Amatek

www.amatek.su

Управляемый (L2+) PoE коммутатор

Руководство по эксплуатации

Модель:
AN-SM28P24

EAC

v.1.0 02.2023

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

Важные предупреждения

Внимание! Обязательно изучите настоящее «**Руководство по эксплуатации**» перед использованием оборудования. Данное оборудование является сложным техническим устройством. Помните, неправильное подключение оборудования может вывести его из строя!

ПРЕДОСТЕРЕЖЕНИЕ

ОПАСНОСТЬ ПОРАЖЕНИЯ ЭЛЕКТРИЧЕСКИМ ТОКОМ

ВАЖНО: Используйте только источник питания, тип которого указан на этикетке устройства.

Мы не несем ответственности за любые убытки, возникшие от любого неправильного использования изделия, даже если мы были предупреждены о возможности таких убытков.

Символ молнии со стрелкой внутри равностороннего треугольника предназначен для предупреждения пользователя о наличии неизолированного «опасного напряжения» внутри корпуса изделия, которое может быть достаточной величины, чтобы представлять опасность поражения человека электрическим током.

Восклицательный знак внутри равностороннего треугольника предназначен для предупреждения пользователя о наличии важных инструкций по эксплуатации и техническому обслуживанию (ремонту) в документации, прилагаемой к устройству.

ROHS
все продукты, предлагаемые производителем, соответствуют требованиям директивы европейского права об ограничении использования опасных веществ (RoHS), которая означает, что производственные процессы и продукты производятся по бессвинцовой технологии и без опасных веществ, указанных в директиве.

Знак перечеркнутого мусорного контейнера означает, что продукт после окончания срока службы должен быть собран и утилизирован отдельно от других бытовых отходов.

Данное устройство в бытовых условиях может вызывать радиопомехи, в этом случае от пользователя может потребоваться принятие соответствующих мер.

Предупреждение

Данное оборудование генерирует, использует и может излучать радиочастотную энергию и, если оно установлено или используется не в соответствии с инструкциями производителя, может излучать вредные радиопомехи. Эксплуатация данного оборудования в жилых зонах может вызвать радиопомехи в окружающей среде, в этом случае пользователь может быть обязан принять меры в соответствии с действующим законодательством.

Ответственность

Информация, содержащаяся в данном документе, актуальна на момент публикации. Любые пункты настоящего Руководства по эксплуатации, а также разделы меню управления оборудованием, могут быть изменены производителем, в любое время без предварительного уведомления. Производитель не гарантирует и не несет никакой юридической ответственности за точность, полноту или полезность данного Руководства по эксплуатации.

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

Меры предосторожности

Безопасность

Сохраните «Руководство по эксплуатации» для дальнейшего использования.

Производитель не несет ответственности за неправильную эксплуатацию оборудования, если такой случай произошел из-за несоответствия данного Руководства в связи с изменением характеристик или меню управления оборудованием, не описанных в данном Руководстве по эксплуатации.

Обновленные версии данного Руководства размещаются на сайте www.amatek.su.

Задавайте все вопросы по обслуживанию квалифицированному специалисту в разделе «Поддержка» на сайте www.amatek.su или по телефону Федеральной службы поддержки Amatek 8-800-707-10-40 (звонок по России бесплатный).

Запрещается производить ремонт устройства самостоятельно. Любые работы по обследованию и ремонту оборудования должны производиться только специально обученным персоналом.

Устройства, подключенные к Интернету, могут столкнуться с проблемами безопасности сети. Пожалуйста, усильте меры по защите личной информации и безопасности данных. Если вы обнаружите, что устройство может нести угрозу безопасности сети, пожалуйста, свяжитесь с нами своевременно.

Пожалуйста, примите к сведению, что вы несете ответственность за правильную настройку всех паролей и других параметров безопасности данного продукта; храните эти данные в надежном месте.

Обновление внутреннего программного обеспечения не рекомендуется производить самостоятельно без участия технической поддержки производителя.

Заземление

Это продукт Класса защиты 1 (снабжен защитным заземлением, подключающимся к розетке). Вилка должна быть вставлена только в сетевую розетку, снабженную защитным заземляющим контактом. Любой обрыв заземляющего проводника внутри или за пределами устройства может сделать его опасным. Умышленный обрыв заземляющего контакта запрещен.

Установка и подключение

Монтаж и настройку рекомендуется производить силами квалифицированного персонала. Продавец не несет ответственности за неисправности, полученные вследствие неправильного подключения оборудования или его ненадлежащего использования.

Все работы по установке и управлению оборудованием должны отвечать требованиям и нормам по технике безопасности и пожарной безопасности. Продавец не несет финансовой или юридической ответственности за возгорание или поражение электрическим током вследствие несоблюдения пожарной безопасности, несоблюдения техники безопасности или некорректного монтажа оборудования.

Данное оборудование должно работать только от источника питания, тип которого указан на приборе, на упаковке или в документации к оборудованию. Перед использованием необходимо проверить соответствие подаваемого напряжения питания.

Данное оборудование предназначено для использования в прохладном сухом помещении. Не устанавливайте данное устройство во влажной среде или в местах, где возможно попадание воды на устройство.

В случае попадания внутрь корпуса устройства посторонних предметов или жидкости, немедленно отключите питание и обратитесь к квалифицированному персоналу для проверки устройства перед повторным запуском.

Не устанавливайте данное устройство вблизи источников тепла, таких как радиаторы, обогреватели, печи, камины и иные устройства, вырабатывающие тепло.

Не устанавливайте данное устройство вблизи источников сильных электромагнитных помех.

Не допускайте длительного воздействия на оборудование прямых солнечных лучей.

Не блокируйте вентиляционные отверстия устройства. Не размещайте устройство на мягкой поверхности (ковры, ткань и т.п.) или вблизи плотных материалов (шторы и пр.), которые могут заблокировать вентиляционные отверстия. Не устанавливайте устройство в местах, подверженных большому скоплению пыли и/или механической вибрации.

Чистка и хранение

Чистите устройство мягкой тканью, не используйте сильнодействующие средства.

Если оборудование не используется в течение нескольких дней или более, отсоедините устройство от сети питания. Никогда не тяните за шнур питания, только за вилку.

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

Содержание

1. Введение **1**
1.1 Описание устройства 1
1.2 Особенности PoE коммутатора 1
1.3 Внешний вид и органы управления коммутатора 2
1.4 Типовая схема подключения PoE коммутатора 2
1.5 Спецификация программных функций 3
2. Доступ к коммутатору через WEB-интерфейс **5**
2.1 Вход в систему (авторизация) 5
2.2 Структура WEB-интерфейса 5
3. Конфигурация системы **6**
3.1 System Information (Системная информация) 6
3.2 Network (Конфигурация сети) 7
3.3 User Account (Учетные записи пользователей) 7
3.4 Log Configuration (Настройки системного журнала) 8
3.5 Telnet Configuration (Настройки Telnet) 10
3.6 HTTPS Configuration (Настройки HTTPS) 10
3.7 Diagnostics Test (Тест соединений) 10
4. Port Configuration (Конфигурация портов) **12**
4.1 Port Setting (Настройка портов) 12
4.2 Storm Control (Защита от широковещательного шторма) 13
4.3 Port Rate limit (Ограничение скорости порта) 15
4.4 Port Mirroring (Зеркалирование портов) 16
4.5 Link Aggregation (Агрегация портов) 18
4.5.1 Описание интерфейса Link Aggregation 18
4.5.2 Добавление статических групп агрегации 19
4.5.3 Добавление динамических групп агрегации (LACP) 20
4.6 Port Isolation (Изоляция портов) 22
4.7 Port Statistics (Статистика трафика портов) 22
5. POE Setting (Настройки PoE) **23**
5.1 PoE Port Setting (Настройка PoE портов) 23
5.2 PoE Port Timer Setting (Настройка расписания работы PoE) 24
5.3 PoE Port Timer Reboot Setting (Расписание перезагрузки PoE) 24
6. VLAN MANAGEMENT (Управление VLAN) **25**
6.1 VLAN Configuration (Настройка VLAN) 25
6.1.1 Создание VLAN 26
6.1.2 Добавление портов в выбранную VLAN 27
6.1.3 Port Setting (Настройка портов VLAN) 29

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

6.2 MAC VLAN (VLAN на основе MAC адресов) 30
6.3 Protocol VLAN (VLAN на основе протокола) 32
6.4 VOICE VLAN (VLAN IP телефонии) 33
6.4.1 Настройка Voice VLAN 33
6.4.2 Конфигурирование портов Voice VLAN 34
6.4.3 Voice OUI (Настройка Voice OUI) 34
6.4.4 Пример настройки Voice VLAN 35
6.5 SURVEILLANCE VLAN (VLAN системы видеонаблюдения) 37
7. MAC Management (Управление MAC-адресами) 37
7.1 Dynamic Address (Динамическое обновление MAC адресов) 38
7.2 Static Address (Статические MAC-адреса) 38
8. Spanning Tree (Настройка протоколов STP/RSTP/MSTP) 39
8.1 Global Configuration (Глобальные настройки) 40
8.2 MST Instance (Настройка MST экземпляра) 41
8.3 MST Port Setting (Настройка MST портов) 42
8.4 Port Setting (Настройка портов) 43
9. Multicast (Многоадресная рассылка) 44
9.1 IGMP Snooping (Настройка IGMP Snooping) 44
9.2 Group Address (Настройки групп адресов IGMP) 46
9.3 Filtering (Настройка фильтрации рассылок) 47
10. Network Security (Сетевая безопасность) 47
10.1 DoS Attack Resistance (Защита от DoS-атак) 47
10.2 ACL (Настройки ACL) 48
10.2.1 MAC ACL Configuration (Настройки MAC ACL) 48
10.2.2 IPv4 ACL Configuration (Настройки IPv4 ACL) 49
10.2.3 IPv6 ACL Configuration (Настройки IPv6 ACL) 51
10.2.4 ACL Binding (Привязка ACL к портам) 51
11. Advanced Configuration (Дополнительные настройки) 52
11.1 QoS Configuration (Настройки протокола QoS) 52
11.1.1 Basic Configuration (Базовые настройки) 52
11.1.2 Queue Scheduling (Планирование очереди) 53
11.1.3 CoS Mapping (Сопоставление CoS) 54
11.1.4 DSCP Mapping (Сопоставление DSCP) 54
11.1.5 IP Precedence Mapping (Сопоставление IP приоритета) 55
11.2 LLDP Configuration (Настройки протокола LLDP) 55
11.2.1 LLDP Configuration (Настройки LLDP) 55
11.2.2 Port Configuration (Настройки портов LLDP) 56
11.2.3 Neighbor Info (Информация о соседних устройствах) 58

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

11.3 SNMP Configuration (Настройки SNMP) 58
11.3.1 View Configuration (Настройки View) 58
11.3.2 Group Configuration (Настройки групп) 59
11.3.3 Community Configuration (Настройки сообществ) 60
11.3.4 User Configuration (Настройки пользователей SNMP) 60
11.3.5 Engine ID Configuration (Настройки Engine ID) 61
11.3.6 Trap Event Configuration (Настройки Trap событий) 62
11.3.7 Notification Configuration (Настройки уведомлений) 62
11.4 RMON (Протокол RMON) 63
11.4.1 Port Statistics (Статистика мониторинга портов) 63
11.4.2 History Configuration (Настройки сохранения данных) 64
11.4.3 Event Configuration (Настройки групп событий) 65
11.4.4 Alarm Configuration (Настройки групп тревог) 66
11.5 DNS Configuration (Настройки DNS) 67
11.6 System Time (Настройки системного времени) 68
12. DHCP (Настройки DHCP) 69
12.1 DHCP global configuration (Глобальные настройки DHCP) 69
12.2 IP Pool Setting (Настройка пула IP-адресов) 70
12.2 Address Group Setting (Настройка VLAN IF Address Group) 71
12.3 Client List (Информация о списке DHCP клиентов) 71
12.3 Client Static Binding Table (Таблица статической привязки) 72
12.4 DHCP Snooping Configuration (Настройки DHCP Snooping) 72
12.4.1 DHCP Snooping Global Configuration (Основные настройки) 73
12.4.2 IPMV Static Binding (Статическая привязка IPMV) 74
12.4.3 DHCP Option82 Configuration (Настройка Option82) 75
12.4.4 Пример настройки DHCP Option82 76
13. System Maintenance (Обслуживание системы) 78
13.1 Configuration Management (Управление конфигурацией) 78
13.2 Configuration Saving (Сохранение конфигурации) 78
13.3 Device Restart (Перезагрузка коммутатора) 79
13.4 Firmware Management (Обновление прошивки) 79
Приложение 1. Технические характеристики 80
Приложение 2. Гарантийные обязательства 81
П.1 Адрес сервисного центра 81
П.2 Условия выполнения гарантийных обязательств 81

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

1. Введение

1.1 Описание устройства

Управляемый (L2+) PoE коммутатор на 28 портов предназначен для подключения сетевых устройств и обеспечения питания IP устройств по стандарту PoE.

Коммутатор оснащен 24-мя Gigabit Ethernet (10/100/1000Base-T) портами с поддержкой PoE IEEE 802.3af/at и автоматическим определением подключаемых PoE устройств. Кроме того, коммутатор имеет четыре Gigabit Ethernet RJ-45 (1000BaseT) + SFP (1000Base-X) Combo порта для подключения по медному или оптоволоконному кабелю к локальной сети, сети Ethernet или другому коммутатору (Uplink порт). Для подключения по оптоволоконному кабелю необходимо использовать SFP модули (в комплект не входят).

Коммутатор поддерживает функцию автоматического определения MDI/MDIX подключения на всех портах. Возможно использование прямых и кросс кабелей.

Функция PoE WatchDog позволяет дистанционно контролировать сетевую активность подключенных PoE устройств. Если подключенное PoE устройство в течение заданного времени перестает отвечать на запросы, коммутатор перезагружает PoE порт для удаленной перезагрузки сетевого устройства.

Настройка и управление коммутатором осуществляется через WEB-интерфейс, Telnet или консольный порт. Вы можете удаленно управлять функциями и гибко изменять настройки коммутатора.

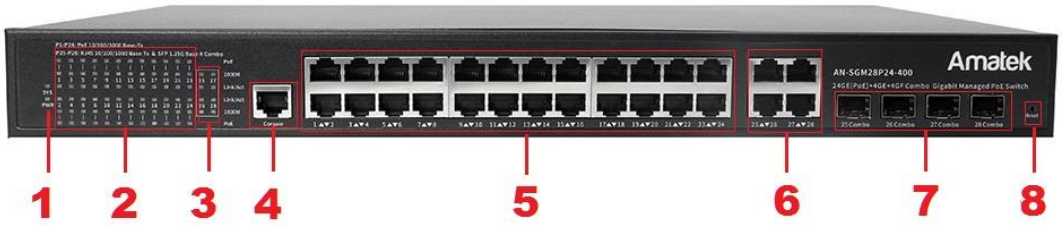
Максимальная мощность PoE составляет 30Вт на порт. Максимальный суммарный бюджет PoE всех портов составляет 400Вт.

1.2 Особенности PoE коммутатора

- 24 коммутируемых Gigabit Ethernet PoE портов и 4 Gigabit Combo Uplink порта.
- Использование стандартов IEEE 802.3, IEEE802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3az EEE, IEEE 802.3x.
- Поддержка питания PoE устройств по стандартам IEEE802.3af, IEEE802.3at.
- Функция автоматического определения MDI/MDIX.
- Функция PoE WatchDog.
- Все порты поддерживают автоматическую адаптацию скорости передачи данных и передачу jumbo фреймов.
- Настройка и управление через WEB-интерфейс, Telnet, Консольный порт.
- Поддержка функций L2+ уровня: VLAN, QOS, MSTP, IGMP, MDL, ACL и др.
- Поддержка PoE Management для коммутации и настройки PoE портов.
- Максимальный суммарный бюджет PoE 400Вт.

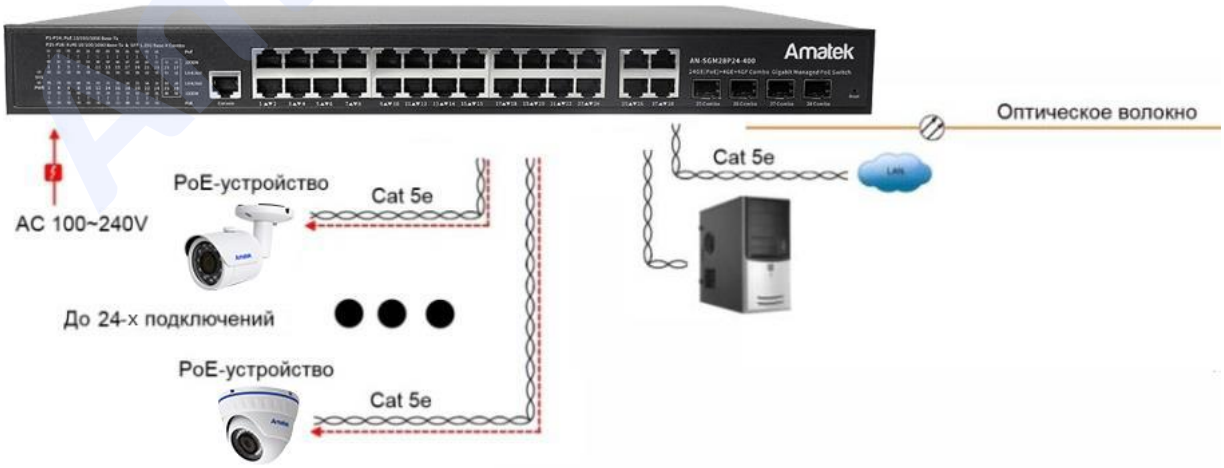
SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.3 Внешний вид и органы управления коммутатора



№	Обозначение	Описание
1	PWR	Индикатор питания от сети 220В
2	1 – 24 / Link/Act / 1000M / PoE	Индикаторы сетевой активности портов с 1 по 24 / Индикаторы питания PoE
3	25 - 28 / / Link/Act / 1000M	Индикаторы сетевой активности Gigabit Combo Uplink портов 25 - 28
4	Console	Консольный порт RJ-45
5	1 - 24	Разъемы RJ-45 портов с 1 по 24 для подключения сетевых устройств (10/100/1000 Base-T) с поддержкой питания PoE
6	25 - 28	Разъемы RJ-45 Combo Uplink портов 25 - 28 для подключения сетевых устройств (1000 Base-T)
7	25 – 28 Combo	Слоты SFP Combo Uplink портов 25-28 для подключения сетевых устройств (1000 Base-X) с использованием оптоволоконного кабеля
8	Reset	Кнопка сброса. Для сброса настроек коммутатора нажмите кнопку «Reset» на 5 секунд.

1.4 Типовая схема подключения PoE коммутатора



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

1.5 Спецификация программных функций

1. Функции Layer 2		
1.1	Port Management	Включение/выключение портов
		Настройки скорости, дуплекса и MTU
		Flow control (Управление потоком)
		Информации о состоянии портов
1.2	Port Mirroring	Зеркалирование портов
1.3	Rate Limit	Ограничение скорости порта.
1.4	Port Isolation	Изоляция порта
1.5	Storm Policing	Защита от широковещательного шторма
1.6	Link Aggregation	Статическая (Static) агрегация в ручном режиме
		Динамическая (Dynamic) агрегация в режиме LACP
1.7	VLAN	Access
		Trunk
		Hybrid
		Разделение QinQ и VLAN на основе порта, протокола и MAC-адреса
		GVRP dynamic VLAN регистрация
		Voice VLAN
1.8	MAC	Статическое добавление или удаление MAC
		Ограничение количества записей MAC-адресов
		Установка динамического времени старения
1.9	Spanning Tree	802.1d (STP)
		802.1w (RSTP)
		802.1s (MSTP)
1.10	Multicast	IGMP Snooping v2/v3
		MLD Snooping v1/v2
1.11	DDM	SFP/SFP+DDM
2. Дополнительные функции		
2.1	ACL	Списки контроля доступа (ACL) основаны на исходном/целевом MAC-адресе, типе протокола, исходном/целевом IP-адресе и порте L4.
2.2	QoS	Классификация обслуживания по 802.1p (CoS)

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

		Классификация по DSCP
		Классификация по исходному/целевому IP-адресу и порту
		SP и WRR алгоритмы
		Committed Access Rate (CAR)
2.3	LLDP	Протокол LLDP (Link Layer Discovery Protocol)
2.4	User Configuration	Добавление/удаление пользователей
2.5	Log	Запись операций, состояние системы и журналы событий
2.6	Attack Resistance	DoS защита
		Защита процессора и ограничение скорости загрузки сообщений
		Привязка ARP (IP-адрес, MAC-адрес, Порт)
2.7	Authentication	802.1x авторизация
2.8	Network Diagnostics	Диагностика сети: Ping, Telnet, трассировка
2.9	System Management	Сброс устройства, сохранение/восстановление конфигурации, обновление прошивки, настройка времени и т.д.
3. Функции управления		
3.1	CLI	Управление командами через консольный порт
3.2	Telnet	Удаленное управление по Telnet
3.3	Web	Настройка L2, обнаружение L2&3
3.4	RMON	Протокол RMON v1
4. Расширенные функции		
4.1 DHCP Snooping и Option 82		
4.2 Конфигурация PoE, управление расписанием и др.		
4.3 Защита от ARP-атак		
4.4 Конфигурация DNS		
4.5 Port security (Конфигурация функций безопасности портов)		
4.7 MVR протокол		
4.8 VCT		
4.9 UDLD протокол		

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

2. Доступ к коммутатору через WEB-интерфейс

WEB-интерфейс позволяет гибко настраивать функции и отслеживать состояние портов коммутатора, используя WEB-браузер (Internet Explorer, Google Chrome, Opera и т.д.)

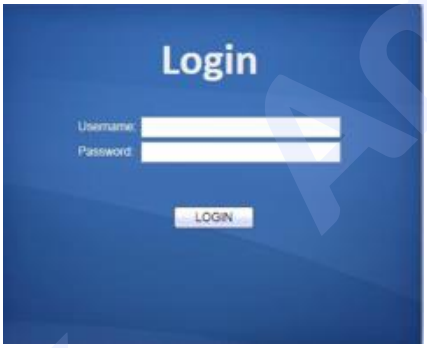
Для начала работы подключите PoE коммутатор к персональному компьютеру (ПК) или локальной сети. Убедитесь, что коммутатор находится в одной подсети с вашим компьютером.

IP адрес коммутатора по умолчанию http://192.168.2.1, маска подсети 255.255.255.0.

2.1 Вход в систему (авторизация)

Введите адрес коммутатора в адресной строке WEB-браузера и нажмите Enter, чтобы перейти на WEB-страницу входа в систему, как показано на рисунке ниже. Далее введите имя пользователя и пароль.

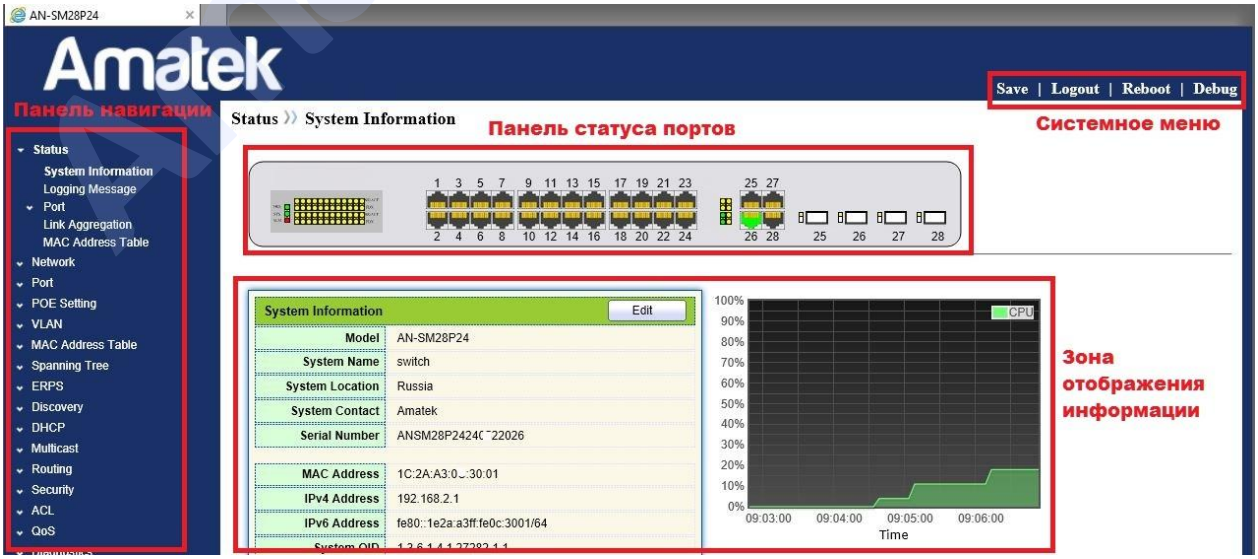
По умолчанию учетная запись администратора имеет логин: **admin**, пароль: **admin**.



При корректном вводе данных вы увидите WEB-страницу «System home» с основной информацией о коммутаторе: наименование модели, MAC адрес, версия прошивки, аппаратная версия, информация о статусе портов.

2.2 Структура WEB-интерфейса

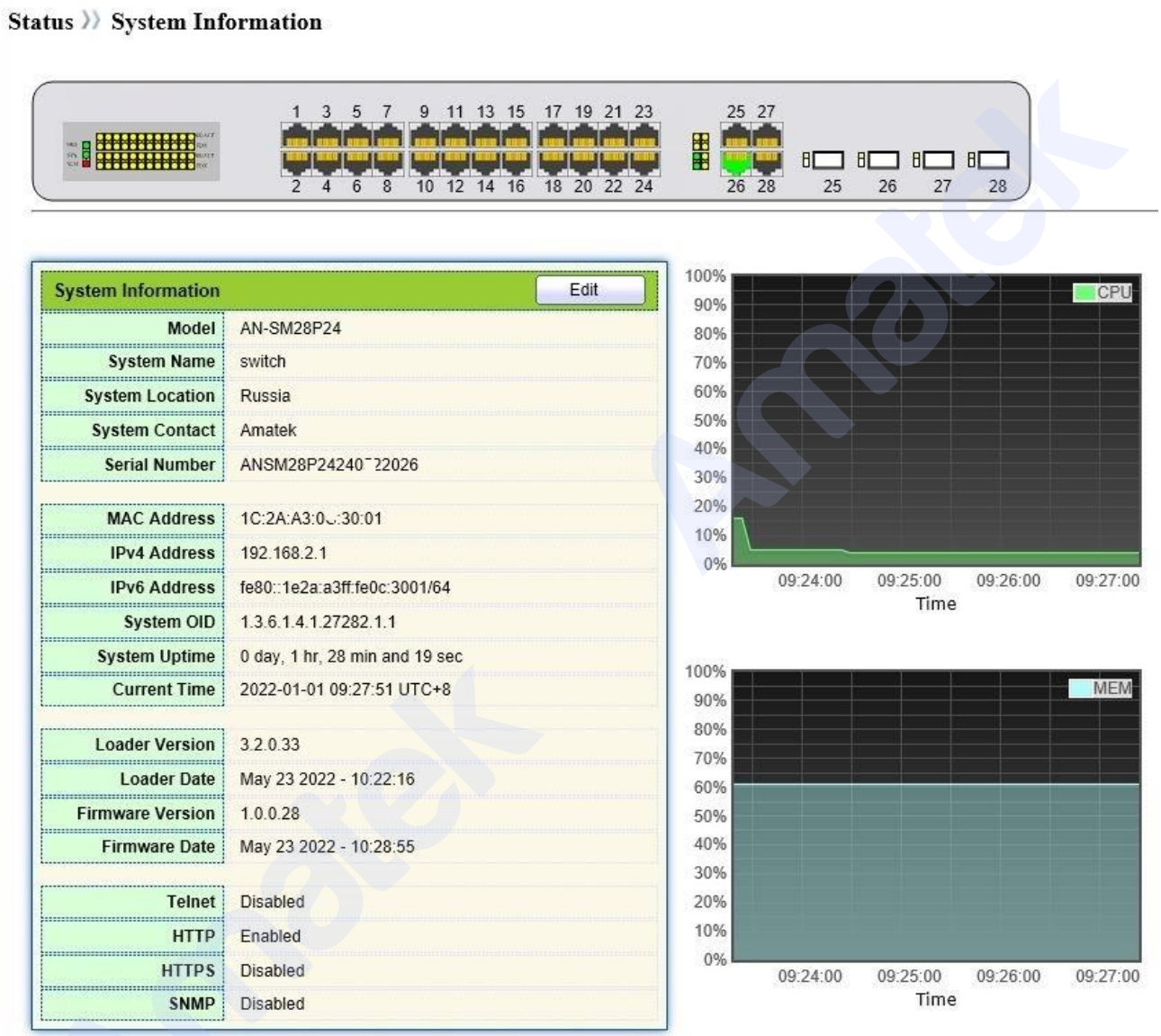
Типовой рабочий WEB-интерфейс системы управления выглядит следующим образом:



3. Конфигурация системы

3.1 System Information (Системная информация)

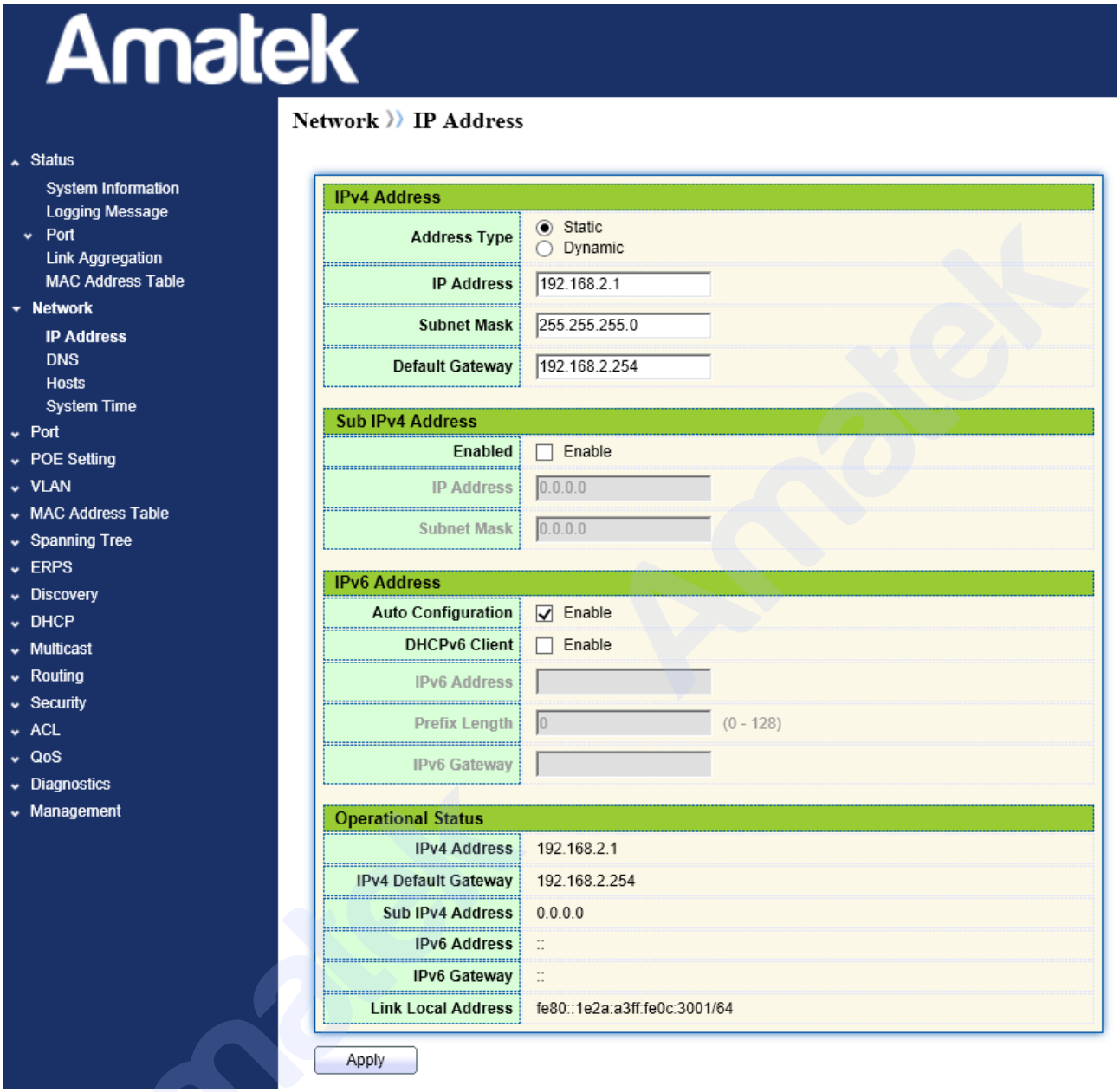
В зависимости от модели коммутатора меню «Системная информация» отображает панель портов и информацию о продукте, в том числе: количество портов, состояния портов, информацию о продукте, состояния включения-выключения функций и т. д.



1. Наведите указатель мыши на порт, чтобы проверить его номер, тип, скорость и состояние.
2. Нажмите «Edit», чтобы изменить поля «System Name» (Название системы), «System Location» (Местоположение) и “System Contact” (Контактные данные) в информации о продукте. Далее нажмите «Apply» для сохранения изменений.

3.2 Network (Конфигурация сети)

Для изменения сетевых настроек нажмите на панели навигации Network -> IP Address.

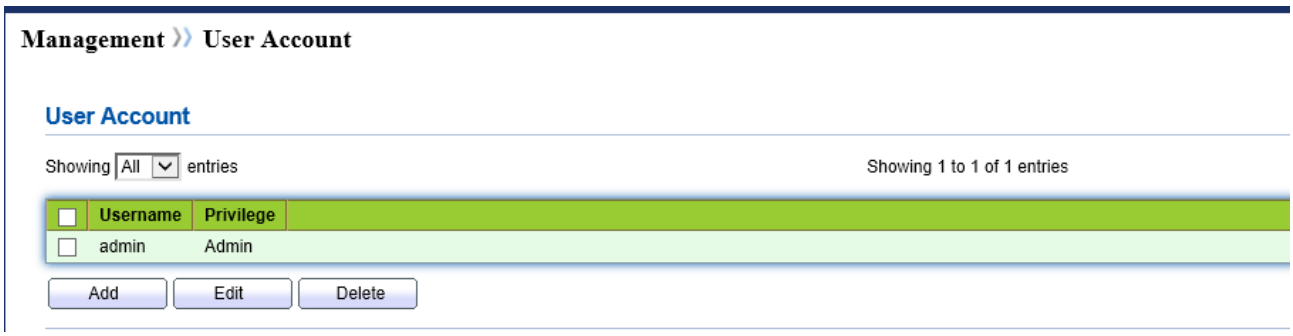


Для изменения сетевых настроек, выполните следующие действия:

Шаг 1: в поле «Address Type» выберите Static (Статический) IP-адрес;
Шаг 2: в поле «IP Address» введите IP-адрес, по умолчанию 192.168.2.1;
Шаг 3: в поле «Subnet Mask» введите маску подсети, по умолчанию 255.255.255.0;
Шаг 4: в поле «Default Gateway» введите адрес шлюза, по умолчанию 192.168.2.254;
Шаг 5: нажмите кнопку «Apply», чтобы сохранить изменения.

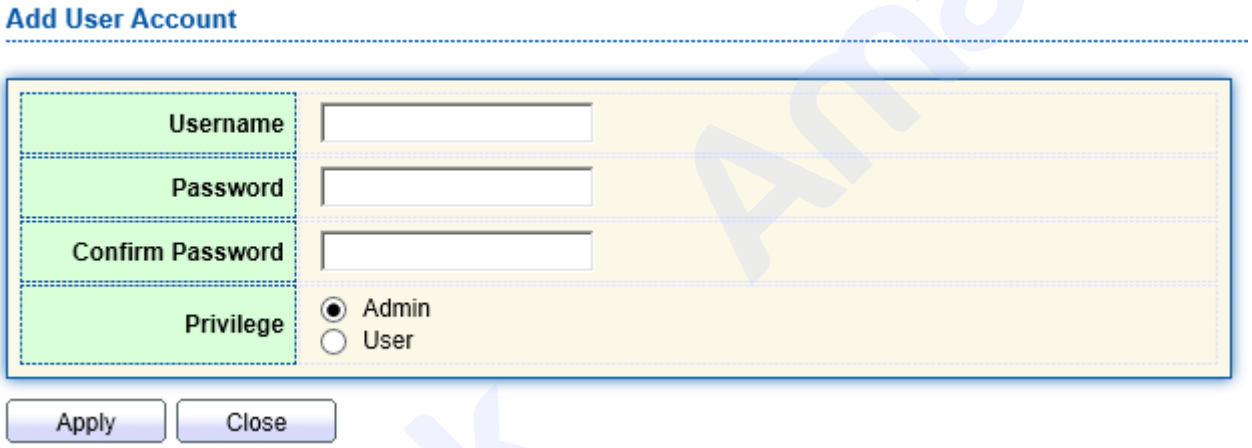
3.3 User Account (Учетные записи пользователей)

Пользователи могут проверять и изменять текущее имя пользователя (Login), пароль и уровень прав пользователя. Для просмотра и изменения учетных записей перейдите «Management» -> «User Account».



Для добавления нового пользователя, выполните следующие действия:

Шаг 1: нажмите кнопку «Add»;
Шаг 2: в поле «Username» введите имя нового пользователя;
Шаг 3: в поле «Password» введите пароль;
Шаг 4: в поле «Confirm Password» повторите пароль;
Шаг 5: в поле «Privilege» выберите права пользователя Admin или User;
Шаг 6: нажмите кнопку «Apply», чтобы сохранить изменения.



Для изменения учетной записи, выберите необходимого пользователя и нажмите кнопку «Edit». Далее внесите необходимые изменения и нажмите кнопку «Apply».

Для удаления учетной записи пользователя, выберите необходимого пользователя и нажмите кнопку «Delete».

3.4 Log Configuration (Настройки системного журнала)

Данное меню отвечает за настройки системного журнала, интеграцию информации, и время обновления информации. Также имеется возможность загрузить журналы работы коммутатора на TFTP-сервер.

Для просмотра и изменения настроек системного журнала, перейдите «Diagnostics» -> «Logging» -> «Property».

Diagnostics » Logging » Property

State	☑ Enable
Aggregation	☑ Enable
Aging Time	300 Sec (15 - 3600, default 300)
Console Logging	
State	☑ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
RAM Logging	
State	☑ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
Flash Logging	
State	☐ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

Apply

Для настройки загрузки системного журнала на TFTP-сервер, перейдите «Diagnostics» -> «Logging» -> «Remote Server». Далее нажмите кнопку «Add» и укажите необходимые параметры удаленного сервера. Нажмите «Apply» для сохранения настроек.

Add Remote Server

Address Type	◉ Hostname ○ IPv4 ○ IPv6
Server Address	
Server Port	514 (1 - 65535, default 514)
Facility	Local 7
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

Apply Close

SEC.RU | Короткий путь к информации 9 Скачано с sec.ru

3.5 Telnet Configuration (Настройки Telnet)

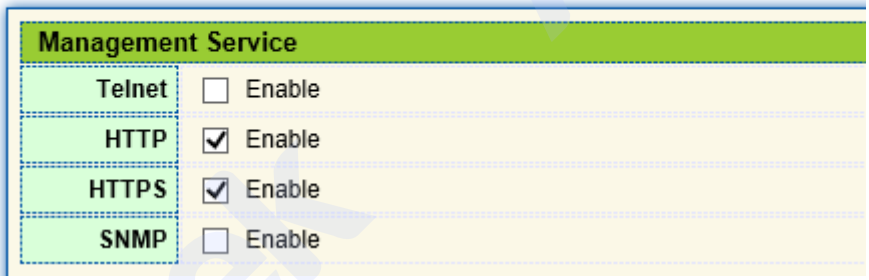
Пользователи могут включить или отключить опцию подключения через Telnet. Для включения/отключения Telnet перейдите «Security» -> «Management Access» -> «Management Service». Далее установите/снимите галочку в поле «Telnet».

Security 〉〉 Management Access 〉〉 Management Service

3.6 HTTPS Configuration (Настройки HTTPS)

Пользователи могут включать или отключать параметры входа по протоколам HTTP и HTTPS.

Security 〉〉 Management Access 〉〉 Management Service

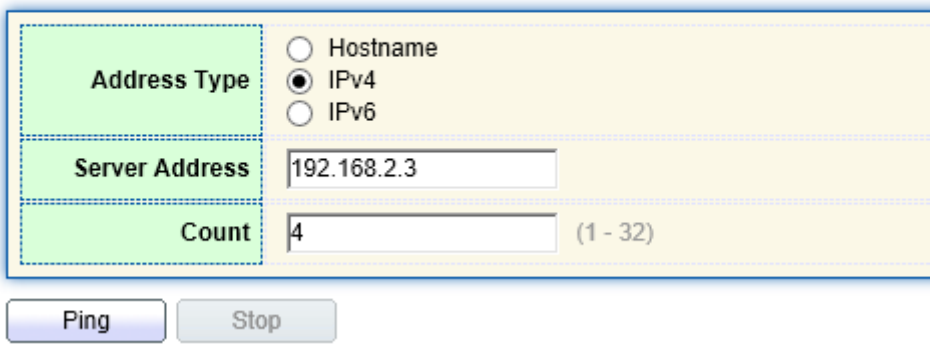


3.7 Diagnostics Test (Тест соединений)

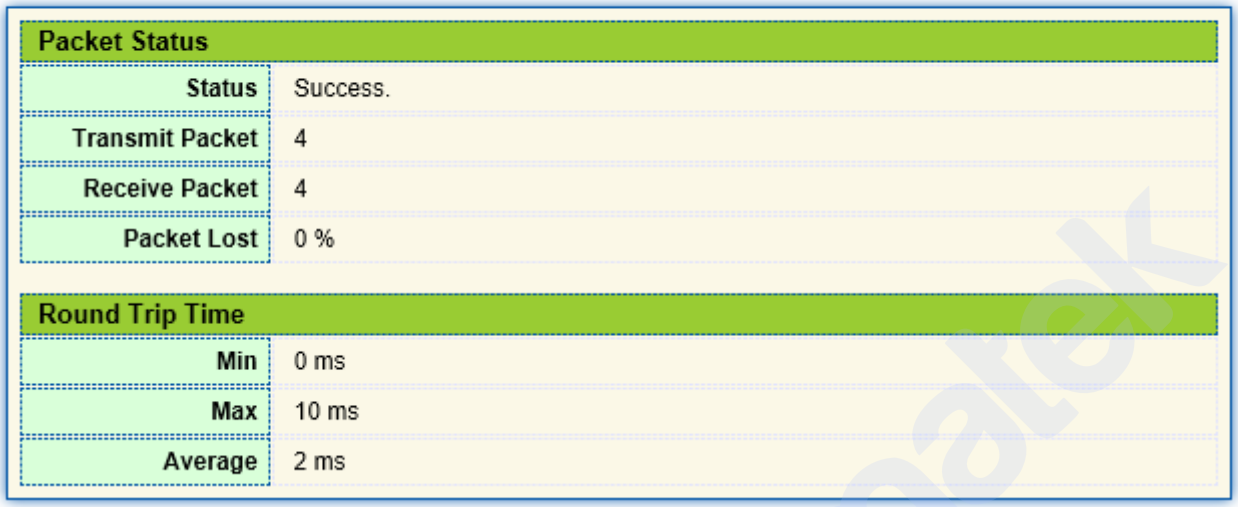
Команда «**Ping**» проверяет доступность указанных IP-адресов / имен хостов и показывает соответствующую статистику соединений.

1. Перейдите «Diagnostics» -> «Ping» на панели навигации. Далее введите имя хоста или IP-адрес, а также количество тестовых пакетов, как показано ниже:

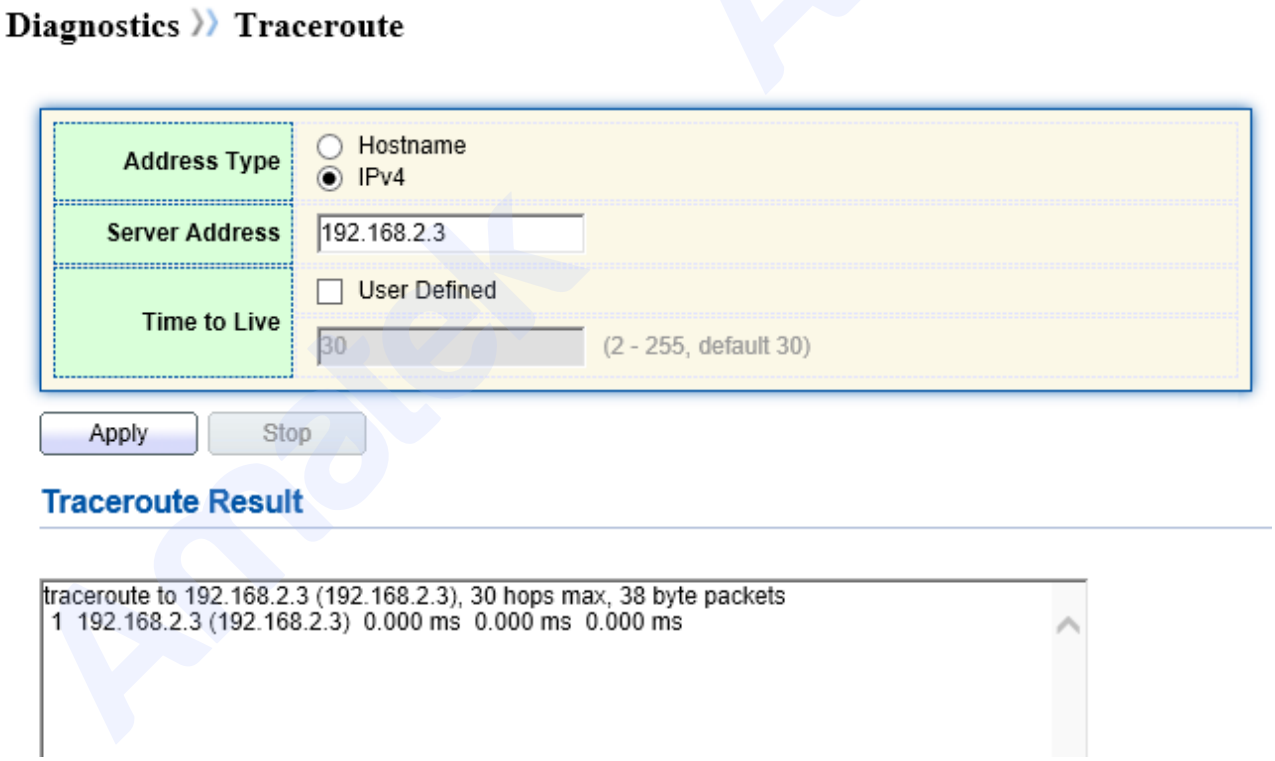
Diagnostics 〉〉 Ping



2. Нажмите «Ping», чтобы запустить тест передачи пакетов для проверки доступности адреса. Результат теста будет показан в окне «Ping Result».



Команда «**Traceroute**» измеряет время от передачи небольшого пакета до его получения от целевого устройства.



Меню «**Copper Test**» (Тест медного кабеля) оценивает состояние входного кабеля и локализует неисправности (ошибка около 5 м) в соответствии с силой отраженного напряжения.

Diagnostics 〉〉 Copper Test

Port	GE27

Copper Test

Copper Test Result

Cable Status	
Port	GE27
Result	OK
Length	N/A

Меню «**Fiber Module**» (Оптоволоконный модуль) оценивает состояние подключенных оптоволоконных SFP модулей.

Diagnostics 〉〉 Fiber Module

Fiber Module Table

	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
○	GE25	N/S	N/S	N/S	N/S	N/S	Insert	Normal

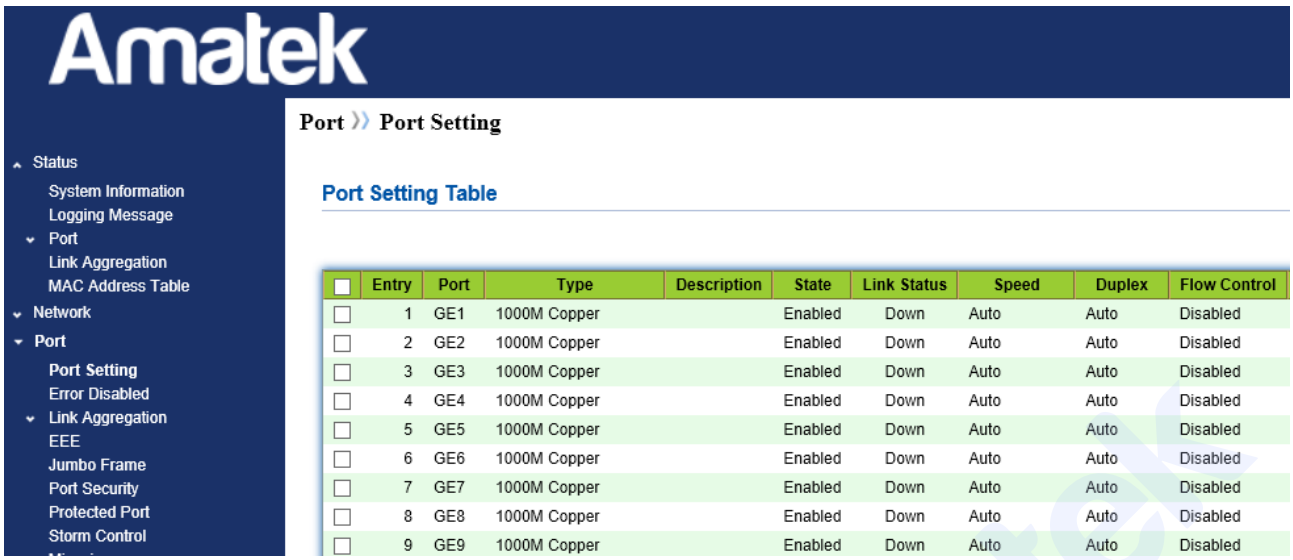
Refresh Detail

Для получения подробной информации о SFP модуле, выберите необходимый порт и нажмите «Detail». Нажмите «Refresh» для обновления информации.

4. Port Configuration (Конфигурация портов)

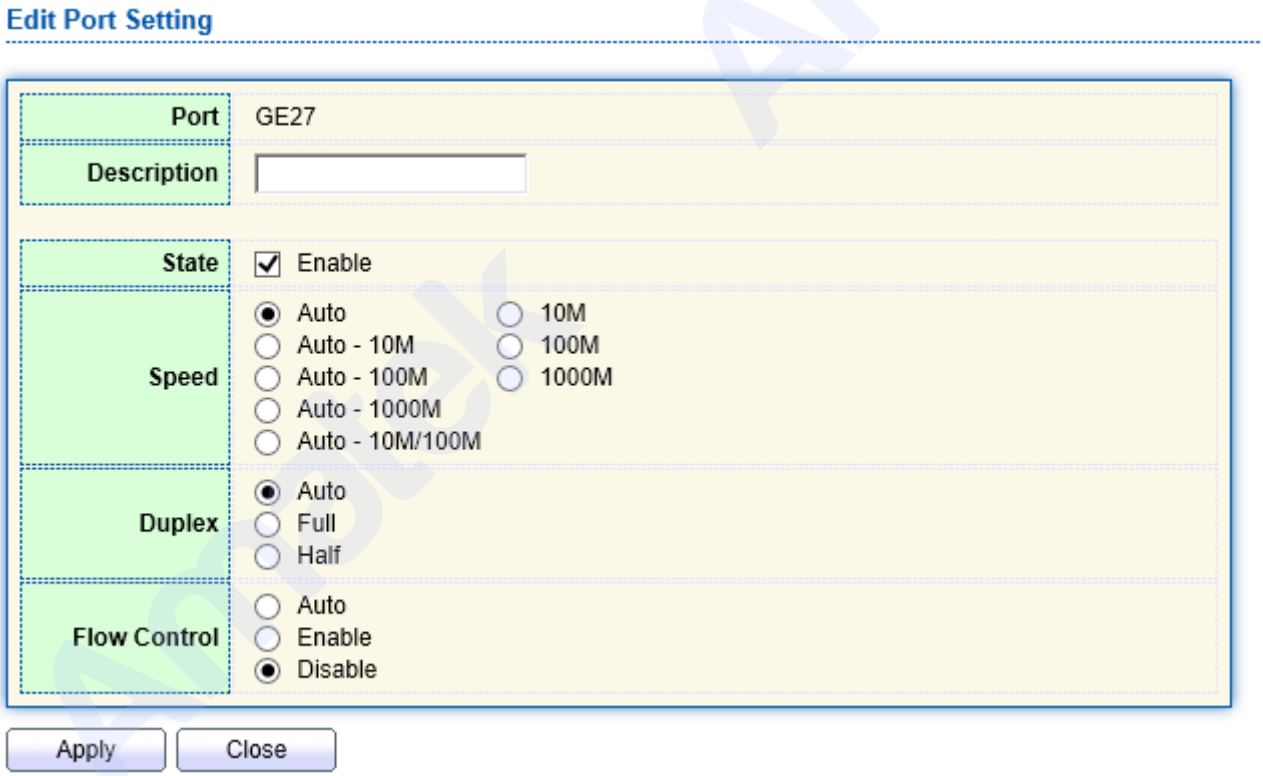
4.1 Port Setting (Настройка портов)

Для более гибкого конфигурирования сети предусмотрена возможность настройки Ethernet портов.



Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled

Изменение конфигурации порта необходимым образом:
Шаг 1: нажмите значок «Edit» для выбора порта или кликните изображение порта;
Шаг 2: на странице конфигурации свойств порта заполните/выберите необходимое значение для настройки;
Шаг 3: нажмите кнопку «Apply», чтобы сохранить изменения.



Примечания:
Вы можете выбрать несколько портов для пакетного конфигурирования.
Если выбранные параметры порта не поддерживаются, изменения не вступят в силу.

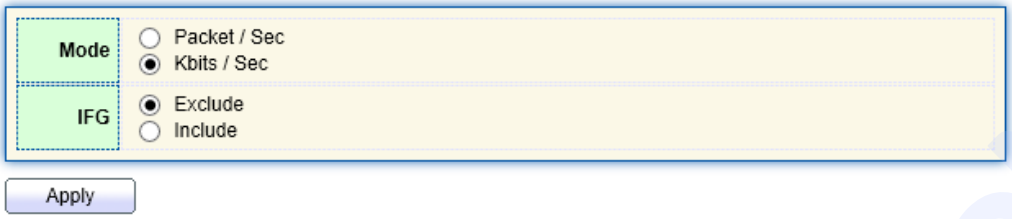
4.2 Storm Control (Защита от широковещательного шторма)

Широковещательный шторм - лавинообразное размножение широковещательных сообщений при появлении в топологии сети замкнутых петель передачи трафика. Взрывной рост передачи пакетов парализует работу сети.

Перейдите «Port» -> Storm Control» на панели навигации, чтобы настроить параметры, связанные с защитой от широковещательных штормов.

Перейдите «Port» -> Storm Control» на панели навигации, чтобы настроить параметры, связанные с защитой от широковещательных штормов.

Port 〉〉 Storm Control



Apply

Port Setting Table

	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
☐	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☑	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	9	GE9	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
☐	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Таблица «Port Setting Table» показывает текущую информацию о значении параметров Storm Control:

- **Port**: номер порта;
- **Broadcast**: управление широковещательными пакетами;
- **Unknown-unicast:** управление неизвестными одноадресными пакетами;
- **Unknown-multicast:** управление неизвестными многоадресными пакетами;

Edit Port Setting

Port	GE2
State	☐ Enable
Broadcast	☐ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Multicast	☐ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Unicast	☐ Enable 10000 Kbps (16 - 1000000, default 10000)
Action	◉ Drop ○ Shutdown

Apply Close

Изменение конфигурации Storm Control необходимым образом:
Шаг 1: выберите необходимый порт и нажмите «Edit»;
Шаг 2: в окне конфигурации свойств Edit Port Setting заполните/выберите необходимое значение параметров;
Шаг 3: нажмите кнопку «Apply», чтобы сохранить изменения.

Примечания:
Вы можете выбрать несколько портов для пакетного конфигурирования.
Если выбранные параметры порта не поддерживаются, изменения не вступят в силу.

4.3 Port Rate limit (Ограничение скорости порта)

Функция Port Rate limit (Ограничение скорости порта) позволяет гибко ограничивать скорость приема/передачи пакетов для каждого порта коммутатора.

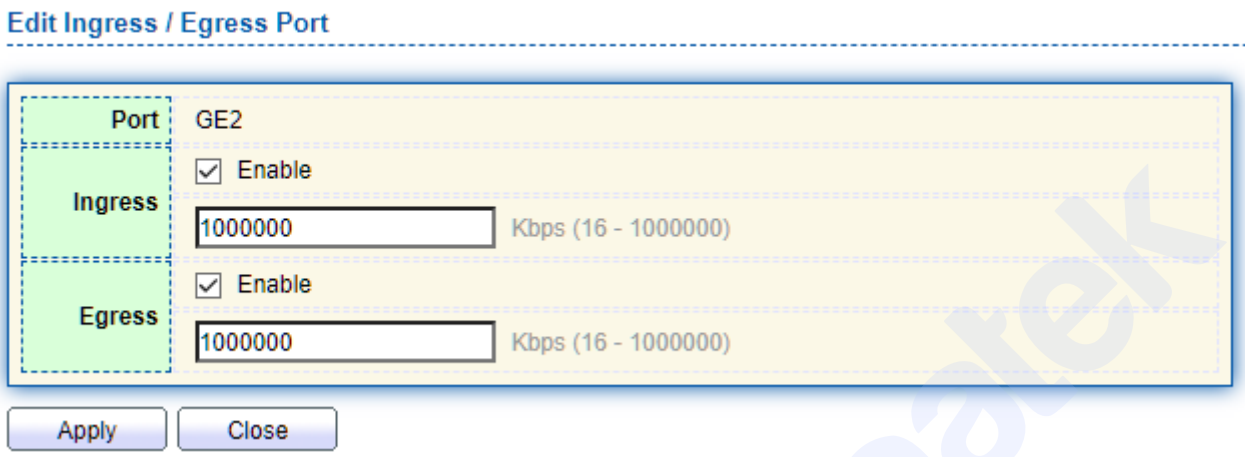
Перейдите «QoS > Rate Limit > Ingress/Egress Port» на панели навигации, чтобы настроить параметры, связанные с ограничением скорости портов.

QoS » Rate Limit » Ingress / Egress Port

Ingress / Egress Port Table

☐	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
☐	1	GE1	Disabled		Disabled	
☐	2	GE2	Disabled		Disabled	
☐	3	GE3	Disabled		Disabled	
☐	4	GE4	Disabled		Disabled	
☐	5	GE5	Disabled		Disabled	
☐	6	GE6	Disabled		Disabled	
☐	7	GE7	Disabled		Disabled	

Ограничение скорости порта:
Шаг 1: отметьте порт для ограничения скорости в таблице портов и нажмите «Edit»
Шаг 2: включите и задайте ограничение скорости приема данных в поле «Ingress»;
Шаг 3: включите и задайте ограничение скорости передачи данных в поле «Egress»;
Шаг 4: нажмите кнопку «Apply», чтобы сохранить изменения.



Параметры конфигурации

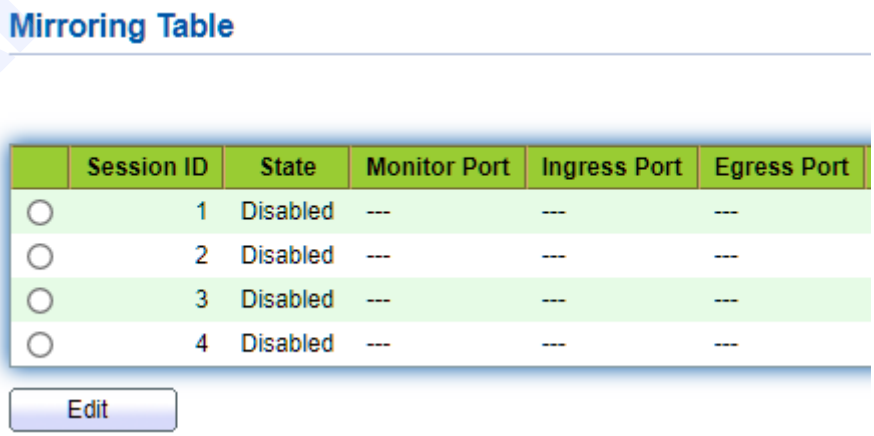
Параметр		Описание
Ingress	Enabled	Вкл./выкл. ограничения скорости приема
	Rate	Диапазон ограничения 16 до 1,000,000 Кбит/с.
Egress	Enabled	Вкл./выкл. ограничения скорости передачи
	Rate	Rate ranges from 16 to 1,000,000 Кбит/с.

Примечания:
Вы можете выбрать несколько портов для пакетного конфигурирования.
Если выбранные параметры порта не поддерживаются, изменения не вступят в силу.

4.4 Port Mirroring (Зеркалирование портов)

Функция зеркалирования портов позволяет дублировать трафик от одного или нескольких портов на отдельно взятый порт. В основном это применяется для анализа и мониторинга трафика в целях безопасности сети.

Перейдите «**Port > Mirroring**» на панели навигации, чтобы настроить параметры зеркалирования портов.



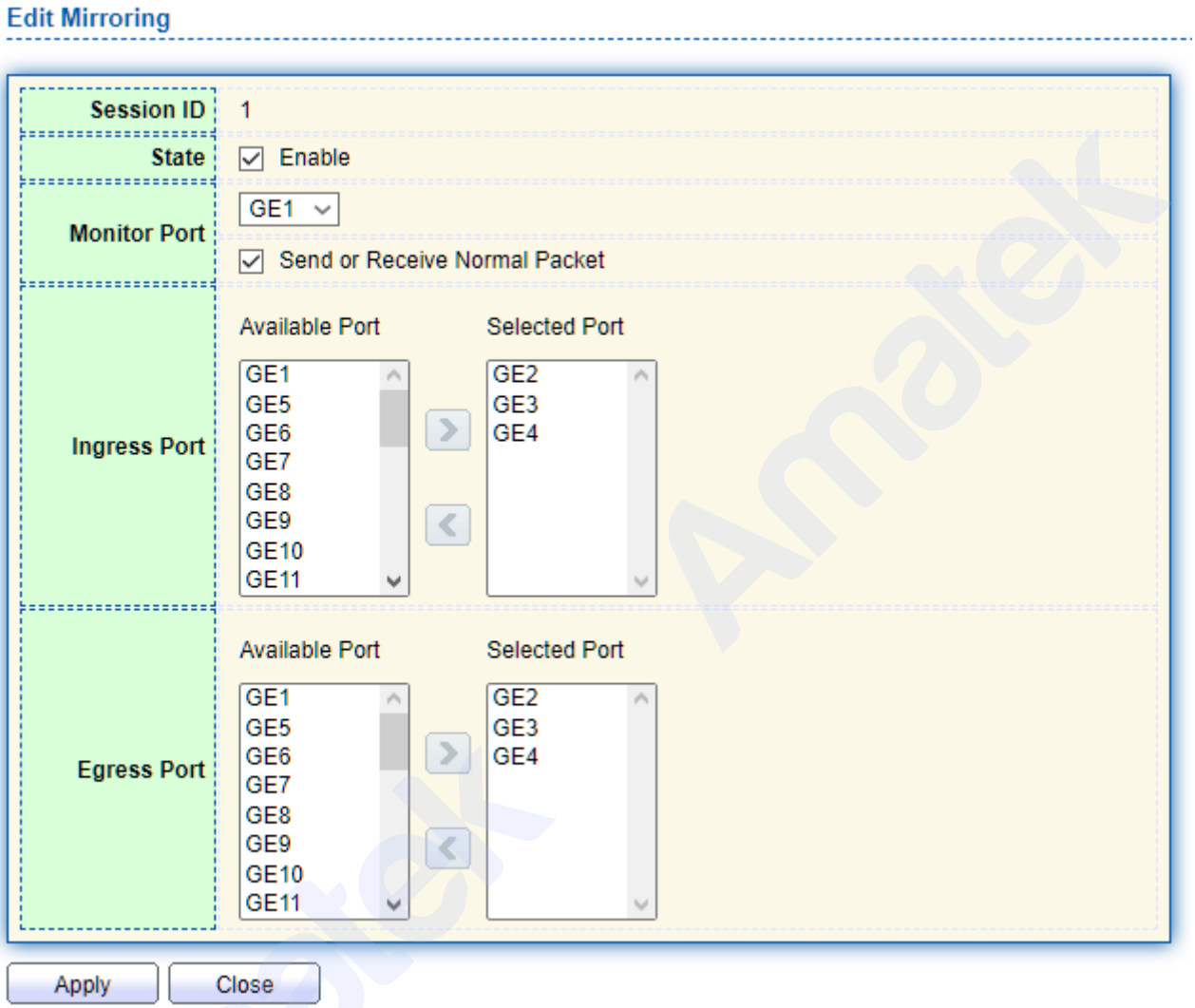
Настройка зеркалирования портов:

Шаг 1: отметьте сессию зеркалирования в таблице «Mirroring Table» и нажмите «Edit»;

Шаг 2: выберите порт-зеркало в поле «Monitor port»;

Шаг 3: выберите порты, трафик которых будет дублироваться на порт-зеркало (отдельно для входящего (Ingress Port) и исходящего (Egress Port) трафика.

Шаг 4: нажмите кнопку «Apply», чтобы сохранить изменения.



Параметры интерфейса

Параметр	Описание
Session ID	Можно настроить до четырех сессий зеркалирования
State	Вкл./выкл. сессии зеркалирования
Monitor port (Destination Port)	Можно выбрать только один физический порт, за исключением порта группы агрегации каналов.
Source Ingress Port	Весь входяший трафик будет зеркалироваться на порт назначения
Source Egress Port	Весь исходящий трафик будет зеркалироваться на порт назначения

Примечания:

Группа агрегации портов не может быть установлена в качестве дистанционного порта-зеркала или исходного порта.

Порты назначения и источника не могут совпадать.

SEC.RU | Короткий путь к информации
17
Скачано с sec.ru

Для правильной работы функции зеркалирования необходимо обязательно выбрать как исходный, так и порт назначения.

4.5 Link Aggregation (Агрегация портов)

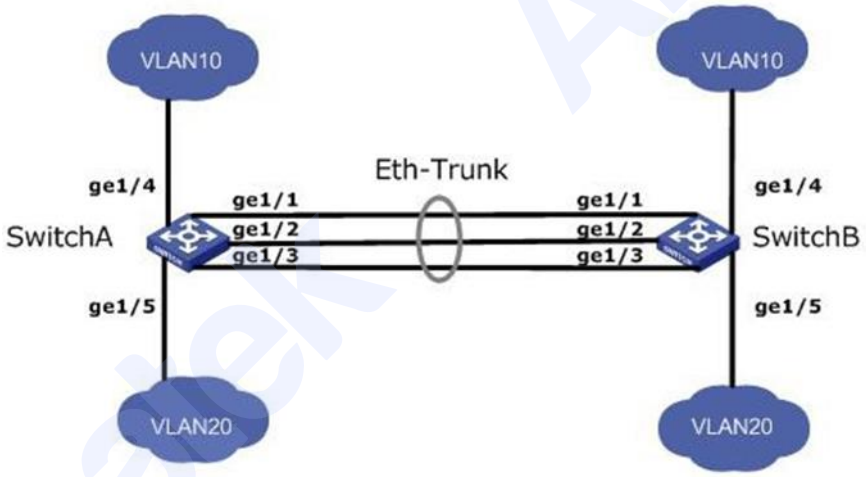
Коммутатор поддерживает агрегацию нескольких портов в одну магистральную сеть с большей пропускной способностью. Link Aggregation расширяет полосу пропускания и надежность передачи, объединяя группу физических каналов в один. Каждая группа агрегации может содержать до 8 портов.

4.5.1 Описание интерфейса Link Aggregation

LAG (группа агрегации каналов) — это логический канал «Eth-Trunk», объединяющий несколько физических каналов (портов).

Технология Link Aggregation объединяет несколько физических интерфейсов в один логический интерфейс без добавления нового оборудования. Эта технология не только повышает надежность, но и распределяет потоковую нагрузку по различным физическим каналам.

Как показано ниже, коммутатор A связан с коммутатором B через три канала Ethernet, объединенных в логический канал Eth-Trunk. Его пропускная способность равна общей пропускной способности трех каналов, что увеличивает пропускную способность. Между тем, эти три канала Ethernet дублируют друг друга, что повышает надежность соединения.



Link Aggregation может помочь решить следующие проблемы:

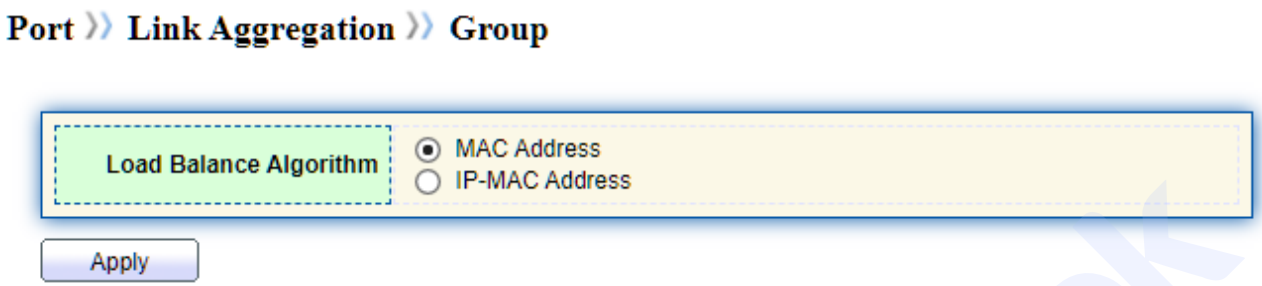
- Недостаточная пропускная способность соединения двух коммутаторов.
- Недостаточная надежность двух коммутаторов, соединенных одним каналом.

Агрегацию каналов можно разделить на ручной режим **Static Mode** и режим **LACP**, в соответствии с использованием протокола управления агрегированием каналов - Link Aggregation Control Protocol (LACP).

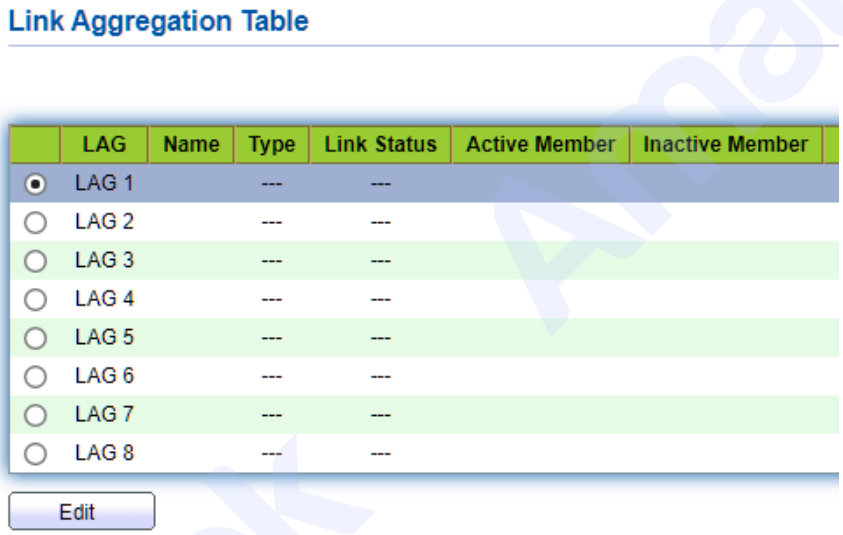
В режиме Static Mode, при установлении «Eth-Trunk», доступ к логическому интерфейсу должен быть добавлен вручную без протокола LACP. Его также называют режимом распределения нагрузки, поскольку все каналы задействованы в пересылке данных и распределении нагрузки. В случае сбоя какой-либо активного канала LAG будет усреднять нагрузку с оставшимися. Этот режим предпочтителен в том случае, если два напрямую подключенных коммутатора требуют большей пропускной способности канала, но не имеют доступа к протоколу LACP.

4.5.2 Добавление статических групп агрегации

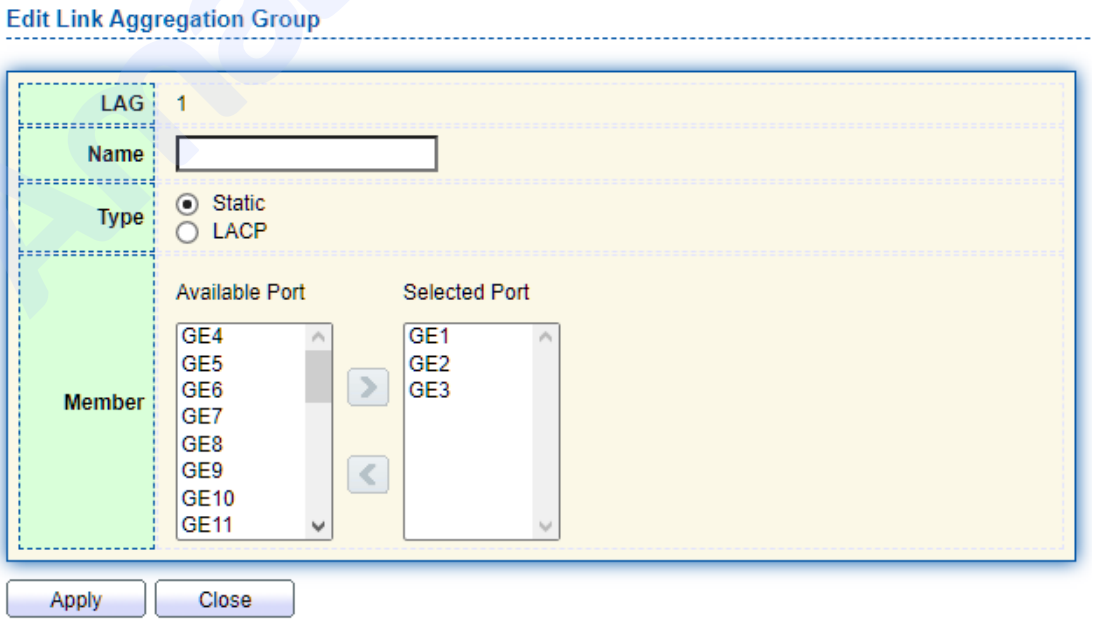
1. Перейдите «Port > Link Aggregation > Group» на панели навигации, чтобы настроить группы агрегации портов. Далее выберите алгоритм балансировки нагрузки с помощью переключателя и нажмите «Apply» для сохранения изменений.



2. Выберите одну из 8 доступных групп агрегации LAG и нажмите «Edit».



3. Выберите режим агрегации Static и укажите порты-участники группы агрегации. Нажмите «Apply» для сохранения изменений.



Настройки интерфейса

Параметр	Описание
LAG	Номер группы агрегации.
Name	Название группы агрегации
Type	Выбор режимов Static и LACP
Member	В каждой группе LAG доступно до 8 портов-участников.

Примечания:

Коммутатор поддерживает 8 групп агрегации, до 8 портов в каждой группе.

Группа агрегации портов должна гарантировать, что скорость портов-участников, дуплекс, состояние портов-участников согласованы или не могут изменяться после настройки.

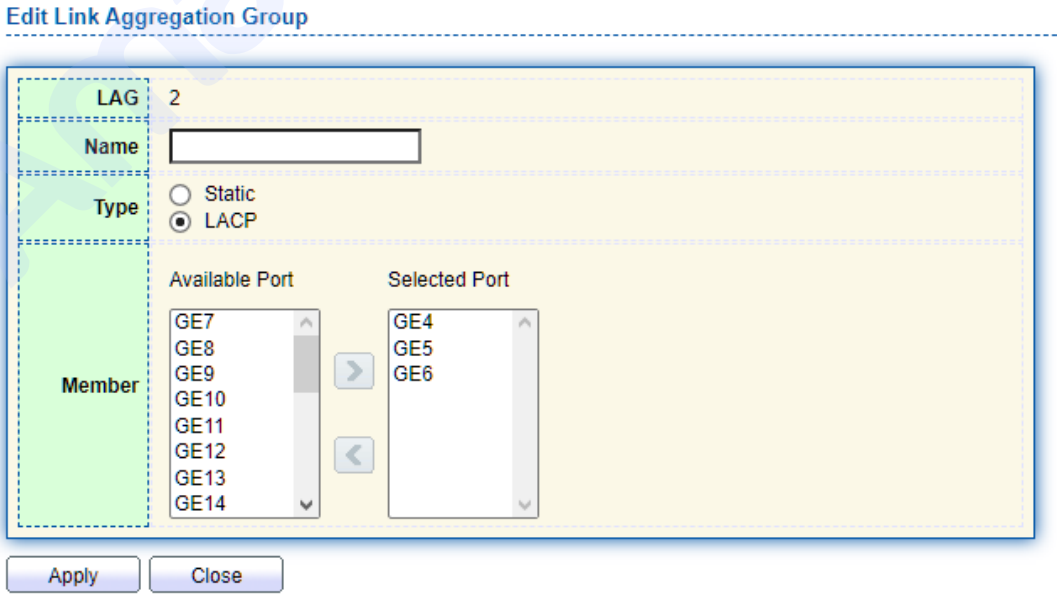
4.5.3 Добавление динамических групп агрегации (LACP)

LACP (протокол управления агрегацией каналов), основанный на стандарте IEEE 802.3ad, динамически агрегирует и дезагрегирует каналы. Он обменивается информацией с противоположными сетевыми устройствами через LACPDU (блок данных протокола управления агрегацией каналов).

Когда порт использует LACP, он информирует противоположное сетевое устройство о системном приоритете, MAC-адресе системы, приоритете и номере порта, а также рабочем ключе для передачи LACPDU. Противоположное сетевое устройство сравнивает полученную информацию с информацией, сохраненной другими портами, таким образом достигая соглашения об участии порта в динамической агрегации или выходе из нее. Динамическая агрегация LACP автоматически создается или удаляется системой коммутатора, то есть внутренние порты могут добавляться или удаляться сами по себе. Можно объединять только порты, подключенные к одному и тому же устройству с одинаковой скоростью, дуплексом и базовой конфигурацией.

Для настройки LACP групп агрегации выполните следующие действия:

1. Перейдите «Port > Link Aggregation > Group» на панели навигации, выберите одну из 8 доступных групп агрегации LAG и нажмите «Edit».
2. Выберите режим LACP и добавьте порты-участники в группу агрегации. Нажмите «Apply» для сохранения изменений.



3. Нажмите «Port > Link Aggregation > LACP» на панели навигации, чтобы настроить параметры LACP. Укажите значение параметра «System Priority» (Системный приоритет) и нажмите «Apply» для сохранения изменений.

Port 〉〉 Link Aggregation 〉〉 LACP

System Priority: 32768 (1 - 65535, default 32768)

Apply

LACP Port Setting Table

	Entry	Port	Port Priority	Timeout
☐	1	GE1	1	Long
☐	2	GE2	1	Long
☐	3	GE3	1	Long
☐	4	GE4	1	Long
☐	5	GE5	1	Long
☐	6	GE6	1	Long

4. Выберите необходимые порты и нажмите «Edit» для настройки параметров приоритет порта и метод тайм-аута. Нажмите «Apply» для сохранения изменений.

Edit LACP Port Setting

Port: GE4-GE6

Port Priority: 1 (1 - 65535, default 1)

Timeout: ◉ Long ○ Short

Apply Close

Настройки интерфейса

Параметр	Описание
Mode	Static режим Необходимо создать статическое агрегирование каналов и добавить порты-участники для повышения пропускной способности и надежности между двумя сетевыми устройствами в случае, если LACP недоступен для одного из них.
	LACP режим Соединения между двумя сетевыми устройствами могут выполнять агрегирование каналов в динамическом режиме LACP. Резервные каналы обеспечивают бесперебойную передачу данных путем замены частично вышедших из строя звеньев.
System Priority	Протокол LACP определяет активный и пассивный режимы между двумя устройствами в соответствии с системным приоритетом.

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

Port Priority	LACP определяет динамический режим участника группы LAG в зависимости от приоритета порта в вышестоящей системе.
Timeout Period	Этот параметр определяет частоту передачи сообщений LACP.

Примечания:

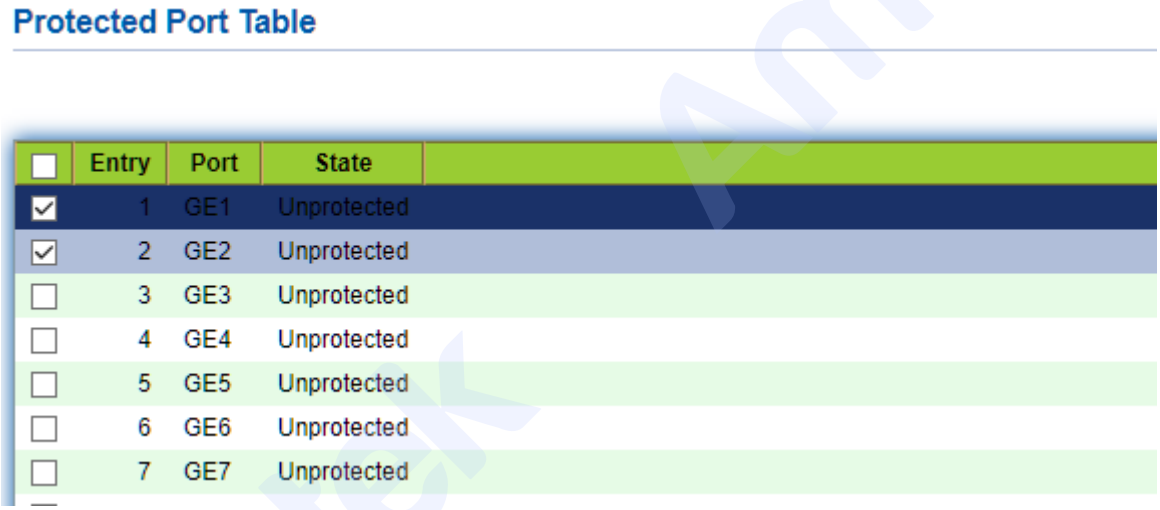
Коммутатор поддерживает максимум 8 групп агрегации, до 8 портов в каждой группе.
Группы агрегации могут использовать разные методы агрегирования.
Группа агрегации портов должна гарантировать, что скорость портов-участников, дуплекс, состояние портов-участников согласованы или не могут изменяться после настройки.

4.6 Port Isolation (Изоляция портов)

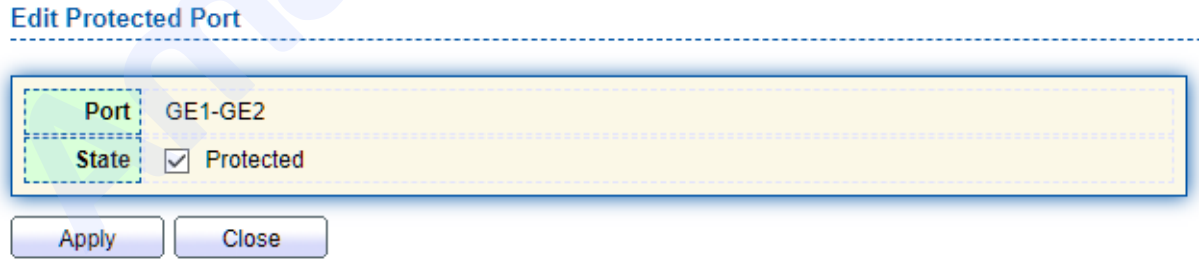
Функция Port isolation (изоляция портов) позволяет предотвратить передачу данных между несколькими устройствами, подключёнными к различным портам без настройки VLAN.

Для настройки изоляция портов выполните следующие действия:

1. Перейдите «Порт > Protected Port» на панели навигации, отметьте порты, которые нужно изолировать. Далее нажмите «Edit», чтобы включить функцию.



2. Установите галочку в поле «State» для включения изоляции выбранных портов. Нажмите «Apply» для сохранения изменений.



4.7 Port Statistics (Статистика трафика портов)

Данный раздел меню показывает подробную статистику трафика для всех портов. Статистика может обновляться или сбрасываться вручную пользователями.

Примечание:

Удаленную статистику восстановить невозможно. Пожалуйста, убедитесь в необходимости обнуления статистики.

Для просмотра статистики трафика портов выполните следующие действия:

1. Перейдите «Management > RMON > Statistics» на панели навигации

Statistics Table

Refresh Rate 0 sec

	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes
	1	GE1	0	0	0	0	0	0	0	0	0	0	0	0
	2	GE2	0	0	0	0	0	0	0	0	0	0	0	0
	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0
	4	GE4	0	0	0	0	0	0	0	0	0	0	0	0

2. В поле «Refresh Rate» установите период автоматического обновления статистики.
3. Нажмите «Refresh» для обновления статистики вручную.
4. При необходимости обнуления статистики нажмите «Clear».
5. Для просмотра подробной статистики трафика порта выберите необходимый порт и нажмите «View».

5. POE Setting (Настройки PoE)

PoE (Power over Ethernet) — технология, позволяющая передавать удалённому устройству электрическую энергию вместе с данными, через стандартную витую пару в сети Ethernet. При этом используется только один кабель Ethernet, который, наряду с функцией передачи данных, используется для питания удаленного устройства. Это обеспечивает большую гибкость в размещении сетевых устройств и во многих случаях существенно снижает затраты на установку.

5.1 PoE Port Setting (Настройка PoE портов)

Для настройки портов PoE выполните следующие действия:

1. Перейдите «POE Setting > PoE Port Setting » на панели навигации.

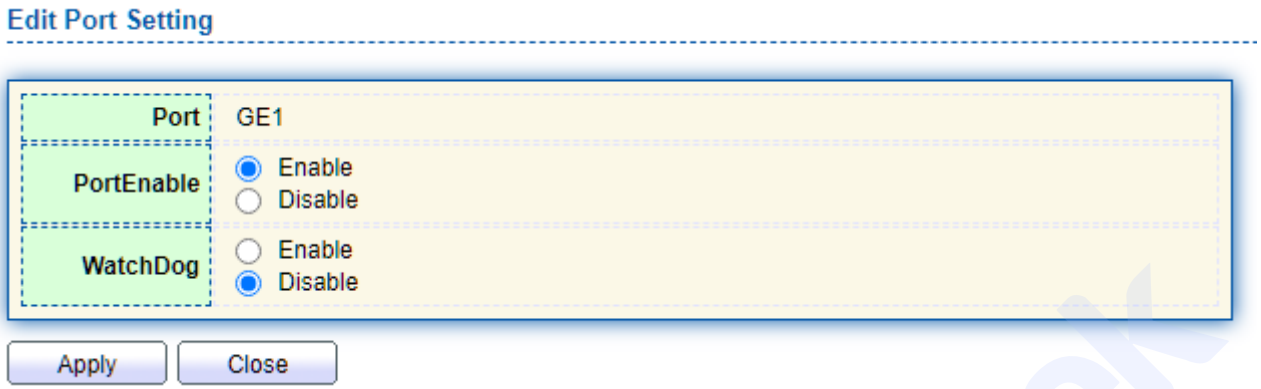
System info

System Power(mW)	0
System Temperature(C)	31
Refresh Rate	○ None ○ 5 sec ◉ 10 sec ○ 30 sec

Port Setting Table

	Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)	WatchDog
	1	GE1	Enabled	Off	AF(N)	0	N/A	N/A	N/A	Disabled
	2	GE2	Enabled	Off	AF(N)	0	N/A	N/A	N/A	Disabled
	3	GE3	Enabled	Off	AF(N)	0	N/A	N/A	N/A	Disabled
	4	GE4	Enabled	Off	AF(N)	0	N/A	N/A	N/A	Disabled
	5	GE5	Enabled	Off	AF(N)	0	N/A	N/A	N/A	Disabled
	6	GE6	Enabled	Off	AF(N)	0	N/A	N/A	N/A	Disabled
	7	GE7	Enabled	Off	AF(N)	0	N/A	N/A	N/A	Disabled

2. Выберите необходимый порт и нажмите «Edit» для настройки параметров. Нажмите «Apply» для сохранения изменений.

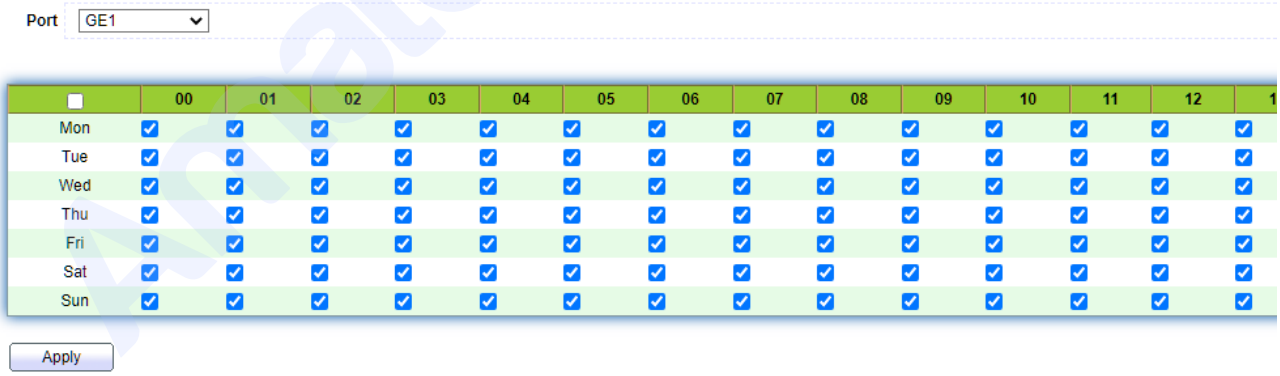


Настройки интерфейса

Параметр	Описание
Port Enable	Включить/отключить PoE питание на выбранном порту.
WatchDog	Включить/отключить функцию WatchDog. Функция PoE Watchdog позволяет дистанционно контролировать сетевую активность подключенных PoE устройств. Если подключенное PoE устройство в течение 2 минут перестает отвечать на запросы, коммутатор на короткое время прерывает подачу питания на PoE порт для удаленной перезагрузки сетевого устройства.

5.2 PoE Port Timer Setting (Настройка расписания работы PoE)

Для настройки расписания работы PoE портов перейдите «POE Setting > POE Port Timer Setting». Выберите необходимый порт и укажите время работы по дням недели. Нажмите «Apply» для сохранения изменений.

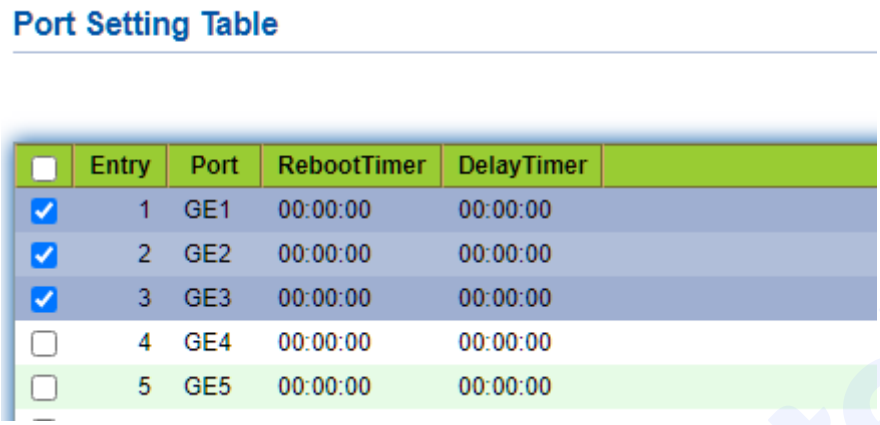


5.3 PoE Port Timer Reboot Setting (Расписание перезагрузки PoE)

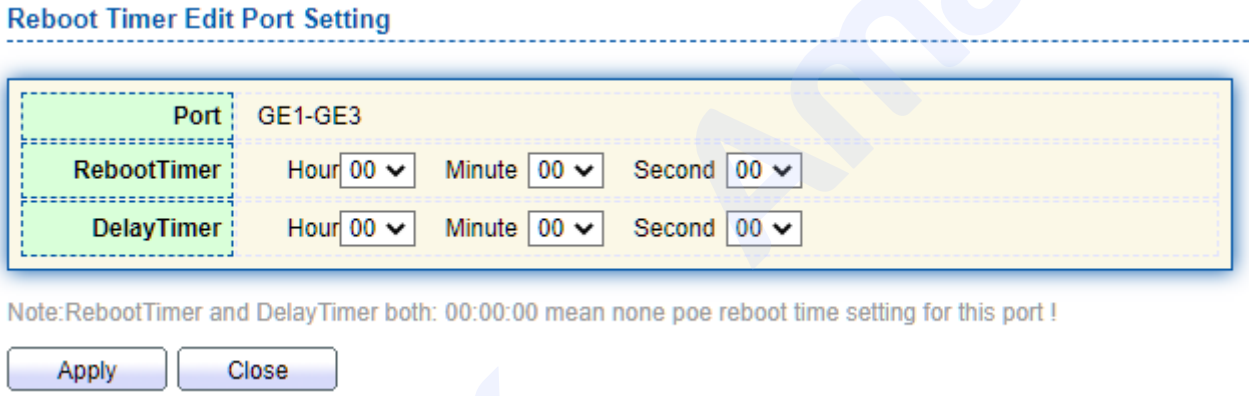
Вы можете настроить расписание перезагрузки питания PoE по каждому порту для удаленной перезагрузки сетевых PoE устройств.

Для настройки расписания перезагрузки PoE портов выполните следующие действия:

1. Перейдите «POE Setting > PoE Port Timer Reboot Setting». Выберите необходимые порты и нажмите «Edit»



2. Укажите время перезагрузки и длительность отключения питания PoE. Нажмите «Apply» для сохранения изменений.



Примечание:

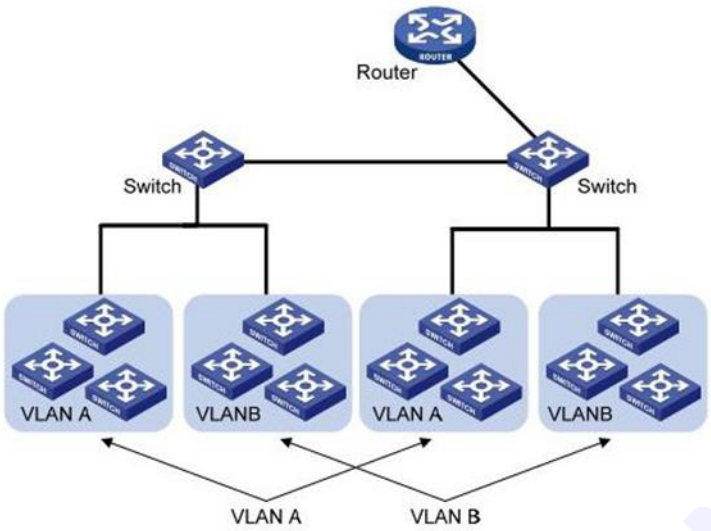
Значение Reboot Timer и Delay Timer 00:00:00 означает, что для этого порта не задано время перезагрузки PoE.

6. VLAN MANAGEMENT (Управление VLAN)

6.1 VLAN Configuration (Настройка VLAN)

VLAN (Virtual Local Area Network) - виртуальная локальная компьютерная сеть. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным устройствам группироваться вместе, даже если они не находятся в одной физической сети.

Как показано ниже, каждая VLAN в качестве широковещательного домена делит физическую локальную сеть на логические локальные сети. Конечные устройства внутри VLAN, могут обмениваться сообщениями посредством традиционной передачи данных.

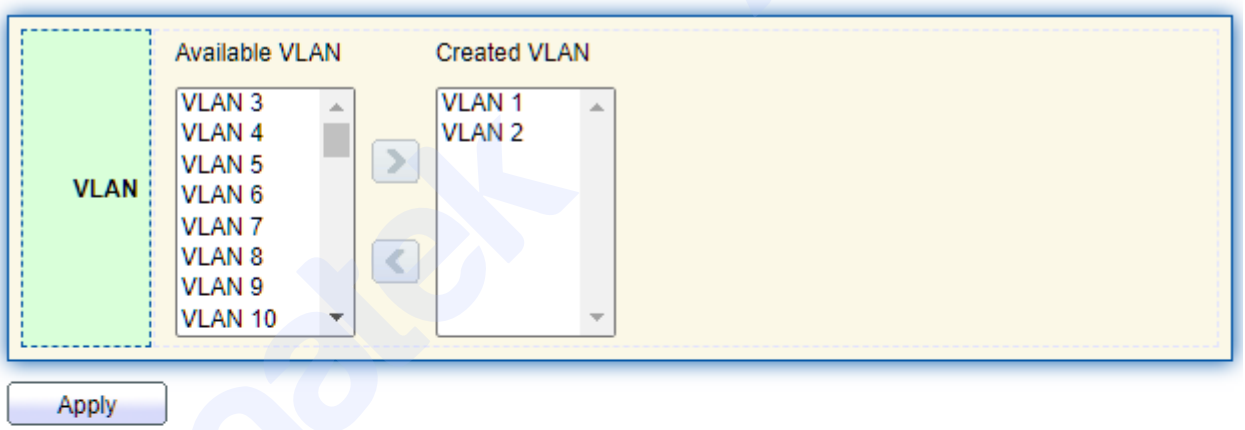


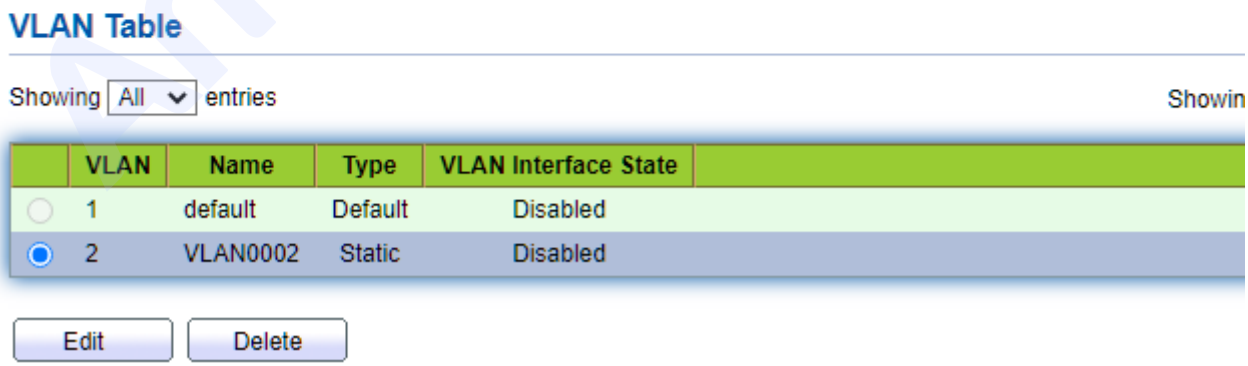
Данный управляемый коммутатор совместим с типами VLAN на основе 802.1Q, протоколов, MAC-адресов и портов. Для конфигурации по умолчанию следует использовать режим 802.1Q VLAN.

6.1.1 Создание VLAN

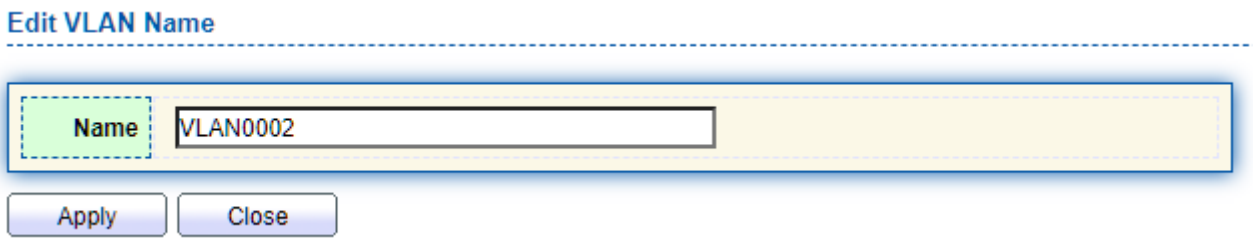
Для добавления новой VLAN, выполните следующие действия:

1. Перейдите «VLAN > VLAN > Create VLAN». Выберите новый номер VLAN в поле «Available VLAN» и переместите его в поле «Created VLAN». Нажмите «Apply» для сохранения изменений.





2. Созданная VLAN будет отображаться в таблице VLAN. При необходимости изменить название VLAN, выберите нужную VLAN и нажмите «Edit». Измените название виртуальной сети и нажмите «Apply» для сохранения изменений.



Настройки интерфейса

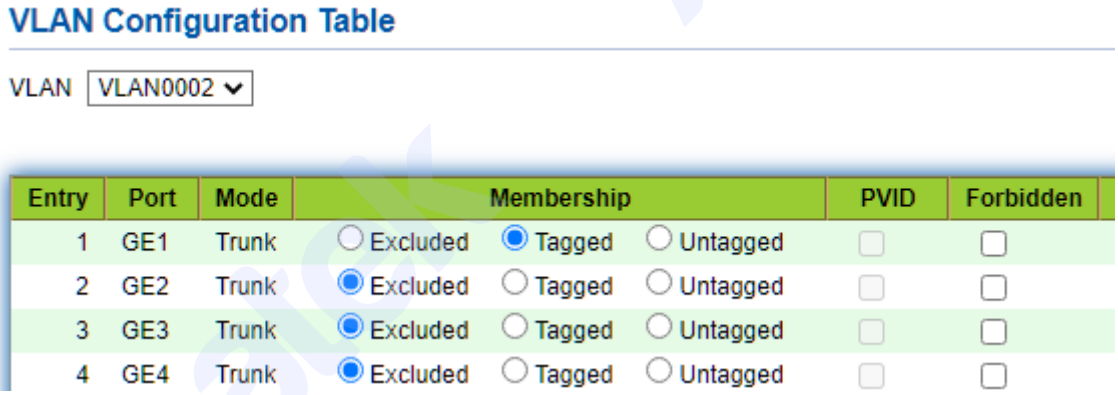
Параметр	Описание
VLAN ID	Необходимо выбрать идентификатор VLAN в диапазоне от 1 до 4094. По умолчанию используется VLAN 1. В настройках «По умолчанию» все порты принадлежат VLAN1.
Name	Имя VLAN, «default» - VLAN по умолчанию;

6.1.2 Добавление портов в выбранную VLAN

Существует два метода добавления портов. Один из них - добавить несколько портов в одну VLAN, другой — добавить порт в несколько VLAN.

Первый метод:

Перейдите «VLAN > VLAN > VLAN Configuration» на панели навигации. В поле «VLAN» выберите нужную виртуальную сеть. Отметьте номера портов-участников Tagged (тегированных) или Untagged (нетегированных). Нажмите кнопку «Apply», чтобы сохранить изменения.



Настройки интерфейса

Параметр	Описание
VLAN	Идентификатор настраиваемой VLAN
Member	Назначение порта-участника VLAN: Excluded - порт исключен из данной VLAN. Tagged - порт является тегированным членом этой VLAN. Untagged - порт является нетегированным членом этой VLAN.
PVID	Идентификатор Port VLAN ID
Forbidden	Запрещено пересылать сообщения VLAN в данный порт

Второй метод:

Перейдите «VLAN > VLAN > Membership». Выберите порт для настройки и нажмите «Edit», чтобы настроить его атрибуты. Нажмите кнопку «Apply», чтобы сохранить изменения.

Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
◉	1	GE1	Trunk	1UP	1UP
○	2	GE2	Trunk	1UP	1UP
○	3	GE3	Trunk	1UP	1UP
○	4	GE4	Trunk	1UP	1UP
○	5	GE5	Trunk	1UP	1UP

Edit Port Setting

Port: GE2

Mode: Trunk

Membership: 10 | 1UP, 2T, 3T, 4T, 5T, 6T, 7T, 8T

○ Forbidden
○ Excluded
◉ Tagged
○ Untagged

☐ PVID

Apply Close

Настройки интерфейса

Параметр	Описание
Port	Настраиваемый порт
Mode	Текущий режим VLAN в конфигурации порта: **Hybrid** - порт в этом режиме может принадлежать к нескольким VLAN, может передавать multiple VLAN пакеты, может передавать пакеты данных Tagged и Untagged. **Access** - порт помечен, как Untagged (нетегированный), в этом режиме порт может принадлежать только одной VLAN. **Trunk** - порт помечен, как Taggged (тегированный), в этом режиме порт может принадлежать нескольким VLAN, может передавать multiple VLAN пакеты, может передавать только пакеты данных типа Tagged.
Member	Назначение порта-участника VLAN: Forbidden - запрещен трафик этой VLAN в данный порт. Excluded - порт исключен из данной VLAN. Tagged - порт является тегированным членом этой VLAN. Untagged - порт является нетегированным членом этой VLAN. PVID - идентификатор Port VLAN ID

6.1.3 Port Setting (Настройка портов VLAN)

Перейдите «VLAN > VLAN > Port Setting» что бы просмотреть текущую информацию и изменить настройки режима портов VLAN.

Port Setting Table

	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
☐	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
☐	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
☐	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
☐	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100

Примечания:

1. **Access**: порт будет помечен, как Untagged (нетегированный), в этом режиме порт может принадлежать только одной VLAN, по умолчанию используется VLAN 1, обычно используется с устройством, подключенным напрямую к коммутатору.
2. **Trunk**: порт будет помечен, как Tagged (тегированный), в этом режиме порт может принадлежать нескольким VLAN, может передавать multiple VLAN пакеты, может передавать только пакеты данных типа Tag, обычно используется вместе с другими коммутаторами в сети.
3. **Hybrid**: порт этого режима может принадлежать к нескольким VLAN, может передавать multiple VLAN пакеты, может передавать пакеты данных Tag и Untag.
4. Когда порт переведен в режим Trunk, он будет удален из предыдущего Untag VLAN.

Для изменения режима порта выберите один или несколько портов и нажмите «Edit», чтобы настроить параметры. Далее нажмите кнопку «Apply», чтобы сохранить изменения.

Edit Port Setting

Port	GE1-GE3
Mode	◉ Hybrid ○ Access ○ Trunk ○ Tunnel
PVID	1 (1 - 4094)
Accept Frame Type	◉ All ○ Tag Only ○ Untag Only
Ingress Filtering	☐ Enable
Uplink	☐ Enable
TPID	

Apply Close

Настройки интерфейса

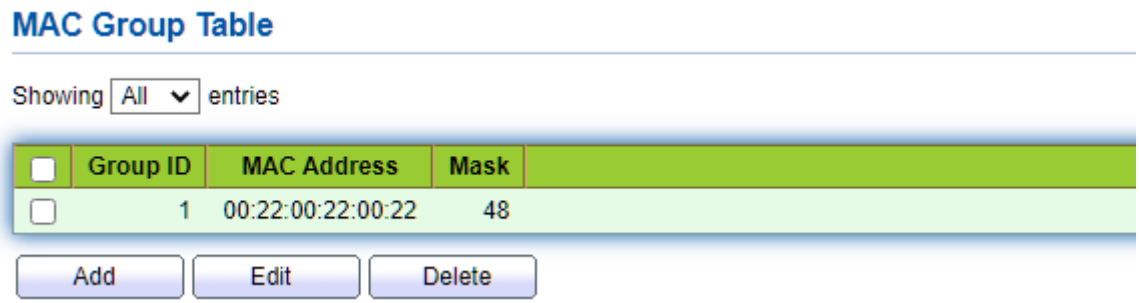
Параметр	Описание
Port	Настраиваемый порты
Mode	Текущий режим VLAN в конфигурации порта: **Access:** порт будет помечен, как Untagged (нетегированный), в этом режиме порт может принадлежать только одной VLAN, обычно используется с конечным устройством, подключенным напрямую к коммутатору. **Trunk:** порт будет помечен, как Tagged (тегированный), в этом режиме порт может принадлежать нескольким VLAN, может передавать multiple VLAN пакеты, может передавать только пакеты данных типа Tag, обычно используется вместе с другими коммутаторами в сети. Когда порт переведен в режим Trunk, он будет удален из предыдущего Untag VLAN. **Hybrid:** порт этого режима может принадлежать к нескольким VLAN, может передавать multiple VLAN пакеты, может передавать пакеты данных Tag и Untag.
PVID	PVID (Port VLAN Identifier) – идентификатор Port VLAN ID, к которой относится оборудование, подключенное к порту.
Accept Frame Type	Типы пакетов данных, принимаемых портами: All - все пакеты Tag Only - будут получены только пакеты данных типа Tag. Untag Only: будут получены только пакеты данных типа Untag.
Ingress Filtering	Фильтрация пакетов VLAN, исключенных на данном порту.
Uplink	Независимо от того, в режиме Uplink или нет
TPID	Идентификационный номер тега VLAN

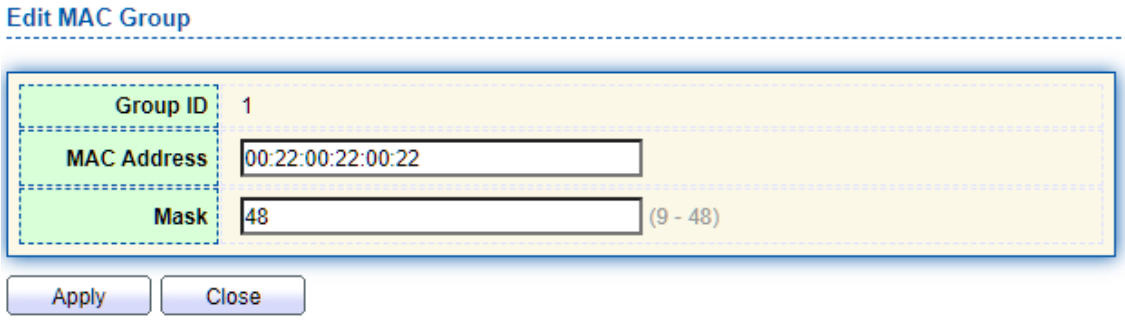
6.2 MAC VLAN (VLAN на основе MAC адресов)

MAC VLAN (VLAN, основанный на MAC-адресах) — это технология, позволяющая распределять трафик по VLAN на основе MAC-адреса: каждый пользователь с уникальным MAC-адресом может быть назначен определенному VLAN, в зависимости от обозначенных требований. Это дает возможность отказаться от повторной настройки VLAN при изменении местоположения пользователя: в независимости от местоположения в сети, трафик пользователя будет определен в свой VLAN.

Для добавления новой группы MAC адресов, выполните следующие действия:

1. Перейдите «VLAN > MAC VLAN > MAC Group» на панели навигации. Нажмите «Add» для создания группы MAC адресов.

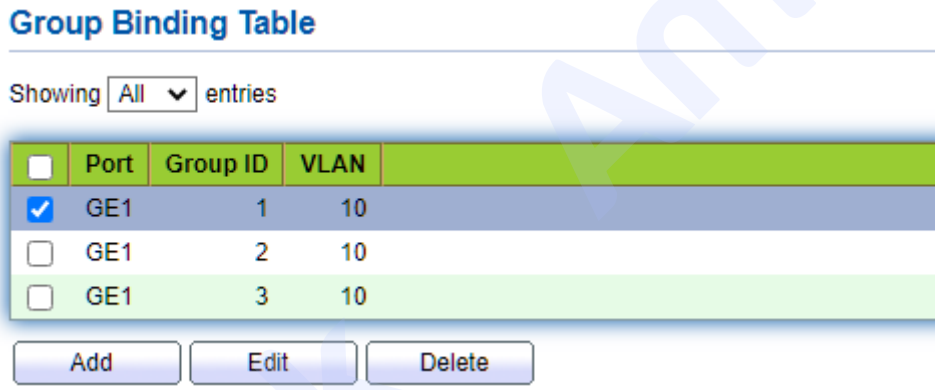




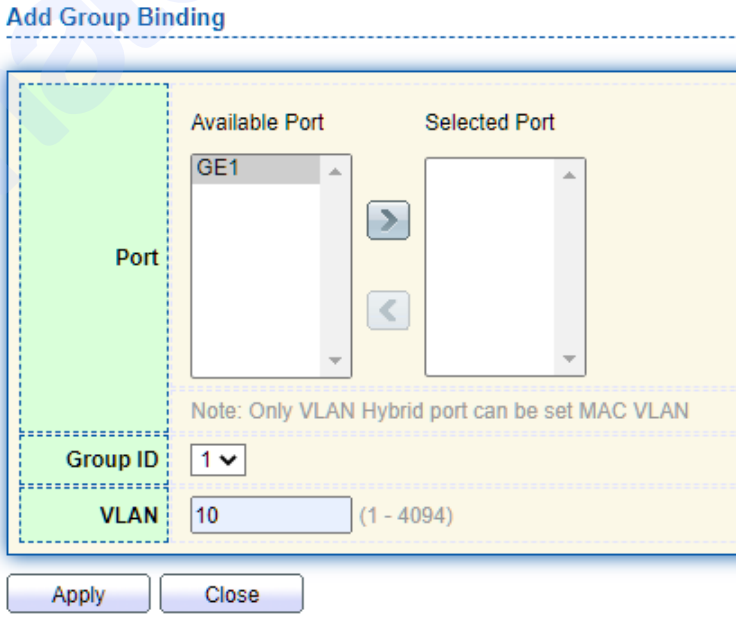
Настройки интерфейса

Параметр	Описание
Group ID	Идентификатор MAC VLAN Group
MAC Address	MAC-адрес для привязки к VLAN
Mask	Маска MAC-адреса

2. Перейдите «VLAN > MAC VLAN > Group Binding» на панели навигации. Нажмите «Add» для привязки группы MAC адресов к порту VLAN.



3. Выберите необходимый порт, группу MAC адресов и VLAN, к которой необходимо привязать данную группу. Далее нажмите кнопку «Apply», чтобы сохранить изменения.

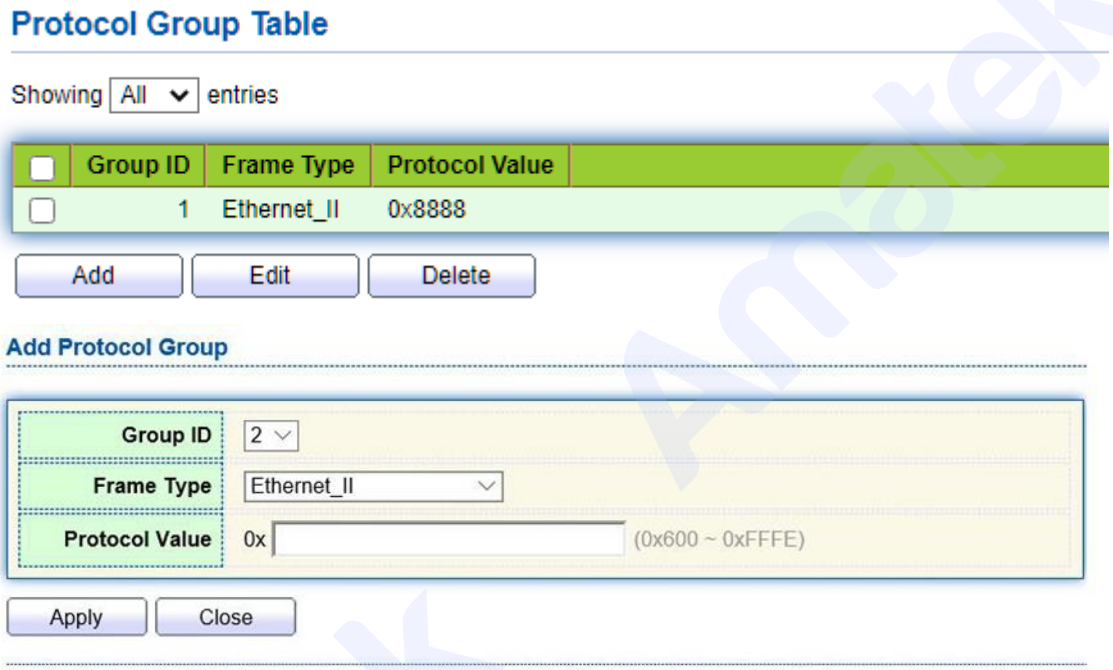


6.3 Protocol VLAN (VLAN на основе протокола)

VLAN на основе протокола распределяет различные идентификаторы VLAN в соответствии с типом протокола (семейства) и форматом инкапсуляции сообщений, полученных интерфейсами.

Администраторы должны подготовить схему сопоставления между доменом протокола Ethernet кадра и идентификатором VLAN ID, который будет добавлен при получении кадров без тегов.

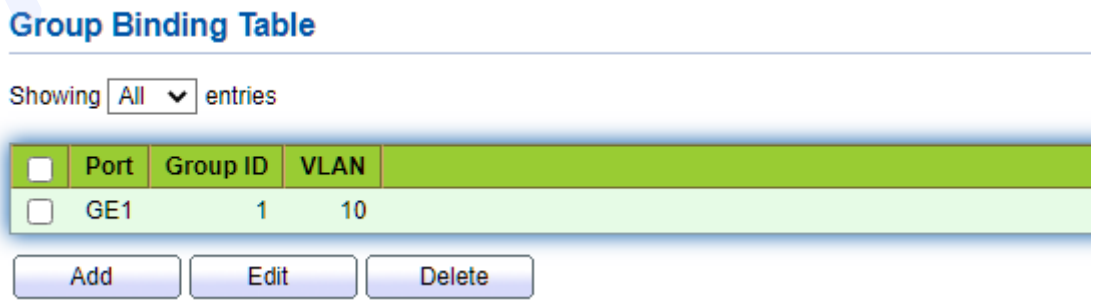
1. Перейдите «VLAN > Protocol VLAN > Protocol Group» на панели навигации. Нажмите «Add» для создания группы протоколов. Выберите тип кадров и введите значение Protocol Value. Далее нажмите кнопку «Apply», чтобы сохранить изменения.

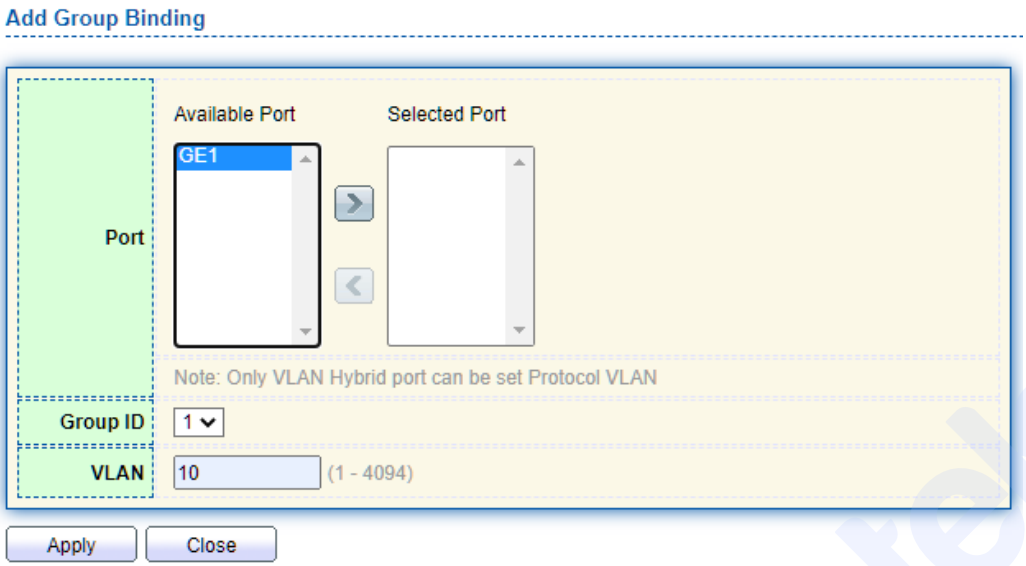


Настройки интерфейса

Параметр	Описание
Group ID	Идентификатор Protocol VLAN Group
Frame Type	Тип кадров: Ethernet_II, IEEE802.3 LLC, RFC 1042
Protocol Value	Диапазон значений от 0x600 до 0xFFFE

2. Перейдите «VLAN > Protocol VLAN > Group Binding» на панели навигации. Нажмите «Add», чтобы связать Group ID, номер порта и идентификатор VLAN. Далее нажмите кнопку «Apply», чтобы сохранить изменения.



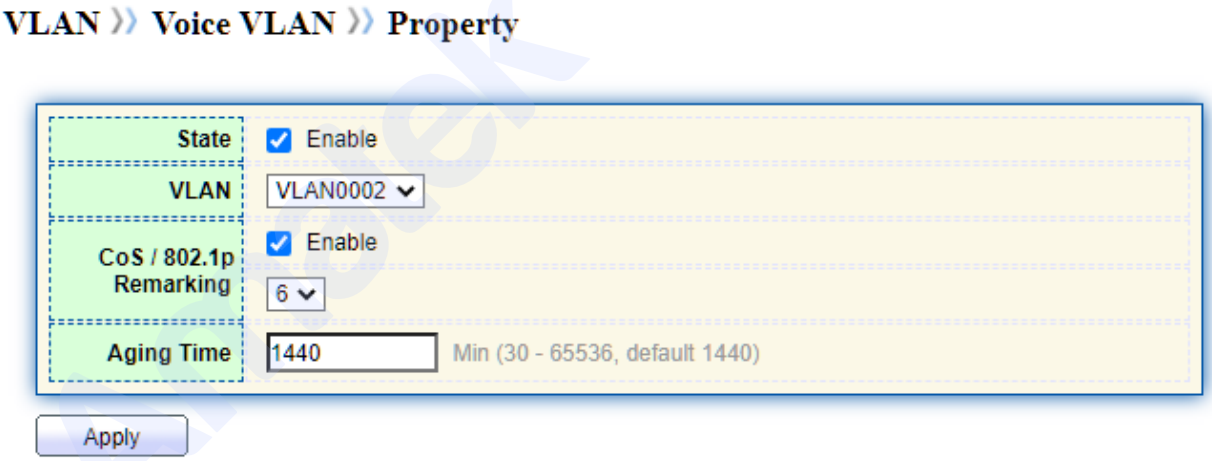


6.4 VOICE VLAN (VLAN IP телефонии)

Voice VLAN (голосовая виртуальная локальная сеть) используется для изоляции голосового трафика. Использование Voice VLAN позволяет обеспечить безопасность голосового трафика и повысить приоритет пакетов голосового трафика в сети для улучшения качества IP телефонии.

6.4.1 Настройка Voice VLAN

Для добавления Voice VLAN, перейдите «VLAN > Voice VLAN > Property» и выполните следующие действия:



Шаг 1: поставьте «галочку» в поле «State»: Enable (Включено);
Шаг 2: выберите идентификатор VLAN ID (уже существующей VLAN);
Шаг 3: задайте уровень приоритета трафика CoS /802.1p;
Шаг 4: задайте Aging Time (срок действия) в минутах;
Шаг 5: нажмите кнопку «Apply», чтобы сохранить изменения.

Примечание:
Идентификатор Voice VLAN ID и идентификатор Surveillance VLAN ID не могут совпадать.

6.4.2 Конфигурирование портов Voice VLAN

Настройте порты Voice VLAN. Вы должны выбрать режим порта 2 уровня: Trunk (магистральный) или Hybrid (гибридный). Режим Access можно настроить только в Manual (ручном) режиме. Присоединение порта к Voice VLAN может быть в режиме Auto (с тегом) или Manual (вручную).

Port Setting Table

	Entry	Port	State	Mode	QoS Policy
☑	1	GE1	Disabled	Auto	Voice Packet
☐	2	GE2	Disabled	Auto	Voice Packet
☐	3	GE3	Disabled	Auto	Voice Packet
☐	4	GE4	Disabled	Auto	Voice Packet
☐	5	GE5	Disabled	Auto	Voice Packet

Edit Port Setting

Port	GE1
State	☑ Enable
Mode	◉ Auto ○ Manual
QoS Policy	◉ Voice Packet ○ All

Apply Close

Для изменения режима порта Voice VLAN, выполните следующие действия:

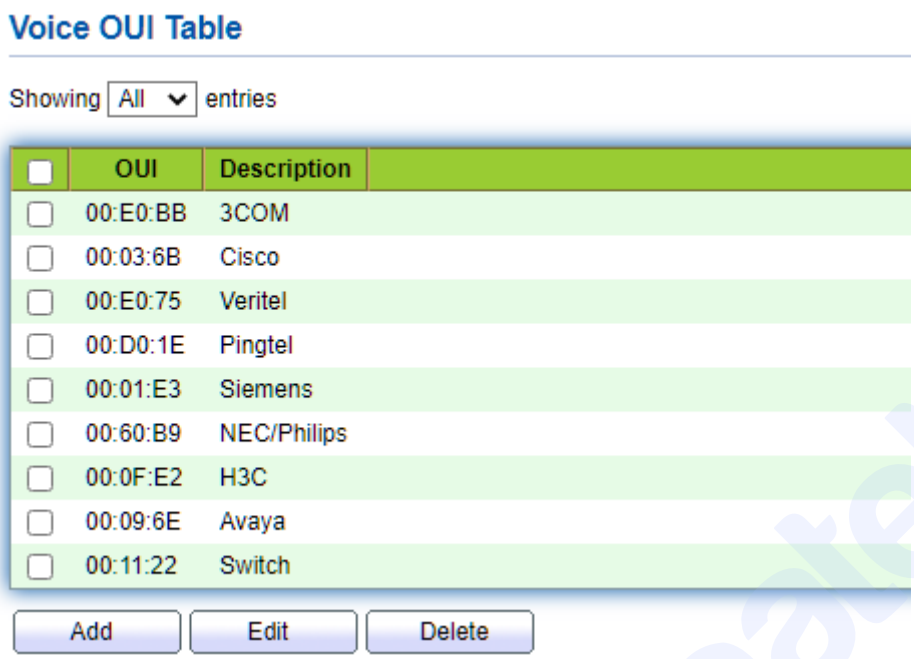
Шаг 1: выберите один или несколько портов и нажмите «Edit»;
Шаг 2: в поле «State» задайте статус порта: Enabled (Включено);
Шаг 3: в окне «Mode» задайте режим порта: Auto (авто) или Manual (вручную);
Шаг 4: в окне «QoS Policy» задайте приоритет трафика: Голосовые пакеты или All (все);
Шаг 4: нажмите кнопку «Apply», чтобы сохранить изменения.

6.4.3 Voice OUI (Настройка Voice OUI)

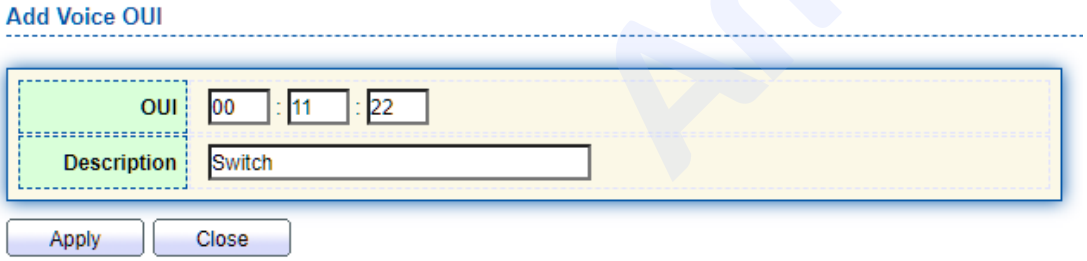
Классификация фреймов данных, относящихся к фреймам VoIP-оборудования, базируется на OUI (Organizationally Unique Identifier - Организационный уникальный идентификатор) – первые 24 бита MAC-адреса отправителя.

Для настройки Voice OUI, перейдите «VLAN > Voice VLAN > Voice OUI». Вы увидите таблицу записей Voice OUI для оборудования основных производителей IP телефонии.

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



При необходимости создания новой записи, выполните следующие действия:



Шаг 1: в поле «OUI» укажите адрес OUI;
Шаг 2: в поле «Description» введите описание OUI;
Шаг 3: нажмите «Apply», чтобы сохранить изменения.

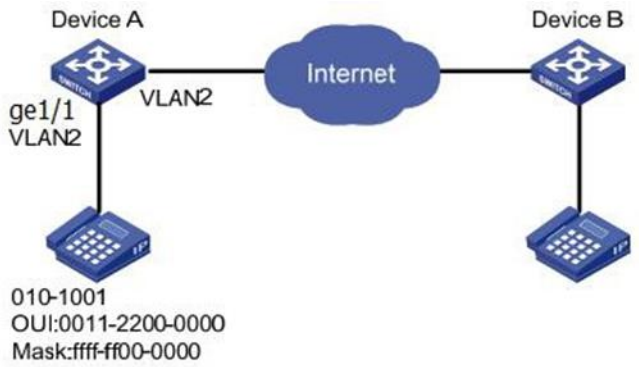
Примечания:

1. Максимальное количество OUI записей 16;
2. Адрес OUI действителен только для Unicast адресов (одноадресная рассылка);
3. Для редактирования записи Voice OUI нажмите «Edit»;
4. Для удаления записи Voice OUI нажмите «Delete»

6.4.4 Пример настройки Voice VLAN

Например, необходимо настроить Voice VLAN, чтобы порты, имеющие доступ к IP-телефонии, могли входить/выходить в Voice VLAN и передавать внутри нее голосовой поток. Настройте VLAN2 для безопасной работы с голосовой виртуальной сетью Voice VLAN, которая позволяет передавать только голосовые данные. Оборудование IP-телефонии передает голосовой поток без тегов на порт GE1, входной магистральный порт. Так же необходимо настроить записи OUI (0011-22) и настроить сетевую схему Voice VLAN в автоматическом режиме, как показано ниже.

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



1. Создайте виртуальную сеть VLAN2.

VLAN Table

Showing All entries

	VLAN	Name	Type	VLAN Interface State
○	1	default	Default	Disabled
○	2	VLAN0002	Static	Disabled

Edit Delete

2. Настройте порт GE1 коммутатора A в режиме Trunk.

Port Setting Table

	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100

3. Перейдите «VLAN > Voice VLAN > Voice OUI» на панели навигации, чтобы добавить диапазон MAC-адресов OUI. Введите первые 24 бита MAC-адреса голосового устройства: 00:11:22. Нажмите «Apply», чтобы сохранить изменения.

Add Voice OUI

OUI 00 : 11 : 22

Description IP phone

Apply Close

4. Включите Voice VLAN и добавьте порт GE1 в режиме Auto. Нажмите «Apply», чтобы сохранить изменения.

VLAN » Voice VLAN » Property

State ☑ Enable

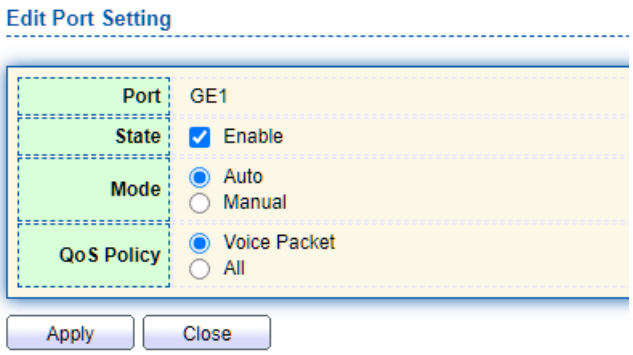
VLAN VLAN0002

CoS / 802.1p Remarking ☐ Enable 6

Aging Time 1440 Min (30 - 65536, default 1440)

Apply

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



Port Setting Table

	Entry	Port	State	Mode	QoS Policy
	1	GE1	Enabled	Auto	Voice Packet
	2	GE2	Disabled	Auto	Voice Packet

6.5 SURVEILLANCE VLAN (VLAN системы видеонаблюдения)

Surveillance VLAN используется для изоляции трафика видео потока системы видеонаблюдения. Использование Surveillance VLAN позволяет обеспечить безопасность данных видеонаблюдения и повысить приоритет трафика видео потока без ущерба для передачи обычных данных сети.

Настройка Surveillance VLAN осуществляется аналогично Voice VLAN (смотри пункт 6.4 VOICE VLAN).

7. MAC Management (Управление MAC-адресами)

MAC Address Table (Таблица MAC-адресов) — это таблица, отображающая MAC-адреса и порты пересылки, которые являются основой для быстрой передачи трафика L2. Таблица MAC-адресов может быть создана динамически или статически. Статическая конфигурация заключается в ручной настройке соответствия между MAC-адресами и портами. Динамическое обучение - это процесс, в котором коммутатор изучает соответствие между MAC-адресами и портами и регулярно обновляет таблицу MAC.

Существует два типа пересылки сообщений в соответствии с информацией из таблицы MAC-адресов:

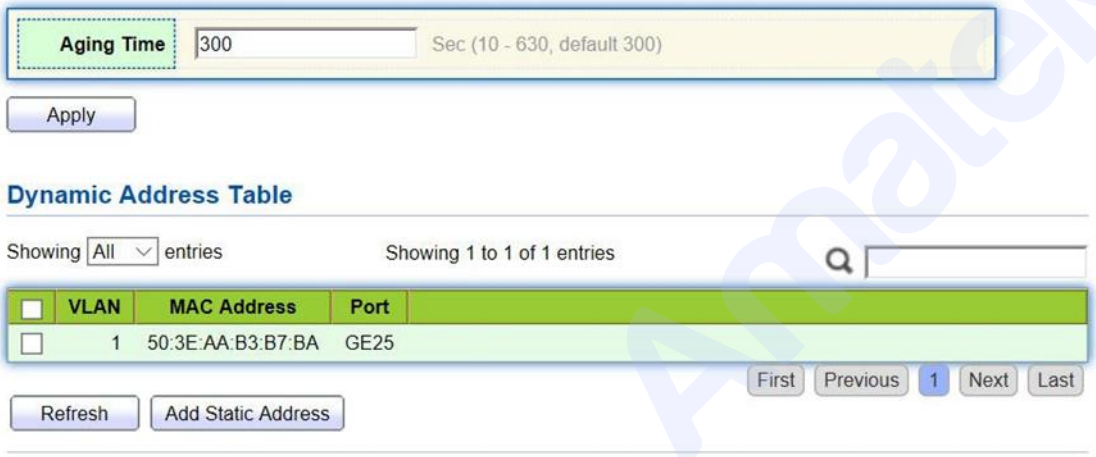
- Unicast mode (Одноадресный режим): коммутатор напрямую передает сообщения с выхода таблицы, когда таблица переадресации MAC-адресов содержит соответствующие записи с MAC-адресом назначения.
- Broadcast mode (Широковещательный режим): когда коммутатор получает сообщения с адресом назначения, полным F-битов, или если в таблице переадресации нет записи, соответствующей MAC-адресу назначения, коммутатор будет пересылать сообщения на все порты, кроме принимающего порта.

7.1 Dynamic Address (Динамическое обновление MAC адресов)

На этой странице меню можно проверить информацию и настроить Aging time (время устаревания) таблицы динамических MAC-адресов. Динамический MAC адрес будет «привязываться» к порту автоматически (после получения и обработки фрейма), и через некоторое Aging time будет удаляться.

Таблица динамических MAC-адресов нуждается в постоянных обновлениях, чтобы соответствовать изменениям локальной сети. Система автоматически генерирует записи, которые ограничены сроком их жизни (т. е. временем устаревания).

Для настройки времени устаревания перейдите «MAC Address Table > Dynamic Address». В поле «Aging time» укажите необходимое время в диапазоне от 10 до 630 секунд. Нажмите «Apply», чтобы сохранить изменения.



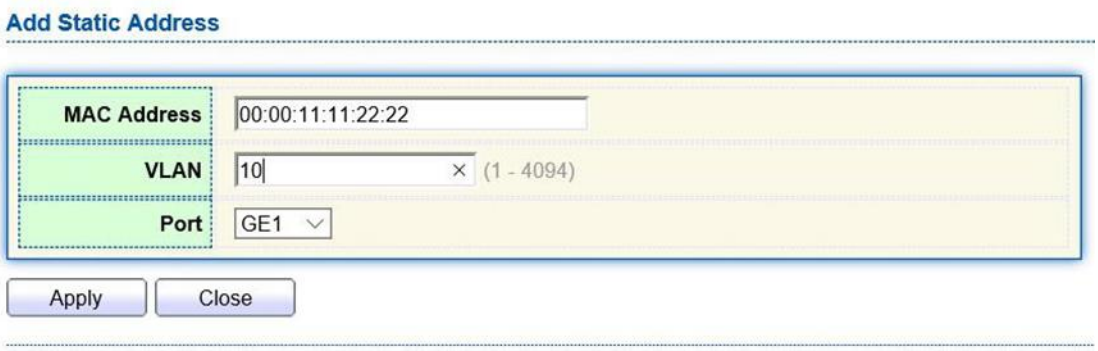
Примечания:

1. Рекомендуемое Aging time (время устаревания) по умолчанию составляет 300 секунд.
2. Нажмите «Refresh» для ручного обновления таблицы MAC-адресов.
3. Нажмите «Add Static Address» для добавления MAC-адреса в статические адреса.

7.2 Static Address (Статические MAC-адреса)

Статические MAC-адреса настраиваются пользователем вручную, имеют наивысший приоритет, хранятся постоянно и не могут быть перезаписаны динамическими MAC-адресами.

Для настройки статических MAC-адресов перейдите «MAC Address Table > Static Address». Для добавления статического MAC-адреса нажмите «Add». Укажите параметры MAC-адреса. Далее нажмите «Apply», чтобы сохранить изменения. При необходимости удаления MAC-адреса из таблицы нажмите «Delete».



Настройки интерфейса

Параметр	Описание
MAC Address	Введите новый MAC-адрес
VLAN	Укажите VLAN ID
Port	Выберите номер порта. Это должен быть порт-участник VLAN.

8. Spanning Tree (Настройка протоколов STP/RSTP/MSTP)

В топологии сети Ethernet часто используются дополнительные соединения для резервирования каналов и обеспечения надежности сети. Однако такие соединения будут создавать петли в коммутационной сети, что может привести к широковещательному шторму, нестабильному списку MAC-адресов и другим сетевым сбоям. Для борьбы с этими явлениями используются протоколы STP (IEEE 802.1D), RSTP (IEEE 802.1W) и MSTP (IEEE 802.1S). Протокол MSTP совместим с RSTP и STP, тогда как RSTP совместим с STP.

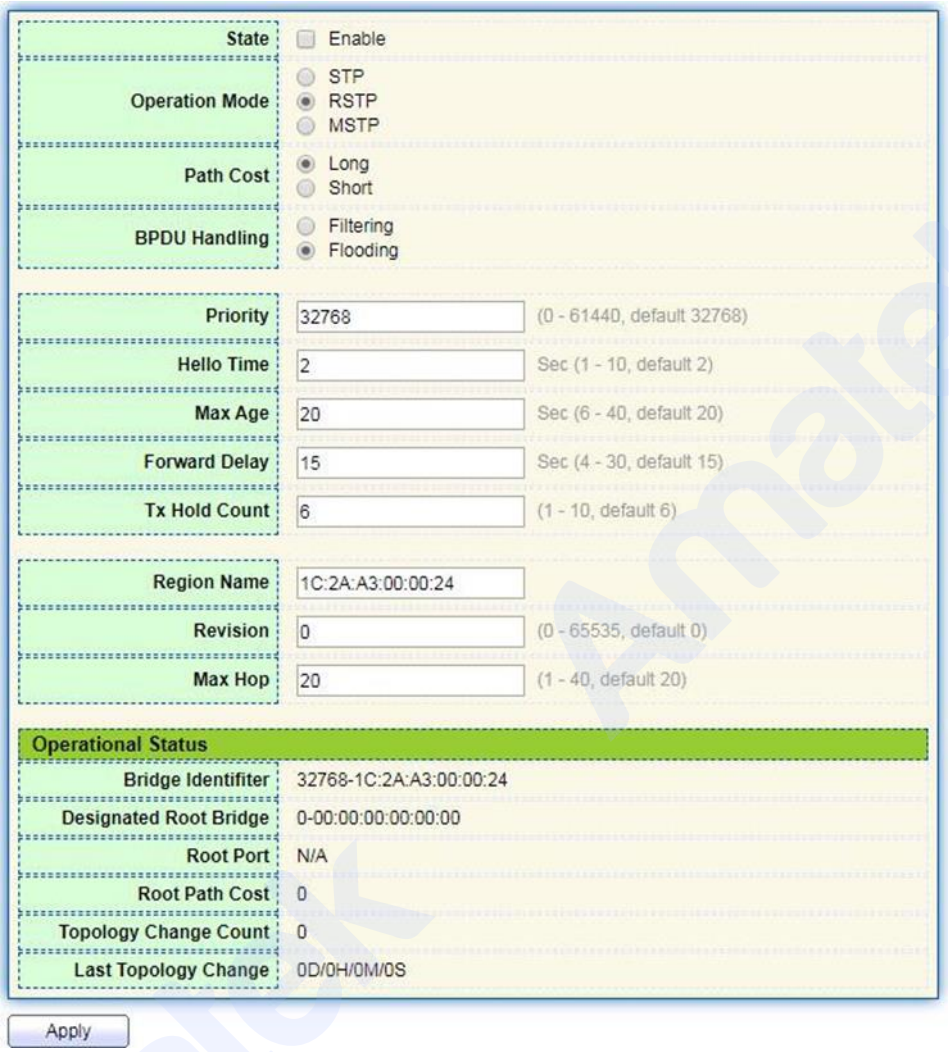
Разница между протоколами показана в таблице.

Протокол	Описание	Применение
STP (Spanning Tree Protocol)	Основной задачей STP является устранение петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями. STP решает эту задачу, автоматически блокируя избыточные соединения.	Все VLAN могут совместно использоваться без различия в пользовательском или бизнес трафике данных.
RSTP (Rapid spanning tree protocol)	Версия протокола STP с ускоренной реконфигурацией дерева, использующегося для исключения петель (исключения дублирующих маршрутов) в соединениях коммутаторов Ethernet с дублирующими линиями.	
MSTP (Multiple Spanning Tree Protocol)	Является расширением протокола RSTP, который позволяет настраивать отдельное связующее дерево для любого VLAN или группы VLAN, создавая множество маршрутов передачи трафика и позволяя осуществлять балансировку нагрузки.	Различает пользовательский и бизнес трафик для распределения нагрузки. Различные VLAN перенаправляют поток через отдельные связующие деревья.

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

8.1 Global Configuration (Глобальные настройки)

Для настройки глобальных параметров STP/RSTP/MSTP перейдите «Spanning Tree > Property» на панели навигации. Укажите параметры протокола. Далее нажмите «Apply», чтобы сохранить изменения.



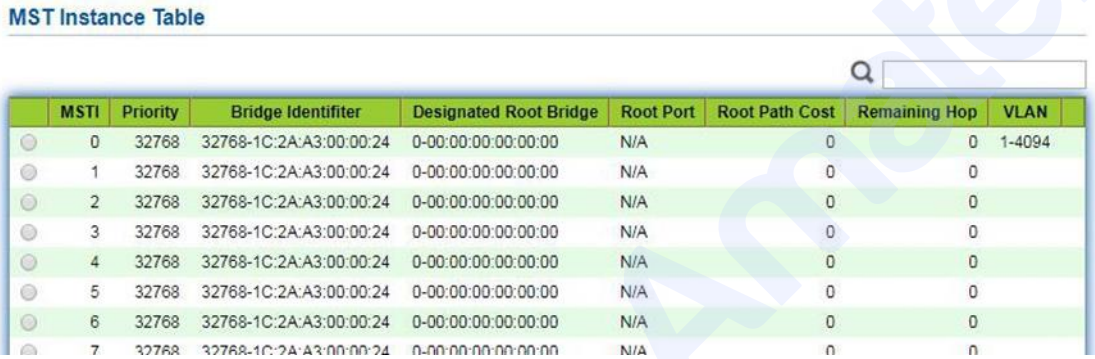
Настройки интерфейса

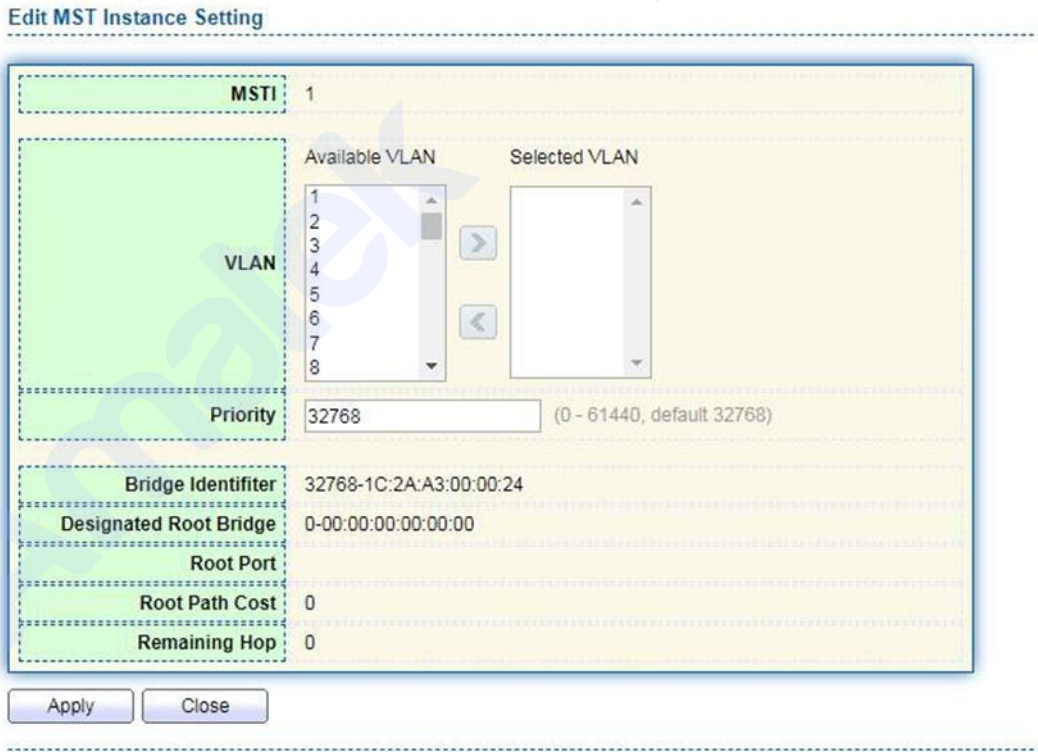
Параметр	Описание
Enabled	Установите флажок, чтобы включить функцию Spanning Tree
Operation Mode	Выбор протокола STP/RSTP/MSTP
Path Cost Mode	Режим пути: Long (длинный) / Short (короткий)
BPDU Handling	Метод обработки сообщений BPDU, полученных устройством
Priority	Приоритет
Hello Time	Интервалы между Hello (приветственными) сообщениями
Max Age	Максимальное время старения
Forward Delay	Время задержки
Region Name	Имя региона MST. Мастер-плата коммутатора устанавливает MAC-адрес по умолчанию. Используется для идентификации региона MST

8.2 MST Instance (Настройка MST экземпляра)

MST работает с концепцией регионов. Коммутаторы, настроенные для использования MST, должны выяснить, работают ли их соседи под управлением MST. Если коммутаторы имеют одинаковые атрибуты, они будут находиться в одном регионе. Это необходимо, чтобы была возможность разделения сети на один или несколько регионов. При этом в каждом регионе формируются независимые связующие деревья. Каждое связующее дерево называется экземпляр - MSTI (MST Instance), а каждый домен называется регион - MSTR (Multiple Spanning Tree Region).

Для настройки MST экземпляров перейдите «Spanning Tree > MST Instance» на панели навигации. Выберите экземпляр MSTI и нажмите «Edit». Укажите параметры. Далее нажмите «Apply», чтобы сохранить изменения.





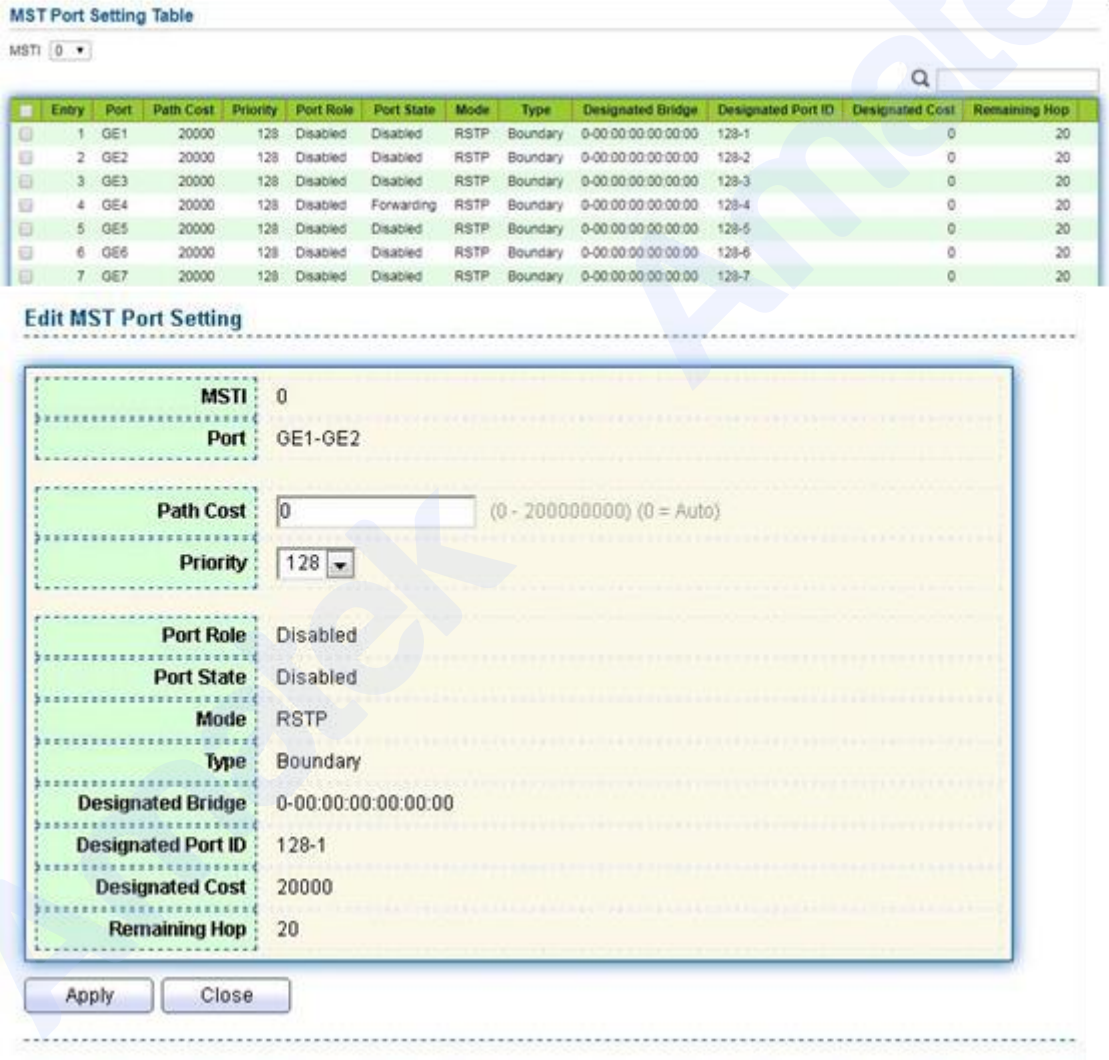
Настройки интерфейса

Параметр	Описание
MSTI	Номер MST экземпляра
VLAN	Номер VLAN, сопоставленный с экземпляром

Priority	Установите для указанного экземпляра приоритет, кратный 4096, в диапазоне от 0 до 65 535, по умолчанию - 32 768
Bridge ID	Идентификатор моста экземпляра связующего дерева, соответствующего этому устройству, состоит из приоритета и MAC-адреса
Designated Root Bridge	Назначенный корневой мост
Root Port	Корневой порт выбранного экземпляра
Root Path Cost	Стоимость пути до корневого моста

8.3 MST Port Setting (Настройка MST портов)

Для настройки MST портов перейдите «Spanning Tree > MST Port Setting» на панели навигации. Выберите MSTI и порты, нажмите «Edit». Укажите параметры. Далее нажмите «Apply», чтобы сохранить изменения.



Настройки интерфейса

Параметр	Описание
MSTI	Номер MST экземпляра
Port	Номер порта для настройки
Path Cost	Введите значение стоимости пути. Используйте стандарт IEEE 802.1t со значением в диапазоне от 0 (Auto) до 200 000 000.

Priority	Выберите приоритет порта с меньшим значением, представляющим более высокий приоритет. Приоритет порта влияет на роль интерфейса в указанном MSTI. В разных MSTI пользователи могут настраивать приоритеты для одного и того же порта. В результате поток различных VLAN может перенаправляться по физическим каналам для обеспечения распределения нагрузки VLAN
Port Role	3 типа корневых портов: specified (указанный порт), backup (резервный порт) и disabled (отключенный порт)
Port State	3 состояния порта: Discarding, Forwarding и Disabled
Mode	Текущий режим STP
Type	Типы портов в экземпляре: boundary (граничные) и internal (внутренние) порты.

8.4 Port Setting (Настройка портов)

Для настройки портов перейдите «Spanning Tree > Port Setting» на панели навигации. Выберите порт, нажмите «Edit». Укажите параметры. Далее нажмите «Apply», чтобы сохранить изменения.

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-4	20000
5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000

Edit Port Setting

Port	GE1
State	☑ Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Edge Port	☐ Enable
BPDU Filter	☐ Enable
BPDU Guard	☐ Enable
Point-to-Point	◉ Auto ○ Enable ○ Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

Apply Close

Настройки интерфейса

Параметр	Описание
Port	Номер порта для настройки
State	Enable – STP включено
Edge Port	Edge (граничный) порт должен быть подключен непосредственно к оконечному устройству, а не к другому коммутатору или сетевому сегменту. Он может быстро перейти в состояние пересылки, поскольку изменения топологии не создают петель. Настраиваемый Edge порт может быть быстро переведен в состояние пересылки с помощью STP. Для этого рекомендуется, чтобы порты, подключенные непосредственно к оконечным устройствам, были настроены как Edge порты (Enable)
BPDU Filter	Включить фильтр BPDU
BPDU Guard	Включить защиту BPDU. По умолчанию выключено. Если BPDU Guard включен, устройство отключит порты, получающие BPDU, и уведомит NMS. Такие порты могут быть восстановлены только вручную администратором.
Point-to-Point	Auto (автоматический) режим - указывает состояние соединения между автоматической проверкой по умолчанию и Point-to-Point (точка-точка) соединениями. Enable (включено) режим - указывает, что конкретный порт подключен к каналам Point-to-Point (точка-точка). Disable (отключено) режим - указывает, что конкретный порт не может подключиться к каналам Point-to-Point.

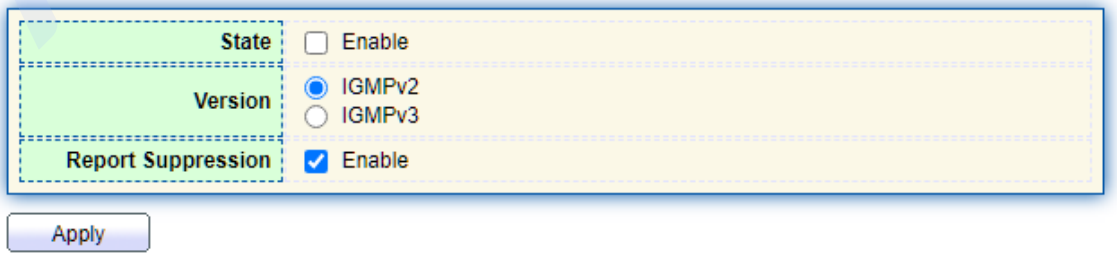
9. Multicast (Многоадресная рассылка)

9.1 IGMP Snooping (Настройка IGMP Snooping)

Функция IGMP Snooping (Internet Group Management Protocol Snooping) разработана для ограничения широковещательной ретрансляции группового трафика потребителям, которые явно не заявили о своей заинтересованности в нём. Это позволяет коммутатору исключать такой трафик из потоков, направляемых через порты, к которым не подключены его потребители, тем самым существенно снижая нагрузку на сеть.

IGMP Snooping используется для отслеживания IGMP-сообщений и контроля multicast трафика. На основе IGMP-сообщений коммутатор ведет таблицу переадресации multicast, трафик отправляется только на порты, с которых поступил запрос на многоадресную группу.

Для настройки IGMP Snooping перейдите «Multicast > IGMP Snooping > Property» на панели навигации. Укажите параметры. Нажмите «Apply», чтобы сохранить изменения.



Далее выберите необходимую VLAN и нажмите «Edit» для настройки. Укажите параметры. Нажмите «Apply», чтобы сохранить изменения.

VLAN Setting Table

	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
☐	1	Disabled	Enabled	2	125	10	2	1	Disabled
☑	2	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Edit VLAN Setting

VLAN	2
State	☐ Enable
Router Port Auto Learn	☑ Enable
Immediate leave	☐ Enable
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

Apply Close

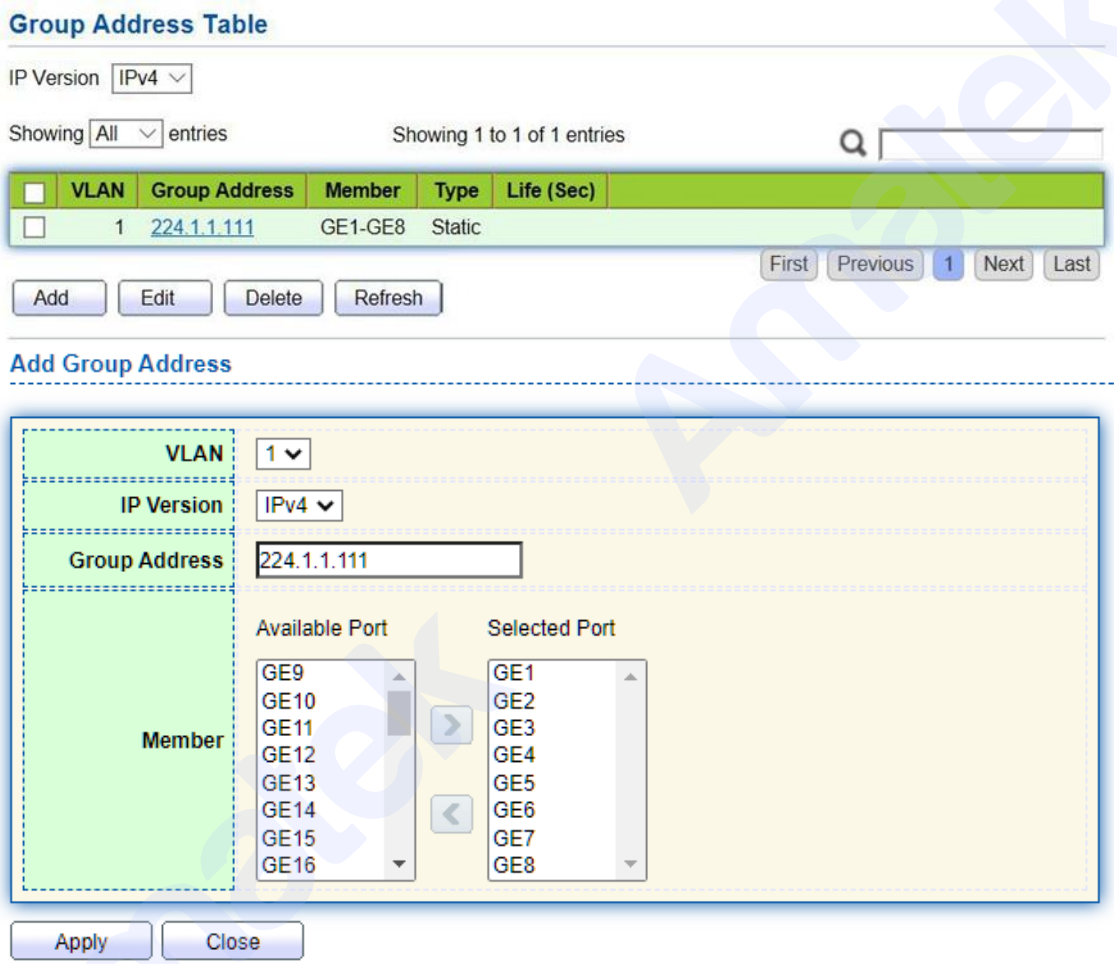
Настройки интерфейса

Параметр	Описание
VLAN	Идентификатор VLAN
State	Включить или отключить отслеживание IGMP в данной VLAN
Routed Port Auto Learning	Автоматическое обучение маршрутизируемого порта
Immediate leave	
Query Robustness	Максимальное количество многоадресных запросов
Query Interval	Интервал между запросами
Query Max Response Interval	Тайм-аут (превышение максимального времени ответа) запроса
Last Member Query Counter	Максимальное количество запросов для последнего участника
Last Member Query Interval	Интервал между запросами

9.2 Group Address (Настройки групп адресов IGMP)

IGMP Snooping настраивает многоадресную VLAN, подключая разных пользователей портов коммутатора к данной многоадресной VLAN для получения многоадресных рассылок. Таким образом, многоадресный поток может передаваться только внутри многоадресной VLAN, что экономит полосу пропускания. Кроме того, безопасность и пропускная способность сети повышаются, поскольку многоадресные VLAN полностью изолированы от пользовательских VLAN.

Для настройки Group Address перейдите «Multicast > General > Group Address» на панели навигации. Нажмите «Add» Укажите параметры. Нажмите «Apply», чтобы сохранить изменения. При необходимости удалить группу адресов нажмите «Delete».



Настройки интерфейса

Параметр	Описание
VLAN	Идентификатор VLAN, к которой принадлежит группа многоадресной рассылки (выберите существующую VLAN).
IP Version	IPv4 или IPv6 версия многоадресного IP-адреса
Multicast Address	Введите многоадресный адрес
Member	Добавьте порты-участники многоадресной рассылки

9.3 Filtering (Настройка фильтрации рассылок)

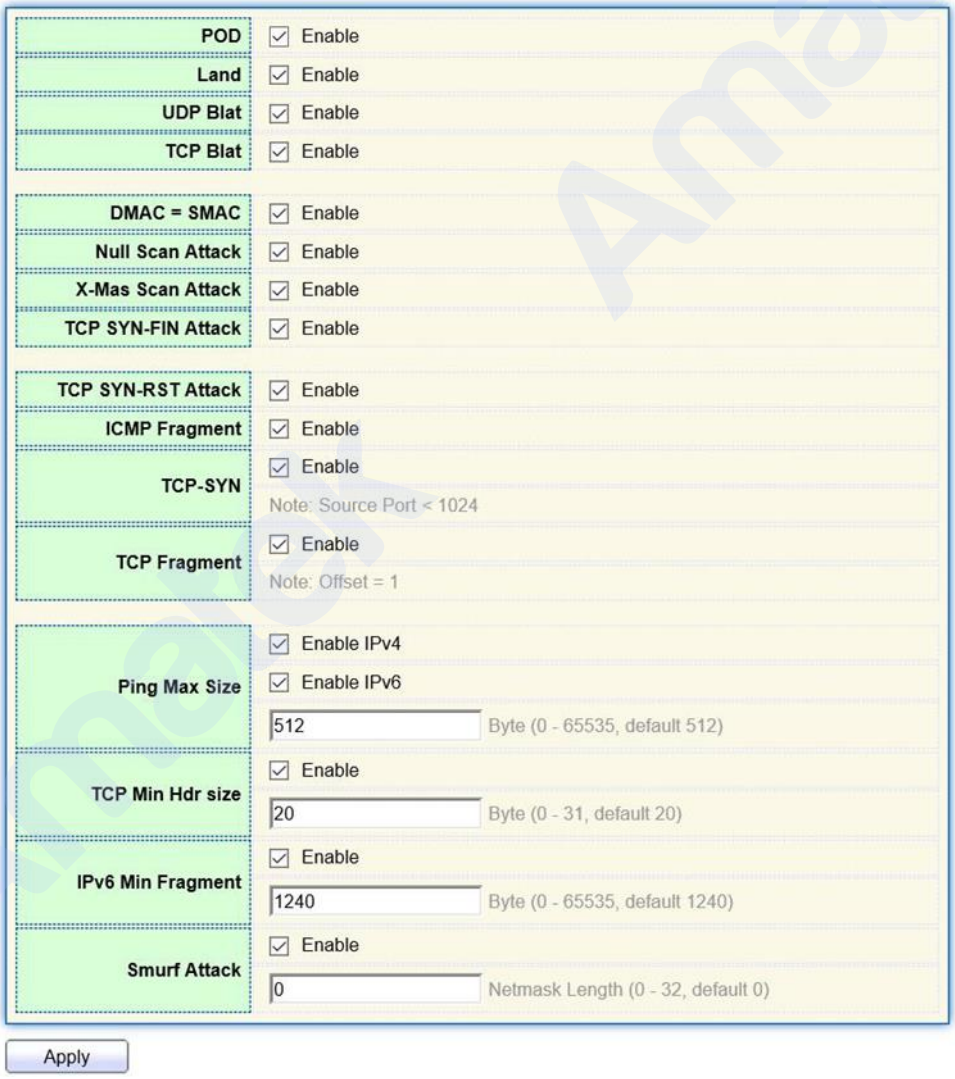
На странице «Filtering Profile» вы можете настроить профили фильтрации многоадресной рассылки. Вы также можете редактировать или удалять профили, нажав «Edit» или «Delete». Далее на странице «Filtering Binding» необходимо привязать профили фильтрации к соответствующим портам.

10. Network Security (Сетевая безопасность)

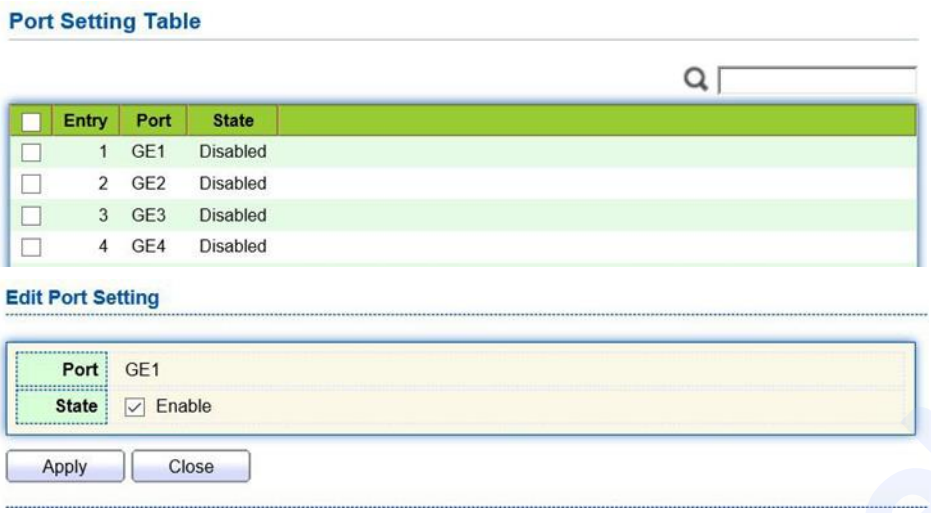
10.1 DoS Attack Resistance (Защита от DoS-атак)

Включите функцию DoS Attack Resistance, чтобы сделать коммутатор более безопасным.

1. Для настройки параметров защиты от атак перейдите «Security > DoS > Property» на панели навигации. Укажите параметры. Нажмите «Apply», чтобы сохранить изменения.



2. Для включения защиты от атак на выбранных портах перейдите «Security > DoS > Port Setting». Отметьте необходимые порты. Нажмите «Edit». Установите флажок «Enable». Далее нажмите «Apply», чтобы сохранить изменения.



10.2 ACL (Настройки ACL)

ACL (Access Control List) — список правил, запрещающих или разрешающих использование ресурсов сети. Списки контроля доступа (ACL) гарантируют, что только авторизованные пользователи имеют доступ к определенным ресурсам, и блокируют любые несанкционированные попытки доступа к сетевым ресурсам. ACL работает с IP-пакетами, но может узнать тип конкретного пакета, проанализировать порты TCP (Transmission Control Protocol) и UDP (User Datagram Protocol).

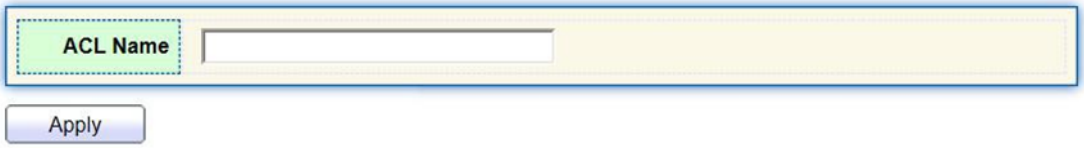
ACL классифицирует пакеты по условиям соответствия, которые могут быть MAC-адресом источника/получателя, IP-адресом источника/получателя, номером порта и т.п. ACL классифицирует пакеты по условиям соответствия, которые могут быть адресом источника/получателя, номером порта и т. д. ACL можно разделить на следующие категории в соответствии с целями приложения:

- Базовый IP ACL - формулирует правила, основанные только на исходном IP-адресе пакетов. Идентификатор ACL находится в диапазоне от 100 до 999.
- Advanced IP ACL - подготавливает правила в соответствии с IP-адресом источника/получателя пакетов, типами протокола, используемого IP, и информацией уровня 3 или 4, такой как характеристики протокола. Идентификатор ACL находится в диапазоне от 100 до 999.
- L2 ACL - правила создаются в соответствии с MAC-адресом источника/получателя пакетов, приоритетом 802.1p и информацией L2, такой как тип протокола. Идентификатор ACL находится в диапазоне от 1 до 99.

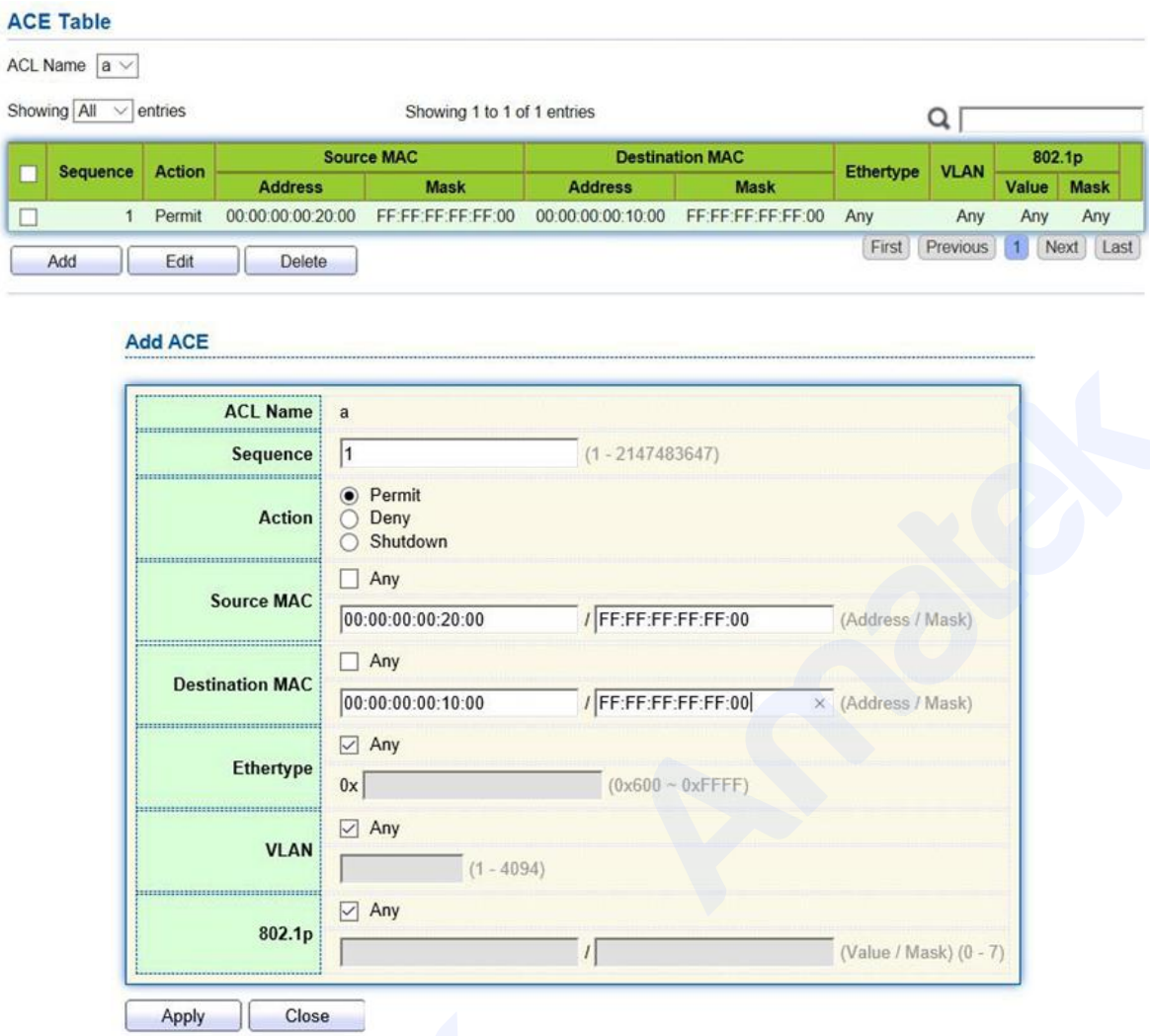
10.2.1 MAC ACL Configuration (Настройки MAC ACL)

L2 ACL (MAC ACL) - правила создаются в соответствии с MAC-адресом источника/получателя, приоритетом VLAN и информацией L2, такой как тип протокола.

1. Для настройки MAC ACL перейдите «ACL > MAC ACL» на панели навигации. Укажите название ACL и нажмите «Apply», чтобы сохранить изменения.



2. Далее перейдите «ACL > MAC ACE» выберите ваш список ACL и нажмите «Add». Задайте параметры. Нажмите «Apply», чтобы сохранить изменения.



Настройки интерфейса

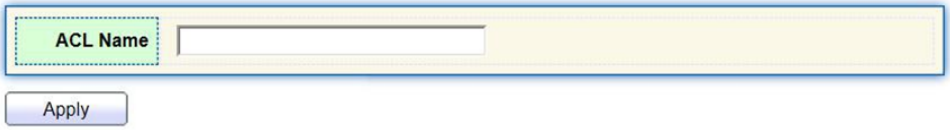
Параметр	Описание
Sequence	MAC ACL находится в диапазоне от 1 до 2147483647
Action	Действия ACL: Permit (Разрешить») или Deny (Запретить), а также Shutdown (Отключить)
Source MAC	Исходный MAC-адрес и маска в формате H.H.H.H.H.H. Выберите «Any», чтобы представить любой MAC-адрес.
Destination MAC	MAC-адрес получателя и маска в формате H.H.H.H.H.H. Выберите «Any», чтобы представить любой MAC-адрес.
Ethernet Type	Введите тип Ethernet правил ACL в диапазоне от 0x600 до 0xFFFF. Выберите «Any», чтобы представить любой тип.
VLAN	Введите ID VLAN для ACL или выберите «Any» для всех VLAN.
802.1p	Введите приоритет VLAN и маску для правил ACL в диапазоне от 1 до 7, выберите «Any», чтобы представить любой приоритет VLAN.

10.2.2 IPv4 ACL Configuration (Настройки IPv4 ACL)

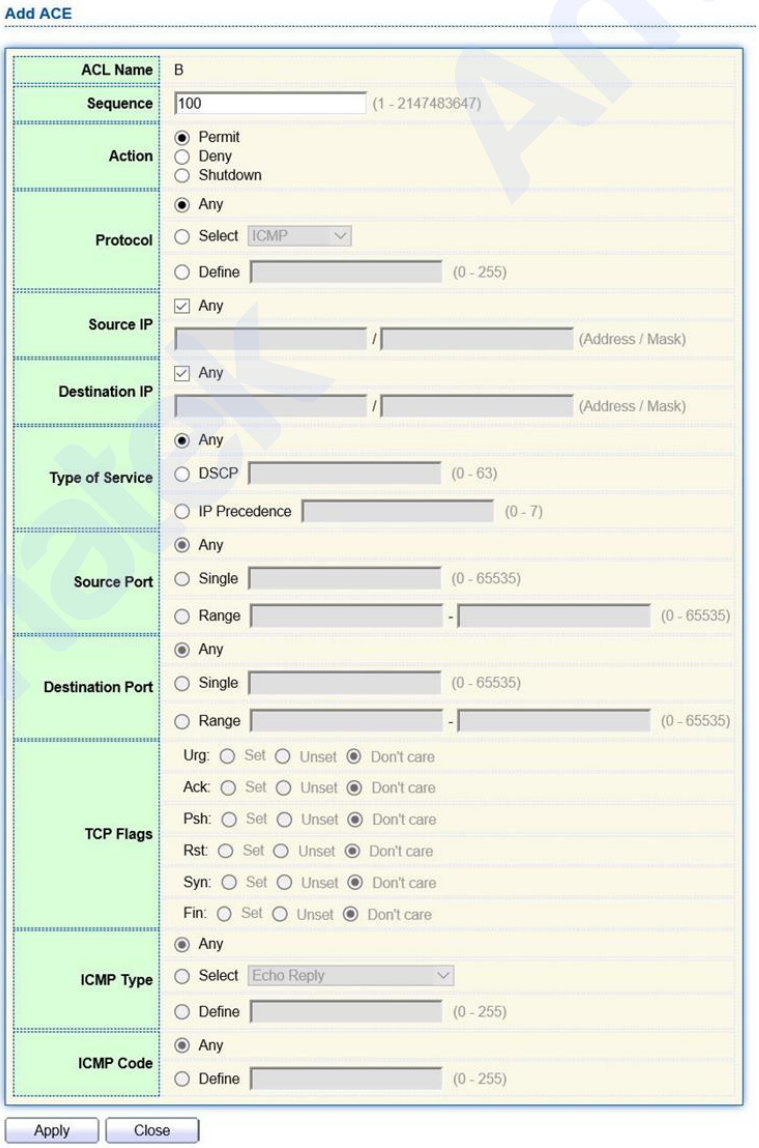
ACL на основе IPv4 (базовый IP ACL) формулирует правила только в соответствии с исходным IP-адресом пакетов. Идентификатор ACL находится в диапазоне от 100 до 999.

Расширенные правила IP ACL создаются в соответствии с IP-адресом источника/получателя пакетов, типом протокола и информацией уровня 3 или 4, такой как характеристики протокола. Идентификатор ACL находится в диапазоне от 100 до 999.

1. Для настройки IPv4 ACL перейдите «ACL > IPv4 ACL» на панели навигации. Укажите название ACL и нажмите «Apply», чтобы сохранить изменения.



2. Далее перейдите «ACL > IPv4 ACE» выберите ваш список ACL и нажмите «Add». Задайте параметры. Нажмите «Apply», чтобы сохранить изменения.



Настройки интерфейса

Параметр	Описание
Sequence	MAC ACL находится в диапазоне от 1 до 2147483647
Action	Действия ACL: Permit (Разрешить») или Deny (Запретить), а также Shutdown (Отключить)
Protocol	Требуется выбрать тип протокола, такой как ICMP, TCP, UDP и т.п. Выберите «Любой» для представления любого протокола.
Source IP	Исходный IP-адрес и маска. Выберите «Any», чтобы представить любой IP-адрес.
Destination IP	IP-адрес получателя и маска. Выберите «Any», чтобы представить любой IP-адрес.
Type of Service	Введите тип службы правил ACL, на пример DSCP (0–63) и приоритет IP (0–7). Выберите «Any», чтобы представить любой тип службы.
Source Port	Введите исходный порт правил ACL: номер одного порта или диапазон (0 - 65535). Выберите «Any», чтобы представить любой исходный порт
Destination Port	Введите порт получателя правил ACL: номер одного порта или диапазон (0 - 65535). Выберите «Any», чтобы представить любой исходный порт
TCP Flags	Введите флаги TCP правил ACL, такие как URG, ACK, PSH, RST, SYN, FIN, с такими действиями, как Set (Установить), Unset (Отменить) и Don’t care (Все равно)
ICMP Type	Введите тип сообщения ICMP правил ACL. Выберите «Any», чтобы представить любой тип ICMP.
ICMP Code	Введите значение кода ICMP правил ACL. Выберите «Any», чтобы представить любое значение поля.

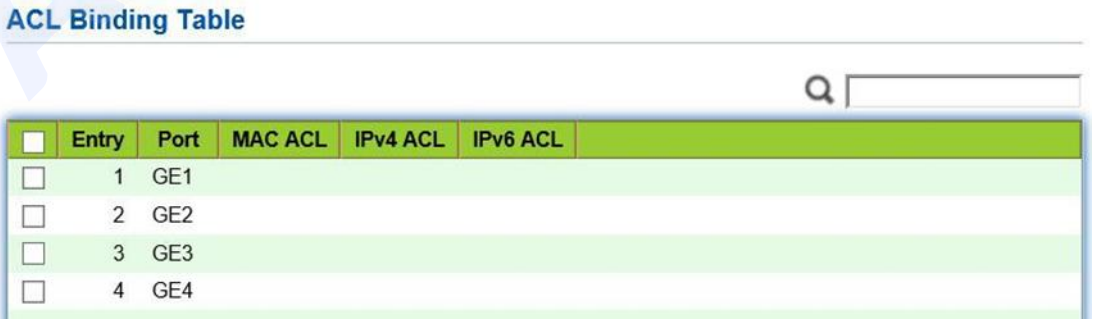
10.2.3 IPv6 ACL Configuration (Настройки IPv6 ACL)

ACL на основе IPv6 настраиваются аналогично IPv4 ACL (см. пункт 10.2.2 IPv4 ACL).

10.2.4 ACL Binding (Привязка ACL к портам)

После создания списка его необходимо привязать к каждому требуемому порту.

Для привязки ACL к выбранным портам перейдите «ACL > ACL Binding». Отметьте необходимые порты. Нажмите «Bind». Выберите название ACL для каждого типа. Далее нажмите «Apply», чтобы сохранить изменения. Для прекращения действия ACL на выбранном порту нажмите «Unbind».



11. Advanced Configuration (Дополнительные настройки)

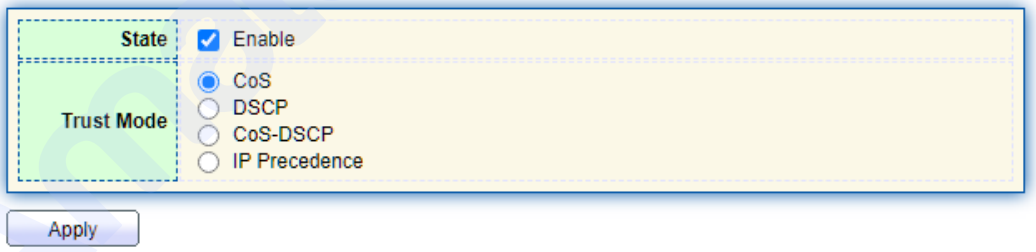
11.1 QoS Configuration (Настройки протокола QoS)

QoS (Quality of Service) - технология предоставления различным классам трафика различных приоритетов в обслуживании. В данном подменю можно настроить конфигурацию приоритетов Quality of Service (качества обслуживания) и Class of Service (класса обслуживания). Рекомендуется настроить для трафика, связанного с передачей звука, видео, финансовых транзакций.

11.1.1 Basic Configuration (Базовые настройки)

Перегрузка сети, возникающая из-за одновременной конкуренции за права использования ресурсов между сообщениями, обычно решается путем планирования очередей пакетов, что позволяет избежать периодических перегрузок сети. Технологии планирования очереди включают SP (строгий приоритет), WFQ (взвешенная справедливая очередь), WRR (взвешенный циклический алгоритм) и DRR (дефицитный циклический алгоритм, который является расширением технологии RR).

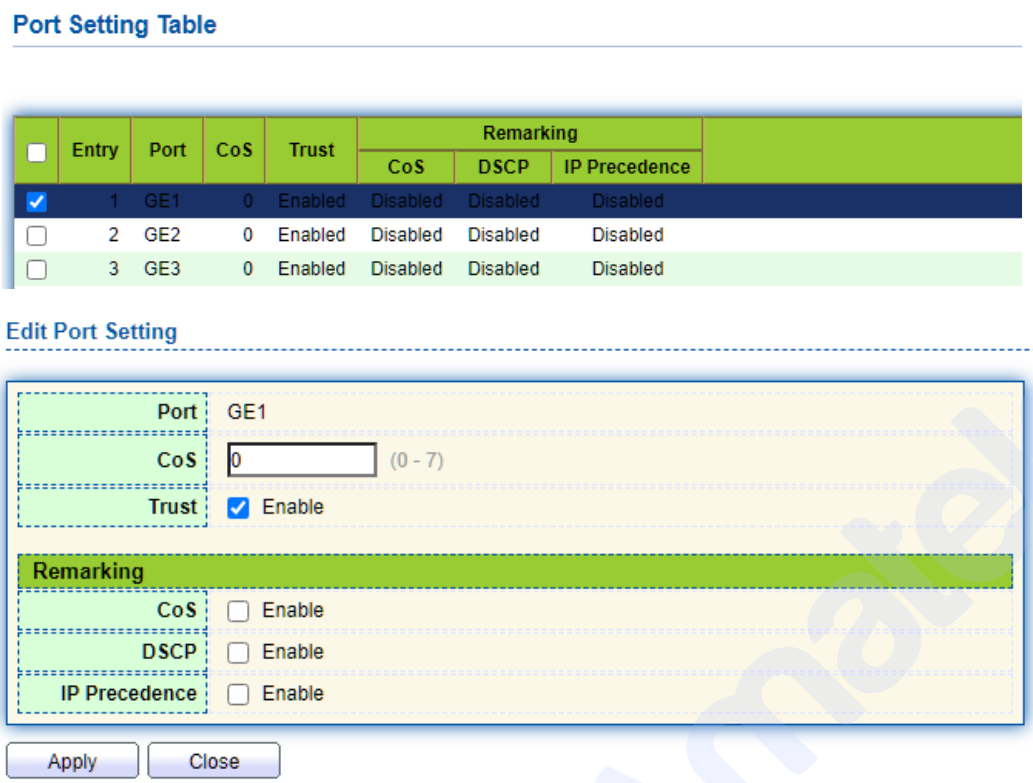
1. Для базовой настройки QoS перейдите «QoS > General > Property» на панели навигации. Выберите Trust Mode и нажмите «Apply», чтобы сохранить изменения.



Настройки интерфейса

Параметр	Описание
State	Включение глобальной функции QoS
Trust Mode	Выберите CoS, DSCP, CoS-DSCP и IP-приоритет.

2. Выберите порт и нажмите «Edit» задайте параметры QoS. Далее нажмите «Apply», чтобы сохранить изменения.

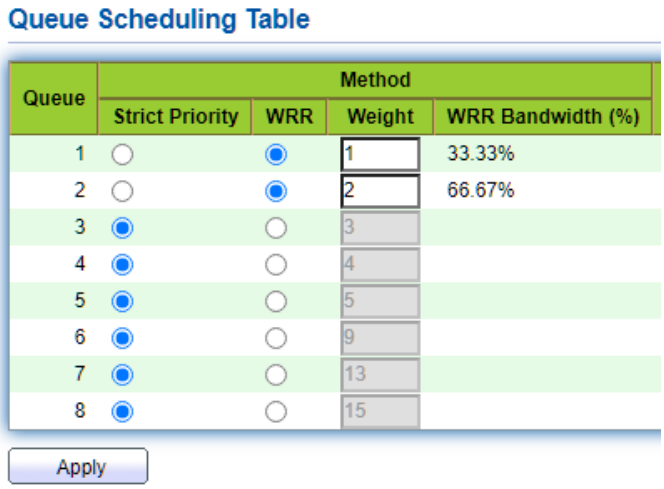


Настройки интерфейса

Параметр	Описание
CoS	Класс обслуживания - установите значение в диапазоне от 1 до 7
Port Trust Mode	Переключение функции QoS порта
CoS	Включите CoS
DSCP	Включите DSCP
IP Precedence	Включите «Приоритет IP»

11.1.2 Queue Scheduling (Планирование очереди)

Для настройки очереди QoS перейдите «QoS > General > Queue Scheduling» на панели навигации. Выберите режим планирования очереди SP или WRR, для WRR укажите вес очереди. Далее нажмите «Apply», чтобы сохранить изменения.

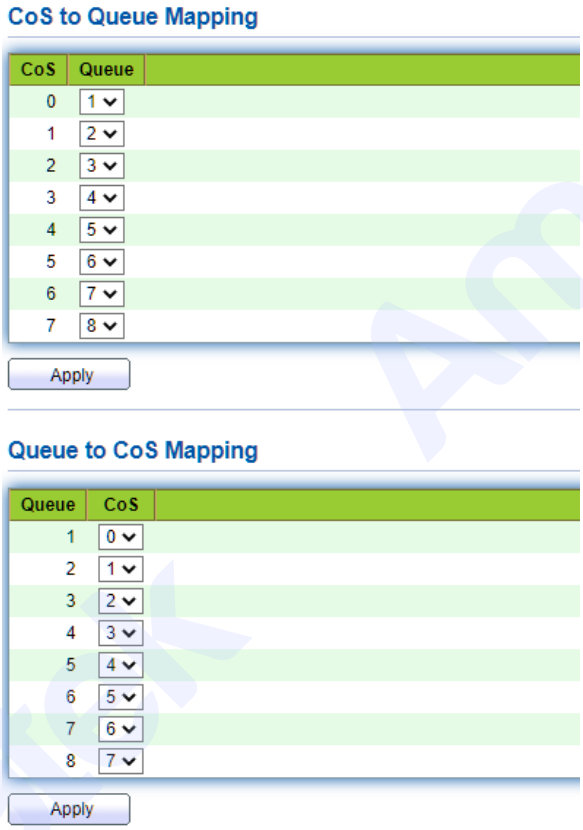


Настройки интерфейса

Параметр	Описание
SP	Режим SP (строгий приоритет)
WRR	Режим WRR (взвешенный циклический алгоритм)
Weight	Вес очереди (процент от полосы пропускания WRR)

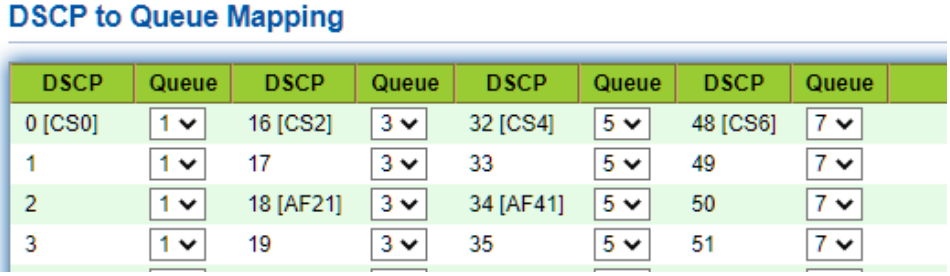
11.1.3 CoS Mapping (Сопоставление CoS)

Перейдите «QoS > General > CoS Mapping» на панели навигации. Укажите сопоставление CoS с очередью и/или очередь с CoS. Далее нажмите «Apply», чтобы сохранить изменения.



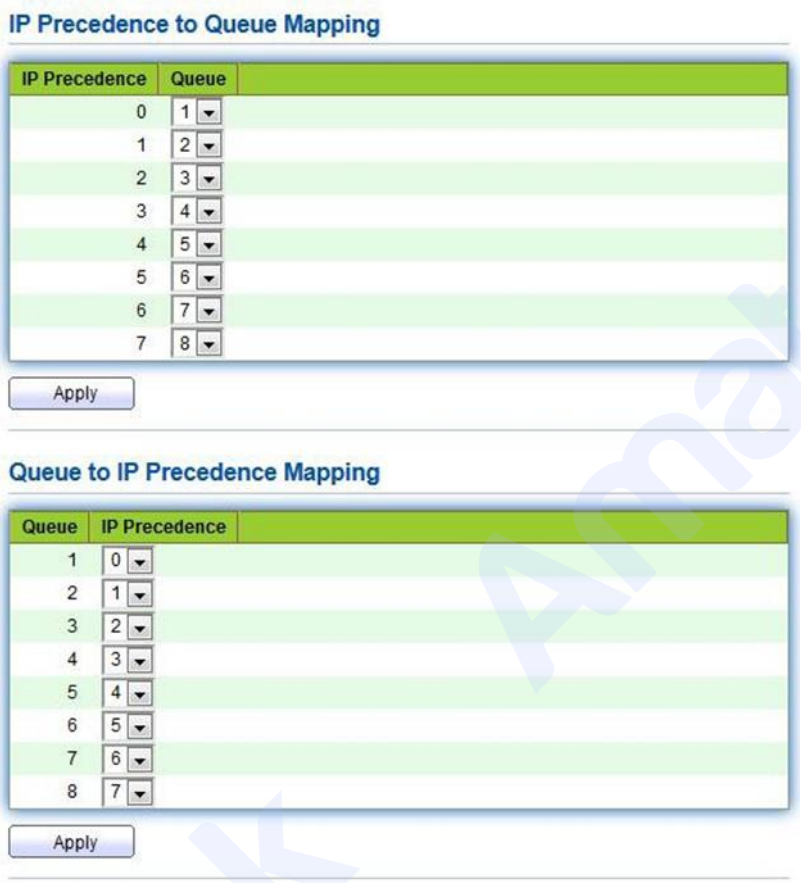
11.1.4 DSCP Mapping (Сопоставление DSCP)

Перейдите «QoS > General > DSCP Mapping» на панели навигации. Укажите сопоставление DSCP с очередью (DSCP to Queue Mapping) и/или сопоставьте каждой очереди значение DSCP (Queue to DSCP Mapping). Далее нажмите «Apply», чтобы сохранить изменения.



11.1.5 IP Precedence Mapping (Сопоставление IP приоритета)

Перейдите «QoS > General > IP Precedence Mapping» на панели навигации. Укажите сопоставление IP Precedence с очередью (IP Precedence to Queue Mapping) и/или сопоставьте каждой очереди значение IP Precedence (Queue to IP Precedence Mapping). Далее нажмите «Apply», чтобы сохранить изменения.

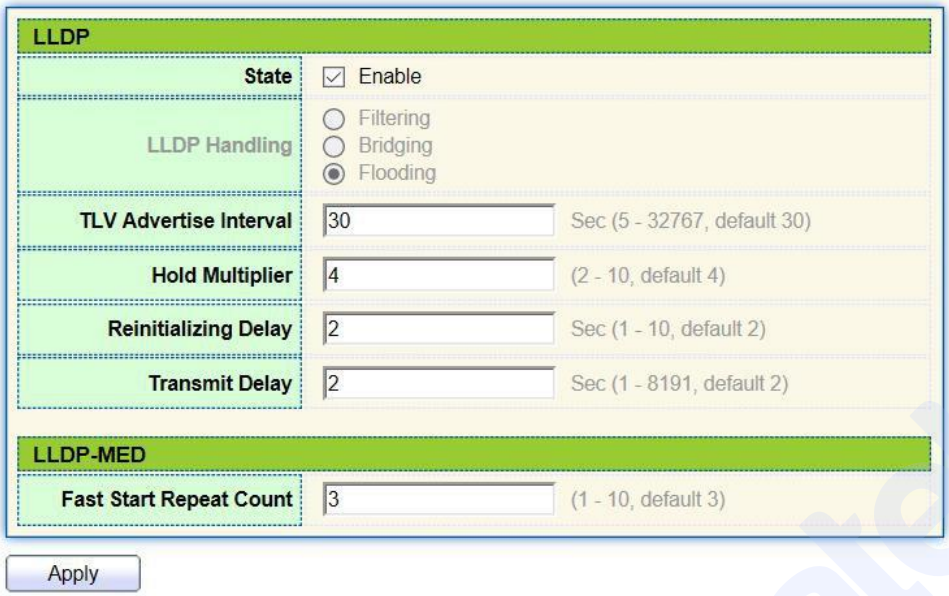


11.2 LLDP Configuration (Настройки протокола LLDP)

LLDP (Link Layer Discovery Protocol) - протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своём существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения. После получения информации устройства сохраняют ее в виде стандартной MIB (Management Information Base).

11.2.1 LLDP Configuration (Настройки LLDP)

Для настройки протокола LLDP перейдите «Discovery > LLDP > Property» на панели навигации. Укажите параметры. Нажмите «Apply», чтобы сохранить изменения.



Настройки интерфейса

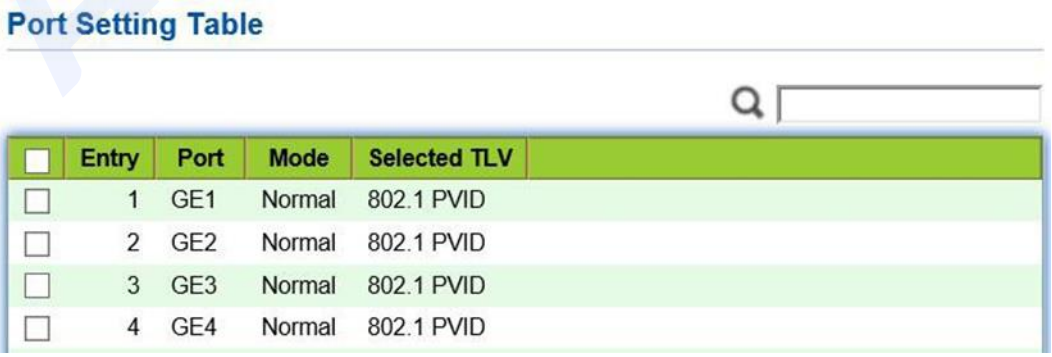
Параметр	Описание
State	Включить или отключить LLDP
LLDP Handling	Выберите обработку LLDP: Filtering, Bridging, Flooding
TLV Advertise Interval	Интервал передачи в диапазоне от 5 до 32767, по умолчанию 30 сек.
Hold Multiplier	Период передачи в диапазоне 2 – 10, по умолчанию 4
Delay Reinitialization	Задержка повторной инициализации, по умолчанию 2 сек.
Transfer Delay	Введите ID VLAN для ACL или выберите «Any» для всех VLAN.
Fast Start Repeat Count	3 сек. по умолчанию для порта LLDP-MED. Диапазон 1 – 10сек.

Примечание:

Сообщение Ethernet, инкапсулированное с помощью LLDPDU (блок данных LLDP), распознается как сообщение LLDP. Каждый TLV представляет собой единицу LLDPDU, переносимую с указанной информацией.

11.2.2 Port Configuration (Настройки портов LLDP)

1. Для настройки портов перейдите «Discovery > LLDP > Port Setting» на панели навигации.



Описание интерфейса

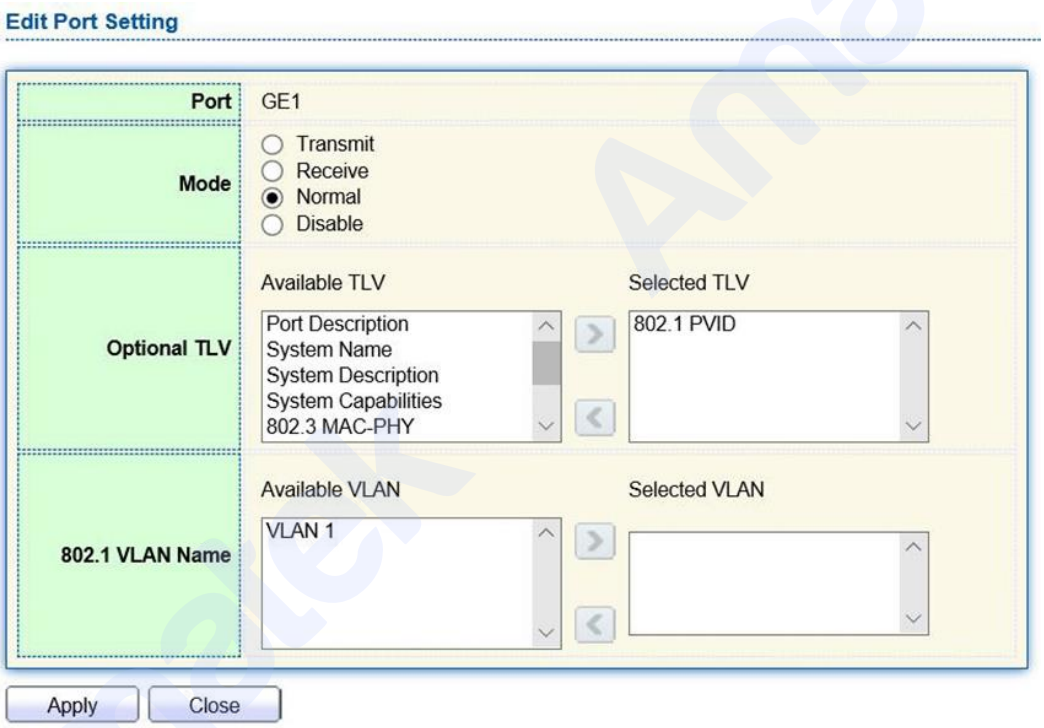
Параметр	Описание
Port	Доступно несколько портов для настройки.
Transmitting & Receiving Mode	Режим передачи / приема LLDP
Selected TLV	Информация о выбранных TLV и VLAN

Примечание:

Протокол LLDP может работать по 4 схемам:

- Transmit - только передача сообщений LLDP;
- Receive - только получение сообщений LLDP;
- Normal - передача и получение сообщений LLDP;
- Disable - ни отправлять, ни получать сообщения LLDP.

2. Выберите необходимый порт и нажмите «Edit». Задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.

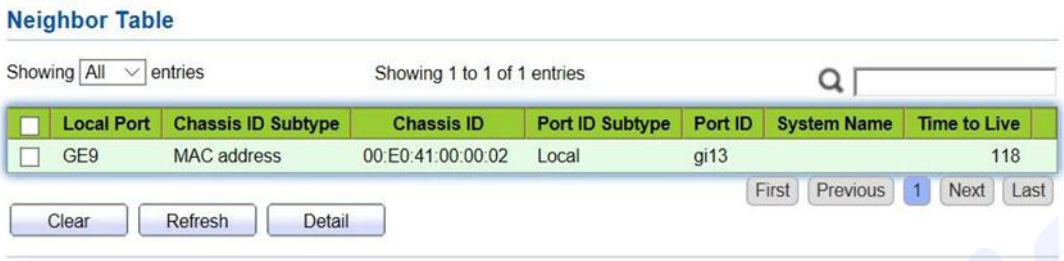


Настройки интерфейса

Параметр	Описание
Port	Доступно несколько портов для настройки.
Mode	Transmit - только передача сообщений LLDP; Receive - только получение сообщений LLDP; Normal - передача и получение сообщений LLDP; Disable - ни отправлять, ни получать сообщения LLDP.
Optional TLV	Выберите необходимую информацию TLV и VLAN
802.1 VLAN Name	Выберите необходимые VLAN

11.2.3 Neighbor Info (Информация о соседних устройствах)

Для просмотра информации о соседних сетевых устройствах перейдите «Discovery > LLDP > Neighbor Info» на панели навигации.



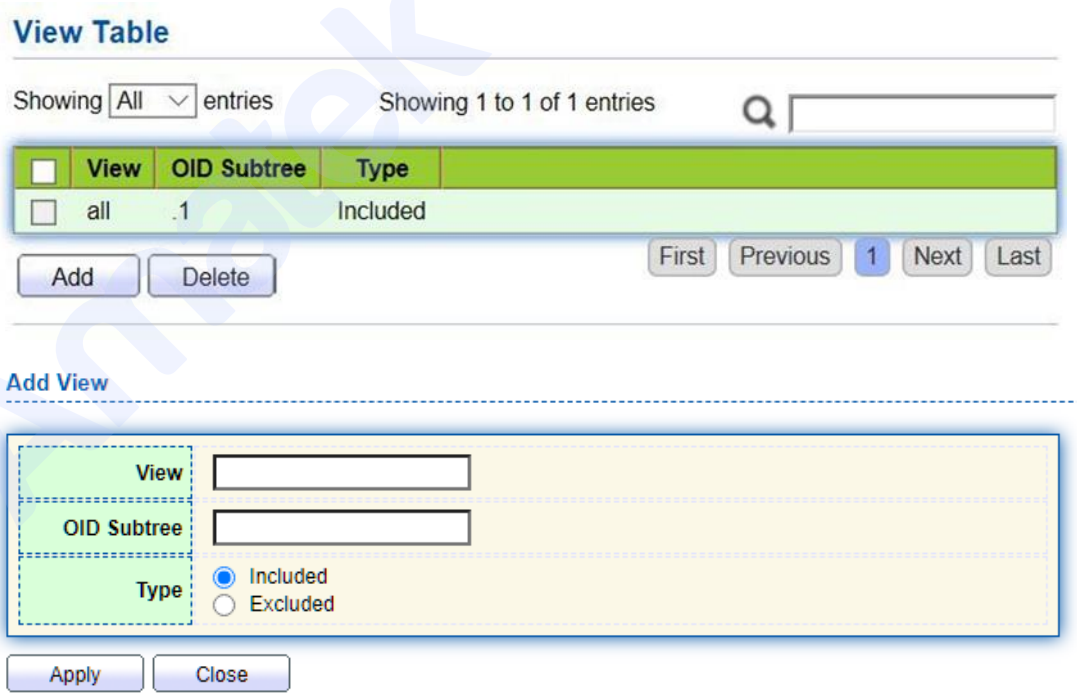
11.3 SNMP Configuration (Настройки SNMP)

SNMP (Simple Network Management Protocol - простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. Протокол обычно используется в системах сетевого управления для контроля подключённых к сети устройств на предмет условий, которые требуют внимания администратора.

SNMP использует базы управляющей информации (MIB) для хранения доступных объектов в иерархическом или древовидном пространстве имен, которое содержит идентификаторы объектов (OID). OID идентифицирует информацию в иерархии MIB, которая может быть прочитана или установлена через SNMP.

11.3.1 View Configuration (Настройки View)

Для настройки View перейдите «Management > SNMP > View». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.

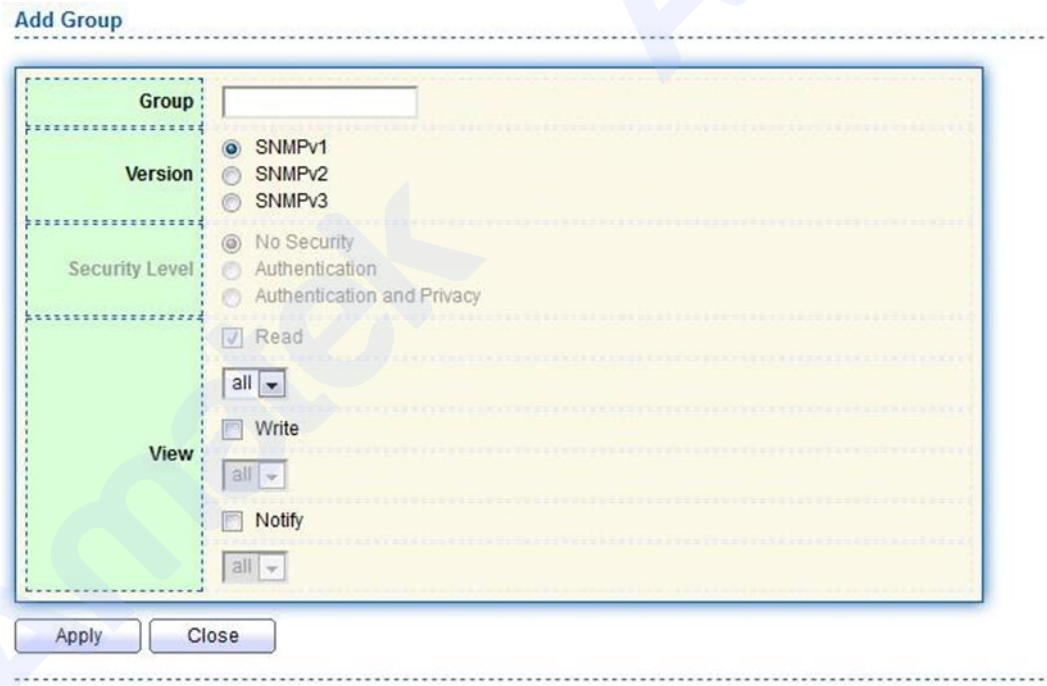


Описание интерфейса

Параметр	Описание
View	Имя просмотра
OID Subtree	Поддерево идентификатора объектов OID
Type	Тип просмотра: “Included” (включенный) или “Excluded” (исключенный).

11.3.2 Group Configuration (Настройки групп)

Для настройки Group перейдите «Management > SNMP > Group». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.

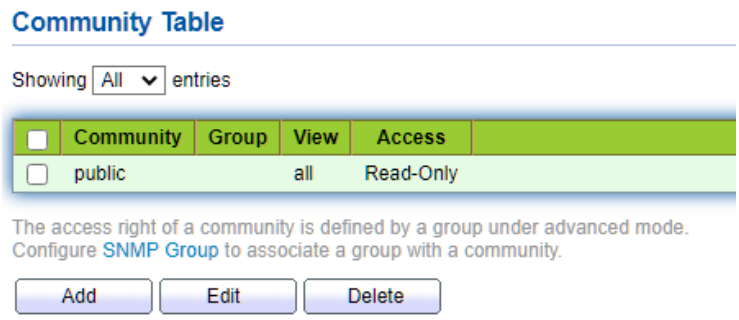


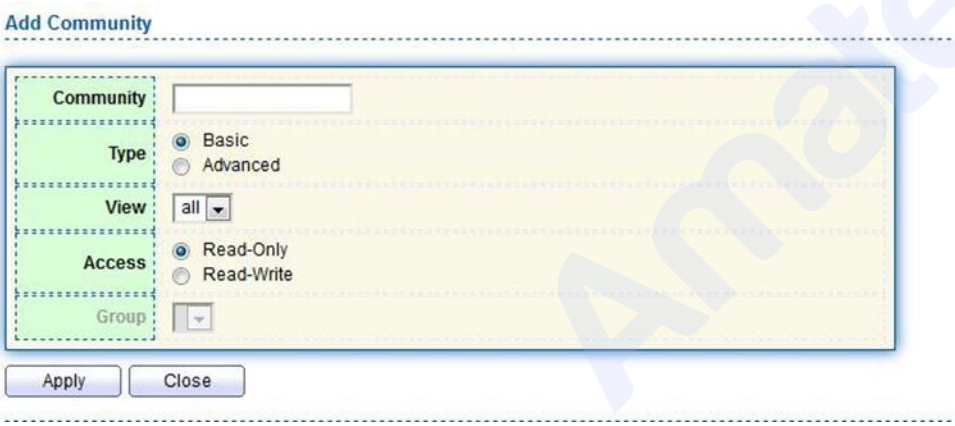
Описание интерфейса

Параметр	Описание
Group	Имя группы
Version	Версия протокола SNMP: V1, V2, V3
Security Level	Уровень безопасности: с авторизацией для версии SNMPv3
View	Тип View: “Read” (Чтение), “Write” (Запись), Notify (Уведомление).

11.3.3 Community Configuration (Настройки сообществ)

Для настройки Community перейдите «Management > SNMP > Community». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.





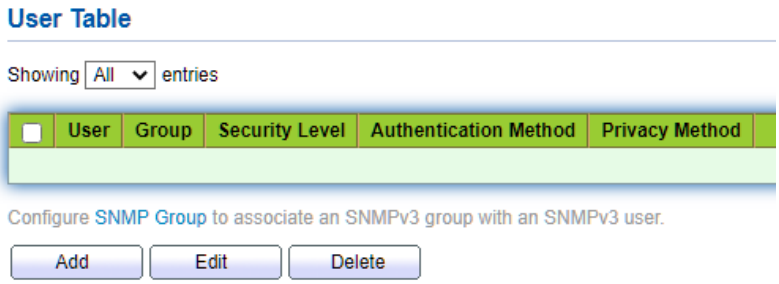
Описание интерфейса

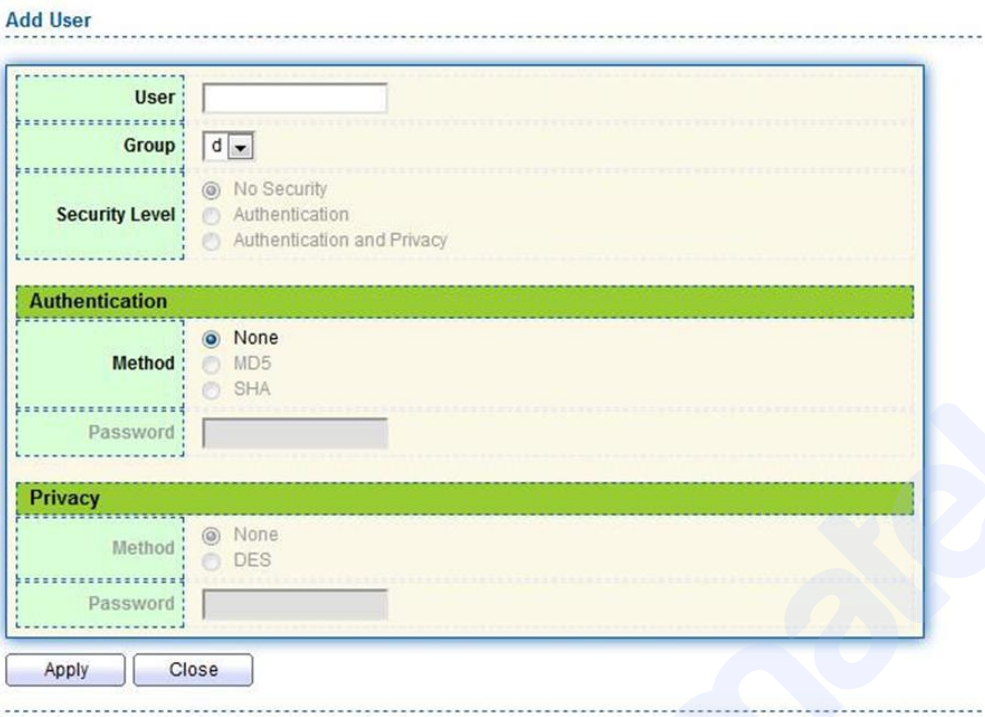
Параметр	Описание
Community	Название сообщества
Group	Имя группы
View	Имя View
Access	Тип доступа: “Read-Only” (Только чтение), “Read-Write” (Чтение-Запись)

Примечание:
Права доступа сообщества определяются группой в расширенном режиме. Настройте группу SNMP, чтобы связать группу с сообществом.

11.3.4 User Configuration (Настройки пользователей SNMP)

Для настройки пользователей перейдите «Management > SNMP > User». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.





Описание интерфейса

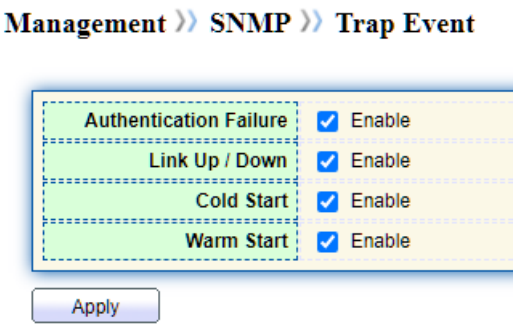
Параметр	Описание
User	Имя пользователя
Group	Выберите название группы
Security Level	Уровень безопасности: с авторизацией для версии SNMPv3
Authentication	Метод авторизации. Password: задайте пароль.
Privacy Password	Метод шифрования. Password: задайте пароль.

11.3.5 Engine ID Configuration (Настройки Engine ID)

Для настройки перейдите «Management > SNMP > Engine ID». Задайте параметры локального Local и удаленного Remote Engine ID. Далее нажмите «Apply», чтобы сохранить изменения.

11.3.6 Trap Event Configuration (Настройки Trap событий)

Для настройки событий Trap перейдите «Management > SNMP > Trap Event». Отметьте необходимые Trap события. Далее нажмите «Apply», чтобы сохранить изменения.

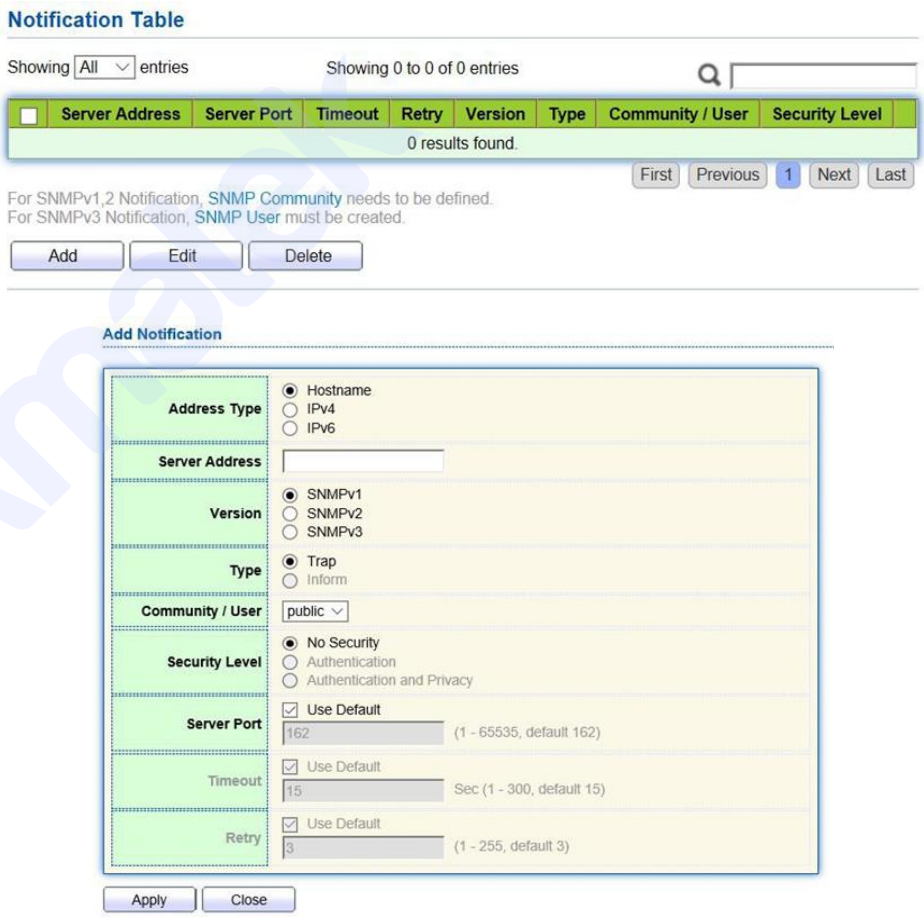


Описание интерфейса

Параметр	Описание
Authen. Failure	Ошибка авторизации
Link Up/Down	Port link up/down
Cold start	«Холодный» запуск
Warm start	«Горячий» запуск

11.3.7 Notification Configuration (Настройки уведомлений)

Для настройки уведомлений перейдите «Management > SNMP > Notification». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.



Настройки интерфейса

Параметр	Описание
Address Type	Тип адреса: «Имя хоста», «IPv4» или «IPv6»
Server Address	Адрес сервера
Version	Версия SNMP: v1, v2 или v3
Type	Тип уведомления: «Trap» (Ловушка) или «Inform» (Информировать)
Community/User	Сообщество или имя пользователя
Security Level	Уровень безопасности: с авторизацией для версии SNMPv3
Server port No.	Порта сервера по умолчанию162, в диапазоне от 1 до 65535
Timeout	Период тайм-аута: в диапазоне 1 - 300с., по умолчанию 15 секунд
Retry	Интервал повтора от 1 до 255 с, по умолчанию 3 с.

Примечание:

Для уведомлений SNMPv1,2 необходимо определить сообщество SNMP.

Для уведомления SNMPv3 необходимо создать пользователя SNMP.

11.4 RMON (Протокол RMON)

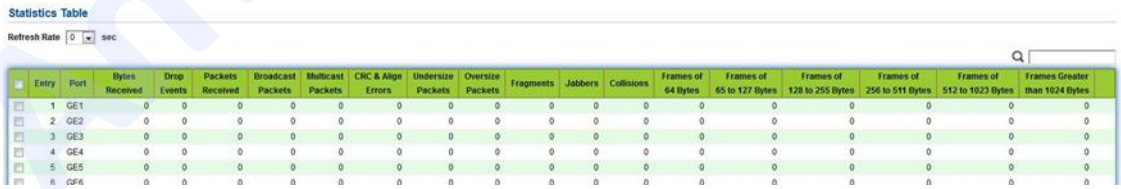
RMON (Remote Network MONitoring - дистанционный мониторинг сети) — протокол мониторинга компьютерных сетей, расширение SNM. В основе RMON, как и в основе SNMP, лежит сбор и анализ информации о характере данных, передаваемых по сети.

RMON включает в себя NMS (Станцию управления сетью) и Agent (Агент), работающий на различных сетевых устройствах. Агент RMON, работающий на сетевых мониторах или детекторах, будет отслеживать и подсчитывать информацию о потоке в сегменте сети, подключенном к порту.

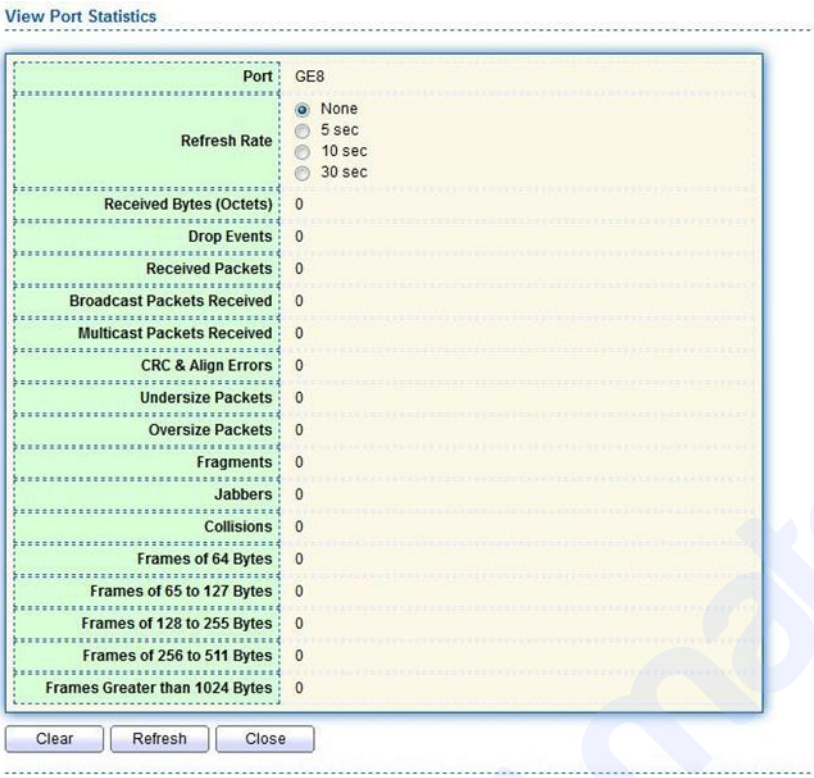
11.4.1 Port Statistics (Статистика мониторинга портов)

Информация в Statistics Table (Таблица статистики) отражает статистику мониторинга каждого порта на коммутаторе, а именно информацию, накопленную с начала создания группы. Статистика включает количество сетевых конфликтов, сообщения об ошибках CRC, широковещательные/многоадресные сообщения, полученные байты и сообщения и т. д. С помощью функций статистики и управления RMON можно отслеживать использование портов и возникшие ошибки.

Для просмотра статистики перейдите «Management > RMON > Statistics».



При необходимости, нажмите "Clear" (Очистить) или “Refresh” (Обновить) статистику выбранного порта. Нажмите «View» (Посмотреть) для просмотра подробной статистики выбранного порта.

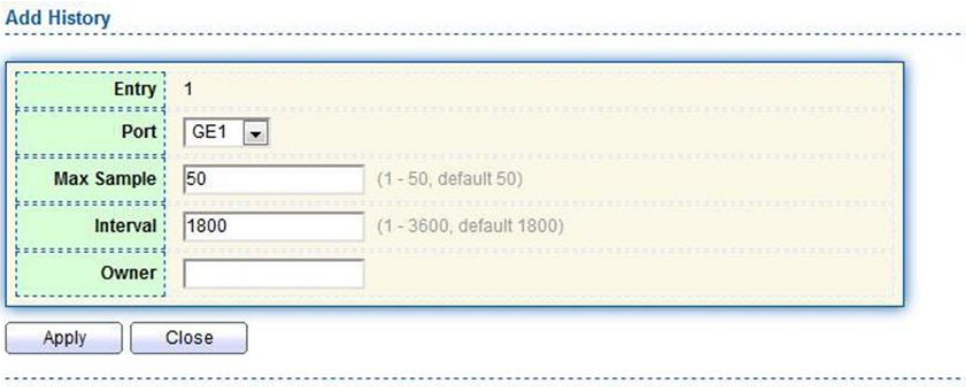


11.4.2 History Configuration (Настройки сохранения данных)

После настройки группы истории RMON коммутаторы будут периодически собирать и временно сохранять сетевую статистику для простоты обработки, предоставляя history (сохраненные) данные о потоках сегментов сети, пакетах ошибок, широковещательных пакетах, использовании пропускной способности и другую статистику. Управление history (сохраненными) данными можно использовать для настройки устройств с точки зрения сбора данных, включая периодический сбор и обслуживание данных указанных портов.

Для настройки сохранения данных перейдите «Management > SNMP > History». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.

Примечание:
Чтобы конфигурация RMON была эффективной, служба SNMP должна быть включена.



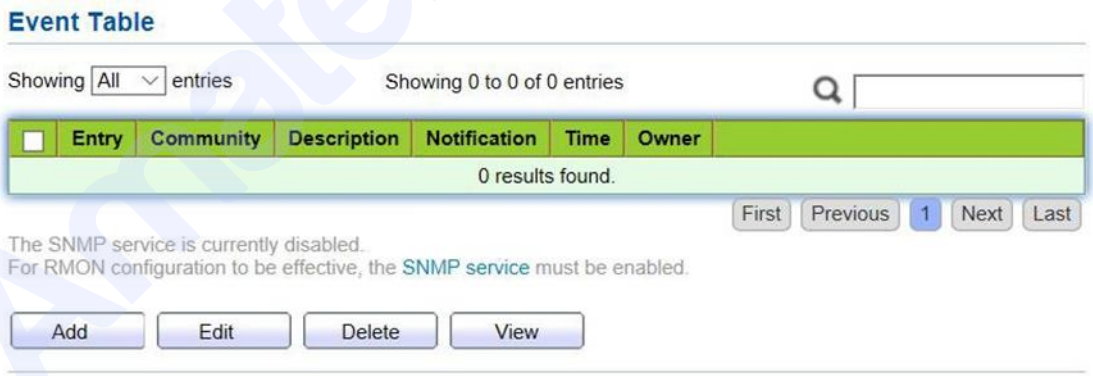
Настройки интерфейса

Параметр	Описание
Entry	Порядковый номер группы
Port	Порт для подсчета статистики
Max Sample	Максимальное количество выборок в диапазоне от 0 до 50, по умолчанию 50.
Interval	Интервал выборки от 1 до 3600с. По умолчанию 1800 секунд
Owner	Владелец

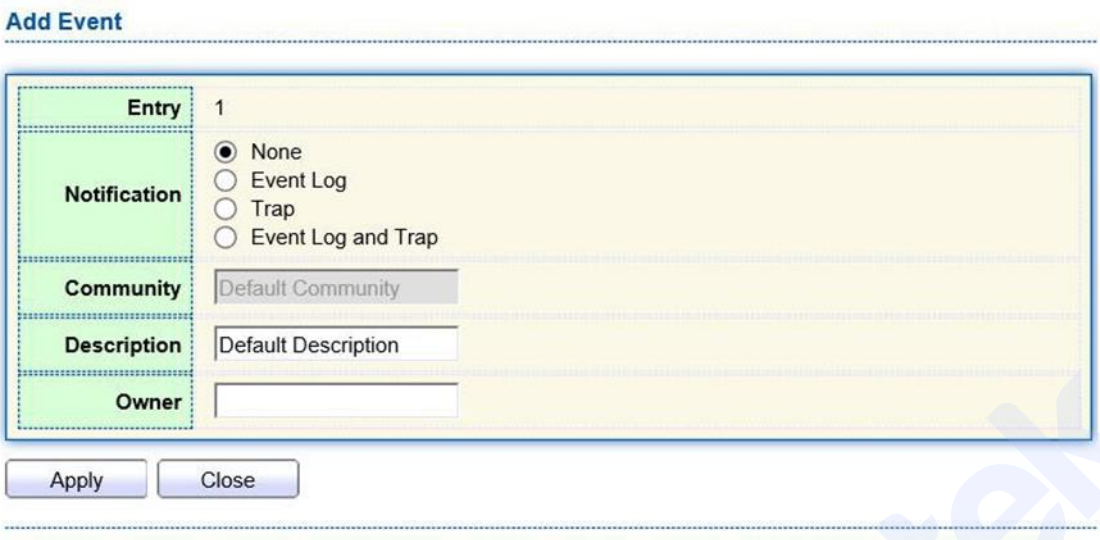
11.4.3 Event Configuration (Настройки групп событий)

Определяя номер события и способ обработки, группа событий в основном предназначена для событий, инициированных элементами конфигурации группы тревог и элементами конфигурации расширенной группы тревог. Имеется несколько вариантов уведомлений: запись в лог-таблицу; передача сообщения Trap в NMS; запись журнала и передача сообщения Trap; Don't care (не уведомлять).

Для настройки групп событий перейдите «Management > SNMP > Event». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.



Примечание:
Чтобы конфигурация RMON была эффективной, служба SNMP должна быть включена.



Настройки интерфейса

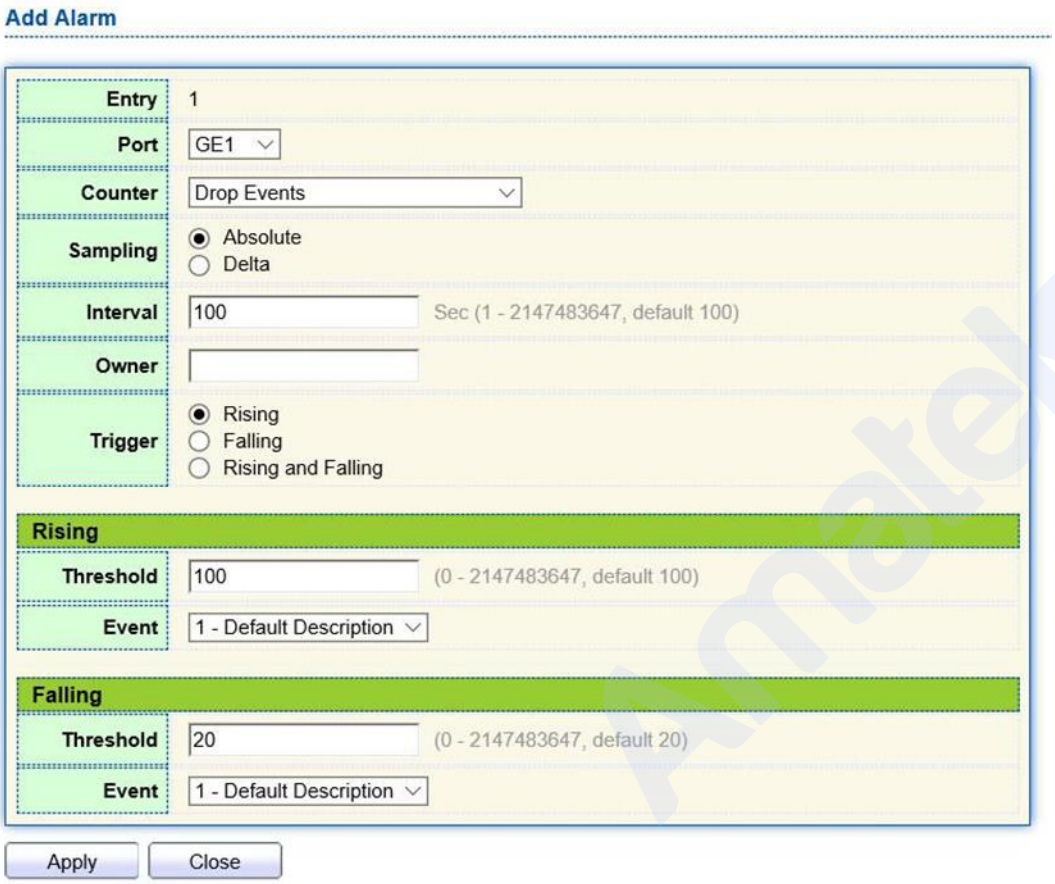
Параметр	Описание
Entry	Порядковый номер группы событий
Community	Сообщество
Description	Описание
Notification	Уведомление: None (не уведомлять), Event Log (запись в журнал событий); Trap (передача сообщения Trap в NMS); запись журнала и передача сообщения Trap;
Time	Время
Owner	Владелец

11.4.4 Alarm Configuration (Настройки групп тревог)

Управление тревожными сигналами RMON отслеживает определенные переменные аварийных сигналов, например, статистику портов. Тревожное событие возникает, когда значение контролируемых данных превышает определенный порог в соответствующем направлении, которое будет обрабатываться в соответствии с предписанным режимом обработки. Определение события реализовано в группе событий. Система будет действовать следующим образом после того, как пользователь определит запись тревоги: Переменная тревоги, определяемая временем выборки, должна быть определена, и значение должно быть сравнено с порогом. Для более высокого порога будет инициировано соответствующее событие.

Для настройки групп тревог перейдите «Management > SNMP > Alarm». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.

Примечание:
Чтобы конфигурация RMON была эффективной, служба SNMP должна быть включена.



Настройки интерфейса

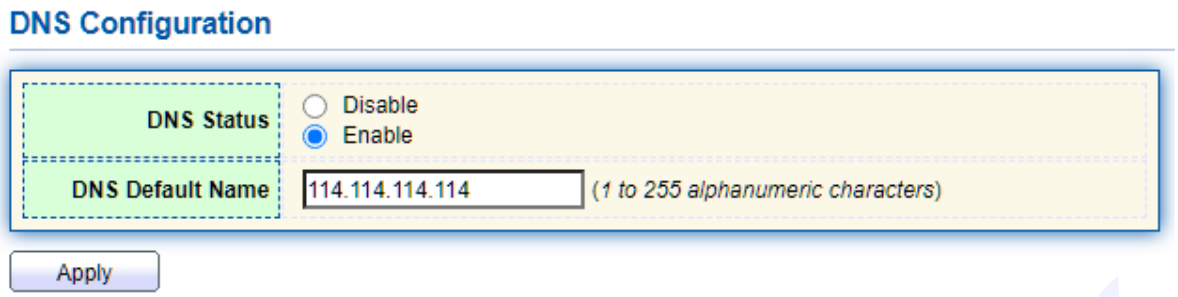
Параметр	Описание
Entry	Порядковый номер группы тревог
Port	Порт для подсчета статистики тревог
Counter	Типы параметров тревог
Interval	Интервал выборки в диапазоне от 1 до 2147483647, по умолчанию100
Sampling	Типы выборки: Absolute (Абсолютный) и Delta (Дельта)
Owner	Владелец
Threshold (Rising)	Порог превышения находится в диапазоне от 0 до 2147483647
Event (Rising)	Индекс группы событий. Соответствующее событие будет активировано при срабатывании тревоги
Threshold (Falling)	Порог снижения находится в диапазоне от 0 до 21474836475
Event (Falling)	Индекс группы событий. Соответствующее событие будет активировано при срабатывании тревоги

11.5 DNS Configuration (Настройки DNS)

DNS (Domain Name System «система доменных имён») - представляет собой распределенную базу данных, которая взаимно сопоставляет доменные имена и IP-адреса. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или сетевого устройства).

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

Для настройки протокола DNS перейдите «Network > DNS». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.



Описание интерфейса

Параметр	Описание
DNS Status	Включение DNS
DNS Default Name	Введите DNS-имя по умолчанию

11.6 System Time (Настройки системного времени)

Данный раздел меню используется для настройки системного времени и выбора источника точного времени (SNTP), перехода на летнее время и т. д.

Для настройки протокола DNS перейдите «Network > System Time». Задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.

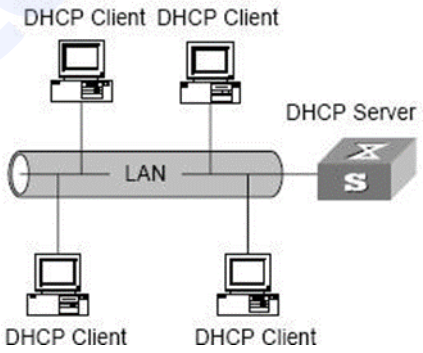
Настройки интерфейса

Параметр	Описание
Time Source	Выберите источник времени: SNTP, ПК или в ручном режиме
Time Zone	Часовой пояс
Address Type	Имя хоста или адрес IPv4 (с источником времени, заданным SNTP)
Server Address	Адрес сервера SNTP
Server Port No.	Номер порта сервера
Date	Дате: гггг/мм/дд (при установке в ручном режиме)
Time	Время: час/мин/сек (при установке в ручном режиме)
Type	Типы перехода на летнее время: «Нет», «циклический», «нециклический», «США» и «Европа».
Offset	Компенсированное время перехода на летнее время
Recurring	Настроить циклический режим летнего времени
Non- Recurring	Настроить нециклический режим летнего времени

12. DHCP (Настройки DHCP)

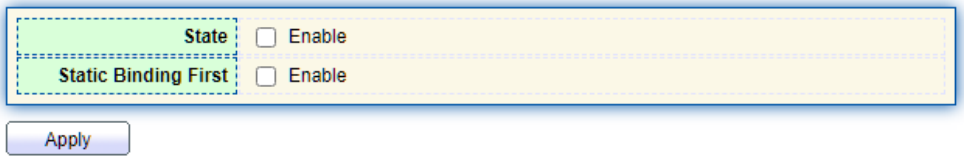
DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки узла) - прикладной протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок.

Типичное применение DHCP обычно включает DHCP сервер и несколько клиентов (например, ПК и ноутбук), как показано на рисунке ниже:

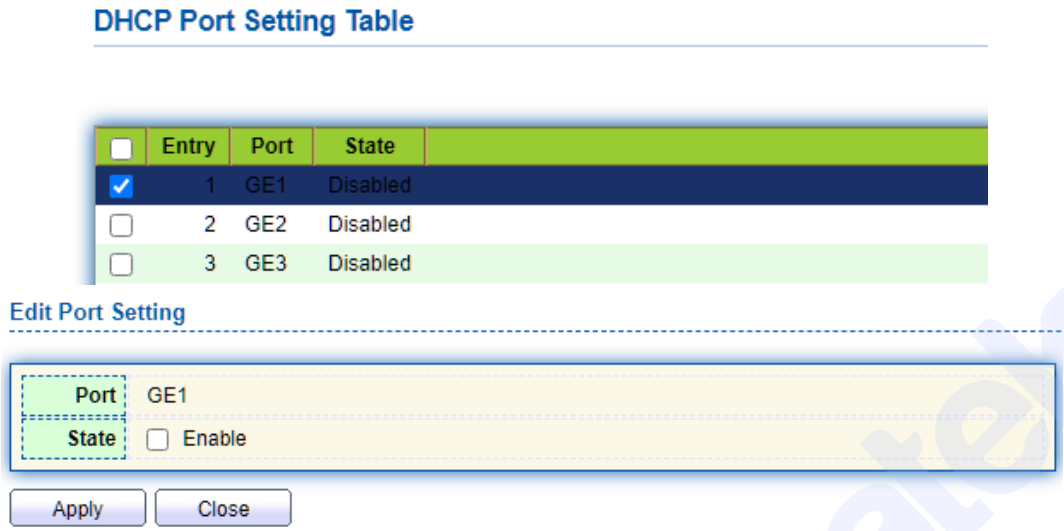


12.1 DHCP global configuration (Глобальные настройки DHCP)

1. Для настройки протокола DHCP перейдите «DHCP > Property». Задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.



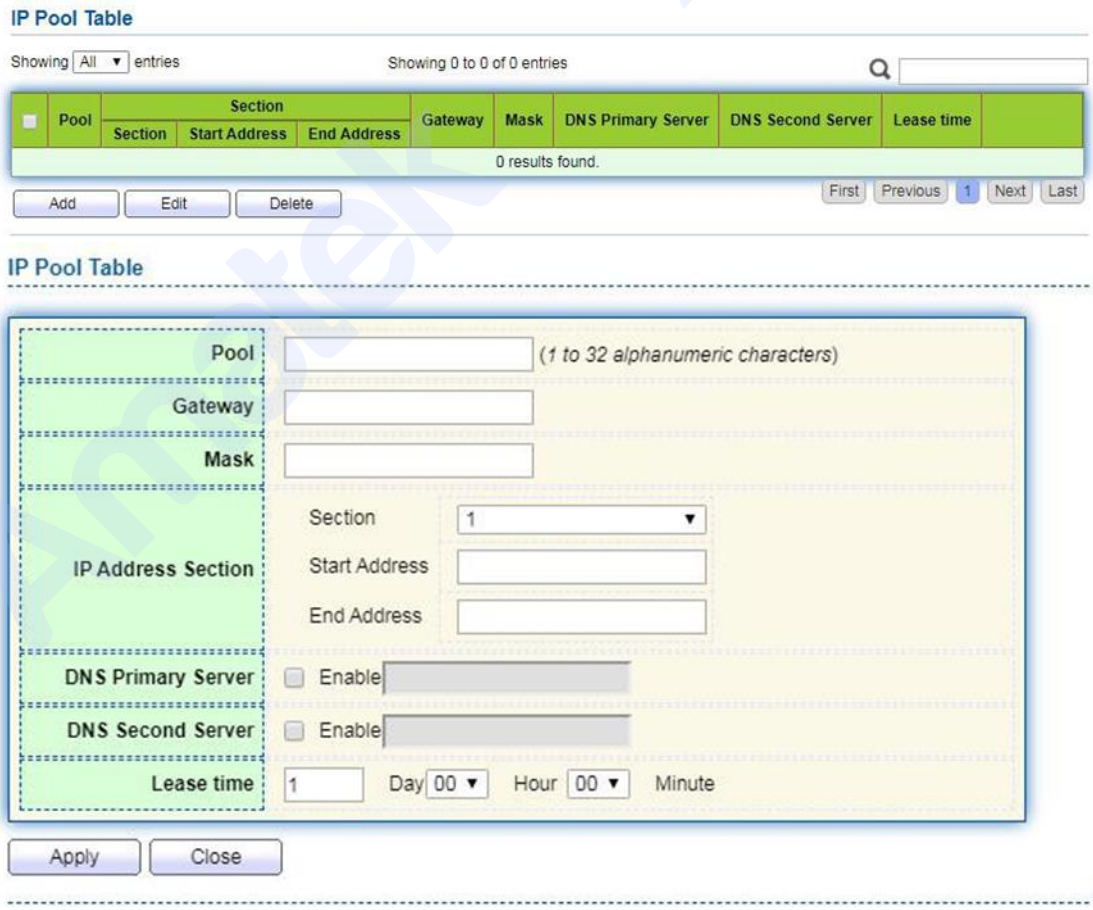
2. Выберите необходимый порт и нажмите «Edit». Включите DHCP для данного порта. Далее нажмите «Apply», чтобы сохранить изменения.



Примечание:
При включении режим DHCP-сервера, необходимо включить эту функцию для порта.

12.2 IP Pool Setting (Настройка пула IP-адресов)

Для настройки пула IP-адресов перейдите «DHCP > IP Pool Setting». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.



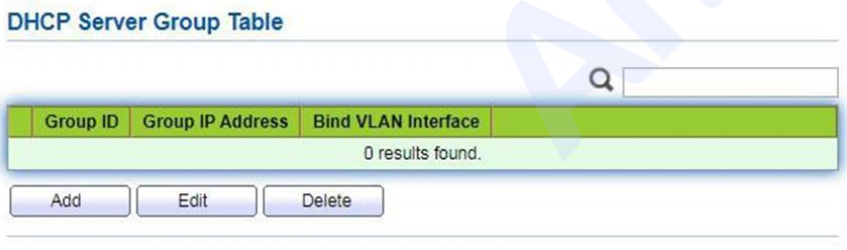
Настройки интерфейса

Параметр	Описание
Pool	Название пула IP-адресов
Gateway	Шлюз
Mask	Маска
IP Address Section	Раздел IP-адреса (до 8 разделов): начальный адрес и конечный адрес
DNS Primary Server	Основной DNS-сервер
DNS Second Server	Дополнительный DNS-сервер
Lease time	Время аренды

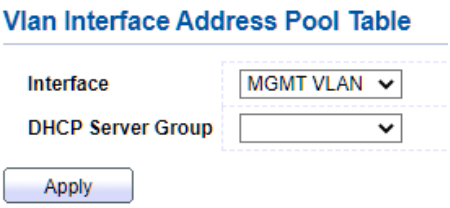
Примечание:
Начальный адрес и конечный адрес не могут содержать адрес шлюза.

12.2 Address Group Setting (Настройка VLAN IF Address Group)

1. Для настройки групп VLAN IF адресов перейдите «DHCP > VLAN IF Address Group Setting». Нажмите «Add», что настроить чтобы настроить группу DHCP серверов. Нажмите «Apply», чтобы сохранить изменения.

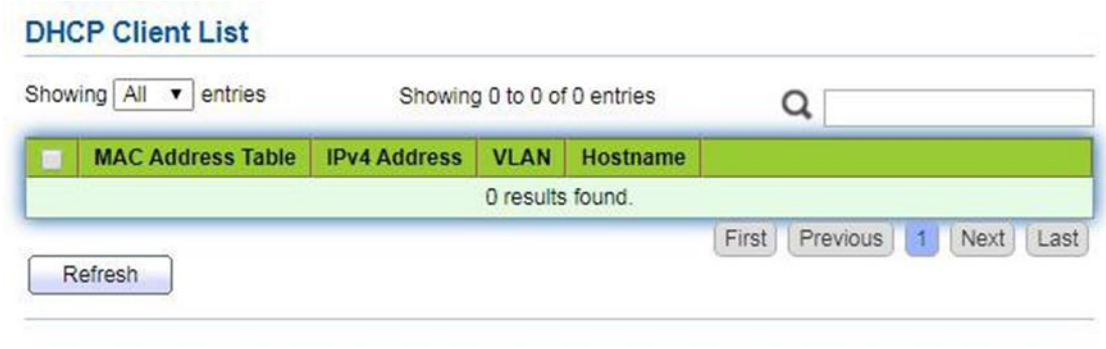


2. Далее выберите интерфейс и группу DHCP серверов. Нажмите «Apply», чтобы сохранить изменения.



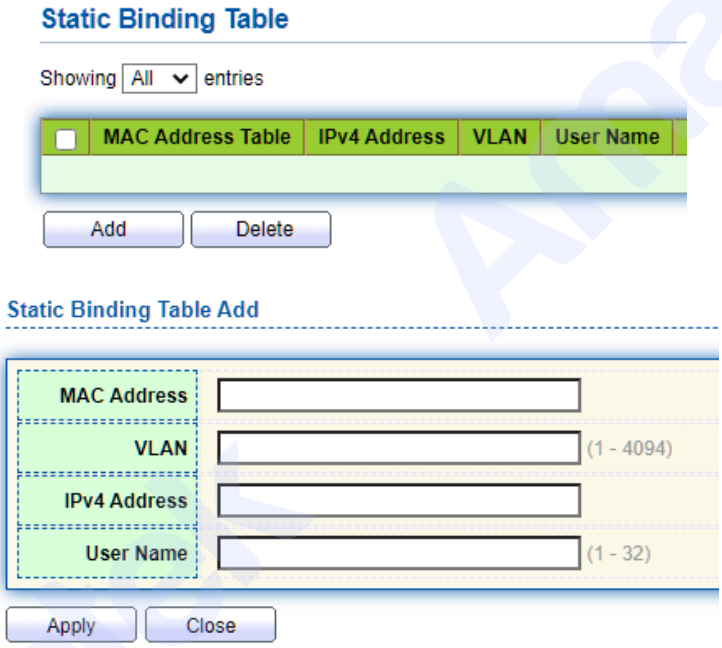
12.3 Client List (Информация о списке DHCP клиентов)

Для просмотра списка DHCP клиентов перейдите «DHCP > Client List». Нажмите «Refresh» для обновления информации.



12.3 Client Static Binding Table (Таблица статической привязки)

Для статической привязки DHCP клиентов перейдите «DHCP > Client Static Binding Table». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.



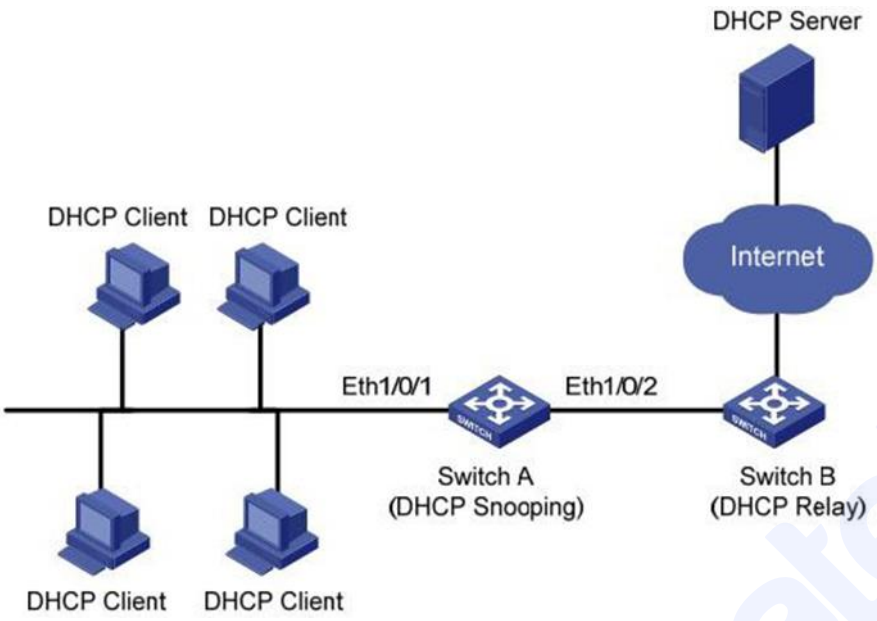
12.4 DHCP Snooping Configuration (Настройки DHCP Snooping)

DHCP snooping — функция коммутатора, предназначенная для защиты от атак с использованием протокола DHCP. Например, атаки с подменой DHCP-сервера в сети или атаки DHCP starvation, которая заставляет DHCP-сервер выдать все существующие на сервере адреса злоумышленнику.

Коммутатор может отслеживать сообщения DHCP и записывать IP-адрес пользователя с помощью DHCP Snooping на канальном уровне. Чтобы гарантировать, что пользователи получают IP-адреса через легальный DHCP-сервер, механизм безопасности DHCP Snooping делит порты на Trust Port (доверенные порты) и Untrust Port (ненадежные порты).

Trust порт прямо или косвенно подключается к легальному DHCP-серверу. Он перенаправляет полученные DHCP-сообщения, чтобы обеспечить правильный IP-адрес для DHCP-клиента. При атаке с подменой DHCP-сервера Untrust порты подключаются к нелегальному DHCP-серверу. Сообщения DHCPACK и DHCPOFFER, полученные от DHCP-сервера через Untrust порт, будут отбрасываться во избежание неправильных IP-адресов.

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

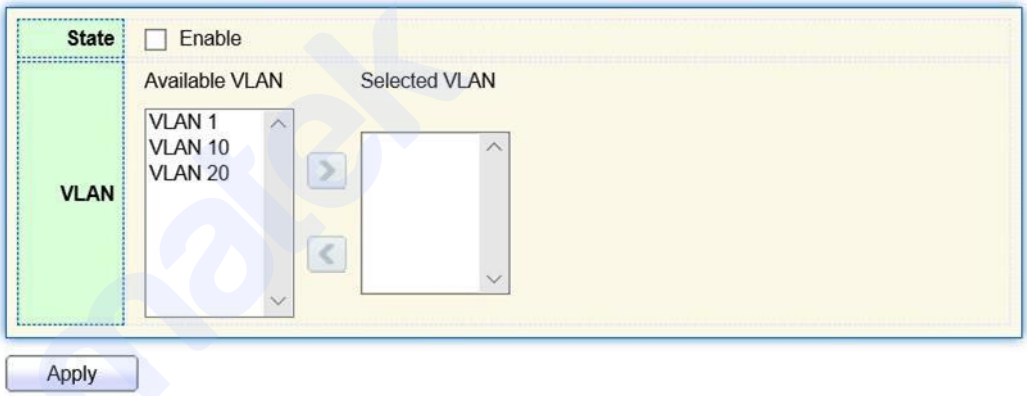


Для получения IP-адреса и MAC-адреса пользователя с DHCP-сервера используются следующие методы:

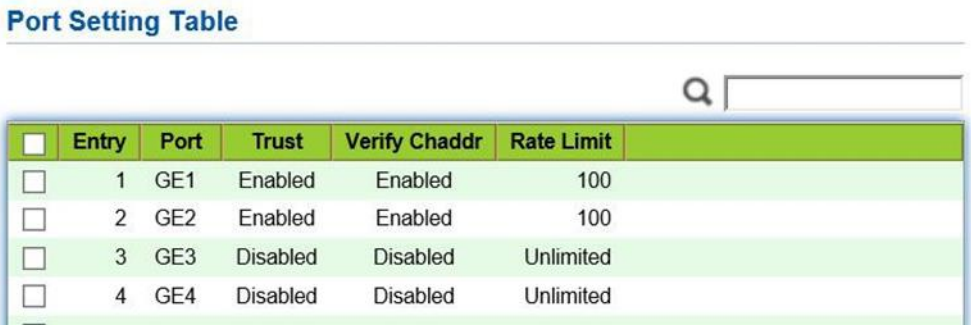
- Отслеживание сообщения DHCPREQUEST
- Отслеживание сообщения DHCPACK

12.4.1 DHCP Snooping Global Configuration (Основные настройки)

1. Для настройки глобальных параметров DHCP Snooping перейдите «Security > DHCP Snooping > Property». Включите функцию, выберите необходимые VLAN. Нажмите «Apply», чтобы сохранить изменения.



2. Далее отметьте необходимый порт и нажмите «Edit». Задайте параметры порта. Нажмите «Apply», чтобы сохранить изменения.



Entry	Port	Trust	Verify Chaddr	Rate Limit
1	GE1	Enabled	Enabled	100
2	GE2	Enabled	Enabled	100
3	GE3	Disabled	Disabled	Unlimited
4	GE4	Disabled	Disabled	Unlimited

Настройки интерфейса

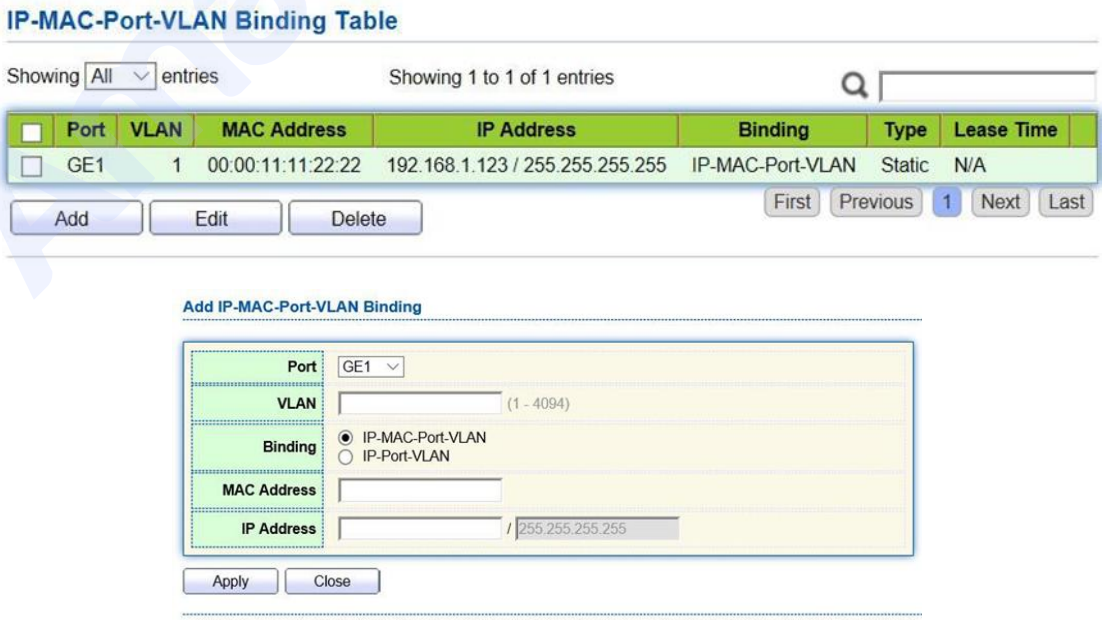
Параметр	Описание
State	Включить DHCP Snooping
VLAN	Номер действующей VLAN DHCP Snooping
Port	Номер порта DHCP Snooping
Trust	Назначение порта Trust (доверенным) портом
Verify Chaddr	Включение проверки непротиворечивости клиентских адресов
Rate Limit	Ограничение скорости порта от 1 до 300pps, 0 – без ограничения

12.4.2 IPMV Static Binding (Статическая привязка IPMV)

В DHCP сети пользователи, получающие статические IP-адреса, могут атаковать сеть, имитируя DHCP сервер, создавая сообщение запроса DHCP и т.п. Легальные пользователи DHCP могут пострадать от атаки с подменой DHCP-сервера.

Включение статических записей на основе привязки IPMV (IP адрес-MAC адрес-Порт - VLAN) или IPV (IP адрес-Порт-VLAN), сгенерированного таблицей привязки DHCP Snooping, может предотвратить такие атаки. Через порт могут проходить только сообщения, соответствующие исходному MAC-адресу и статическим MAC-адресам. Таким образом, для пользователей, не использующих DHCP, могут передаваться только сообщения статических записей MAC, настроенных администраторами вручную, а остальные будут отбрасываться.

Для настройки IPMV Static Binding перейдите «Security > IP Source Guard > IMPV Binding». Нажмите «Add» и задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.



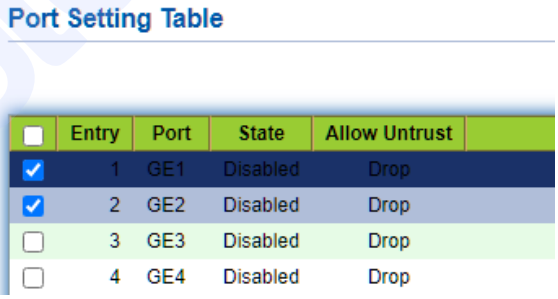
Настройки интерфейса

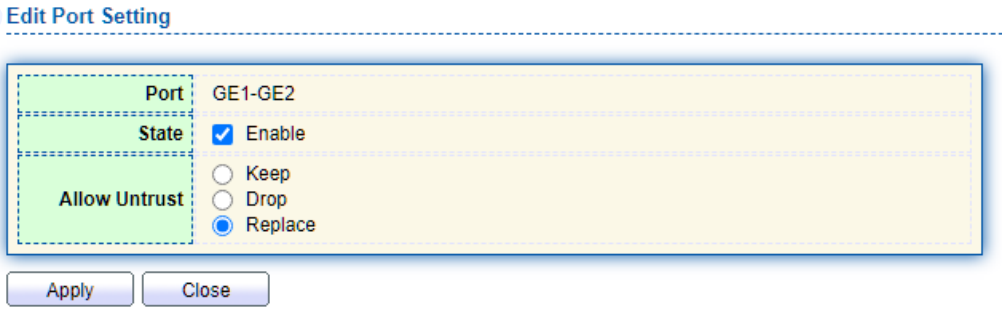
Параметр	Описание
Port	Номер порта группы привязки
VLAN	Привязка идентификатора VLAN
Binding	Выберите тип привязки из IPMV или IPV
MAC Address	Привязка MAC-адреса
IP Address	Привязка IP-адреса

12.4.3 DHCP Option82 Configuration (Настройка Option82)

Функция Option 82 служит для ретрансляции DHCP-сервера. Option 82 - это параметр информации агента ретрансляции в сообщениях DHCP, который записывает местоположение DHCP-клиента. Когда ретранслятор relay DHCP (или устройство DHCP Snooping) получает сообщение запроса, отправленное от DHCP-клиента на DHCP-сервер, администраторы могут добавить Option 82 для определения местонахождения DHCP-клиента и контроля безопасности. Создаются более гибкие подходы к распределению адресов серверами, поддерживающими Опцию 82, в соответствии с политиками распределения IP-адресов и других параметров. Благодаря ретранслятору DHCP клиент и сервер могут общаться, находясь в разных подсетях.

Для настройки параметров DHCP Option 82 перейдите «Security > DHCP Snooping > Option82 Property». Выберите необходимые порты и нажмите «Edit». Задайте параметры. Далее нажмите «Apply», чтобы сохранить изменения.





Настройки интерфейса

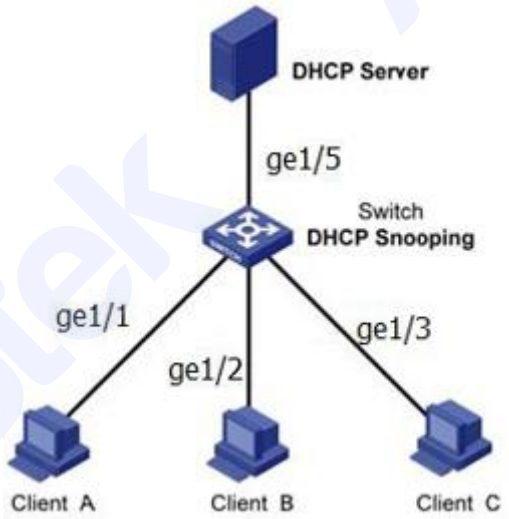
Параметр	Описание
Remote ID	Заполните поле Remote ID (например, «аааaa»)
Port	Номер порта для включения Option 82
Allow Untrust	Untrust Port обрабатывает сообщения с включенной Option 82: Keep - оставить опцию 82 в сообщении без изменений и переслать; Drop - удалить сообщение; Replace - заменить и переслать поле Option 82 в сообщении в соответствии с конфигурацией Circuit ID.

Примечания:

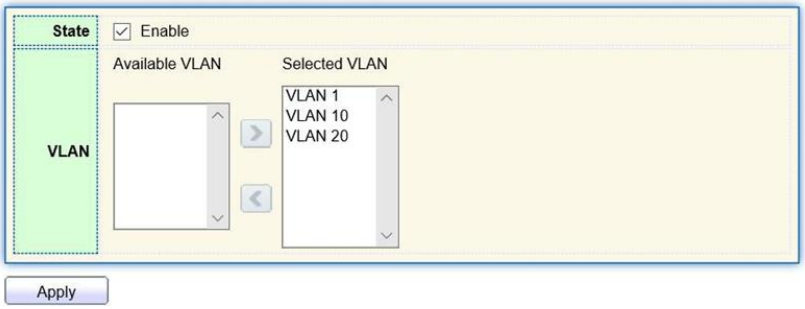
1. Option 82 независимо настраивает подпараметры Circuit ID или Remote ID. Их можно настроить индивидуально или одновременно в произвольном порядке.
2. Параметр DHCP Option 82 должен быть настроен, иначе сообщения DHCP, отправляемые на DHCP-сервер, не будут содержать параметр Option 82.
3. При получении ответного сообщения DHCP от DHCP-сервера сообщение, содержащее параметр Option 82, будет переадресовано после удаления поля или перенаправлено напрямую, если сообщение не содержит Option 82.

12.4.4 Пример настройки DHCP Option82

Как показано ниже, порт коммутатора GE1/5 подключен к DHCP-серверу, а порты GE1/1, GE1/2 и GE1/3 подключены к DHCP-клиентам A, B и C соответственно.



1. Включите DHCP Snooping на коммутаторе. Нажмите «Security > DHCP Snooping > Property» в дереве навигации, чтобы включить функцию следующим образом:



2. Установите GE1-5 в качестве доверенного порта DHCP Snooping: выберите порт 5, нажмите «Edit» и заполните соответствующие параметры следующим образом:

Port Setting Table

Entry	Port	Trust	Verify Chaddr	Rate Limit
1	GE1	Disabled	Disabled	Unlimited
2	GE2	Disabled	Disabled	Unlimited
3	GE3	Disabled	Disabled	Unlimited
4	GE4	Disabled	Disabled	Unlimited
5	GE5	Enabled	Disabled	Unlimited
6	GE6	Disabled	Disabled	Unlimited

3. Настройте порт GE1/3 таким образом, чтобы определяемый пользователем remote ID можно было установить с помощью Option 82. Перейдите «Security > DHCP Snooping > Option82 Property» и настройте порт GE1/3. Далее нажмите «Apply», чтобы сохранить изменения.

Remote ID: ☑ User Defined aaaaa

Operational Status

Remote ID: aaaaa

Apply

Port Setting Table

Entry	Port	State	Allow Untrust
1	GE1	Disabled	Drop
2	GE2	Disabled	Drop
3	GE3	Enabled	Replace
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop

4. Настройте порт GE1/3, чтобы Circuit ID можно было установить с помощью Option 82. Перейдите «Security > DHCP Snooping > Option82 Circuit ID», чтобы настроить порт. Далее нажмите «Apply», чтобы сохранить изменения.

Option82 Circuit ID Table

Showing All entries Showing 1 to 1 of 1 entries

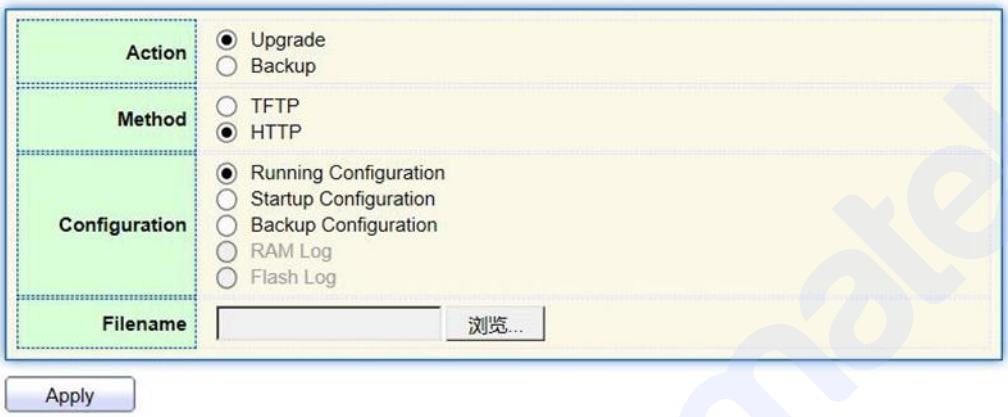
Port	VLAN	Circuit ID
GE3	1	ge1/3

Add Edit Delete First Previous 1 Next Last

13. System Maintenance (Обслуживание системы)

13.1 Configuration Management (Управление конфигурацией)

Для обновления или резервного копирования конфигурации перейдите «Management > Configuration > Manual Upgrade». Выберите Upgrade (обновление) или Backup (резервное копирование). Задайте параметры. Укажите файл конфигурации для обновления или копирования. Далее нажмите «Apply», чтобы сохранить изменения.



13.2 Configuration Saving (Сохранение конфигурации)

Для сохранения конфигурации или восстановления заводских настроек перейдите «Management > Configuration > Save Configuration». Выберите исходный (Source) и целевой (Destination) файлы конфигурации для сохранения. Далее нажмите «Apply», чтобы сохранить изменения.

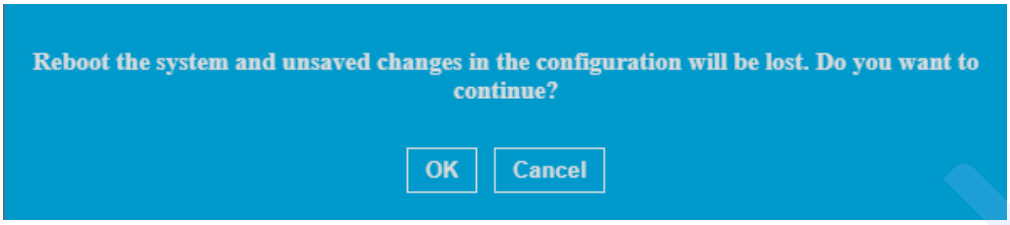
Для восстановления заводских настроек нажмите «Restore Factory Default». Далее нажмите «OK» для подтверждения.

Примечания:

1. После восстановления заводских настроек нажмите «Reboot» для перезагрузки коммутатора с заводскими настройками.
2. Сохраните «Running Configuration» (Рабочую конфигурацию) как «Startup Configuration» (Начальную конфигурацию) и/или «Backup Configuration» (Резервную конфигурацию).
3. Нажмите «Save» в правом верхнем углу, чтобы сохранить текущую конфигурацию в качестве начальной конфигурации.

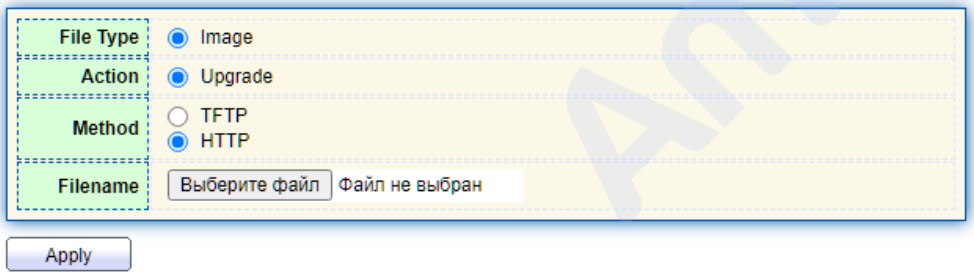
13.3 Device Restart (Перезагрузка коммутатора)

Для перезагрузки устройства нажмите «Reboot» в правом верхнем углу. Далее нажмите «OK» для подтверждения.



13.4 Firmware Management (Обновление прошивки)

Для обновления прошивки перейдите «Management > Firmware > Manual Upgrade». Укажите файл прошивки для обновления в поле «File name». Далее нажмите «Apply», чтобы сохранить изменения.



Приложение 1. Технические характеристики

Модель	**AN-SM28P24**
Общее количество портов	28
Количество портов 10/100/1000Мбит/с +PoE	24
Количество портов Gigabit Combo (RJ45+SFP)	4
Коммуникации	10Base-T: 2 пары кат. 5 (Cat5e) и выше UTP/STP (≤100м); 100Base-TX: 2 пары кат. 5 (Cat5e) и выше UTP/STP (≤100м); 1000Base-TX: 4 пары кат. 5 (Cat5e) и выше UTP/STP (≤100м); Multi-mode Fiber: 50/125, 62.5/125, 100/140um; Single-mode Fiber: 8/125, 8.7/125, 9/125, 10/125um;
Макс. суммарная мощность (бюджет) PoE	400Вт
Макс. мощность PoE на один порт	30Вт
Стандарт PoE	IEEE 802.3af, IEEE 802.3at
Метод PoE	1,2 (+), 3,6 (-), метод A
Скорость пересылки пакетов	41.66Mpps
Пропускная способность	56Гбит/с
Таблица MAC адресов	8K
Управление функциями	WEB-интерфейс, CLI, Telnet, консольный порт (RJ45)
Поддерживаемые стандарты и протоколы	IEEE802.3i (10BASE-T), IEEE802.3u (100BASE-TX), TIA/EIA-785 (100Base-SX), IEEE802.3ab (1000BASE-T), IEEE802.3z (1000Base-LX), IEEE802.3z (1000Base-SX), IEEE802.3x (Flow Control), IEEE802.1d (STP), IEEE802.1s (MSTP), IEEE802.1w (RSTP), IEEE802.1Q (VLAN), IEEE802.3ad (LACP), 802.1x, RFC3619 (EAPS), RFC2236 (IGMPv2), RFC3376 (IGMPv3), RFC2710 (MLDv1), RFC3810 (MLDv2), RFC826 (ARP), RFC791 (IPV4), RFC8200 (IPV6), RFC854 (Telnet), RFC793 (TCP), RFC768 (UDP), RFC792 (ICMP), RFC2131 (DHCP), DNS, RFC1350 (TFTP), HTTP, RFC2818 (HTTPS), RFC5321 (SMTP), UDLD, IEEE802.3ab (LLDP), IEEE802.3af (PoE), IEEE802.3at (PoE+), RFC2819 (RMON)
Дополнительные функции	SNTP, DHCP Option82, DHCP Snooping, DHCP Server, IGMP Snooping V2/V3, MLD Snooping V1/V2, RMON, IPV4, IPV6, контроль ARP запросов (Dynamic ARP inspection)
Настройка и обновление	Импорт/экспорт файла конфигурации, Обновление прошивки через WEB-интерфейс, Создание/удаление учетных записей
Индикация	Link/Activity, PoE, SYS (состояние системы), PWR (питание)
Питание	AC 110-264В, 50/60Гц
Потребляемая мощность (без нагрузки PoE)	<15Вт
Схема охлаждения	Fanless Design – безвентиляторная
Диапазон рабочей температуры	-20°C …+50°C
Диапазон температуры хранения	-40°C …+80°C
Максимальная относительная влажность	RH90% без конденсата
Размеры (ШхГхВ)	440x280x44мм
Способ монтажа	Настольный / монтаж в 19” стойку крепежными элементами

Примечание: Дизайн, технические характеристики и комплектация изделия могут изменяться без предварительного уведомления.

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

Приложение 2. Гарантийные обязательства

Изготовлено в Китае

На данное изделие установлен гарантийный период 24 месяцев с даты продажи, но не более 36 месяцев с даты изготовления (дата изготовления указана в серийном номере на корпусе устройства).

Срок службы изделия составляет 5 лет.

По истечении гарантийного срока изделия мы рекомендуем обратиться в Сервисный центр «AMATEK» для проведения профилактических работ и получения рекомендаций по дальнейшей безопасной эксплуатации изделия.

П.1 Адрес сервисного центра

194100, Россия, Санкт-Петербург,

ул. Литовская, д.10

Тел. 8-800-707-10-40 (звонок по России бесплатный)

Эл. почта: remont@amatek.su

Мы настоятельно рекомендуем обращаться в сервисный центр, если у Вас возникнут какие-либо проблемы, связанные с эксплуатацией и работоспособностью изделия.

Гарантийный талон действителен только при наличии правильно и четко указанных: модели, серийного номера изделия, даты продажи, четких печатей фирмы-продавца, подписи покупателя. Модель и серийный номер изделия должны соответствовать указанным в гарантийном талоне.

Продавец подтверждает принятие на себя обязательства по удовлетворению требований потребителей, установленных действующим законодательством о защите прав потребителей, в случае обнаружения недостатков изделия, возникших по вине производителя. Продавец оставляет за собой право отказать в удовлетворении требований потребителей по гарантийным обязательствам и в бесплатном сервисном обслуживании изделия в случае несоблюдения изложенных ниже условий. Гарантийные обязательства и бесплатное сервисное обслуживание осуществляются в соответствии с требованиями законодательства РФ.

П.2 Условия выполнения гарантийных обязательств

- Под бесплатным гарантийным обслуживанием понимается дополнительное обязательство продавца по устранению недостатков (дефектов) изделия, возникших по вине производителя, без взимания платы с покупателя (потребителя). Бесплатное гарантийное обслуживание оборудования производится при условии квалифицированной установки и эксплуатации изделия.

- Замена в изделии неисправных частей (деталей, узлов, сборочных единиц) в период гарантийного срока не ведет к установлению нового гарантийного срока, как на само изделие, так и на замененные части.

- Гарантийные обязательства не распространяются на следующие принадлежности, входящие в комплектность товара: пульты дистанционного управления, элементы питания (батарейки), соединительные кабели, носители информации различных типов (диски с программным обеспечением и драйверами, карты памяти), внешние устройства ввода-вывода и манипуляторы, монтажные приспособления, инструмент, крепеж,

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

документацию, прилагаемую к изделию, на программное обеспечение (ПО) и драйверы, поставляемые в комплекте с изделием на носителях информации раз личных типов, а также на необходимость переустановки и настройки ПО, за исключением случаев, когда данная необходимость вызвана недостатком изделия, возникшим по вине изготовителя.

- Продавец не несет гарантийных обязательств в следующих случаях:

  (1) Изделие, использовалось в целях, не соответствующих его прямому назначению;

  (2) Нарушены правила и условия эксплуатации, установки изделия, изложенные в данном руководстве и другой документации, передаваемой потребителю в комплекте с изделием;

  (3) Изделие имеет следы попыток неквалифицированного ремонта;

  (4) Обнаружено повреждение гарантийных этикеток или пломб (если таковые имеются);

  (5) Дефект вызван изменением конструкции или схемы изделия, подключением внешних устройств, не предусмотренных изготовителем;

  (6) Дефект вызван действием непреодолимых сил, несчастными случаями, умышленными или неосторожными действиями потребителя или третьих лиц;

  (7) Обнаружены механические повреждения и/или повреждения, вызванные воздействием влаги, высоких или низких температур, коррозией, окислением, попаданием внутрь изделия посторонних предметов, веществ, жидкостей, насекомых или животных, независимо от их природы;

  (8) Повреждения (недостатки) вызваны сменой или удалением паролей изделия, модификацией и/или переустановкой предустановленного ПО изделия, установкой и использованием несовместимого ПО третьих производителей (неоригинального);

  (9) Дефект возник вследствие естественного износа при эксплуатации изделия. При этом под естественным износом понимаются последствия эксплуатации изделия, вызвавшие ухудшение их технического состояния и внешнего вида из-за длительного использования данного изделия;

  (10) Повреждения (недостатки) вызваны несоответствием стандартам или техническим регламентам питающих, кабельных, телекоммуникационных сетей, мощностей сигналов;

  (11) Повреждения вызваны использованием нестандартных (неоригинальных) и/или некачественных (поврежденных) принадлежностей, источников питания, запасных частей, элементов питания, носителей информации различных типов (включая, но, не ограничиваясь DVD дисками, картами памяти, флэш-накопителями).

- Настройка и установка (сборка, подключение и т.п.) изделия, описанные в данном руководстве, должны быть выполнены квалифицированным персоналом или специалистами Сервисного центра. При этом лицо (организация), установившее изделие, несет ответственность за правильность и качество установки (настройки).

- В случае необоснованной претензии, стоимость работ по проверке изделия взымается с покупателя в соответствии с прейскурантом продавца.

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

- Продавец не несет ответственности за возможный вред, прямо или косвенно нанесенный изделием людям, животным, имуществу в случае, если это произошло в результате несоблюдения правил и условий эксплуатации, установки изделия; умышленных или неосторожных действий потребителя или третьих лиц.
- Продавец не несет ответственность за возможный вред, прямо или косвенно нанесенный изделием, в результате потери, повреждения или изменения данных и информации.

Amatek
Amatek

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