злоумышленников или неправильных настроек. Когда граничные порты принимают конфигурационные BPDU, они будут автоматически переключены в состояние неграничных портов и запустится процесс вычисления новой топологии STP. В связи с этим, для защиты устройства от атак злоумышленников применяется BPDU guard. Если граничные порты приняли конфигурационные BPDU, когда эта функция включена, то STP отключит те из них, которые приняли конфигурационные BPDU. По истечении периода времени восстановления эти выключенные порты вновь будут включены.
Port Error Recovery	Восстановление порта после ошибки. Порт, выключенный из-за ошибки, может быть автоматически включен по прошествии определенного времени.
Port Error Recovery Timeout	Время, которое должно пройти до того момента, когда порт, выключенный из-за ошибки, будет включен вновь. Допустимый диапазон значений от 30 до 86400 секунд.

MSTI Mapping (Отображение MSTI) (Рис. 5.2.29.2) (Табл. 5.2.29.2)

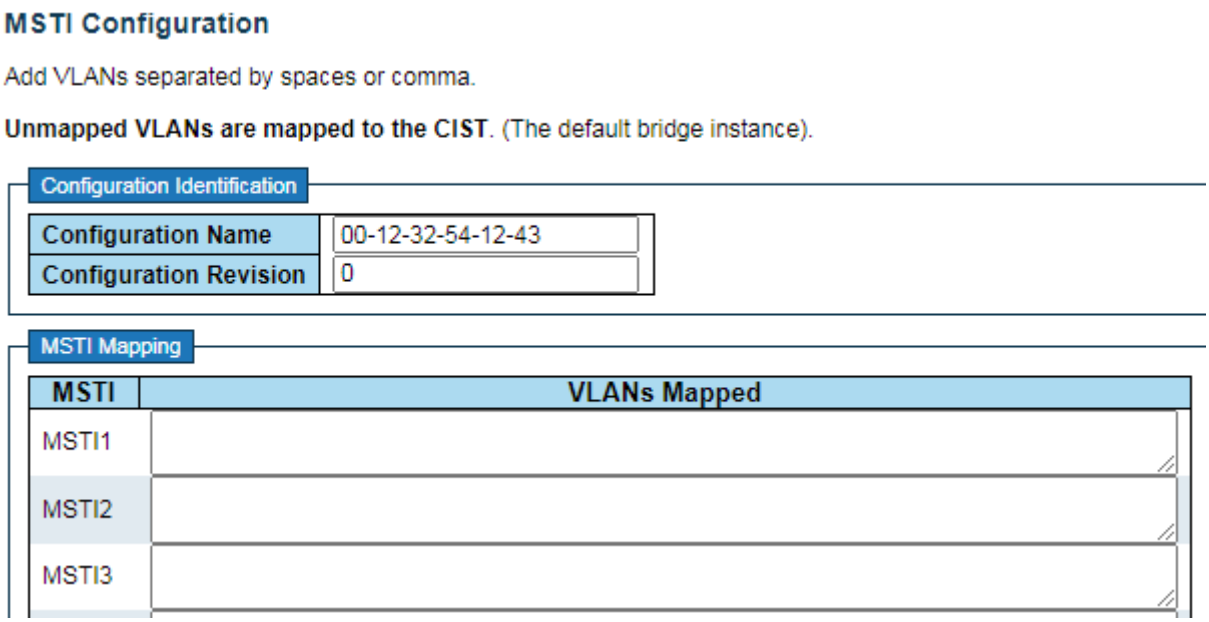


Рис. 5.2.29.2 – Отображение MSTI

Таблица 5.2.29.2 – Отображение MSTI

Configuration Identification (Идентификационные данные конфигурации)	
Configuration Name	Имя MSTI. По умолчанию используется MAC-адрес коммутатора. Максимальная длина 32 символа. Для того, чтобы совместно использовать STP для MSTI, мосты должны иметь одинаковые имена конфигураций и номера версий конфигураций.
Configuration Revision	Номер версии для MSTI. Допустимый диапазон значений: от 1 до 65535.
MSTI Mapping (Отображение MSTI)	
MSTI	Номер копии MSTI.
VLAN Mapped	Задайте номера сетей VLAN, которые будут привязаны к MSTI. Можно ввести как одну VLAN, так и диапазон номеров VLAN. Номера VLAN можно отделять запятыми и использовать тире для указания диапазона VLAN. (Пример: 2,5,20-40). Для неиспользуемых MSTI оставьте поле пустым.

MSTI Priorities (Приоритеты MSTI) (Рис. 5.2.29.3) (Табл. 5.2.29.3).

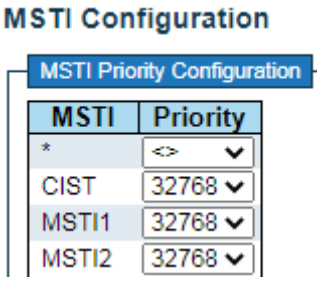


Рис. 5.2.29.3 – Приоритеты MSTI

Таблица 5.2.29.3 – Приоритеты MSTI

MSTI	Отображается номер копии MSTI. “*” – правило приоритета применяется ко всем портам.
Priority	Выберите соответствующий приоритет для каждой копии MSTI.

	Приоритет моста используется при выборе корневого устройства, корневого порта и назначенного порта. Устройство с наивысшим приоритетом становится корневым устройством. Однако, если все устройства имеют одинаковый приоритет, корневым устройством станет устройство с наименьшим MAC-адресом. Имейте в виду, что чем меньше численное значение, тем выше приоритет. Идентификатор моста формируется конкатенацией следующего: приоритет моста плюс номер копии MSTI, конкатенированный с 6- байтным MAC-адресом коммутатора.

CIST Ports (Порты CIST) (Рис. 5.2.29.4) (Табл. 5.2.29.4).

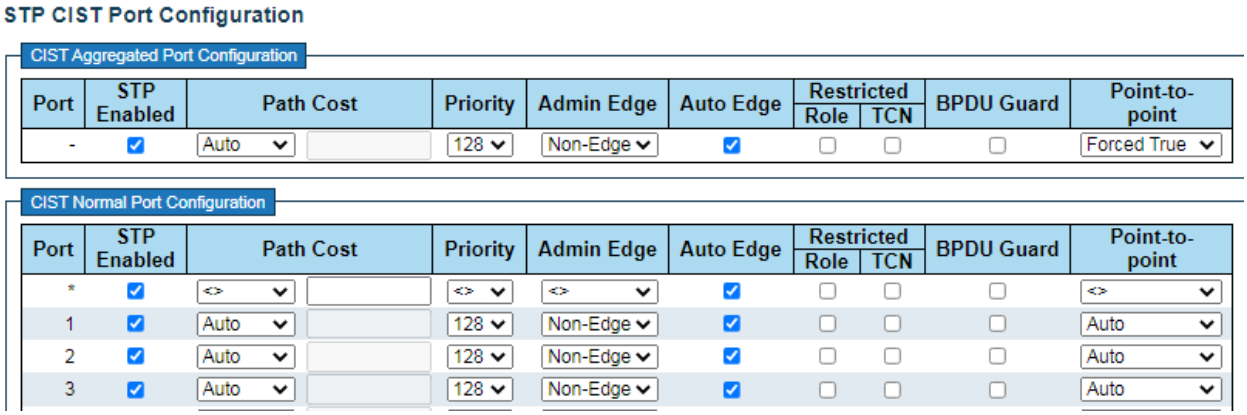


Рис. 5.2.29.4– Порты CIST

Таблица 5.2.29.4– Порты CIST

Port	Номер порта
STP Enabled	Включает функцию STP.
Path Cost	Стоимость маршрута используется для определения наилучшего маршрута между устройствами. Если выбран режим работы “Auto” (Автоматически), при определении стоимости маршрута система автоматически определяет скорость и режим дуплекса. Если требуется ввести значение, выбранное пользователем, выберите “Specific” (Специальный). Допустимые значения: от 1 до 200000000. Пожалуйста, имейте в виду, что стоимость маршрута имеет более высокий приоритет, чем приоритет порта.
Priority	Выберите приоритет порта
Admin Edge	Граница администрирования. Если интерфейс подключен к оконечным узлам, в этом поле можно задать “Edge” (Граница).
Auto Edge	Автоматическое определение границы сети. Установите флаг в этом поле, чтобы включить эту функцию. Когда функция включена, порт автоматически определяет границу сети при приеме BPDU.
Restricted Role	Ограниченная роль. Если включено, порт не будет выбран в качестве корневого для CIST или любого MSTI даже тогда, когда он имеет наилучший приоритет STP.
Restricted TCN	Ограниченный TCN. Если включено, порт не будет распространять принятые уведомления об изменении топологии и сами изменения топологии на другие порты.
BPDU Guard	Данная функция защищает порты от приема BPDU. Позволяет предотвратить петли путем выключения порта при приеме BPDU вместо помещения его в состояние discarding. Если включено,

	порт выключится до тех пор, пока не примет правильный BPDU.
Point-to-Point	Точка-точка. Выберите тип линии, подключенной к интерфейсу: • Auto (Автоматически): Коммутатор автоматически определит, какой интерфейс подключен - либо линия точка-точка, либо разделяемая среда. • Forced True (Принудительная установка соединения точка-точка): Установка соединения точка-точка. • Forced False (Принудительная установка соединения разделяемой среды): Установка соединения разделяемой среды.

MSTIPorts (Порты MSTI) (Рис. 5.2.29.5) (Табл. 5.2.29.5).

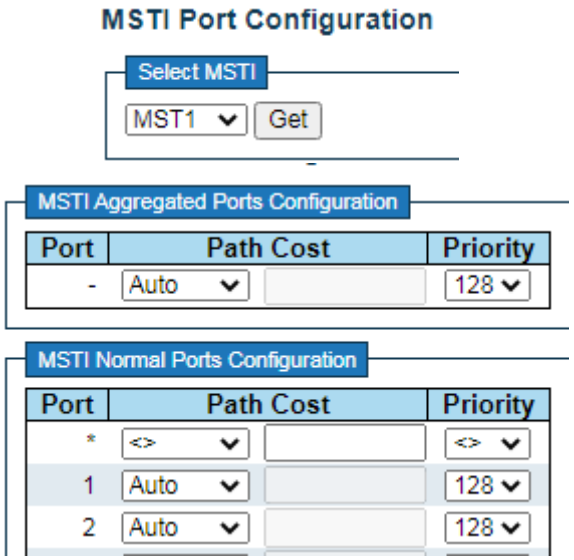


Рис. 5.2.29.5– Порты MSTI

Выберите конкретный MSTI, который требуется настроить, затем нажмите кнопку “Get”.

Таблица 5.2.29.5– Порты MSTI

Port	Номер порта
Path Cost	Стоимость маршрута используется для определения наилучшего маршрута между устройствами. Если выбран режим работы “Auto” (Автоматически), при определении стоимости маршрута система автоматически определяет скорость и режим дуплекса. Если требуется ввести значение, выбранное пользователем, выберите “Specific” (Специальный). Допустимые значения: от 1 до 200000000. Пожалуйста, имейте в виду, что стоимость маршрута имеет более высокий приоритет, чем приоритет порта.
Priority	Выберите приоритет порта.

5.2.30. IPMC Profile (Профиль IPMC)

IPMC профили используются для обеспечения контроля доступа к IP мультикаст потокам. Существует возможность создать 64 профиля с 128 правилами в каждом.

Для доступа к настройкам необходимо перейти по вкладке Configuration→IPMC Profile.

Profile Table (Таблица профиля) (Рис. 5.2.30.1) (Табл. 5.2.30.1).

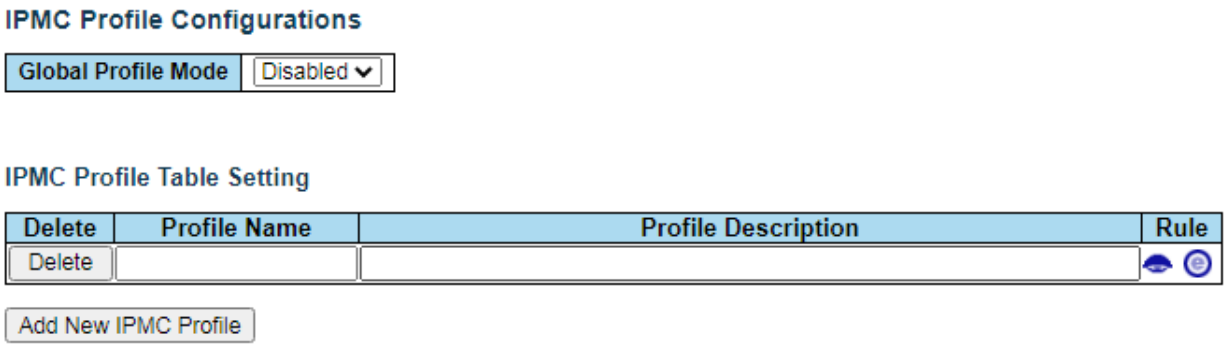


Рис. 5.2.30.1 – Таблица профиля

Таблица 5.2.30.1 – Таблица профиля

IPMC Profile Configuration (Настройкапрофиля IPMC)	
Global Profile Mode	Позволяет включить или выключить функцию IPMC Profile глобально.
IPMC Profile Table Setting (Настройкатаблицыпрофиля IPMC)	
Profile Name	Введите имя для данного профиля.
Profile Description	Введите краткое описание для данного профиля

Кнопка Add New IPMC Profile позволяет добавить новый профиль.

Address entry (Диапазоны адресов) (Рис. 5.2.30.2) (Табл. 5.2.30.2).

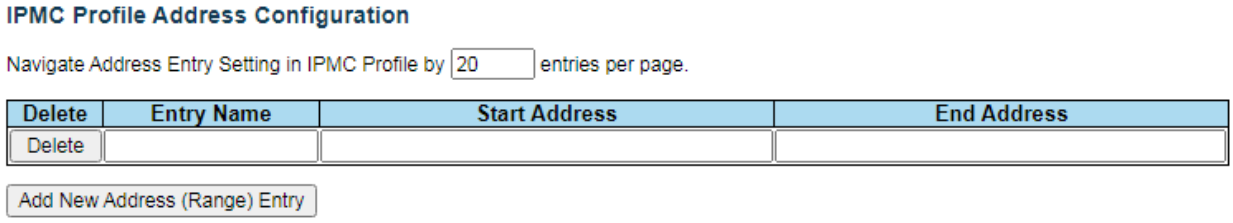


Рис. 5.2.30.2 – Диапазоны адресов

Таблица 5.2.30.2 – Диапазоны адресов

Delete	Удаление текущей записи
Entry Name	Введите имя, которое будет использоваться для индексации диапазона адресов.
Start Address	Введите в этом поле начальный адрес диапазона многоадресных адресов (IPv4 или IPv6).
End Add	Введите в этом поле конечный адрес диапазона многоадресных адресов (IPv4 или IPv6).

Кнопка Add New Address (Range) Entry позволяет добавить новый профиль.

5.2.31. MVR

Протокол MVR - регистрация многоадресных VLAN (Multicast VLAN Registration) позволяет медиасерверу передавать многоадресный поток по одной многоадресной VLAN, при этом клиенты, принимающие поток многоадресной VLAN, могут оставаться в различных сетях VLAN. Клиенты различных VLAN, намеревающиеся вступить в многоадресную группу или выйти из нее, отправляют в порт приемника сообщение IGMP Join (Вступить в группу) либо IGMP Leave (Покинуть группу). Порт приемника,

принадлежащий одной из многоадресных групп, может принимать многоадресный поток от медиасервера.

Далее, MVR изолирует пользователей, не намеревающихся принимать многоадресный трафик и, следовательно, обеспечивать безопасность данных за счет сегрегации VLAN, допускающей только многоадресный трафик в другие сети VLAN, к одной из которых принадлежит абонент. Несмотря на то, что общий многоадресный трафик проходит от MVR VLAN в VLAN различных групп, пользователи различных VLAN IEEE 802.1Q или частных VLAN не могут обмениваться какой-либо информацией (за исключением услуг маршрутизации верхнего уровня).

Для доступа к настройкам необходимо перейти по вкладке Configuration→ MVR. Configuration (Настройка) (Рис. 5.2.31.1) (Табл. 5.2.31.1).

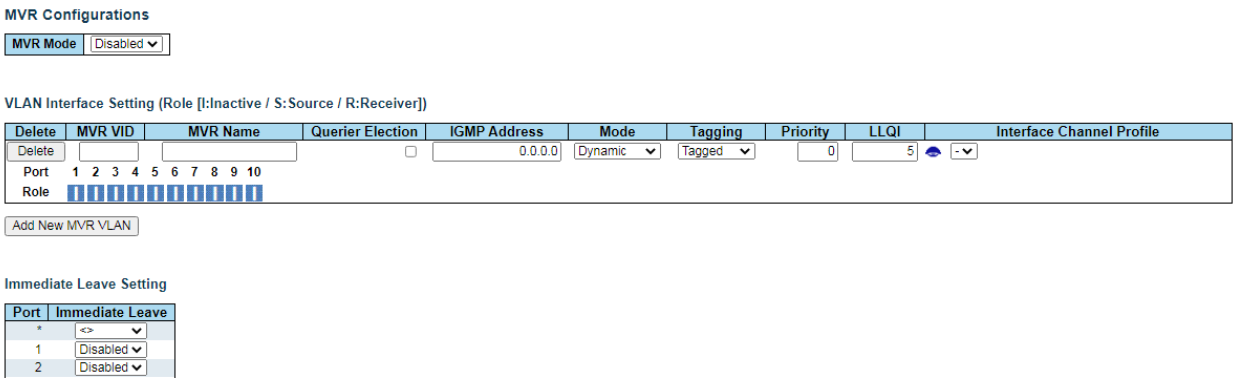


Рис. 5.2.31.1 – Настройка MVR

Таблица 5.2.31.1 – Настройка MVR

MVR Mode	Включение /выключение функции MVR.
VLAN Interface Setting (Настройка интерфейса VLAN)	
MVR VID	Задайте номер VLAN ID многоадресной VLAN. Пожалуйста, имейте в виду, что порты источника MVR не рекомендуется использовать как порты управления VLAN. Порты источника MVR должны быть сконфигурированы, как члены MVR VLAN, однако порты приемников MVR не следует вручную конфигурировать, как члены данной VLAN.
MVR Name	Дополнительно можно задать имя, определенное пользователем для данной многоадресной VLAN. Максимальная длина строки имени MVR равна 32. Разрешается использовать и буквы, и цифры.
Querier Election	Включите, чтобы присоединиться к выбору IGMP Querier в VLAN.
IGMP Address	Задайте одноадресный IPv4-адрес в качестве адреса источника, используемого в заголовке IP кадров управления IGMP.
Mode	Поддерживаются два режима работы MVR: • Dynamic (Динамический): MVR разрешает динамически отправлять сообщения о членстве на порты источника. Этот режим работы задан по умолчанию. • Compatible (Совместимый): Отправка на порты источника сообщений MVR о членстве запрещена.
Tagging	Задайте, следует ли при отправке помечать тегами MVR VID кадры управления IGMP/MLD либо их следует отправлять без тегов.
Priority	Задайте приоритет передачи кадров управления IGMP/MLD. По

	умолчанию, приоритет равен 0. Допустимые значения приоритета: 0 -7.
LLQI	LLQI – это сокращение для Last Listener Query Interval (Интервал запроса последнего слушания); LLQI применяется для настройки максимального времени ожидания сообщения о членстве IGMP/MLD на порту приемника до удаления порта из многоадресной группы. По умолчанию LLQI равно 0,5 секунды. Диапазон допустимых значений: 0-31744 десятых долей секунды.
Interface Channel Profile	Выберите профиль IPMC из раскрывающегося меню.
Port Role	Нажмите на значок роли порта, чтобы изменить состояние роли. • Inactive (I) (Неактивный): По умолчанию, все порты неактивны. Неактивные порты не 86 участвуют в работе MVR. • Source (S) (Источник): Порт (входящего трафика) является портом источника. Порты источников будут принимать и посылать многоадресные данные. Абоненты не могут быть напрямую подключены к портам источника. Имейте в виду, что порты источника не могут быть в то же время портами управления. • Receiver (R) (Приемник): Порт установлен как порт приемника. Клиентские или абонентские порты сконфигурированы, как порты приемников, так что они могут использовать сообщения IGMP/MLD для приема многоадресных данных.
Immediate Leave Setting (Настройка немедленного выхода (из группы))	
Port	Номер порта
Immediate Leave	Выбрав соответствующий раздел списка, можно включить (Enable) или выключить (disable) функцию немедленного выхода из группы. Когда функция включена, устройство немедленно удаляет порт из многоадресного потока, как только оно принимает сообщение leave (Покинуть группу) для этой группы. Данная опция применима только к интерфейсу, сконфигурированному, как приемники MVR.

Кнопка 

позволяет добавить новый MVR.

5.2.32. IPMC

5.2.32.1. IGMP Snooping

Протокол управления группами интернета IGMP (Internet Group Management Protocol) обеспечивает управление участием в многоадресных IP-группах. IGMP используется IP-хостами и соседними многоадресными маршрутизаторами для установления принадлежности к многоадресной группе. Он может использоваться наиболее эффективно при поддержке таких услуг, как потоковое онлайн-видео и игры.

IGMP Snooping – это процесс слушания трафика IGMP. Как следует из названия, IGMP snooping представляет собой функцию, позволяющую коммутатору «прослушивать» обмен данными между хостами и маршрутизаторами, обрабатывая пакеты 3-го уровня (пакеты IGMP, посылаемые по многоадресной сети).

Когда на коммутаторе включен IGMP snooping, он анализирует все пакеты, передаваемые между хостами, подключенными к коммутатору и многоадресными маршрутизаторами в сети. Когда коммутатор принимает отчет IGMP для данной многоадресной группы от хоста, коммутатор добавляет номер порта хоста к

многоадресному списку для этой группы. Когда коммутатор обнаруживает сообщение IGMP Leave (Покинуть группу IGMP), он удаляет порт хоста из ячейки таблицы.

IGMP snooping позволяет эффективно снижать многоадресный трафик при стриминге и других экстенсивно расходующих полосу пропускания IP приложениях. Коммутатор, использующий IGMP snooping, в этом трафике будет передавать хостам только многоадресный трафик. Снижение многоадресного трафика уменьшает число пакетов, обрабатываемых коммутатором (однако при этом требуется увеличение оперативной памяти для обработки многоадресных таблиц) и снижает нагрузку на оконечные хосты, так как их сетевые карты (или операционные системы) не будут принимать и фильтровать весь многоадресный трафик, генерируемый сетью.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ IPMC→IGMP Snooping.

Basic Configuration (Основные настройки) (Рис. 5.2.32.1.1) (Табл. 5.2.32.1.1).

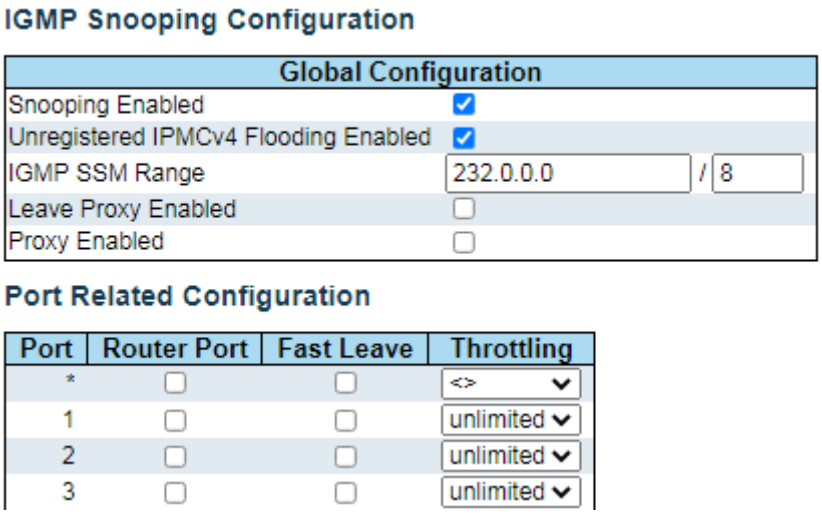


Рис. 5.2.32.1.1– Основные настройки

Таблица 5.2.32.1.1– Основные настройки

Global Configuration (Глобальные настройки)	
Snooping Enabled	Установите флаг, чтобы глобально включить функцию IGMP Snooping. Когда функция включена, данное устройство будет осуществлять мониторинг сетевого трафика и определять, какие хосты будут принимать многоадресный трафик. Коммутатор может пассивно контролировать или анализировать пакеты IGMP Query (Запросы IGMP) и IGMP Report (Отчеты IGMP), передаваемые между многоадресными IP-маршрутизаторами и подписчиками многоадресных IP-услуг для идентификации участников многоадресной группы. Коммутатор анализирует проходящие через него IGMP-пакеты, извлекает из них регистрационную информацию группы и соответствующим образом конфигурирует многоадресные фильтры.
Unregistered IPMCv4 Flooding Enabled	Если флаг в этом поле установлен, включен режим передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика. Установите флаг в этом поле, чтобы включить рассылку пакетов всем узлам.
IGMP SSM Range	Диапазон многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяет поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов.
Leave Proxy Enabled	Подавляет сообщения о выходе из группы, отличающиеся от

	принятых, от последнего порта участника группы. Прокси-сервер сообщений о выходе из группы подавляет все не являющиеся необходимыми сообщения IGMP о выходе из группы таким образом, что коммутатор, не являющийся querier, передает пакет выхода из группы только тогда, когда последний динамический порт-участник покидает многоадресную группу.
Proxy Enabled	Прокси-сервер включен
Port Related Configuration (Настройки, связанные с портом)	
Port	Номер порта
Router Port	Установите флаг в поле данного порта, чтобы назначить его портом маршрутизатора. Если IGMP snooping не может определить местонахождение IGMP querier, Вы можете вручную назначить порт, который подключен к известному IGMP querier (например, к многоадресному маршрутизатору или коммутатору). Этот интерфейс затем вступит во все текущие многоадресные группы, поддерживаемые подключенным маршрутизатором/коммутатором, чтобы гарантировать, что многоадресный трафик прошел на все соответствующие интерфейсы коммутатора.
Fast Leave	Если флаг установлен, включена функция быстрого выхода из группы. Когда принят пакет выхода из группы, коммутатор немедленно удаляет порт из многоадресной услуги, не посылая специфичный для группы запрос IGMP GS на этот интерфейс.
Throttling	Это значение ограничивает максимальное число многоадресных групп, в которые порт может вступить одновременно. Когда для порта будет достигнуто максимальное число групп, новые сообщения с отчетами IGMP о вступлении в группу будут отбрасываться. По умолчанию выбрано неограниченное число групп (unlimited). Допустимый диапазон значений от 1 до 10.

VLAN Configuration (Настройка VLAN) (Рис. 5.2.32.1.2) (Табл. 5.2.32.1.2).

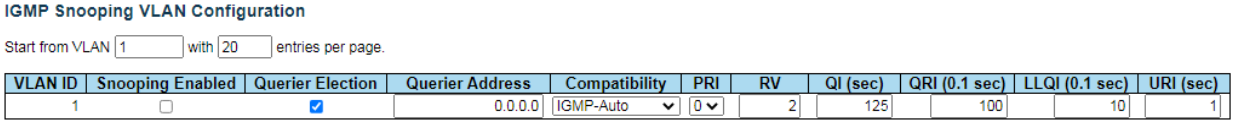


Рис. 5.2.32.1.2 – Настройка VLAN

Таблица 5.2.32.1.2 – Настройка VLAN

VLAN ID	Задайте номер VLAN, используемой для IGMP snooping.
Snooping Enabled	Установите флаг, чтобы включить функцию «прослушивания» на интерфейсе. Когда эта функция включена, коммутатор будет контролировать сетевой трафик на указанном интерфейсе, чтобы определить, какие хосты желают получать многоадресные услуги. Если IGMP snooping включен глобально и IGMP snooping включен на интерфейсе, то приоритетом будет пользоваться IGMP snooping на интерфейсе. Когда флаг в этом поле снят, «прослушивание» может оставаться сконфигурированным на интерфейсе. Однако настройки будут действовать только в том случае, если IGMP snooping включен глобально.
Querier Election	Установите флаг в этом поле, чтобы выбрать порт запросов в VLAN.

	Когда флаг в поле снят, порт будет использоваться как порт IGMP, не посылающий запросов.
Querier Address	Задайте одноадресный IPv4-адрес, используемый в 90 заголовке IP для выбора порта-источника запросов IGMP. Когда это поле не задано, коммутатор будет использовать первый доступный IPv4-адрес управления IP-интерфейса, ассоциированного с этой VLAN.
Compatibility	В этом поле задано, какие хосты и маршрутизаторы могут выполнять операции в сети (в зависимости от выбранной версии IGMP). Доступны следующие варианты: “IGMP-Auto” (Автоматический выбор версии IGMP), “Forced IGMPv1” (Принудительное использование IGMPv1), “Forced IGMPv2” (Принудительное использование IGMPv2), “Forced IGMPv3” (Принудительное использование IGMPv3). По умолчанию применяется “IGMP-Auto” (Автоматический выбор версии IGMP).
PRI	Выберите приоритет интерфейса. В этом поле указано уровень приоритета кадра управления IGMP, сгенерированный системой, которая использована для назначения приоритетов различным классам трафика. Диапазон допустимых значений: от 0 (наименьший приоритет) до 7 (наивысший приоритет). По умолчанию, приоритет интерфейса равен 0.
RV	Переменная надежности RV (robustness variable) позволяет настроить ожидаемые потери пакетов в подсети. Если есть подозрение, что в подсети теряются пакеты, это значение можно увеличить. Значение RV не должно быть нулем или 1. Значение должно быть 2 или более. По умолчанию задано 2.
QI	В поле Query Interval (Интервал между запросами) указан интервал времени между отправкой запросчиком сообщений с общими запросами IGMP (IGMP General Query). По умолчанию задан интервал 125 секунд.
QRI	Query Response Interval – максимальное время ожидания маршрутизатором IGMP приема ответа на сообщение с запросом IGMP General Query. QRI применяется, когда коммутатор функционирует, как запросчик и используется для информирования других устройств о максимальном времени, которое данная система ожидает ответа на общие запросы. По умолчанию задано значение 10 секунд. Диапазон допустимых значений: 0-31744 десятых долей секунды.
LLQI	Last Listener Query Interval – время ожидания ответа на запросное сообщение, специфичное для группы или на запросное сообщение, специфичное для группы и источника.
URI	Unsolicited Report Interval – время ожидания передачи входящим интерфейсом непредусмотренных отчетов IGMP, когда включено их подавление или фильтрация на прокси-сервере. По умолчанию для URI задано значение 1 секунда. Диапазон допустимых значений: от 0 до - 31744 секунд.

Port Filtering Profile (Профиль фильтрации порта) (Рис. 5.2.32.1.3) (Табл. 5.2.32.1.3).

На странице настройки фильтрации порта можно отфильтровать определенный многоадресный трафик по каждому порту отдельно. Перед тем, как выбирать профиль фильтрации, необходимо задать профили на странице IPMC Profile (Профиль IPMC).

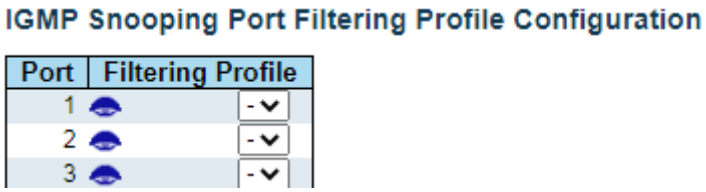


Рис. 5.2.32.1.3 – Профиль фильтрации порта

Таблица 5.2.32.1.3 – Профиль фильтрации порта

Port	Номер порта.
Filtering Profile	Выберите сконфигурированные многоадресные группы, которые запрещены на порту. Когда определенная многоадресная группа выбрана на порту, сообщения IGMP join reports (отчеты о вступлении в группу) на порту отбрасываются.

5.2.32.2. MLD Snooping

Протокол MLD (Multicast Listener Discovery snooping) подобен протоколу IGMP snooping для IPv4 и используется для многоадресного трафика IPv6. Другими словами, MLD snooping конфигурирует порты для ограничения многоадресного трафика IPv6 или управления им таким образом, чтобы он передавался на порты (или пользователям), которым он действительно требуется. В результате, MLD snooping снижает лавинообразную передачу многоадресных пакетов IPV6 по заданным VLAN. Пожалуйста, имейте в виду, что IGMP Snooping и MLD Snooping работают независимо друг от друга. Они могут быть включены одновременно.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ IPMC→ MLD Snooping.

Basic Configuration (Основные настройки) (Рис. 5.2.32.2.1) (Табл. 5.2.32.2.1).

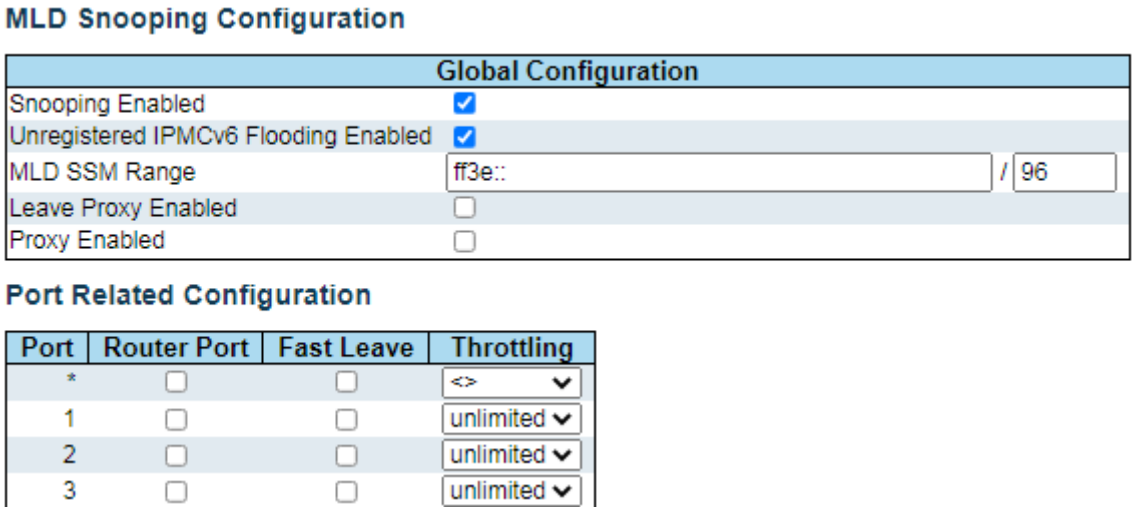


Рис. 5.2.32.2.1 – Основные настройки

Таблица 5.2.32.2.1 – Основные настройки

Global Configuration (Глобальные настройки)	
Snooping Enabled	Установите флаг, чтобы глобально включить функцию MLD Snooping. Когда функция включена, данное устройство будет осуществлять мониторинг сетевого трафика и определять, какие хосты будут принимать многоадресный трафик. Коммутатор может пассивно контролировать или анализировать пакеты MLD Listener Query (Запросы прослушивания MLD) и MLD Report (Отчеты MLD), передаваемые между многоадресными IP

	маршрутизаторами и подписчиками многоадресных IP услуг для идентификации участников многоадресной группы. Коммутатор анализирует проходящие через него IGMP-пакеты, извлекает из них регистрационную информацию группы и соответствующим образом конфигурирует многоадресные фильтры.
Unregistered IPMCv6 Flooding Enabled	Если флаг установлен, включен режим передачи незарегистрированного (не принадлежащего группам) многоадресного IP-трафика. Установите флаг, чтобы включить рассылку пакетов всем узлам.
MLD SSM Range	Диапазон многоадресных адресов для конкретного источника SSM (Source-Specific Multicast), позволяет поддерживающим SSM хостам и маршрутизаторам выполнять модель услуг SSM для групп в заданном диапазоне адресов.
Leave Proxy Enabled	Чтобы предотвратить перегрузку многоадресного маршрутизатора сообщениями о выходе из группы, MLD snooping подавляет их, пока не примет такое сообщение от последнего порта-участника группы. Когда коммутатор работает, как запросчик, функция проксисервера для сообщений о выходе из группы работать не будет.
Proxy Enabled	Когда прокси-сервер MLD включен, коммутатор обменивается сообщениями MLD с маршрутизатором своего восходящего интерфейса и выполняет задачи хоста MLD на восходящем интерфейсе: • Когда приходит запрос, он посылает отчет многоадресного прослушивания группе. • Когда хост вступает в многоадресную группу, в которой нет других хостов, он посылает этой группе непредусмотренные отчеты. • Когда определенную многоадресную группу покидает последний хост, коммутатор посылает непредусмотренный отчет по адресу, используемому всеми маршрутизаторами (FF02::2) при MLDv1.
Port Related Configuration (Настройки, связанные с портом)	
Port	Номер порта
Router Port	Установите флаг, чтобы назначить портом маршрутизатора. Если MLD snooping не может определить местонахождение MLD querier, Вы можете вручную назначить порт, который подключен к известному IGMP querier (например, к многоадресному маршрутизатору или коммутатору). Этот интерфейс затем вступит во все текущие многоадресные группы, поддерживаемые подключенным маршрутизатором /коммутатором, чтобы гарантировать, что многоадресный трафик прошел на все соответствующие интерфейсы коммутатора.
Fast Leave	Если флаг в поле установлен, включена функция быстрого выхода из группы. Когда принят пакет выхода из группы, коммутатор немедленно удаляет порт из многоадресной услуги, не посылая специфичный для группы запрос MLD GS на этот интерфейс.
Throttling	Это поле ограничивает максимальное число многоадресных групп, в которые порт может вступить одновременно. Когда для порта будет достигнуто максимальное число групп, новые сообщения с отчетами MLD о вступлении в группу будут отбрасываться. По умолчанию выбрано неограниченное число групп (unlimited). Допустимый диапазон значений от 1 до 10.

VLAN Configuration (Настройка VLAN) (Рис. 5.2.32.2.2) (Табл. 5.2.32.2.2).

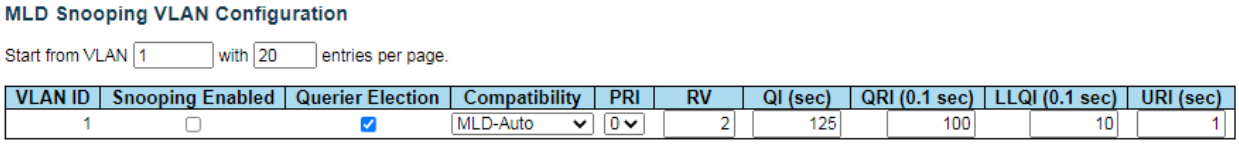


Рис. 5.2.32.2.2 – Настройка VLAN

Таблица 5.2.32.2.2 – Настройка VLAN

VLAN ID	Задайте номер VLAN, используемой для MLD snooping.
Snooping Enabled	Установите флаг в этом поле, чтобы включить функцию «прослушивания» на интерфейсе. Когда эта функция включена, коммутатор будет контролировать сетевой трафик на указанном интерфейсе, чтобы определить, какие хосты желают получать многоадресные услуги.
Querier Election	Установите флаг в этом поле, чтобы выбрать порт запросов в VLAN. Когда флаг в этом поле установлен, коммутатор может использоваться, как запросчик MLDv2, конкурируя с другими многоадресными маршрутизаторами или коммутаторами. Как только коммутатор станет запросчиком, он будет отвечать за отправку на хосты периодических запросов о том, желают ли они принимать многоадресный трафик. Когда флаг в поле снят, порт будет использоваться как порт IGMP, не посылающий запросов.
Compatibility	В этом поле задано, какие хосты и маршрутизаторы могут выполнять операции в сети (в зависимости от выбранной версии MLD). Доступны следующие варианты: “MLD-Auto” (Автоматический выбор версии MLD), “Forced MLDv1” (Принудительная установка версии MLDv1) и “Forced MLDv2” (Принудительная установка версии MLDv2). По умолчанию применяется “MLD-Auto” (Автоматический выбор версии MLD).
PRI	Выберите приоритет интерфейса. В этом поле указано уровень приоритета кадра управления MLD, сгенерированный системой, которая использована для назначения приоритетов различным классам трафика. Диапазон допустимых значений: от 0 (наименьший приоритет) до 7 (наивысший приоритет). По умолчанию, приоритет интерфейса равен 0.
RV	Переменная надежности RV (robustness variable) позволяет настроить ожидаемые потери пакетов в подсети. Если есть подозрение, что в подсети теряются пакеты, это значение можно увеличить. Значение RV не должно быть нулем или 1. Значение должно быть 2 или более. По умолчанию задано 2. Диапазон допустимых значений: 1~255.
QI	В поле Query Interval (Интервал между запросами) указан интервал времени между отправкой запросчиком сообщений с общими запросами IGMP (IGMP General Query). По умолчанию задан интервал 125 секунд. Допустимый диапазон значений от 1 до 31744 секунд.
QRI	Query Response Interval – максимальное время ожидания маршрутизатором IGMP приема ответа на сообщение с запросом IGMP General Query. QRI применяется, когда коммутатор функционирует, как запросчик и используется для информирования других устройств о максимальном времени, которое данная система

	ожидает ответа на общие запросы. По умолчанию для RQI задано значение 10 секунд. Диапазон допустимых значений: 0- 31744 десятых долей секунды.
LLQI	Last Listener Query Interval – время ожидания ответа на запросное сообщение, специфичное для группы или на запросное сообщение, специфичное для группы и источника.
URI	Unsolicited Report Interval – время ожидания передачи входящим интерфейсом непредусмотренных отчетов IGMP, когда включено их подавление или фильтрация на прокси - сервере. По умолчанию для URI задано значение 1 секунда. Диапазон допустимых значений: от 0 до 31744 секунд.

Port Filtering Profile (Профиль фильтрации порта) (Рис. 5.2.32.2.3) (Табл. 5.2.32.2.3)

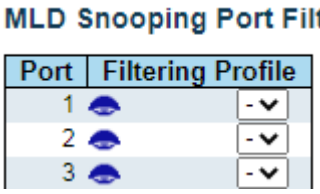


Рис. 5.2.32.2.3 – Профиль фильтрации порта

Таблица 5.2.32.2.3 – Профиль фильтрации порта

Port	Номер порта.
Filtering Profile	Выберите сконфигурированные многоадресные группы, которые запрещены на порту. Когда определенная многоадресная группа выбрана на порту, сообщения MLD join reports (отчеты о вступлении в группу) на порту отбрасываются.

5.2.33. LLDP

Протокол LLDP (Link Layer Discovery Protocol) является протоколом канального уровня, на котором сетевые устройства обмениваются информацией о себе с другими устройствами, напрямую соединенными через сеть. Используя LLDP, два устройства, на которых функционируют сетевые протоколы разных уровней, могут обучаться информации друг друга. Для обнаружения соседних устройств используется набор атрибутов, ссылающийся на TLV. Устройство может передавать и принимать такую детальную информацию, как описание порта, описание системы и ее возможностей, адрес управления.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ LLDP.

Configuration (Настройка) (Рис. 5.2.33.1) (Табл. 5.2.33.1).

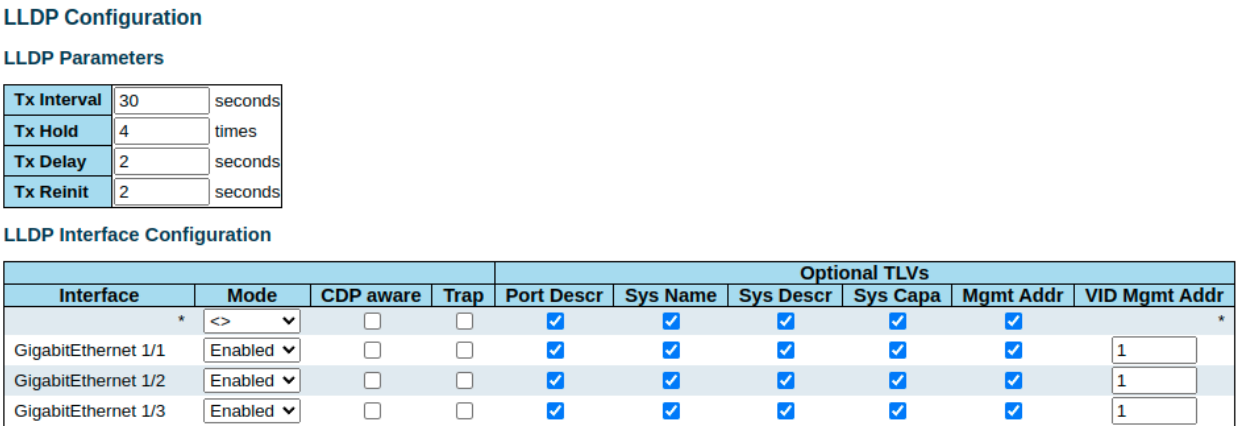


Рис. 5.2.33.1 – Настройка LLDP

Таблица 5.2.33.1 – Настройка LLDP

LLDP Parameters (Параметры LLDP)	
Tx Interval	Задайте интервал между кадрами LLDP, отправляемыми соседям данного устройства для обновления информации о данном устройстве. Допустимые значения: от 5 до 32768 секунд. По умолчанию задано 30 секунд.
Tx Hold	Данная настройка определяет, как долго кадры LLDP будут считаться правильными и используется для вычисления TTL. Диапазон допустимых значений: 2~10 раз. По умолчанию задано 4.
Tx Delay	Задайте задержку между кадрами LLDP, содержащими изменения конфигурации. Tx Delay не может превышать 1/4 от интервала Tx. Допустимые значения: от 1 до 8192 секунд.
Tx Reinit	Задайте задержку между кадром отключения и новой инициализацией LLDP. Допустимые значения: от 1 до 10 секунд.
LLDP Interface Configuration (Настройка интерфейса LLDP)	
Interface	Интерфейс
Mode	Выберите соответствующий режим работы LLDP: • Disabled (Выключен): Информация LLDP посылаться не будет, информация LLDP, принятая от соседних устройств будет отброшена. • Enabled (Включить): Информация LLDP будет посылаться, информация LLDP, принятая от соседних устройств будет проанализирована. • Rx Only (Только прием): Коммутатор будет анализировать информацию LLDP, принятую от соседних устройств. • Tx Only (Только передача): Коммутатор будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, принятую от соседних устройств.
CDP Aware	Операция CDP aware (Распознавание CDP) используется для декодирования входящих кадров CDP (Cisco Discovery Protocol). Если эта опция включена, CDP TLVs, которые могут быть отображены в соответствующее поле таблицы соседних устройств LLDP будут декодированы, в противном случае эти кадры будут отброшены. CDP TLVs отображаются в поле таблицы соседних устройств LLDP.
Optional TLVs	Для обнаружения соседних устройств, LLDP использует несколько атрибутов. Эти атрибуты содержат описания типа, длины и значений

	и ссылаются на TLVs. Данное устройство может передавать такую детальную информацию, как описание порта, имя и описание системы и ее возможностей, адрес управления. Если нежелательно, чтобы соседние устройства обладали этой информацией, снимите флаг в этом поле.

LLDP-MED (Рис. 5.2.33.2) (Табл. 5.2.33.2).

Протокол LLDP для конечных медиаустройств LLDP-MED (LLDP for Media Endpoint Devices) является расширением LLDP и работает между конечными устройствами, такими как IP-телефоны и сетевыми устройствами (например, коммутаторами). Протокол LLDP-MED обеспечивает поддержку приложений передачи голоса по IP (VoIP) и дополнительные TLVs для обнаружения, обеспечения политики сети, функции Power over Ethernet, управления реестром и информации о местоположении.

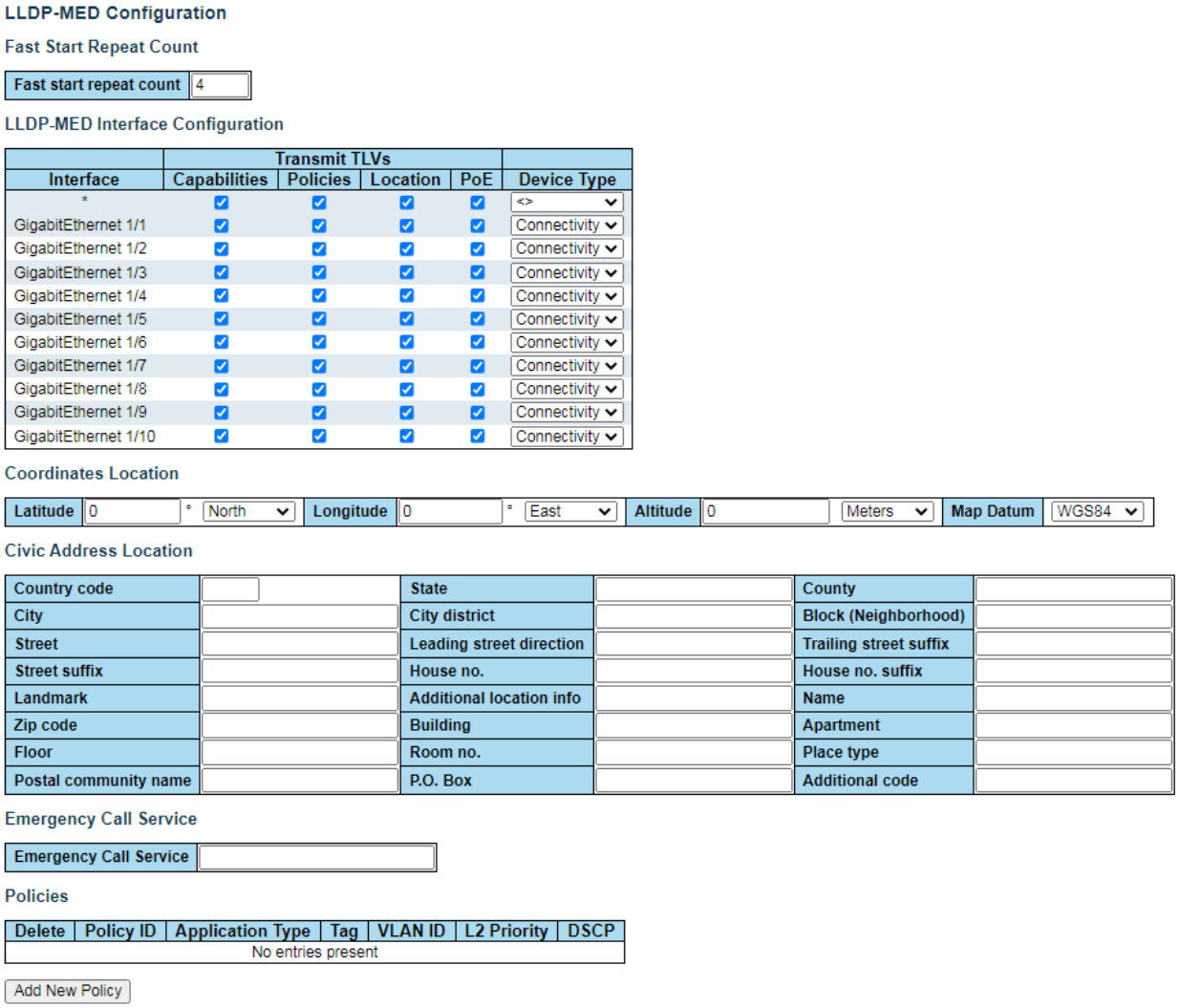


Рис. 5.2.33.2 – Настройка LLDP-MED

Таблица 5.2.33.2 – Настройка LLDP-MED

Fast Start Repeat Count	Быстрый старт и идентификация местоположения при аварийном вызове (Emergency Call Service Location Identification Discovery) для конечных устройств является важным аспектом VoIP-систем. Кроме того, лучше всего предоставлять только те части информации, которые действительно важны для конечного устройства данного типа (например, оповещать о правилах работы в голосовой сети

	следует только те устройства, которые могут работать с голосовым трафиком). Это необходимо также и для сохранения ограниченного пространства LLDPU и уменьшения проблем с безопасностью и целостностью системы, которые могут возникать изза того, что информация о правилах работы в сети будет попадать на не предназначенные для этой информации устройства. В связи с этим, в LLDPMED для достижения соответствующих свойств определен этап взаимодействия LLDP-MED Fast Start (Быстрый старт LLDP-MED) между протоколом и уровнем приложений на вершине протокола. Параметр Fast start repeat count (Число повторов быстрого старта) позволяет задать, сколько раз будет повторен быстрый старт передачи. Рекомендуемое значение (4 раза) означает, что с интервалом 1 секунда будут переданы 4 кадра LLDP, если принят кадр LLDP с новой информацией. Следует отметить, что LLDP-MED и механизм LLDP-MED Fast Start предназначены только для работы на линиях между устройствами соединения по сети, поддерживающими LLDP-MED и конечными устройствами и неприменимы к линиям между элементами инфраструктуры LAN, включая и устройства соединения по сети или линии другого типа.
LLDP-MED Interface Configuration	
Interface	Интерфейс, к которому применяется конфигурация.
Transmit TLVs	При установленном флажке, соответствующие параметры коммутатора включаются в передаваемую информацию LLDP-MED .
Device Type	Тип устройства
Coordination Locations (Координаты местоположения)	
Latitude	Широта должна быть приведена в диапазоне 0-90 градусов и содержать не более 4 цифр. Можно задать экваториальное положение либо на север от экватора (North) либо на юг (South) от экватора.
Longitude	Долгота должна быть приведена в диапазоне 0-180 градусов и содержать не более 4 цифр. Можно указать направление – либо на восток от нулевого меридиана (East) либо на запад от нулевого меридиана (West).
Altitude	Высота должна быть приведена в диапазоне от - 32767 до 32767 и содержать не более 4 цифр. Можно выбрать единицы измерения высоты – либо в метрах, либо в этажах.
Meters	Метры высоты, отсчитываются от заданного датума (нулевого уровня) по вертикали.
Map Datum	Параметр Map Datum используется для выбора системы координат: • WGS84: (Географические, трехмерные) – Всемирная геодезическая система 1984, CRS Code 4327, нулевой меридиан: гринвичский. • NAD83/NAVD88: Североамериканская система координат 1983, CRS Code 4269, нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - North American Vertical Datum of 1988 (NAVD88). Эта пара систем координат используется для указания местоположения на земле, на водных пространствах, подверженных приливам и отливам (для которых можно использовать систему координат NAD83/MLLW). • NAD83/MLLW: Североамериканская система координат 1983, CRS Code 4269, нулевой меридиан: гринвичский; связанная с этой система координат по вертикали - Mean Lower Low Water (MLLW). Эта пара связанных систем координат используется при указании

	местоположения в океане, на морях и на других водных пространствах.
Civic Address Location (Указание гражданского адреса) Стандартная форма гражданского адреса (IETF Geopriv Civic Address) базируется на конфигурационной информации местоположения (Location Configuration Information) и обозначается как Civic Address LCI.	
Country Cod	Код страны по стандарту ISO 3166, состоящий из двух прописных букв ASCII. Пример: DK, DE или US.
State	Единица административно-территориального деления (штат, кантон, регион, провинция, префектура).
Country	Округ.
City	Город, поселок.
City District	Район города, округ города, административный район города.
Block	Квартал, блок.
Street	Улица. Пример: ул. Ленина
Leading street direction	Направление главной улицы. Пример: N.
Trailing street suffix	Навигационный суффикс улицы. Пример: SW
Street suffix	Суффикс улицы. Пример: Проезд.
House no.	Номер дома
House no. suffix	Суффикс номера дома: Пример: B, 1/2.
Landmark	Адрес какого-либо заметного объекта на местности. Пример: Кремль.
Additional Location Info	Дополнительная информация о местоположении. Пример: Северное крыло.
Name	ФИО резидента или лица, арендующего офис.
Zip Code	Почтовый код
Building	Строение. Пример: Аквапарк.
Apartement	Апартамент, номер. Пример: Apt 34.
Floor	Этаж
Room no.	Номер комнаты
Place type	Тип площади
Postal community name	ФИО почтового адресата
P.O. Box	Номер абонентского ящика
Additional Code	Добавочный код
Emergency Call Service	Служба спасения
Policies (Правила)	
Policy Id	Задайте идентификатор ID для этой группы правил
Application Type	Типы приложений, в том числе: “Voice” (Голосовой вызов), “Voice Signalling” (Сигнализация голосового вызова), “Guest Voice” (Гостевой голосовой вызов), “Guest Voice Signalling” (Сигнализация гостевого голосового вызова), “Softphone Voice” (Голосовой вызов по софтофону), “Video Conferencing” (Видеоконференция), “Streaming” (Потоковая передача), “Video Signalling” (Сигнализация видеопотока).
Tag	Тег, указывающий, использует ли заданный тип приложения «тегированную» VLAN или «не тегированную» VLAN.
VLAN ID	Задайте VLAN ID для порта.

L2 Priority	Задайте один из восьми уровней приоритета (0-7), как определено в 802.1D-2004.
DSCP	Задайте одно из значений 64-точечного кода (0-63)

Кнопка Add New Policy предназначена для добавления нового правила.

5.2.34. POE

Power over Ethernet (PoE) – технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными через стандартную витую пару в сети Ethernet. Данная технология предназначается для IP-телефонии, точек доступа беспроводных сетей, IP-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ PoE.
Power over Ethernet Configuration (Настройка PoE) (Рис. 5.2.34.1) (Табл. 5.2.34.1).

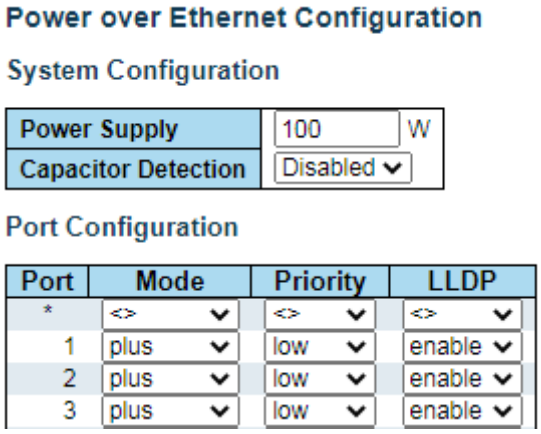


Рис. 5.2.34.1 – Настройка PoE

Таблица 5.2.34.1 – Настройка PoE

Глобальные настройки	
Power Supply	Настройка максимальной мощности, которую может обеспечить источник питания.
Capacitor Detection	Включение/выключение функции `capacitor-detect`
Настойка портов	
Port	Номер порта
Mode	Выбор режима poe для порта Plus - включает PoE IEEE 802.3bt с поддержкой устаревшей поддержки Standard - включает режим соответствия PoE IEEE 802.3bt Disable- PoE отключено для порта
Priority	Установка приоритета. Существует три уровня приоритета мощности: низкий, высокий и критический. Приоритет используется в том случае, когда удаленным устройствам требуется больше энергии, чем может обеспечить источник питания. В этом случае порт с самым низким приоритетом будет
LLDP	Включение/выключение обработки параметров PoE, полученных через LLDP.

5.2.35. MAC Table. Таблица MAC-адресов

Для доступа к настройкам необходимо перейти по вкладке Configuration→MAC Table. MACAddressTableConfiguration (Настройка таблицы MAC-адресов) (Рис. 5.2.35.1) (Табл. 5.2.35.1).

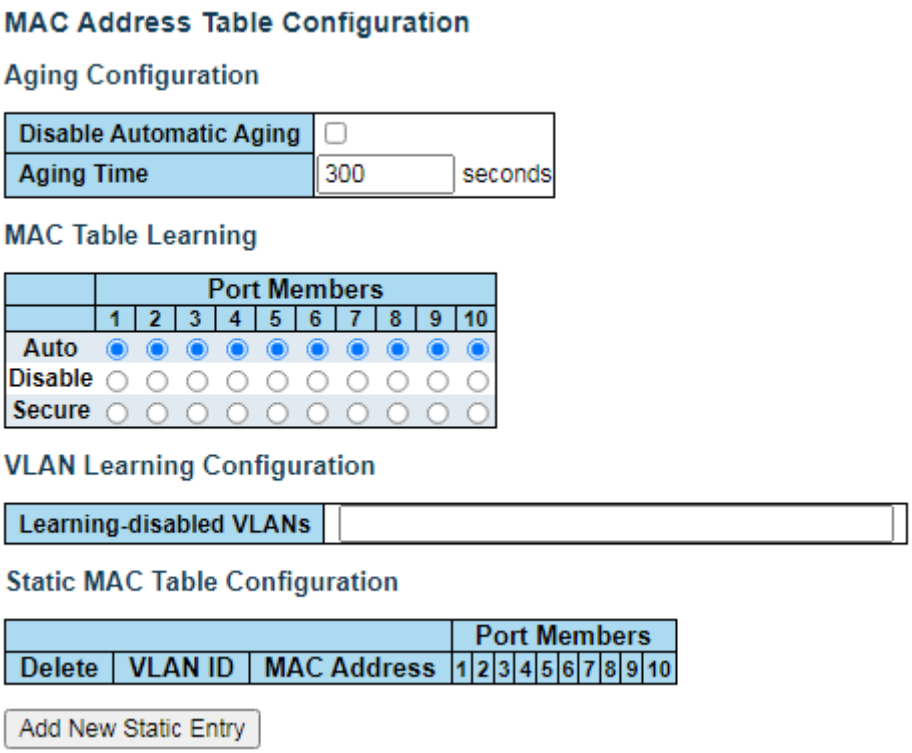


Рис. 5.2.35.1 – Настройка таблицы MAC – адресов

Таблица 5.2.35.1 – Настройка таблицы MAC - адресов

Disable Automatic Aging	Отключить автоматическое устаревание. MAC - адреса, полученные обучением, будут присутствовать в таблице постоянно.
Aging Time	Задайте срок устаревания для MAC - адресов, полученных обучением, которые будут присутствовать в таблице MAC - адресов. Диапазон допустимых значений: от 10 до 1000000 секунд.
MAC Learning Table	На каждом порту можно включить одну из трех опций: • Auto (Автоматически): на данном порту обучение будет выполнено автоматически, как только будет принят неизвестный MACадрес. • Disable (Выключить): Функция обучения MAC-адресам выключена. • Secure (Только безопасные MAC-адреса): Обучение будет выполнено только для статических MAC-адресов, перечисленных в списке “Static MAC Table Configuration”. Другие MAC-адреса будут отброшены. Удостоверьтесь в том, что линия, используемая для управления коммутатором добавлена в таблицу статических MAC-адресов до включения режима обучения статическим адресам. В противном случае линия управления будет потеряна и ее можно будет восстановить только путем использования другого небезопасного порта либо при подключении коммутатора по последовательному интерфейсу.
Learning-disabled	В этом поле отображаются VLAN с отключенным обучением. Когда

VLANs	НОВЫЙ MAC-адрес поступает в виртуальную локальную сеть с отключенным обучением, MAC-адрес не будет изучен. По умолчанию поле пустое. Можно создать больше сетей VLAN, используя синтаксис списка, в котором отдельные элементы разделены запятыми. Диапазоны указываются с помощью тире, разделяющей нижнюю и верхнюю границы.
Static MAC Table Configuration (Настройка таблицы статических MAC - адресов): Эта таблица используется для установки статических MAC - адресов вручную. Общее число элементов таблицы, которые можно ввести, равно 64.	
Delete	Удаляет MAC - адрес из ячейки таблицы
VLAN ID	Задайте идентификатор VLAN ID для этого MAC - адреса.
Port Members	Установите (или снимите) флаги у соответствующих портов. Если входящий пакет имеет тот же MAC-адрес назначения, что и указанный в VID, он будет передан непосредственно в порт, отмеченный флагом.

Кнопка 

предназначена для добавления MAC – адреса.

5.2.36. VLANs

Использование виртуальных локальных сетей VLAN (Virtual Local Area Network) является популярным и недорогим способом сегментирования развернутой сети по логически сгруппированным устройствам безотносительно к их физическим соединениям. Сети VLAN также сегментируют сеть на различные широковещательные домены таким образом, что пакеты передаются на порты внутри VLAN, которой они принадлежат.

Сети VLAN повышают безопасность. Устройства, которые часто связываются друг с другом группируются в одну и ту же VLAN. Если устройства данной VLAN желают связаться с устройствами в другой VLAN, трафик должен пройти через устройство маршрутизации или коммутатор 3-го уровня.

Сети VLAN упрощают управление трафиком. В обычных сетях, не сегментированных на VLAN, легко возникает перегрузка, обусловленная широковещательным трафиком, адресованного всем устройствам. Сводя к минимуму распространение широковещательного трафика по всей сети, сети VLAN облегчают работу устройствам группы, часто связывающимся с другими устройствами в той же VLAN за счет деления всей сети на несколько доменов вещания.

Сети VLAN упрощают замену устройств или их установку в другое место. В традиционных сетях, когда устройство требуется переместить в другое место (например, перенести со 2 этажа на 4 этаж), администратору сети потребуется изменить IP-адрес или даже подсеть сети либо заново протянуть кабели. Однако, при использовании сетей VLAN, исходные настройки можно сохранить, а прокладку кабелей – свести к минимуму.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ VLANs.

VLAN Configuration (Настройка VLAN) (Рис. 5.2.36.1) (Табл. 5.2.36.1).

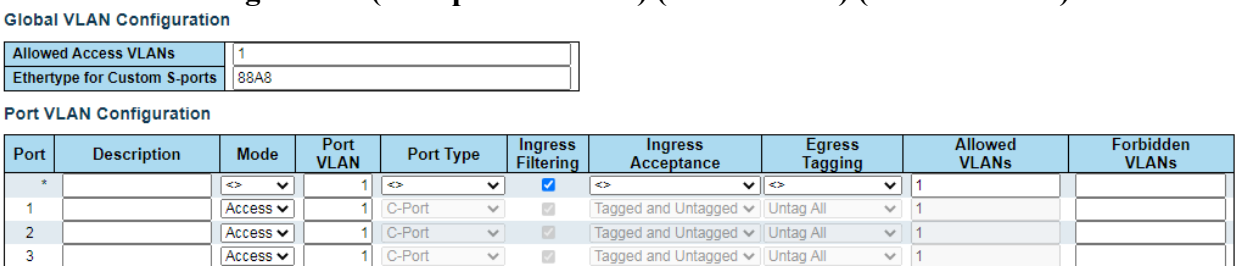


Рис. 5.2.36.1 – Настройка VLAN

Таблица 5.2.36.1 – Настройка VLAN

Global VLAN Configuration (Глобальная конфигурация VLAN)	
Allowed Access VLANs	Это поле показывает разрешенные Access VLAN, таким образом, эта настройка влияет только порты, настроенные в режиме access. Порты в других режимах являются членами всех VLAN, указанных в поле Allowed Access VLANs. По умолчанию, только VLAN 1 включено.
Ethertype for Custom Sports	Задайте тип ethertype/TPID, используемый для специализированных s-портов.
Port VLAN Configuration (Настройка VLAN на порту)	
Port	Номер порта. “*” означает применение ко всем портам.
Mode	Режим работы порта (по умолчанию access) определяет фундаментальное поведение порта. Порт может находиться в одном из трех режимов, как описано ниже: • Access (Доступ): Порты доступа, как правило, используется для подключения к конечным станциям. Динамические функции, такие как Voice VLAN могут добавить порт к большему количеству VLAN. Порты доступа имеют следующие характеристики: - Принадлежит ровно к одной VLAN (port VLAN). - Принимает не тегированные и стегированные кадры. - Удаляет все кадры, которые не классифицируются как access VLAN. - На выходе все кадры, классифицированные как Access VLAN, передаются без тегов. Другие (динамически добавленные VLAN) передаются с тегами. • Trunk (Магистральные): Магистральные порты могут передавать трафик на несколько виртуальных локальных сетей одновременно и, как правило, используется для подключения к другим коммутаторам. Магистральные порты имеют следующие характеристики: - По умолчанию, trunk-порт является членом всех VLAN (1-4095). - VLAN, членом которых является магистральный порт, может быть ограничено путем использования Allowed VLAN. - Кадры, классифицированные с VLAN, членом которых порт не является, отбрасываются. - По умолчанию, все кадры, кроме кадров, классифицированных как port VLAN, передаются тегированными. Кадры, классифицированные в port VLAN, не получают C-тегами на выходе - Можно настроить устройство тегировать на выходе все кадры, в этом случае только тегированные кадры будут приниматься на входе. • Hybrid (Гибридные): Гибридные порты схожи с портами типа Trunk во многих отношениях, но имеют дополнительные функции. В дополнение к характеристикам, описанным для trunk-портов, гибридные порты имеют следующие возможности: - Могут быть сконфигурирован как VLAN unaware, C-tag, S-tag или Scustom tag. - С возможностью фильтрации на входе. - Обработка входящих кадров и конфигурацию выходного тегирования можно настроить независимо.
Port VLAN	Задайте VLAN ID для порта. Допустимый диапазон значений: от 1

	до 4095. По умолчанию задано 1.
Port Type	Выбор типа порта. Операция для входящего и исходящего трафика порта каждого типа описана в таблице 3.86a.
Ingress Filtering	Если фильтрация входящих кадров включена и входящий кадр не принадлежит VLAN, указанному на данном порту, такой кадр отбрасывается. Если фильтрация входящих кадров выключена и входящий кадр не принадлежит VLAN такой кадр принимается и передается в коммутатор. По умолчанию фильтрация входящих кадров включена для портов в режимах access и trunk.
Ingress Acceptance	Гибридные порты позволяют изменять режим обработки входящих кадров. • Tagged and Untagged: Тегированные и не тегированные кадры принимаются. • Tagged Only: только тегированные кадры принимаются. Не тегированные - отбрасываются. • Untagged Only: только не тегированные кадры принимаются. Тегированные - отбрасываются.
Egress Tagging	Порты в режимах Trunk и Hybrid могут контролировать тегирование кадров на выходе. • Untag Port VLAN: Кадры с меткой VLAN совпадающей с port VLAN передаются не тегированными. Остальные кадры передаются со своими метками. • Tag All: Все кадры передаются с метками. • Untag All: Все кадры передаются без меток. Эта опция доступна только в режиме Hybrid.
Allowed VLANs	Порты в режимах Trunk и Hybrid могут контролировать членами каких VLAN они могут становиться. Порты в режиме Access может быть членом только одной VLAN, access VLAN. Поле может быть оставлено пустым. В таком случае, порт не будет членом ни одной VLAN.
Forbidden VLANs	Порт может быть сконфигурирован так, чтобы никогда не становиться членом определенных VLAN. Это может быть полезно при использовании динамических протоколов, работающих с VLAN, например GVRP. По умолчанию, поле оставлено пустым и ограничений не накладывается.

Таблица 5.2.36.1a– Операция для входящего и исходящего трафика

Тип порта	Операция	
	Операция над входящим трафиком	Операция над исходящим трафиком
Unaware	Все входящие кадры, вне зависимости от того есть ли у них тег или нет, тегируются меткой port VLAN (PVID).	Разрешенные VLAN не удаляются на выходе
C-port	1. Если во входящем тегированном кадре TPID=0x8100, он передается. 2. Если кадр не тегированный, или	Исходящие кадры тегируются меткой C-tag.

	приоритетно тегированный в него добавляется тег port VLAN.	
S-port	Если во входящем тегированном кадре TIPID=0x8100 или 0x88A8, он передается. Если кадр Исходящие кадры тегируются меткой S-tag. 108 не тегированный или приоритетно тегированный в него добавляется тег port VLAN.	Исходящие кадры тегируются меткой S-tag.
S-Custom-port	1. Если во входящем тегированном кадре TIPID=0x8100 или Ethertype for Custom Sports он передается. 2. Если кадр не тегированный, или приоритетно тегированный в него добавляется тег port VLAN.	Исходящие кадры тегируются меткой Custom S-tag.

SVL (Рис. 5.2.36.2) (Табл. 5.2.36.2).

В SVL одна или несколько сетей VLAN сопоставляются с идентификатором фильтра (FID). По умолчанию существует взаимно-однозначное сопоставление от VLAN к FID, и в этом случае коммутатор действует как мост IVL, но с SVL несколько VLAN могут совместно использовать одни и те же записи в таблице MAC-адресов.

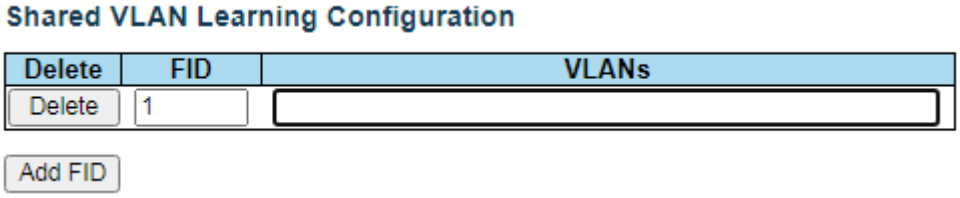


Рис. 5.2.36.2 – Настройка SVL

Таблица 5.2.36.2 – Настройка SVL

Delete	Удаление текущей записи
FID	Идентификатор фильтра (FID) – это идентификатор, который VLAN получает в таблице MAC-адресов, когда действует SVL. Никакие две строки в таблице не могут иметь одинаковый FID, и FID должен быть числом от 1 до 63.
VLANs	Список сетей VLAN, отображаемых в FID. Синтаксис следующий: отдельные сети VLAN разделяются запятыми. Диапазоны указываются с помощью тире, разделяющей нижнюю и верхнюю границы. Одна и та же VLAN может быть членом только одного FID.

Кнопка Add FID предназначена для добавления новой строки в таблицу SVL. FID будет предварительно заполнен первым неиспользованным FID

5.2.37. VLAN Translation

Для доступа к настройкам необходимо перейти по вкладке Configuration→ VLAN Translation.

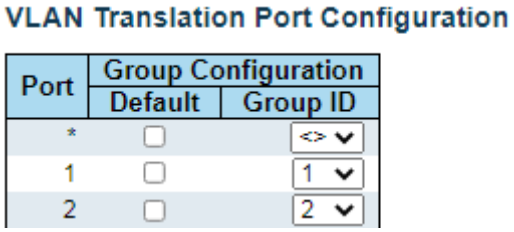


Рис. 5.2.37.1 – Настройка портов

Таблица 5.2.37.1 – Настройка портов

Port	Удаление текущей записи
Default	установите флаг, чтобы настроить порт коммутатора на использование группы трансляции VLAN по умолчанию.
Group ID	Номер группы. Порт можно настроить для использования любой из групп, но только одной.

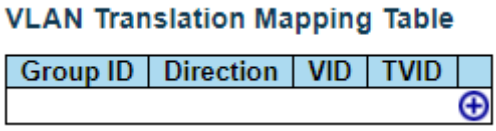


Рис. 5.2.37.2 – Настройка групп

Таблица 5.2.37.2 – Настройка групп

Group ID	Номер группы.
DIR	Указывает направление трансляции VLAN и относится к коммутатору. Направление может быть 'Ingress', когда трансляция происходит на идентификаторе VLAN фреймов, поступающих в порт коммутатора, 'Egress', где трансляция происходит на идентификаторе VLAN фреймов, покидающих порт коммутатора, или 'Both', где перевод осуществляется по обоим указанным выше направлениям.
VID	идентификатор VLAN
TVID	преобразованный идентификатор VLAN, в который будет преобразован идентификатор VLAN кадра.

5.2.38. Private VLANs (Частные VLAN)

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Private VLANs.

Эта страница используется для конфигурирования частных VLAN. Здесь можно добавить новые частные VLAN и изменить существующие VLAN. Частные VLAN основаны на маске порта источника и не соединяются с обычными VLAN. Это означает, что номера VLAN ID обычных VLAN и номера VLAN ID частных VLAN могут быть одинаковыми. Чтобы была возможна передача пакетов, порт должен принадлежать и

обычной, и частной VLAN. По умолчанию, все порты VLAN являются неподдерживаемыми и принадлежат как обычной VLAN 1, так и частной VLAN 1.

Неподдерживаемый порт VLAN может принадлежать только одной обычной VLAN, однако он может принадлежать множеству частных VLAN.

PVLAN Membership (Принадлежность к Private VLAN) (Рис. 5.2.38.1**) (Табл.** 5.2.38.1**).**

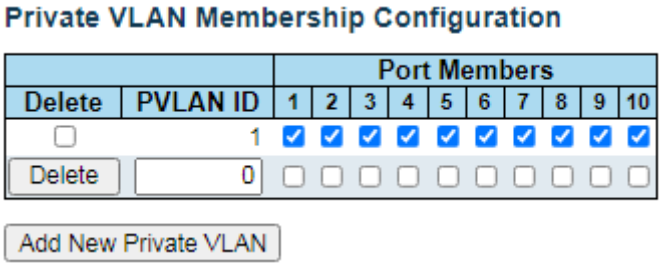


Рис. 5.2.38.1 – Принадлежность к Private VLAN

Таблица 5.2.38.1 – Принадлежность к Private VLAN

Delete	Удаляет текущую запись
PVLAN ID	Задайте номер PVLAN ID.
Port Members	Установите флаг в поле, если требуется, чтобы порт принадлежал определенной частной VLAN. Чтобы удалить порт из частной VLAN, снимите флаг в соответствующем поле.

Кнопка 

предназначена для добавления новой принадлежности к VLAN.

Port Isolation (Изоляция порта) (Рис. 5.2.38.2) (Табл. 5.2.38.2).

Частные VLAN используются для группировки портов с целью предотвращения связи внутри PVLAN. Изоляция порта используется для предотвращения связи между портами клиентов в одной и той же VLAN или частной VLAN. Порт, который изолирован от остальных портов не может передавать какой-либо одноадресный, многоадресный или широковещательный трафик в любые другие порты той же самой VLAN или PVLAN.

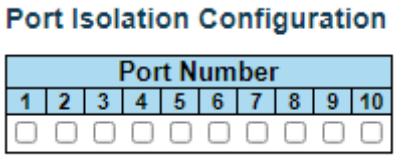


Рис. 5.2.38.2 – Изоляция порта

Таблица 5.2.38.2 – Изоляция порта

Port Number	Установите флаг, если желательно, чтобы порт или порты были изолированы от остальных портов.

5.2.39. VCL

Для доступа к настройкам необходимо перейти по вкладке Configuration→ VCL.

MAC-based (На основе MAC-адресов) (Рис. 5.2.39.1) (Табл. 5.2.39.1).

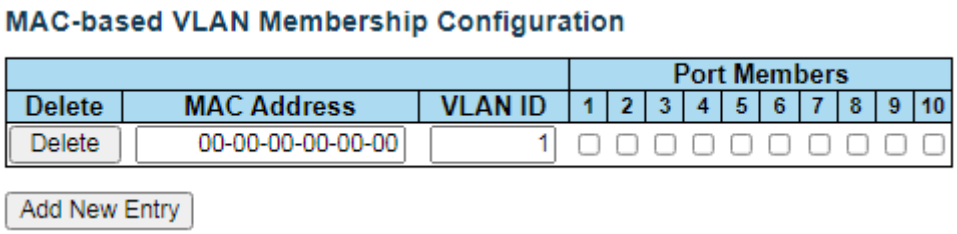


Рис. 5.2.39.1– MAC-based

Таблица 5.2.39.1– MAC-based

Delete	Удаляет текущую запись
MAC Address	Указан MAC - адрес источника. Имейте в виду, что MAC - адрес источника может отображаться только в один VLAN ID.
VLAN ID	Отображает данный MAC-адрес в связанный с ним VLAN ID.
Port Members	Порты, которые принадлежат данной VLAN.

Кнопка 

предназначена для добавления новой записи.

Protocol to Group (Рис. 5.2.39.2**) (Табл.** 5.2.39.2**).**

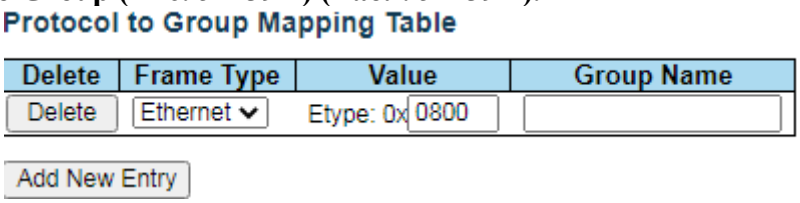


Рис. 5.2.39.2 – Protocol to Group

Таблица 5.2.39.2 – Protocol to Group

Delete	Удаляет текущую запись
Frame Type	Можно выбрать один из трех типов кадров. Поле значения (value) изменится соответствующим образом автоматически.
Value	• Ethernet: Значение типа Ether (Etype). По умолчанию задано 0x0800. Диапазон допустимых значений: от 0x0600 до 0xffff. • SNAP: для типа кадра SNAP отображаются значения идентификатора OUI (Organizationally Unique Identifier – уникальный идентификатор организации) и идентификатора протокола 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 для OUI задано шестнадцатеричное значение 000000, то для protocol ID в поле значения типа Ethernet указан протокол, работающий на вершине SNAP. Если OUI является идентификатором определенной организации, то protocol ID – это значение, назначенное этой организацией протоколу, работающему на вершине SNAP. Другими словами, если в поле OUI задано 00-00-00, то значение PID будет etherType (0x0600-0xffff). Если значение OUI отличается от 00-00-00, то правильное значение PID будет любым значением в диапазоне от 0x0000 до 0xffff. • LLC (Логическое управление линией): включает в себя значения DSAP (Destination Service Access Point – точка доступа назначения

	услуг) и SSAP (Source Service Access Point - точка доступа источника услуг). По умолчанию значение равно 0xff. Диапазон допустимых значений: от 0x00 до 0xff.
Group Name	Имя группы. Поле может содержать не более 16 алфавитно-цифровых символов (a-z; AZ) или целых чисел (0-9).

Кнопка 

предназначена для добавления новой записи.

Group to VLAN (Отображение группы в VLAN) (Рис. 5.2.39.3) (Табл. 5.2.39.3).

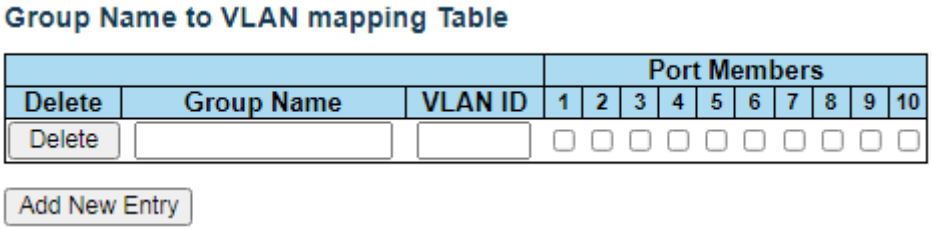


Рис. 5.2.39.3– Group to VLAN

Таблица 5.2.39.3 – Group to VLAN

Delete	Удаляет текущую запись
Group Name	имя группы. Поле может содержать не более 16 алфавитно-цифровых символов (a-z; A-Z) или целых чисел (0-9).
VLAN ID	номер VLAN ID
Port Members	Назначенные порты

Кнопка 

предназначена для добавления новой записи.

IP Subnet-based VLAN (VLAN на основе IP-подсети) (Рис. 5.2.39.4) (Табл. 5.2.39.4).

На странице IP Subnet-based VLAN configuration можно задать отображение не тегированных входящих кадров в конкретную VLAN, если в таблице отображения IP-подсети в VLAN найден IP-адрес источника. Когда включена классификация VLAN на основе IP-подсети, адрес источника не тегированных входящих кадров проверяется по таблице отображения IP- подсети в VLAN. Если адрес источника для данной подсети найден, то кадрам назначается VLAN, указанный в этой ячейке таблицы. Если согласующейся IP-подсети не обнаружено, не тегированные кадры классифицируются, как принадлежащие VLAN, которой принадлежит принявший их порт (с номером PVID).

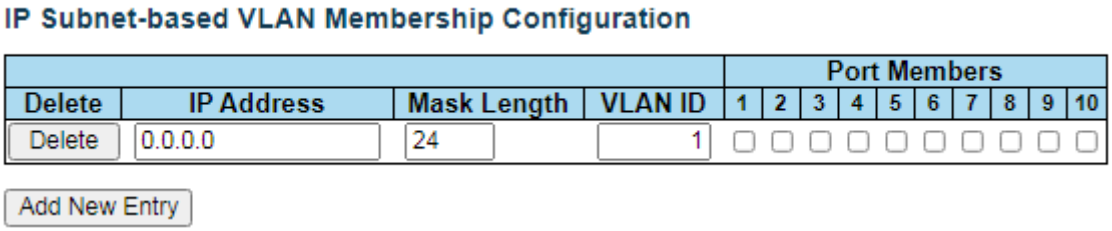


Рис. 5.2.39.4 – VLAN на основе подсетей

Таблица 5.2.39.4 – VLAN на основе подсетей

Delete	Удаляет текущую запись
IP Address	IP-адрес для данного правила
Mask Length	Длина маски сети
VLAN ID	Номер VLAN ID

Port Members	Порты, назначенные данному правилу

Кнопка Add New Entry предназначена для добавления новой записи.

5.2.40. QoS (Качество обслуживания)

Сетевой трафик всегда непредсказуем, поэтому основным фактором обеспечения качества является предоставление наилучшего способа доставки. Для преодоления этой проблемы используется понятие качества обслуживания (Quality of Service (QoS)) применяемое ко всей сети. Гарантируется, что сетевой трафик будет приоритизирован в соответствии с заданным критерием, и прием будет производиться с использованием обработки по приоритетам.

QoS позволяет назначить различные классы сетевых услуг различным типам трафика, например, мультимедийному, видео, трафику конкретного протокола, критичному по времени трафику, трафику резервного копирования файлов. Чтобы задать приоритеты пакетов на данном коммутаторе, перейдите на страницу “Port Classification” (Классификация порта).

Для доступа к настройкам необходимо перейти по вкладке Configuration→ QoS.

Port Classification (Классификация на портах) (Рис. 5.2.40.1) (Табл. 5.2.40.1).

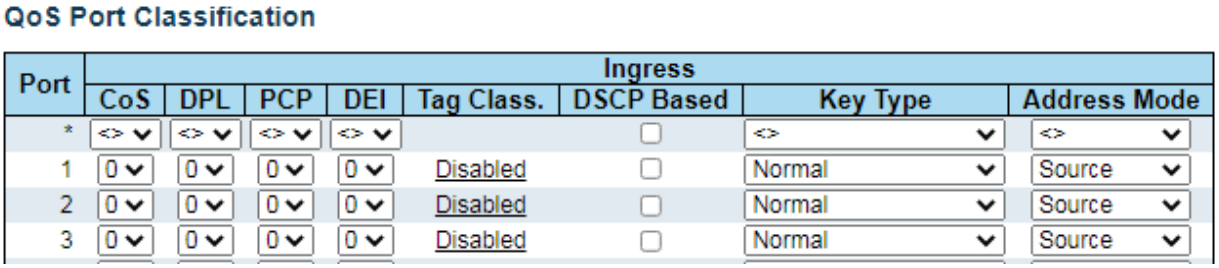


Рис. 5.2.40.1 – Классификация QoS на портах

Таблица 5.2.40.1 – Классификация QoS на портах

Port	Номер порта. “*” означает применение ко всем портам.
Cos	Класс CoS, выбираемый по умолчанию. Класс CoS с номером 0 имеет наименьший приоритет. По умолчанию задано 0.
DP Level	Выберите приоритет отбрасывания: 0: Подтвержденные кадры. 1: Кадры, которые могут быть отброшены.
PCP	Выберите соответствующее значение пользовательского приоритета (Priority Code Point) для не тегированных кадров.
DEI	Выберите соответствующее значение индикатора отбрасывания по критерию (Drop Eligible Indicator) для не тегированных кадров.
Tag Class	В этом поле отображен режим классификации для тегированных кадров на данном порту: • Disabled (Выключен): для тегированных кадров используется класс QoS и уровень DP по умолчанию. • Enabled (Включен): для тегированных кадров используется значение PCP и DEI из таблицы (PCP, DEI) to (QoS class, DP level) Mapping.
DSCP Based	Установите флаг в поле, чтобы включить QoS на основе DSCP (входящий порт).
Key Type	Тип определяющего ключа, сгенерированный для кадров, полученных через порт. Допустимые значения: Normal: соответствует внешнему тегу, SMAC/DMAC, IP-протоколу,

	DSCP, SIP/DIP, SPORT и DPORT. Double Tag: четверть ключа, соответствует внутреннему и внешнему тегу. IP Address: половина ключа, совпадение внутреннего и внешнего тега, SIP и DIP. Для кадров, не относящихся к IP, используйте только внешний тег. MAC and IP Address: Полный ключ, совпадающий внутренний и внешний тег, SMAC, DMAC, SIP и DIP.
Address Mode	режим IP/MAC-адреса, определяющий, должна ли классификация QCL основываться на адресах источника (SMAC/SIP) или назначения (DMAC/DIP) на этом порту. Этот параметр используется только в том случае, если тип ключа Normal. Допустимыми значениями являются: Source: позволяет сопоставлять SMAC/SIP. Destination: позволяет сопоставлять DMAC/DIP.

Port Policing (Ограничение скорости на портах) (Рис. 5.2.40.2) (Табл. 5.2.40.2).

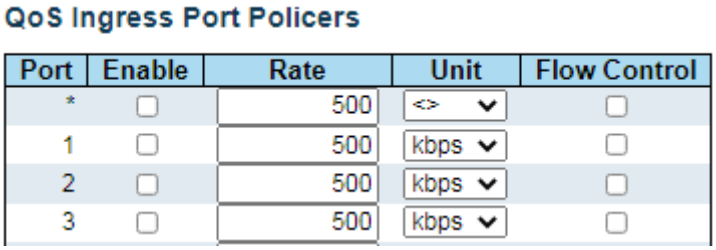


Рис. 5.2.40.2 – Ограничение скорости на портах

Таблица 5.2.40.2 – Ограничение скорости на портах

Port	Номер порта. “*” означает применение ко всем портам.
Enabled	Установите флаг в этом поле, чтобы включить функцию ограничения скорости на порту.
Rate	Задайте скорость, до которой будет ограничена скорость на порту. По умолчанию задано 500 кбит/с. Допустимый диапазон для kbps (кбит/с) и fps (кадров/с): от 100 до 1000000. Допустимый диапазон для Mbps (Мбит/с) и kfps (кадров/с): от 1 до 3300 Мбит/с.
Unit	Единицы измерения ограничения скорости
Flow Control	Если управление потоком включено и порт работает в режиме управления потоком, то будут отправляться кадры pause, вместо отбрасывания входящих кадров.

Queue Policing (Ограничение скорости в очередях) (Рис. 5.2.40.2) (Табл. 5.2.40.2).

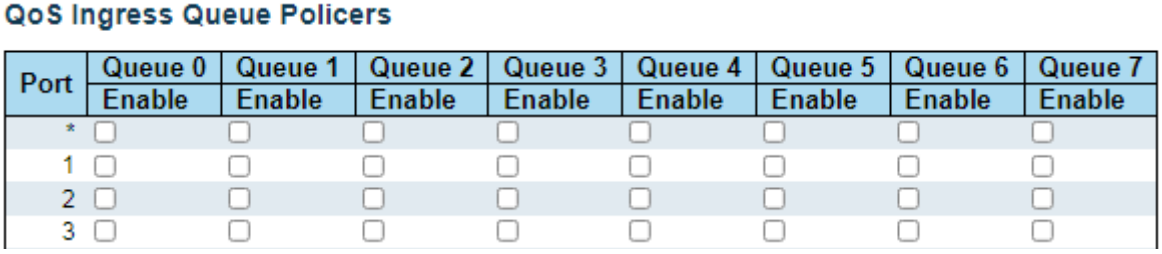


Рис. 5.2.40.2 – Ограничение скорости в очередях

Таблица 5.2.40.2 – Ограничение скорости в очередях

Port	Номер порта. “*” означает применение ко всем портам.

Queue 0~7 Enable	Установите флаг в соответствующем поле, чтобы включить функцию ограничения скорости в очередях на портах коммутатора
Rate	Скорость, до которой будет ограничена скорость в очереди. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с.
Unit	Единицы измерения ограничения скорости очереди входящих кадров.

Port Scheduler (Рис. 5.2.40.3) (Табл. 5.2.40.3).

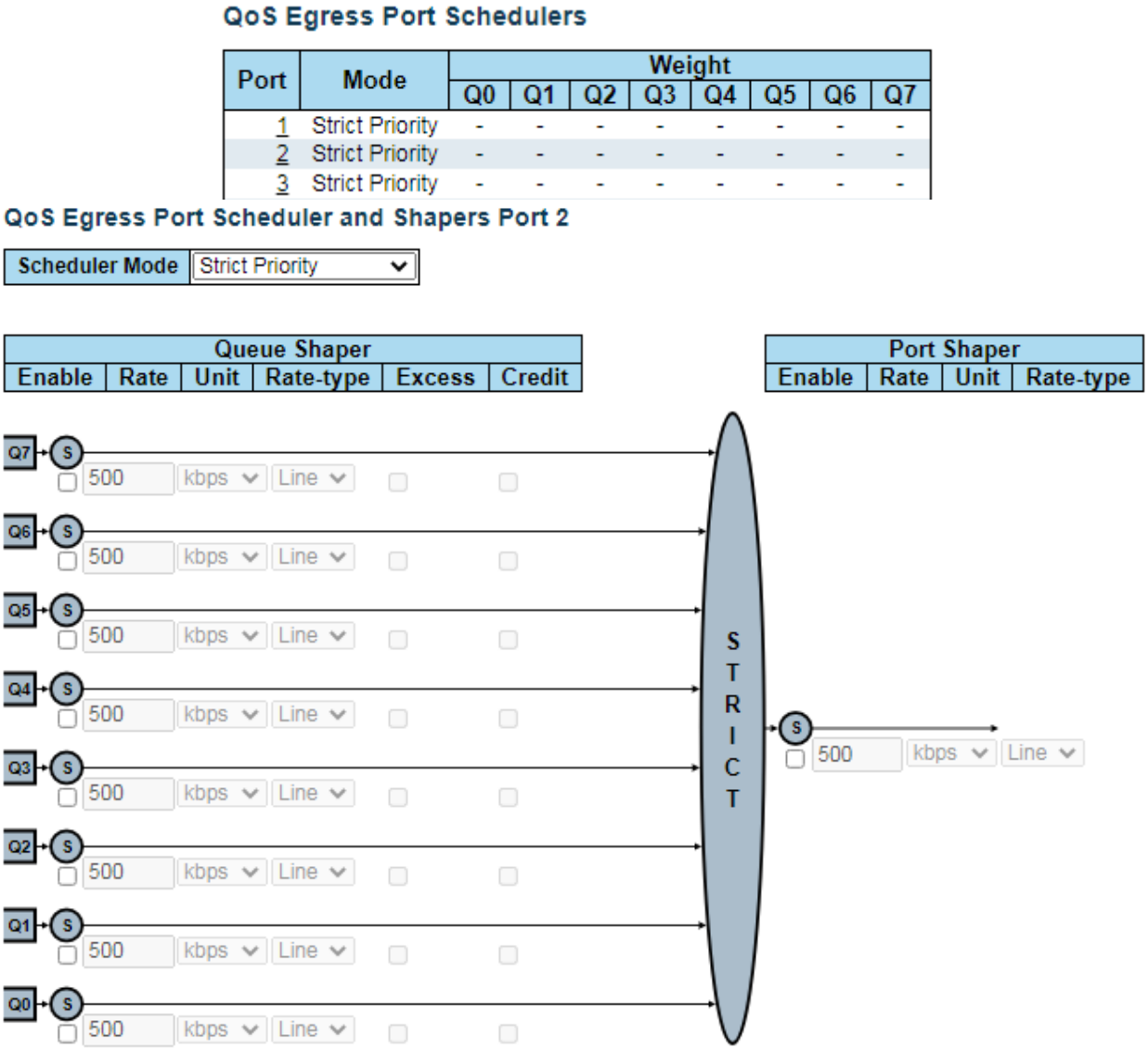


Рис. 5.2.40.3 – Port Scheduler

Таблица 5.2.40.3 – Port Scheduler

Port	Нажмите мышью на порт, чтобы задать детальные настройки диспетчера порта.
Mode	Отображается выбранный режим работы
Weight	Отображается вес в процентах, присвоенный очередям Q0~Q7.

Scheduler Mode	Устройство обеспечивает два режима работы с очередями. • Strict mode (Строгий режим работы): В этом режиме кадры из выходных очередей с более высокими приоритетами будут передаваться первыми (по сравнению с кадрами, находящимися в очередях с низкими приоритетами). • Weight mode (Режим работы с весами): для очередей с взвешиванием DWRR (Deficit Weighted Round-Robin – циклическое взвешивание с учетом дефицита) должен быть задан вес в каждой очереди. Обслуживание очередей при DWRR во многом подобно WRR, однако следующая очередь обслуживается только тогда, когда ее счетчик дефицита (Deficit Counter) становится меньше размера переданного пакета.
Queue Shaper (Формирователь трафика очереди)	
Enable	Нажмите мышью это поле, чтобы включить формирователь для некоторой очереди на выбранном порту.
Rate	Задайте скорость, до которой формирователь очереди будет ограничивать скорость. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с.
Unit	Выберите единицы измерения скорости, которые будет использовать формирователь очереди при ограничении скорости.
Port Shaper (Формирователь трафика порта): Задайте скорость, с которой трафик может покидать данную очередь.	
Enable	Установите флаг в этом поле, чтобы включить формирователь трафика порта.
Rate	Задайте скорость, до которой будет ограничена скорость на выходе формирователя трафика порта. По умолчанию задано 500 кбит/с. Допустимый диапазон значений для kbps (кбит/с): от 100 до 1000000. Допустимый диапазон значений для Mbps (Мбит/с): от 1 до 3300 Мбит/с.
Unit	Выберите единицы измерения скорости.

Port Shaping (Формирование трафика портов) (Рис. 5.2.40.3a).

Нажмите на номер порта, чтобы изменить или переустановить настройки формирователя трафика порта, в частности, ограничение скорости.

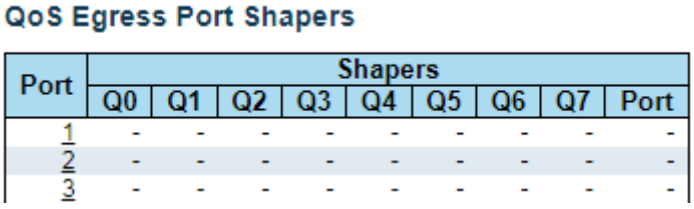
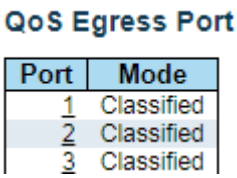


Рис. 5.2.40.3a– PortShaping

Port Tag Remarking (Изменение тегов на порту) (Рис. 5.2.40.4) (Табл. 5.2.40.4).



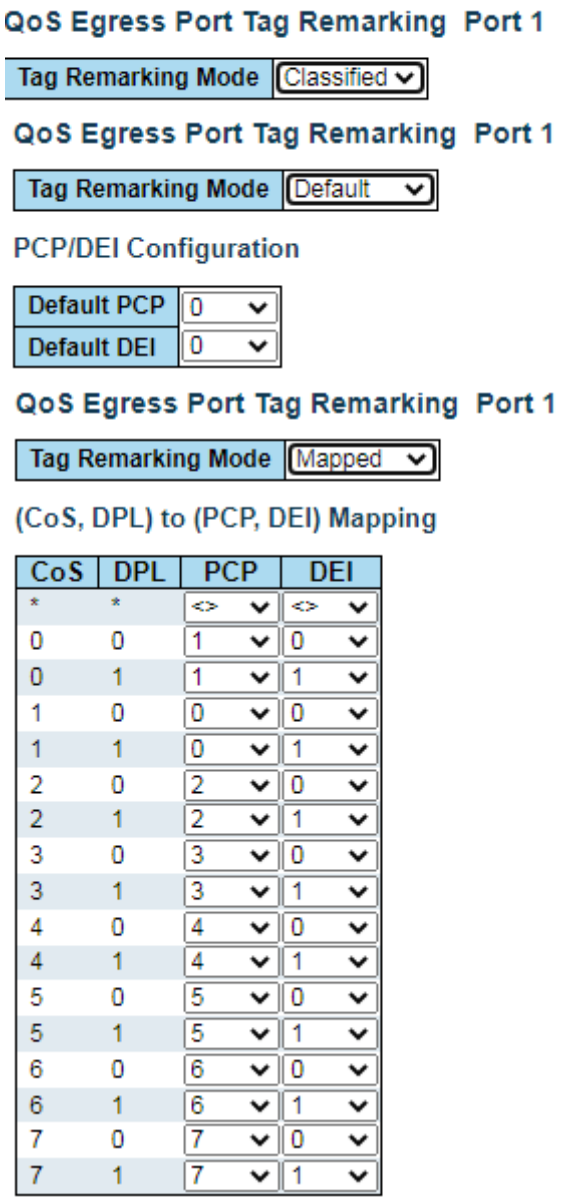


Рис. 5.2.40.4 – Изменение тегов на порту

Таблица 5.2.40.4 – Изменение тегов на порту

Port	Нажмите мышью на порт, чтобы задать детальные настройки.
Tag Remarking Mode	Выберите соответствующий режим работы изменения тегов на этом порту. • Classified (Классифицированный): используются классифицированные значения PCP/DEI. • Default (Значения по умолчанию): используются значения PCP/DEI, заданные по умолчанию - PCP:0; DEI:0). • Mapped (Отображение): используется отображение значений классов QoS и уровней DP в значения PCP/DEI.
PCP/DEI Configuration	Настройка значений PCP/DEI для режима Default.
QoS Class/DP level	Показаны опции отображения для значений классов QoS и уровней DP (приоритетов отбрасывания).
PCP	Изменение тегов согласующихся исходящих кадров в соответствии с указанным приоритетом Priority Code Point либо в соответствии с пользовательским приоритетом. (Диапазон: 0~7; По умолчанию

	задано: 0)
DEI	Изменение тегов согласующихся исходящих кадров в соответствии с заданным индикатором соответствия критерию отбрасывания (Drop Eligible Indicator). (Диапазон: 0~1; По умолчанию задано: 0)

Port DSCP (Настройка трансляции DSCP на порту) (Рис. 5.2.40.5) (Табл. 5.2.40.5).

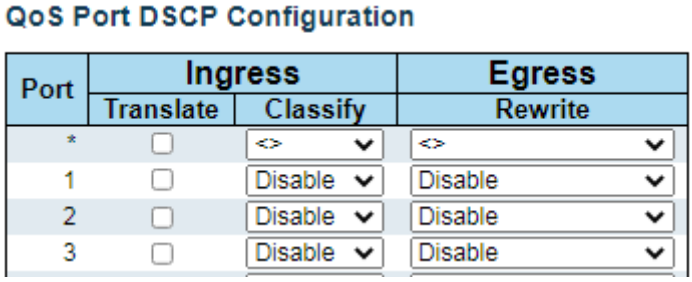


Рис. 5.2.40.5 – Настройка трансляции DSCP на порту

Таблица 5.2.40.5 – Настройка трансляции DSCP на порту

Port	Номер порта. “*” означает применение ко всем портам.
Ingress Translate	Установите флаг в поле, чтобы включить трансляцию значений DSCP на основе выбранного метода классификации
Ingress Classify	Выберите соответствующий метод классификации: • Disable (Выключить): Классификация DSCP входящих кадров не выполняется. • DSCP=0: Классификация выполняется, если DSCP входящих кадров равен 0. • Selected (Выбрано): классифицируются только DSCP, для которых включена классификация в таблице трансляции DSCP. • All (Все): классифицируются все поля DSCP.
Egress Rewrite	Значения DSCP исходящих кадров будут переписаны на порту. • Disable (Выключить): Перезапись значений DSCP исходящего трафика выключена. • Enable (Включить): Перезапись значений DSCP исходящих кадров включена, но отображение после перезаписи не выполняется. • Remap DP aware (Отображение поддерживаемых DP заново): Кадр с DSCP, поступивший от анализатора, снова отображается и помечается новым значением DSCP. В зависимости от уровня DP кадра, новое значение DSCP берется из таблицы трансляции DSCP из поля Egress Remap DP0 или DP1. • Remap DP aware (Отображение неподдерживаемых DP заново): Кадр с DSCP, поступивший от анализатора снова отображается и помечается новым значением DSCP. Новое значение DSCP всегда берется из таблицы трансляции DSCP из поля Egress Remap DP0.

DSCP-Based QoS (Настройка качества обслуживания по DSCP) (Рис. 5.2.40.6) (Табл. 5.2.40.6).

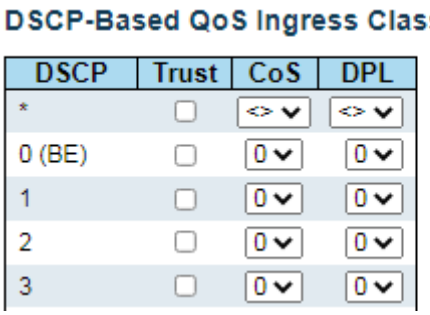


Рис. 5.2.40.6 – Настройка качества обслуживания по DSCP

Таблица 5.2.40.6 – Настройка качества обслуживания по DSCP

DSCP	Значение DSCP входящего пакета. Диапазон допустимых значений DSCP: от 0 до 63.
Trust	Установите флаг в этом поле, чтобы указать, что значение DSCP является надежным. Только надежные значения DSCP отображаются в соответствующий класс QoS и приоритет отбрасывания DPL (drop precedence level). Кадры с ненадежными значениями DSCP считаются не-IP кадрами.
CoS	Выберите класс QoS для соответствующего значения DSCP для 123 обработки входящих кадров. По умолчанию задано 0. Диапазон допустимых значений: от 0 до 7
DPL	Выберите приоритет отбрасывания DPL для соответствующего значения DSCP для обработки входящих кадров. По умолчанию задано 0. Значение “1” дает более высокий приоритет отбрасывания

DSCPTranslation (Трансляция DSCP) (Рис. 5.2.40.7) (Табл. 5.2.40.7).

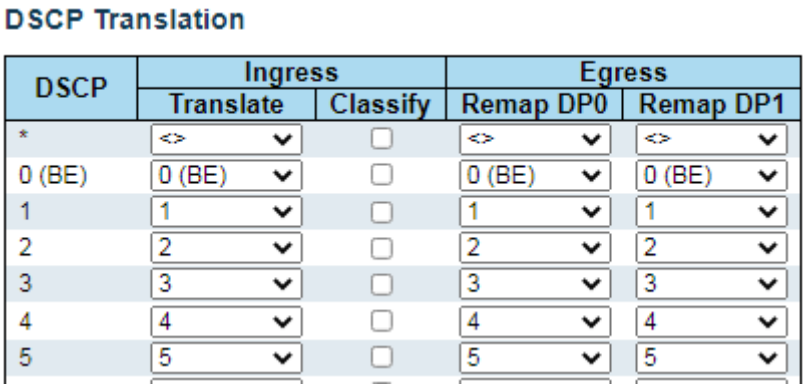


Рис. 5.2.40.7 – Трансляция DSCP

Таблица 5.2.40.7– Трансляция DSCP

DSCP	Значение DSCP входящего кадра. Диапазон допустимых значений DSCP: от 0 до 63.
Ingress Translate	Включает трансляцию значений DSCP входящих кадров на основе заданного метода классификации.
Ingress Classify	Включает классификацию на входящей стороне, как определено в таблице настройки DSCP QoS на порту.
Egress Remap	Заново отображает значение DP в выбранное значение DSCP.

DSCPClassification (Классификация DSCP) (Рис. 5.2.40.8) (Табл. 5.2.40.8).

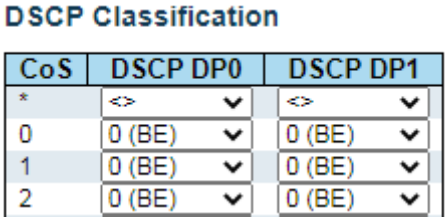


Рис. 5.2.40.8 – Классификация DSCP

Таблица 5.2.40.8 – Классификация DSCP

CoS	Список актуальных значений классов QoS
DSCP:	Выберите значение DSCP для отображения в класс QoS

QoS Control List Configuration (Список управления QoS) (Рис. 5.2.40.9) (Табл. 5.2.40.9).

Список управления качеством обслуживания используется для установки правил обработки входящих пакетов по типу кадра, MAC-адресу, значениям VID, PCP, DEI. Как только QCE привязан к порту, трафик согласуется с первым элементом списка управления QoS, которому назначен класс QoS, уровень приоритета отбрасывания и значение DSCP. Трафику, не согласующемуся ни с какими QCE, назначается класс QoS, используемый для порта по умолчанию.

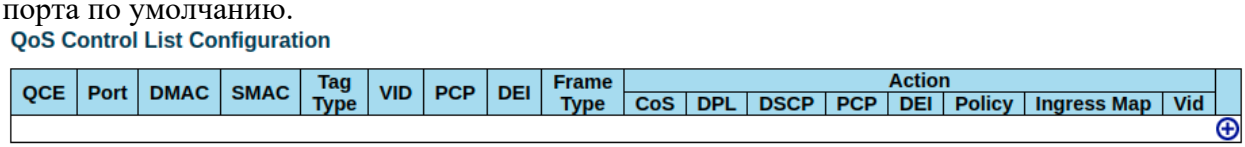


Рис. 5.2.40.9– Список управления QoS

Таблица 5.2.40.9 – Список управления QoS

QCE	Отображается номер элемента списка QCL
Port	Отображается номер порта, использующего этот QCL
DMAC	MAC-адрес назначения. Возможны следующие значения: Any (Любой), Broadcast (Широковещательный), Multicast (Многоадресный), Unicast (Одноадресный).
SMAC	MAC - адрес источника
VID	Отображается VLAN ID (1-4095)
PCP	Отображается значение PCP.
DEI	Отображается значение DEI
Frame type	Отображается тип кадра, поиск которого будет производиться во входящих кадрах. Возможны следующие типы кадров: Any (Любой), Ethernet, LLC SNAP, IPv4, IPv6.
Action	Отображается операция классификации, выполняемая на входящих кадрах, когда настройки параметров согласуются с содержимым кадра.

Storm Control (Управление широковещательным штормом) (Рис. 5.2.40.10) (Табл. 5.2.40.10).

Управление широковещательным штормом используется для предотвращения ухудшения производительности сети или полного прекращения ее работы. Управление осуществляется путем установки пороговых значений для трафика, подобного широковещательному, одноадресному или многоадресному. Ухудшение производительности сети или полное прекращение ее работы могут быть обусловлены неполадками в работе сетевых устройств, плохой отладкой и неправильными настройками

прикладного ПО. Защита сети от штормов может быть осуществлена путем установки пороговых значений для определенного трафика на устройстве. Любые указанные пакеты, при приеме которых превышено заданное пороговое значение, будут отброшены.

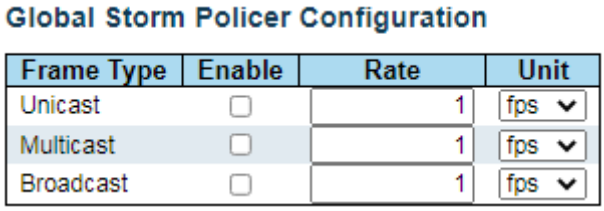


Рис. 5.2.40.10 – Управление широковещательным штормом

Таблица 5.2.40.10 – Управление широковещательным штормом

Enable	Включает подавление шторма для пакетов типов Unicast (Одноадресный), Multicast (Многоадресный), Broadcast (Широковещательный).
Rate	Выберите пороговое значение в пакетах в секунду. Принятые пакеты, при которых превышено выбранное значение, будут отброшены.
Unit	Единицы измерения

Weighted Random Early Detection (WRED) (Рис. 5.2.40.11) (Табл. 5.2.40.11).

Отслеживает длину очереди и отбрасывает некоторый процент пакетов в очереди для улучшения производительности сети.

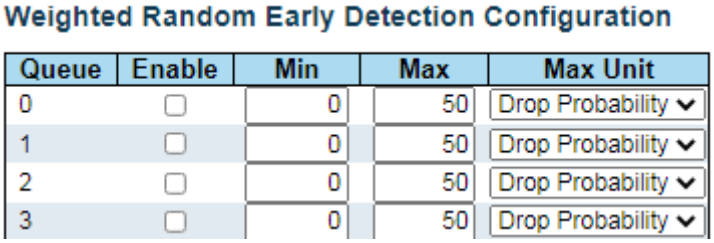


Рис. 5.2.40.11 – WRED

Таблица 5.2.40.11 – WRED

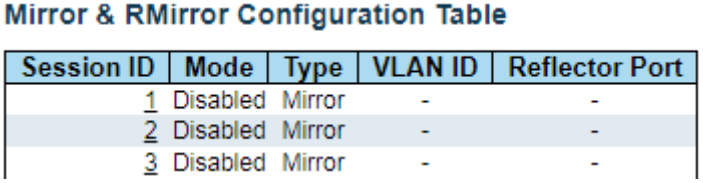
Queue	Номер очереди (CoS)
Enable	Определяет, включен ли WRED для этой записи
Min	Нижний порог уровня заполнения.
Max	Верхний порог уровня заполнения.
Max Unit	Управляет вероятностью падения для кадров

5.2.41. Mirroring (Зеркалирование)

Для отладки сетевых проблем, исходящий трафик может быть скопирован на зеркальном порту, где может быть подключен анализатор.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Mirroring

Mirroring (Зеркалирование) (Рис. 5.2.41.1) (Табл. 5.2.41.1).



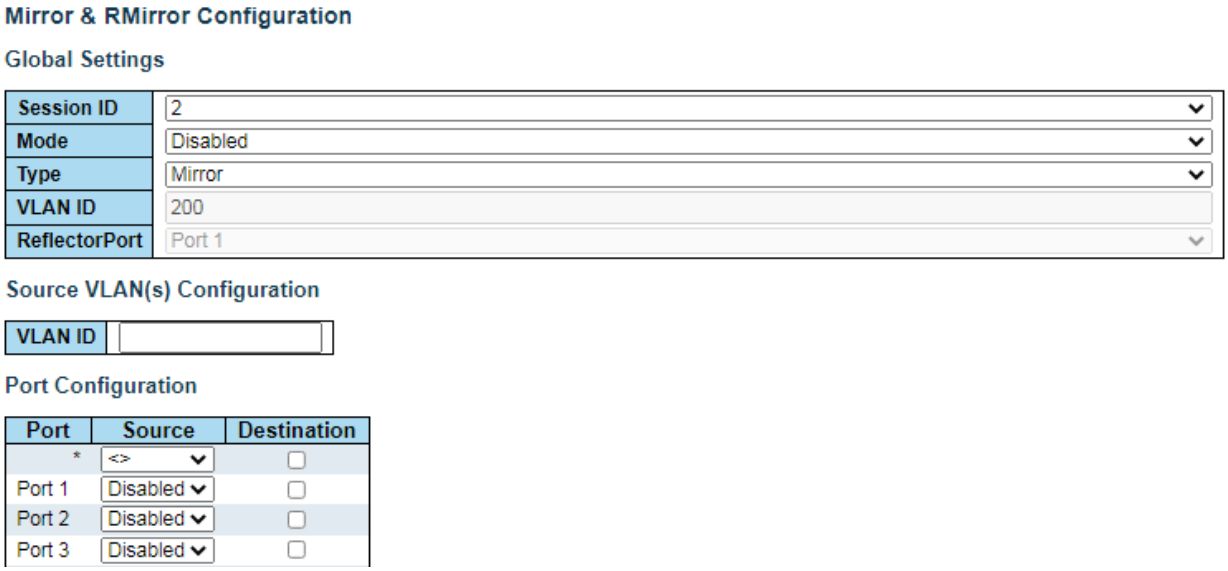


Рис. 5.2.41.1 – Зеркалирование

Таблица 5.2.41.1 – Зеркалирование

Session ID	Идентификатор сессия. Выберите идентификатор сеанса для настройки
Mode	Включение/выключение зеркального отображения или дистанционного зеркалирования.
Type	• Mirror – Зеркало; • Source – Источник; • Intermediate – Промежуточный; • Destination – Назначение;
VLAN ID	Идентификатор VLAN указывает, куда будет скопирован мониторный пакет. Идентификатор VLAN по умолчанию - 200.
Reflector Port	Порт, с которого отправляется трафик
Source VLANs	Зеркалирование на основе VLAN
Port Configuration (Настройки порта)	
Port	Номер порта
Source	Имеется четыре режима, которые можно использовать на каждом порту индивидуально. • Disabled (Выключен): Функция зеркалирования на данном порту выключена. • Rx only (Только принимаемый трафик): на зеркальный порт будут направлены только кадры, принятые данным портом. • Tx only (Только передача): на зеркальный порт будут направлены только кадры, переданные данным портом. • Enable (Включить): на зеркальный порт будут переданы кадры, принятые и переданные данным портом.
Destination	Порт назначения, который получает копию трафика из исходного порта.

UPnP

5.2.42. Voice VLAN. Голосовой VLAN

Для доступа к настройкам необходимо перейти по вкладке Configuration→ Voice VLAN.

Configuration (Настройка) (Рис. 5.2.42.1) (Табл. 5.2.42.1).

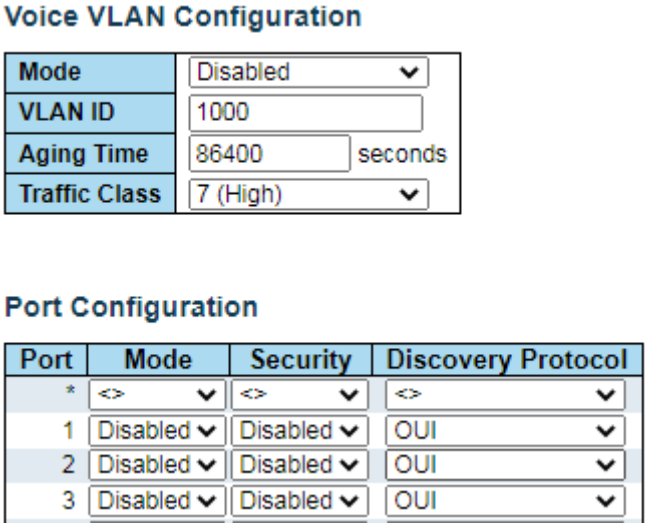


Рис. 5.2.42.1 – Настройка

Таблица 5.2.42.1 – Настройка

Voice VLAN Configuration (Настройка голосовой VLAN)	
Mode	Включить/выключить голосовой VLAN. Прежде чем включить голосовой VLAN, отключите MSTP, чтобы избежать конфликта.
VLAN ID	Идентификатор VLAN
Aging Time	Указывает время безопасного обучения. Допустимый диапазон составляет от 10 до 10000000 секунд.
Traffic Class	Указывает класс трафика. Весь трафик в Voice VLAN будет иметь этот класс.
Port Configuration (Настройка порта)	
Port	Номер порта
Mode	• Disabled – отключен; • Auto - включение режима автоматического определения; • Forced - принудительное подключение.
Security	Включить/выключить режим безопасности порта VLAN. Когда эта функция включена, все нетелефонные MACадреса в VLAN будут заблокированы на 10 секунд.
Discovery Protocol	Указывает протокол обнаружения порта. Работает только при режиме «Auto». Возможные протоколы обнаружения: • OUI: обнаружение телефонного устройства по адресу OUI. • LLDP: обнаружение телефонного устройства LLDP. • Both: OUI и LLDP. Мы должны включить функцию LLDP перед активацией протокола обнаружения на «LLDP» или «Both». Изменение протокола обнаружения на «OUI» или «LLDP» приведет к перезапуску процесса автоматического обнаружения.

OUI Table (Таблица OUI) (Рис. 5.2.42.2) (Табл. 5.2.42.2).

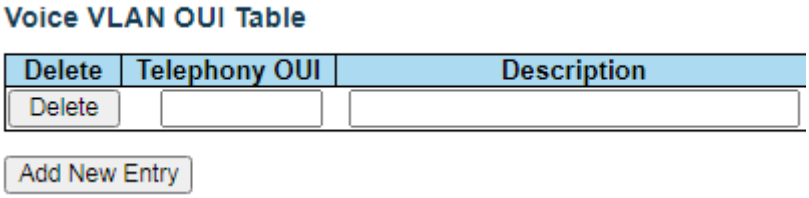


Рис. 5.2.42.2 – Таблица OUI

Таблица 5.2.42.2 – Таблица OUI

Delete	Удаляет текущую запись
Telephony OUI	Адрес OUI – это глобальный уникальный идентификатор, присвоенный IEEE. Он должен состоять из 6 символов, формат ввода - «xx-xx-xx» (x - шестнадцатеричная цифра).
Description	Описание адреса OUI. Допустимая длина строки от 0 до 32.

Кнопка Add New Entry предназначена для добавления новой записи.

5.2.43. UPnP

Для доступа к настройкам необходимо перейти по вкладке Configuration→UPnP.
Настройка UPnP (Рис. 5.2.43.1) (Табл. 5.2.43.1)

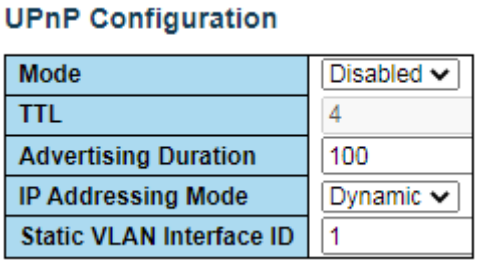


Рис. 5.2.43.1 – Настройка UPnP

Таблица 5.2.43.1 – Настройка UPnP

Mode	Включает или выключает функцию UPnP. При включении автоматически создается два правила списка доступа (ACE) для перенаправления соответствующих UPnP пакетов к процессору. При выключении правила автоматически удаляются.
TTL	Параметр TTL (Time to live – время жизни) используется для указания того, сколько шагов может сделать уведомление UPnP (SSDP) до своего исчезновения.
Advertising Duration	Этот параметр определяет, насколько часто могут посылаться уведомления UPnP. Длительность переносится пакетами протокола SSDP (Simple Service Discover Protocol), которые информируют пункт управления о том, насколько часто следует принимать сообщения с уведомлениями SSDP от коммутатора. По умолчанию установлена длительность уведомления 100 секунд. Однако, вследствие ненадежности протокола UDP рекомендуется уменьшать длительность, так как чем она меньше, тем быстрее обновляется состояние UPnP.
IP Addressing Mode	Режим IP-адресации предоставляет два способа определения назначения IP-адреса: **Динамический**: Выбор по умолчанию для UPnP. Модуль UPnP помогает пользователям выбрать IP-адрес коммутатора. Он находит

	первый доступный системный IP-адрес. **Статический**: Пользователь указывает IP-интерфейс VLAN для выбора IP-адреса коммутирующего устройства.
Static VLAN Interface ID	Индекс конкретного интерфейса IP VLAN. Он будет применяться только в статическом режиме IP-адресации. Допустимые настраиваемые значения находятся в диапазоне от 1 до 4095. Значение по умолчанию - 1.

5.2.44. MRP и MVRP

Multiple Registration Protocol (MRP) – это общая структура, рекомендованная IEEE для использования в сетевых мостах, сетевых коммутаторах, или других аналогичных устройствах с возможностью регистрации и перерегистрации специальных атрибутов, таких как идентификаторы VLAN и членство в мультикастовых группах в больших локальных сетях LAN.

Протокол множественных регистраций VLAN Multiple VLAN Registration Protocol (MVRP) является сетевым протоколом второго уровня для автоматической конфигурации информации VLAN в коммутаторах. Он был определён приложением 802.1ak к рекомендациям IEEE 802.1Q-2005.

В пределах второго уровня сетевой модели OSI MVRP обеспечивает динамический обмен информации о VLAN и конфигурацию необходимых VLAN. Например, поставлена задача добавить определённый порт коммутатора в VLAN, или сетевое устройство, поддерживающее VLAN и подключённое в порт коммутатора требует переконфигурации, и все необходимые транки динамически созданы на других коммутаторах, поддерживающих MVRP. Для выполнения этой задачи без возможностей MVRP потребуется ручная конфигурация VLAN или какой-либо проприетарный метод производителя. Если же выполнять эту задачу средствами MVRP, который использует динамические значения VLAN в фильтруемой базе данных. Если коротко – MVRP помогает динамически поддерживать конфигурации VLAN в статических конфигурациях сетей.

802.1Q даёт возможность:

- Динамически конфигурировать и распределять информацию о принадлежности VLAN через механизмы MVRP.
- Статически конфигурировать информацию о принадлежности VLAN посредством механизмов менеджмента, которые позволяют управлять регистрационными данными о статических записях регистраций VLAN.
- Поддерживать комбинированные статические и динамические конфигурации, при которых некоторые VLAN конфигурируются посредством механизмов менеджмента, а для других VLAN сохраняется возможность динамической конфигурации средствами MVRP.

Для доступа к настройкам необходимо перейти по вкладке Configuration→ MRP.
Настройка MRP (Рис. 5.2.44.1) (Табл. 5.2.44.1)

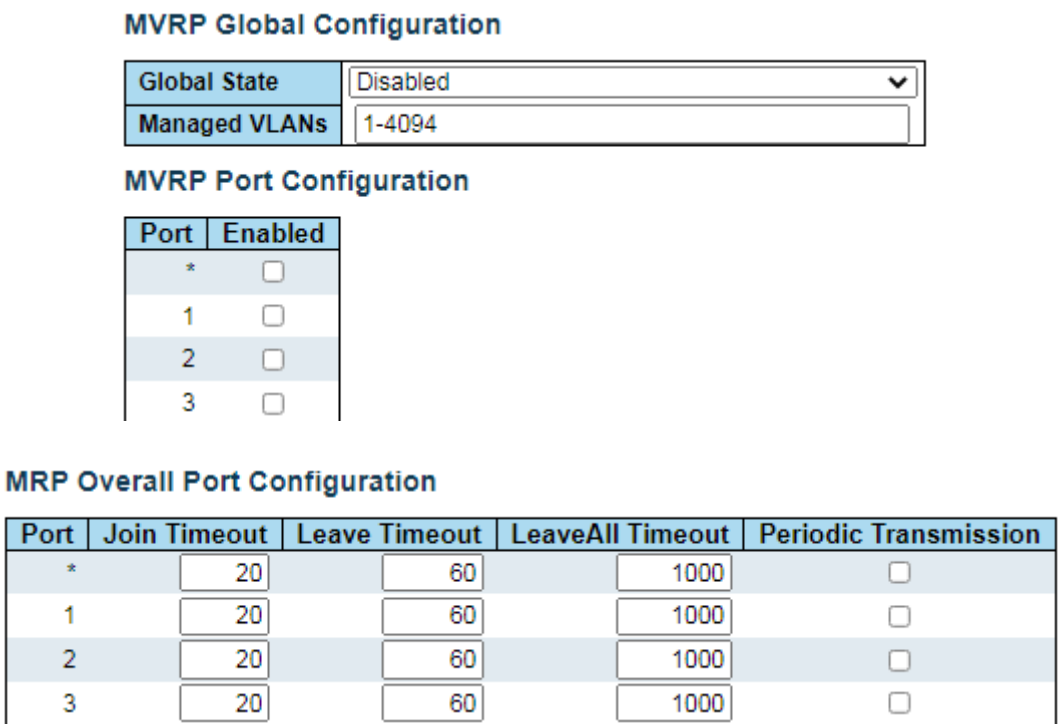


Рис. 5.2.44.1– Настройка MVRP

Таблица 5.2.44.1– Настройка MVRP

Global State	Включение/выключение функции MVPR
Managed VLANs	Настройка списка VLAN, управляемых MVRP
Настройка портов	
Port	Номер порта
Enabled	Включение функции MVRP на порту
Join Timeout	таймер присоединения. Значения от 1-20cc. По умолчанию значение 20cc
Leave Timeout	таймер отключения. Значения от 60-300cc. По умолчанию значение 60cc
LeaveAll Timeout	таймер отключения от всех мультикастовых групп. Значения 1000-5000cc. По умолчанию – 1000cc
Periodic Transmission	Включение функции PeriodicTransmission для всех приложений MRP на порту

5.2.45. GVRP

Для доступа к настройкам необходимо перейти по вкладке Configuration→GVRP.
Global Configuration (Глобальные настройки) (Рис. 5.2.45.1) (Табл. 5.2.45.1).

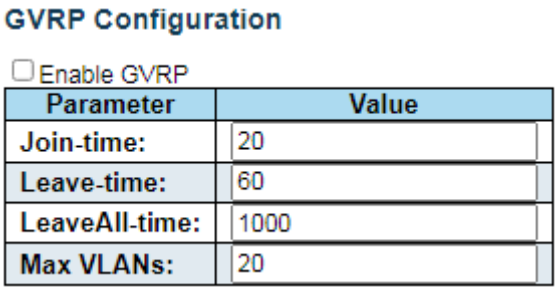


Рис. 5.2.45.1– Глобальные настройки

Таблица 5.2.45.1– Глобальные настройки

Enable GVRP	Включение протокола GVRP глобально.
Join-time	Значение в диапазоне 1-20, указываемое в сентисекундах (сотых секунды). По умолчанию, значение равно 20.
Leave-time	Значение в диапазоне 60-300, указываемое в сентисекундах (сотых секунды). По умолчанию, значение равно 60.
Leave All-time	Значение в диапазоне 1000-5000, указываемое в сентисекундах (сотых секунды). По умолчанию, значение равно 1000.
Max VLANs	Максимальное значение VLAN, поддерживаемое GVRP.

Port Configuration (Настройки порта) (Рис. 5.2.45.2) (Табл. 5.2.45.2)

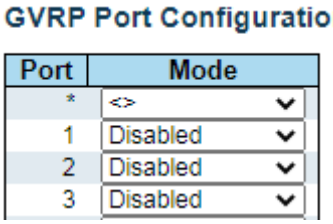


Рис. 5.2.45.2 – Настройки порта

Таблица 5.2.45.2 – Настройки порта

Port	Номер порта
Mode	Позволяет настроить режим работы GVRP на порту

5.2.46. sFlow

Для доступа к настройкам необходимо перейти по вкладке Configuration→sFlow sFlow Configuration (Настройки sFlow) (Рис. 5.2.46.1) (Табл. 5.2.46.1).

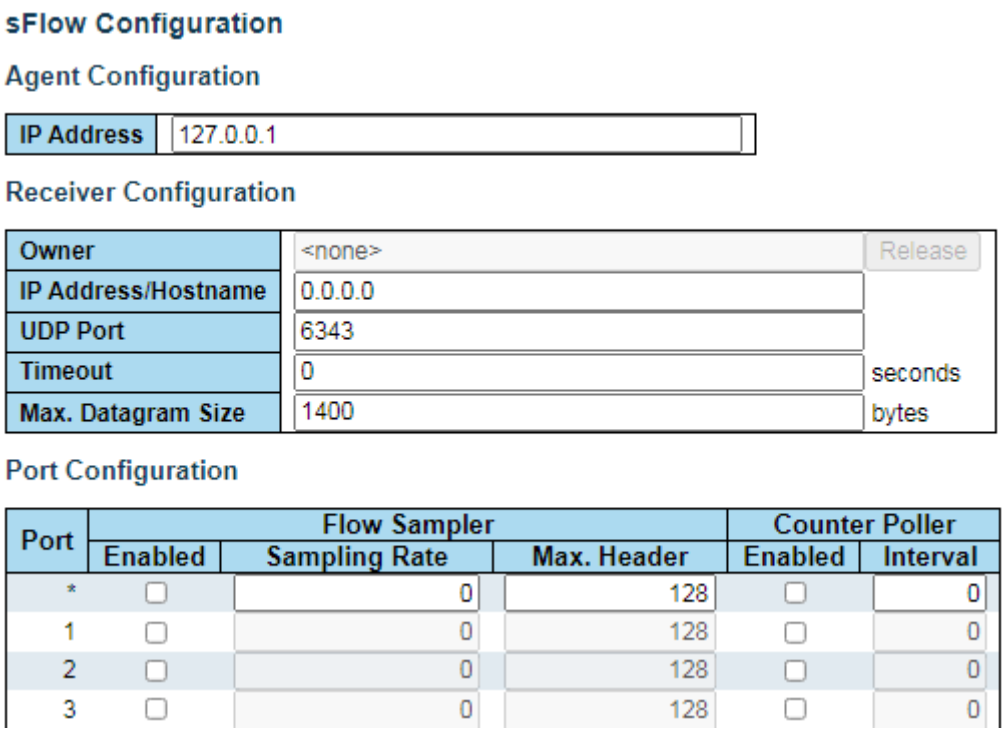


Рис. 5.2.46.1 – Настройки порта

Таблица 5.2.46.1– Настройки порта

Agent Configuration (Настройки агента)	
IP Address	IP-адрес, используемый в качестве IP-адреса агента в sFlow. Он служит уникальным ключом, который будет идентифицировать агента в течение длительных периодов времени. Поддерживаются адреса IPv4 и IPv6.
Receiver Configuration (Конфигурация приемника)	
Owner	• None - не сконфигурирован / не востребован. • Configured through local management – сконфигурирован через Web или CLI; • Если sFlow в настоящий момент сконфигурирован через SNMP, содержит строку, идентифицирующую приемник sFlow.
IP Address/Hostname	IP-адрес или имя хоста приемника sFlow.
UDP Port	Просматриваемый порт UDP
Timeout	Таймаут
Max. Datagram Size	Максимальное количество байтов данных, которое может быть отправлено в одной тестовой датаграмме
Port Configuration (Настройки порта)	
Port	Номер порта
Flow Sampler Enabled	Включает или отключает выборку потока на порту.
Flow Sampler Sampling Rate	Статистическая частота дискретизации для выборки пакетов.
Flow Sampler Max. Header	Максимальное количество байтов, которое должно быть скопировано из пакета, выбранного для выборки, в дейтаграмму sFlow.
Counter Poller Enabled	Включает или отключает опрос счетчика на этом порту.
Counter Poller Interval	Интервал опроса. Допустимый диапазон: от 1 до 3600 секунд.

5.2.47. DDMI (интерфейс цифрового диагностического мониторинга)

Усовершенствованный цифровой интерфейс позволяет установить связь в реальном времени между коммутатором и трансивером SFP. Это позволяет коммутатору получать доступ к рабочим параметрам в оптоволоконном канале.

DDMI контролирует:

• температуру
• напряжение питания
• передаваемый ток смещения.
• Передаваемая мощность
• Полученная мощность

Для доступа к настройкам необходимо перейти по вкладке Configuration→DDMI.

Настройка DDMI (Рис. 5.2.47.1) (Табл. 5.2.47.1)

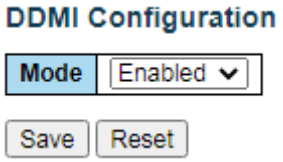


Рис. 5.2.47.1 – Настройки порта

Таблица 5.2.47.1 – Настройки порта

Mode	Включение/выключение функции DDMI. Функция DDMI включена по умолчанию.

5.2.48. UDLD

Для доступа к настройкам необходимо перейти по вкладке Configuration→UDLD.

Протокол второго уровня, созданный для автоматического обнаружения потери двухсторонней коммуникации на линиях связи

Port Configuration (Настройки порта) (Рис. 5.2.48.1) (Табл. 5.2.48.1)

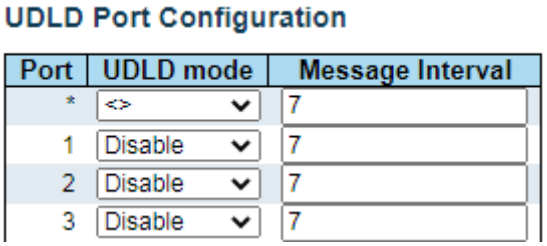


Рис. 5.2.48.1– Настройки порта

Таблица 5.2.48.1– Настройки порта

Port	Номер порта
UDLD mode	Включить/выключить UDLD на порту
Message Interval	Интервал сообщений

Приложение 1 – Обращение в службу технической поддержки

Обращение в службу технической поддержки ЗАО НПО «Телеком» вы можете осуществить следующими способами:

– заполнить форму обратной связи на сайте компании http://npotelecom.ru;

– написать письмо на почту help@npotelecom.ru;

– позвонить по телефону 8 (3412) 57-30-32.

Обращение в службу ремонта ЗАО НПО «Телеком» вы можете осуществить следующими способами:

– написать письмо на почту remont@npotelecom.ru;

– позвонить по телефону 8 (3412) 57-30-39.

При любом обращении необходимо указать суть проблемы, название устройства, серийный номер, версию ПО, указать контакты для обратной связи.