Серия ES-2024

Коммутатор Ethernet

Руководство пользователя

Версия 3.80
6/2007
Редакция 1

ПАРАМЕТРЫ ВХОДА ПО УМОЛЧАНИЮ	
IP-адрес	**http://192.168.1.1**
Имя пользователя	**admin**
Пароль	**1234**

ZyXEL

www.zyxel.com

Сведения об этом руководстве пользователя

Целевая аудитория

Данное руководство предназначено для пользователей, занимающихся настройкой ES-2024 с использованием Web-конфигуратора. Читатель должен быть знаком как минимум на базовом уровне с основными понятиями и топологией сетей TCP/IP.

Дополнительная документация

- Краткое руководство по началу работы

  В кратком руководстве по началу работы приводится информация о настройке аппаратного обеспечения.
- Онлайновая справка Web-конфигуратора

  Встроенная Web-справка содержит описания отдельных экранов и дополнительную информацию.
- Справочное руководство по интерфейсу командной строки

  Справочное руководство по интерфейсу командной строки предназначено для пользователей, занимающихся настройкой ES-2024 с использованием команд.

Для настройки коммутатора предпочтительнее использовать Web-конфигуратор.

- Вспомогательный диск

  Дополнительную документацию можно найти на прилагаемом компакт-диске.
- Web-сайт ZyXEL

  Дополнительную документацию и сертификаты изделий можно найти на сайте www.zyxel.com.

Отзывы по руководству пользователя

Помогая нам, вы помогаете себе. Свои замечания, вопросы или предложения по улучшению любых руководств пользователя просьба направлять по следующему почтовому адресу или адресу электронной почты. Спасибо!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Тайвань.

E-mail: techwriters@zyxel.com.tw

Условные обозначения

Предупреждения и примечания

Предупреждения и примечания выделяются в данном руководстве пользователя следующим образом.

В предупреждениях приводится информация о ситуациях, которые могут причинить вред пользователю или устройству.

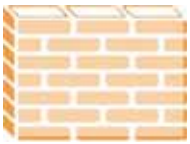
В примечаниях приводится важная информация (например, дополнительные требования по настройке или полезные советы) или рекомендации.

Обозначения

- Коммутаторы ES-2024A и ES-2024PWR могут называться в данном руководстве пользователя как «ES-2024», «коммутатор», «устройство», «система» или «продукт». Различия отмечаются по мере необходимости.
- Обозначения продукта, наименования экранов, метки полей и варианты выбора приводятся **полужирным** шрифтом.
- Нажимаемые клавиши заключаются в квадратные скобки и записываются заглавными буквами, например, [ENTER] означает клавишу «Enter» или «возврат каретки» на клавиатуре.
- «Ввести» означает набрать один или несколько символов с последующим нажатием клавиши [ENTER]. «Выбрать» означает, что необходимо выбрать один из предложенных вариантов.
- Для ключевых слов команд используется шрифт `courier new`.
- Правая угловая скобка (>) при перечислении имен экранов обозначает нажатие мыши. Например, **Maintenance > Log > Log Setting** означает, что добраться до соответствующего экрана можно последовательным нажатием на **Maintenance** в навигационной панели, **Log** в подменю и, наконец, на вкладке **Log Setting**.
- Стрелка (`-->`) указывает, что данная строка является продолжением предыдущей строки.
- В качестве единиц измерения могут использоваться «метрические» значения или «научные» значения. Например, «к» для «кило» может обозначать «1000» или «1024», «М» для «мега» может обозначать «1000000» или «1048576» и т.д.
- Сокращение «т.к.» означает «так как», «т.е.» означает «то есть» или «иными словами».

Значки на рисунках

На рисунках в данном руководстве пользователя могут использоваться следующие общие значки. Значок коммутатора не является точным изображением устройства.

Коммутатор 	Компьютер 	Ноутбук 
Сервер 	DSLAM-мультиплексор 	Межсетевой экран 
Телефон 	Коммутатор 	Маршрутизатор 

Предупреждения по безопасности

В целях вашей безопасности внимательно прочитайте и следуйте всем предупреждениям и указаниям.

- НЕ используйте данный продукт вблизи воды, например, в сыром подвале или неподалеку от плавательного бассейна.
- НЕ подвергайте устройство воздействию сырости, пыли или агрессивных жидкостей.
- НЕ кладите ничего поверх устройства.
- НЕ занимайтесь установкой, обслуживанием и не эксплуатируйте устройство во время грозы. Существует опасность поражения электрическим током в результате удара молнии.
- К устройству разрешается подключать ТОЛЬКО подходящие дополнительные модули.
- НЕ открывайте устройство. В результате вскрытия или снятия защитных кожухов вы подвергаете себя опасности прикосновения к оголенным токоведущим участкам с опасным высоким напряжением и иным рискам. Обслуживать или разбирать данное устройство разрешается ТОЛЬКО квалифицированному сервисному персоналу. Для получения дополнительной информации свяжитесь с поставщиком.
- Убедитесь, что кабели подключены к нужным портам.
- Аккуратно расположите соединительные кабели так, чтобы никто не мог наступить или споткнуться о них.
- Перед обслуживанием или разборкой обязательно отсоедините все кабели от устройства.
- Используйте с устройством ТОЛЬКО подходящий адаптер питания или шнур питания. Подключайте его к источнику питания с требуемым номиналом напряжения (например, 110 В перем. тока в Северной Америке или 230 В перем. тока в Европе).
- НЕ кладите ничего на адаптер питания или шнур питания и НЕ располагайте продукт в таком месте, где кто-нибудь может наступить на адаптер питания или шнур питания.
- НЕ используйте устройство, если адаптер питания или шнур повреждены, так как в этом случае существует опасность поражения электрическим током.
- Если адаптер питания или шнур питания повреждены, отсоедините их от устройства и от сети питания.
- НЕ пытайтесь отремонтировать адаптер питания или шнур питания. Обратитесь к местному поставщику и закажите новый.

- Не используйте устройство вне помещений; все соединения также должны проходить внутри помещений. Существует опасность поражения электрическим током в результате удара молнии.
- ВНИМАНИЕ: В СЛУЧАЕ УСТАНОВКИ БАТАРЕИ НЕПРАВИЛЬНОГО ТИПА (на материнской плате) СУЩЕСТВУЕТ ОПАСНОСТЬ ВЗРЫВА. СОБЛЮДАЙТЕ УКАЗАНИЯ ПО УТИЛИЗАЦИИ ИСПОЛЬЗОВАННЫХ БАТАРЕЙ. Сдавайте использованные батареи в пункты утилизации электрических и электронных компонентов. Подробную информацию об утилизации данного изделия можно получить в местном муниципалитете, службе утилизации бытовых отходов или в магазине, где оно было приобретено.
- НЕ заслоняйте вентиляционные отверстия устройства, так как ограниченный приток воздуха может послужить причиной повреждения устройства.
- Устройства, поддерживающие подачу или получение питания по витой паре (PoE), а также подключенные к ним кабели Ethernet должны располагаться целиком внутри помещений.

Данное изделие подлежит утилизации. Соблюдайте надлежащие требования по утилизации.

Обзор содержания

Содержание

Перечень рисунков

Перечень таблиц

Часть I
Введение

1

Знакомство с коммутатором

В этой главе описаны основные характеристики и способы применения коммутатора.

1.1 Введение

Данный автономный коммутатор Ethernet второго уровня оснащен 24 портами 10/100 Мбит/с и двумя портами Gigabit Ethernet/mini-GBIC. Модель ES-2024PWR поддерживает функцию питания устройств по витой паре (PoE).

Управлять и настраивать коммутатор можно с помощью встроенного Web-конфигуратора. Кроме того, коммутатор поддерживает управление через Telnet, SSH (Secure SHell), любую программу-эмулятор терминала с подключением через консольный порт, а также с помощью приложений на основе простого протокола сетевого управления (SNMP) от сторонних производителей.

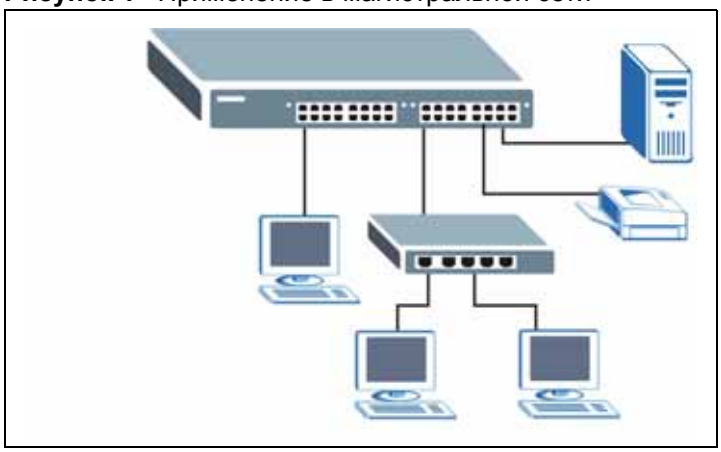
Полный перечень функций программного обеспечения, доступных на коммутаторе, можно найти в прил. A на стр. 265.

1.1.1 Применение в магистральной сети

В данной конфигурации коммутатор является идеальным решением для малых сетей, которые ожидают стремительного роста в ближайшем будущем. Данный коммутатор может использоваться автономно для группы активных пользователей. К портам коммутатора можно подключать компьютеры или другие коммутаторы.

В этом примере все компьютеры могут совместно использовать высокоскоростные приложения на сервере. Для расширения сети достаточно просто добавить другие сетевые устройства, например, коммутаторы, маршрутизаторы, компьютеры, принт-серверы и т.д.

Рисунок 1 Применение в магистральной сети

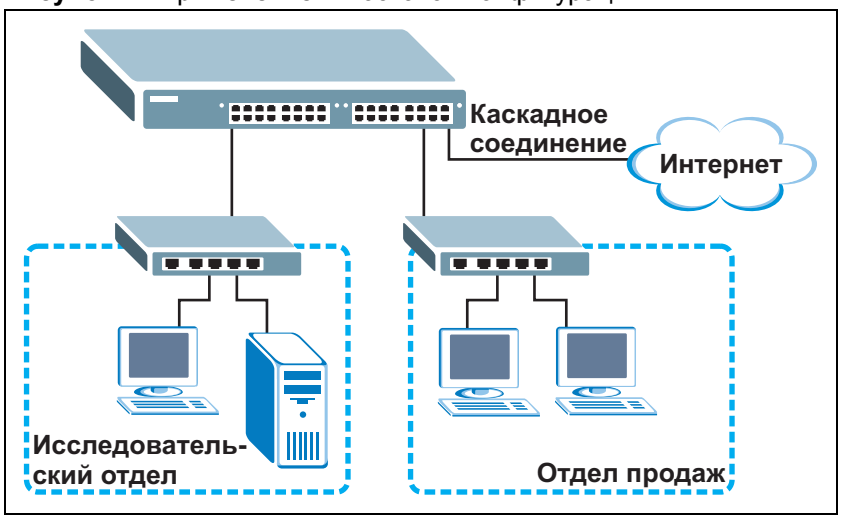


1.1.2 Пример мостовой конфигурации

В этом примере коммутатор соединяет различные отделы компании (**Исследовательский отдел** и **Отдел продаж**) с корпоративной магистралью. Это позволяет уменьшить «состязание» за пропускную способность и устранить «узкие места» в сети и подключении к серверу. Все пользователи, которым требуется большая пропускная способность, могут подключаться к высокоскоростным серверам своих отделов через коммутатор. Использование порта Gigabit Ethernet/mini-GBIC коммутатора позволяет обеспечить высокоскоростной канал для каскадного соединения.

Кроме того, коммутатор облегчает задачи контроля и обслуживания, позволяя сетевым администраторам централизованно расположить несколько серверов.

Рисунок 2 Применение в мостовой конфигурации

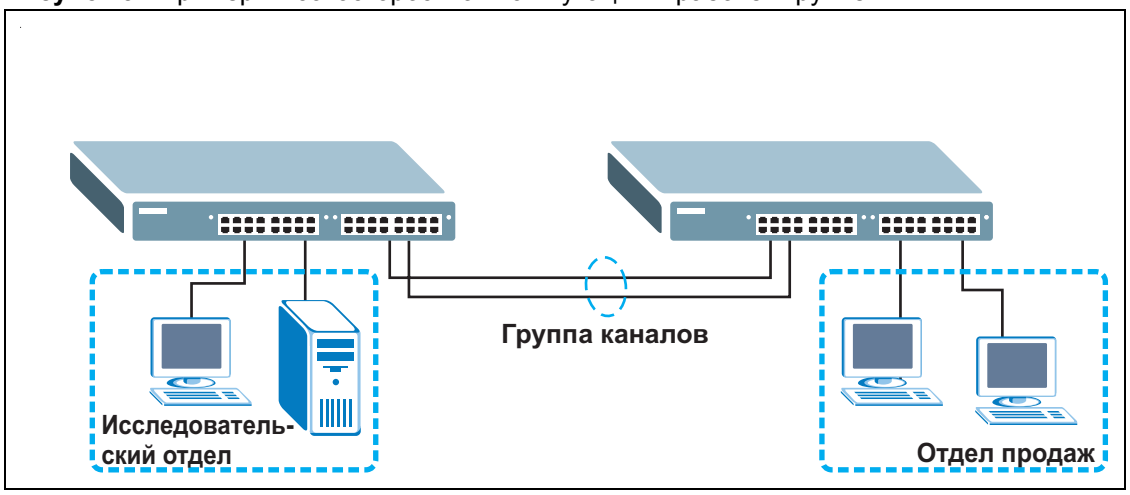


1.1.3 Пример высокоскоростной коммутации

Данный коммутатор идеально подходит для соединения двух сетей, которым требуется высокая пропускная способность. В приведенном примере для соединения этих двух сетей используется группирование портов.

Переход на высокоскоростные локальные сети, например, работающие по технологии ATM, для большинства пользователей нецелесообразен из-за высокой стоимости замены всех имеющихся Ethernet-кабелей и карт адаптеров, реструктуризации сети и сложности технического обслуживания. Данный коммутатор позволяет добиться такой же пропускной способности, как и в сети ATM, но при существенно меньших затратах и с возможностью использования имеющихся адаптеров и коммутаторов. Более того, сохраняется существующая структура локальной сети, так как все порты могут свободно связываться друг с другом.

Рисунок 3 Пример высокоскоростной коммутации в рабочей группе



1.1.4 Примеры применения в сетях VLAN на базе IEEE 802.1Q

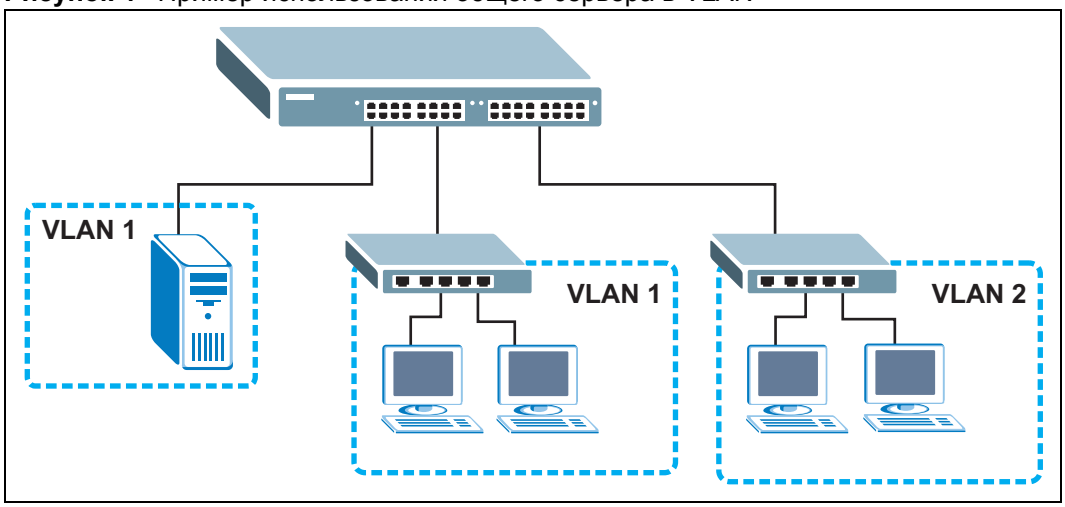
Виртуальные локальные сети (VLAN, Virtual Local Area Network) позволяют разделить одну физическую сеть на несколько логических. Станции в логической сети принадлежат к одной группе. Станция может принадлежать к нескольким группам. При использовании сетей VLAN станция не может отправлять или принимать данные от станций, не принадлежащих к той же группе (группам); это возможно лишь в том случае, если трафик проходит через маршрутизатор.

Дополнительную информацию о виртуальных локальных сетях можно найти в гл. 8 на стр. 83.

Порты в одной группе VLAN принадлежат к одному домену широковещательной передачи кадров. Это позволяет повысить производительность сети за счет уменьшения широковещательного трафика. Группы VLAN можно изменять в любой момент, добавляя, перемещая или изменяя порты без переподключения кабелей.

Общие ресурсы, например, сервер, могут использоваться всеми портами в той же сети VLAN, что и сервер. Как показано на приведенном ниже рисунке, в сеть VLAN 1 необходимо включить только те порты, которым требуется доступ к серверу. Порты также могут принадлежать к другим группам VLAN.

Рисунок 4 Пример использования общего сервера в VLAN



1.2 Способы управления коммутатором

Для управления коммутатором доступны следующие способы.

- Web-конфигуратор. Именно этот способ рекомендуется применять для повседневного управления коммутатором при помощи (поддерживаемого) браузера. См. гл. 4 на стр. 47.
- Интерфейс командной строки. Интерфейс командной строки является альтернативой Web-конфигуратору и может потребоваться для настройки расширенных функций. См. Справочное руководство по интерфейсу командной строки.
- FTP. Протокол передачи файлов File Transfer Protocol можно использовать для обновления встроенного программного обеспечения и резервного копирования/восстановления конфигурации. См. разд. 26.8 на стр. 217.
- SNMP. Мониторинг и/или управление устройством возможно с использованием менеджера SNMP. См. разд. 27.3 на стр. 222.

1.3 Полезные советы по управлению коммутатором

Чтобы сделать коммутатор более защищенным, а управление коммутатором – более эффективным, необходимо регулярно выполнять следующие действия.

- Меняйте пароль. Используйте пароль, который трудно угадать, и который включает в себя различные виды символов, включая буквы и цифры.
- Запишите пароль и сохраните его в надежном месте.

- Осуществляйте резервное копирование конфигурации (и ознакомьтесь с порядком ее восстановления). Восстановление более ранней версии конфигурации может оказаться полезным в случае нестабильной работы или отказа устройства. Если вы забыли свой пароль, можно восстановить на коммутаторе заводские настройки по умолчанию. При наличии резервной копии более ранней версии файла конфигурации вам не придется повторно настраивать коммутатор от начала и до конца. Вы сможете просто восстановить последнюю конфигурацию.

2

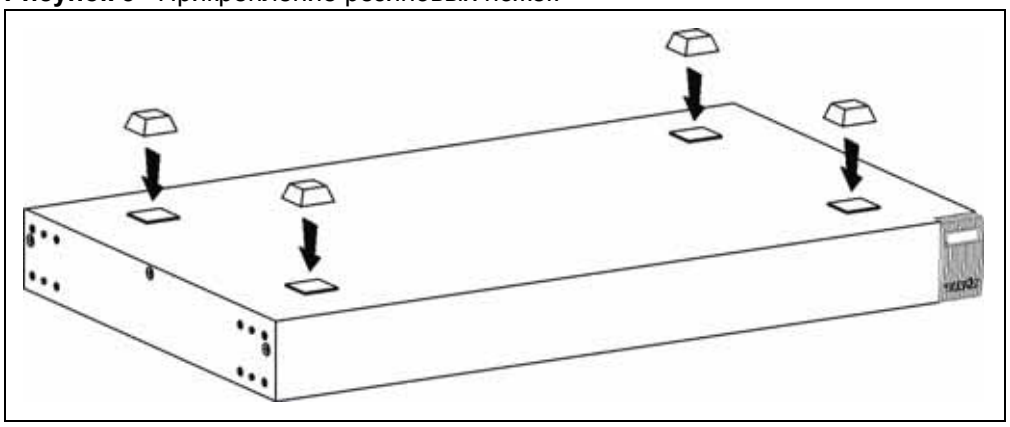
Установка и подключение аппаратного обеспечения

В данной главе описаны процедуры установки и подключения коммутатора.

2.1 Установка на столе

1. Убедитесь, что коммутатор сухой и чистый.
2. Установите коммутатор на ровной горизонтальной поверхности, достаточно устойчивой, чтобы выдержать вес коммутатора и подключенных к нему кабелей. Убедитесь, что рядом есть розетка.
3. Убедитесь, что вокруг коммутатора имеется достаточно свободного пространства для циркуляции воздуха и подключения кабелей и шнура питания.
4. Удалите наклейки с резиновых ножек.
5. Прикрепите резиновые ножки к каждому углу днища коммутатора. Эти ножки защищают коммутатор от вибрации и обеспечивают наличие свободного места между устройствами, установленными друг на друга.

Рисунок 5 Прикрепление резиновых ножек



НЕ заслоняйте вентиляционные отверстия. При установке устройств друг на друга убедитесь, что между ними есть свободное пространство.

Чтобы обеспечить нормальную вентиляцию, оставьте зазор как минимум в 4 дюйма (10 см) спереди и 3,4 дюйма (8 см) сзади коммутатора. Это особенно важно при установке в закрытой стойке.

2.2 Установка коммутатора в стойку

В данном разделе перечислены требования и меры предосторожности при установке устройства в аппаратную стойку, а также описана собственно процедура установки.

2.2.1 Требования к установке коммутатора в аппаратную стойку

- Два кронштейна.
- Восемь винтов M3 с плоской головкой и крестовая отвертка #2.
- Четыре винта M5 с плоской головкой и крестовая отвертка #2.

Использование винтов неправильного типа может повредить устройство.

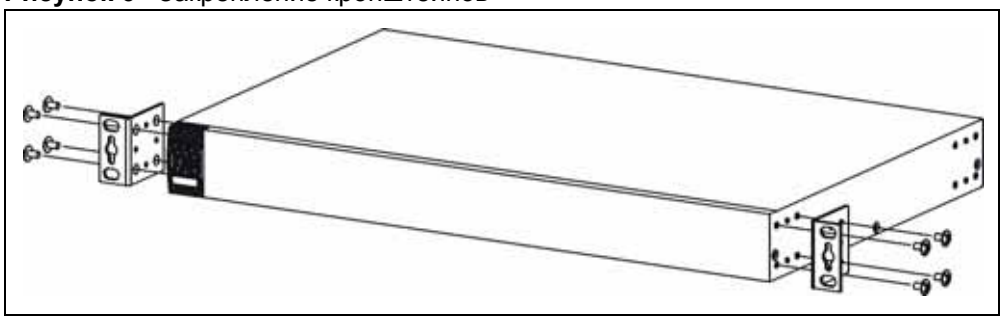
2.2.1.1 Меры предосторожности

- Убедитесь, что стойка может выдержать общий вес всего оборудования, которое в нее установлено.
- Убедитесь, что положение коммутатора не нарушает устойчивость стойки и не смещает центр тяжести к ее верхней части. Перед установкой примите все необходимые меры предосторожности для надежного закрепления стойки.

2.2.2 Крепление кронштейнов к коммутатору

1 Приложите кронштейн к одной и боковых панелей коммутатора, совместив четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели коммутатора.

Рисунок 6 Закрепление кронштейнов



2 С помощью крестовой отвертки #2 прикрепите кронштейн к коммутатору винтами M3 с плоской головкой.

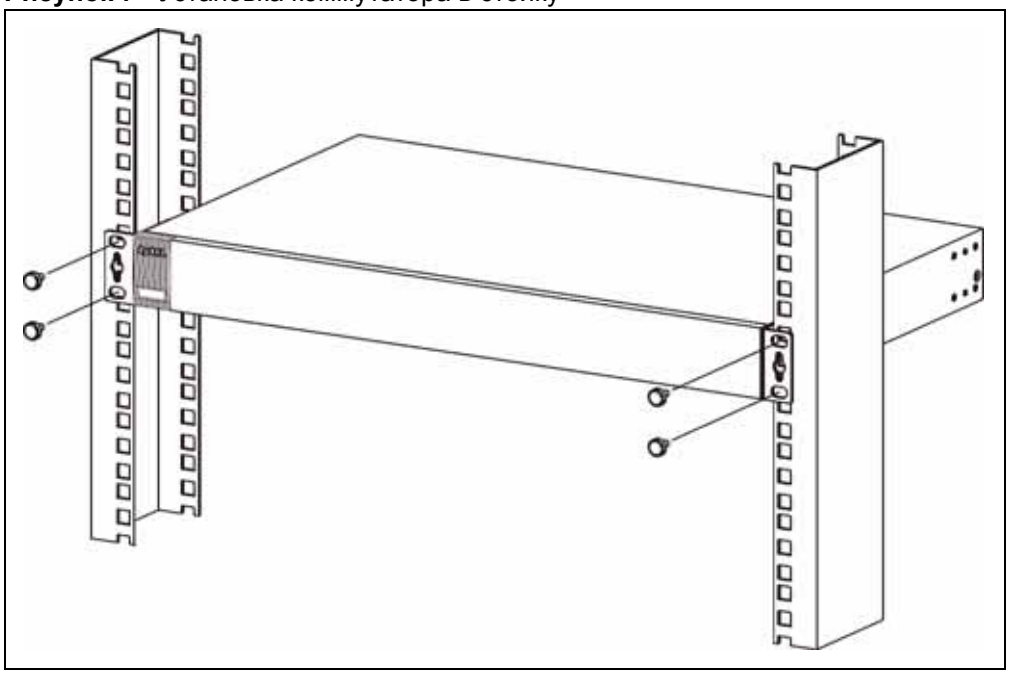
3 Повторите шаги 1 и 2, чтобы закрепить кронштейн на другой стороне коммутатора.

4 Теперь коммутатор можно устанавливать в стойку. Переходите к следующему разделу.

2.2.3 Установка коммутатора в стойку

1 Приложите кронштейн (уже прикрепленный винтами к боковой панели коммутатора) к одной стороне стойки и совместите два отверстия для винтов на кронштейне с такими же двумя отверстиями в стойке.

Рисунок 7 Установка коммутатора в стойку



2 С помощью крестовой отвертки #2 прикрепите кронштейн к стойке винтами M5 с плоской головкой.

3 Повторите шаги 1 и 2, чтобы закрепить кронштейн на другой стороне стойки.

3

Обзор аппаратного обеспечения

В данной главе описаны передняя и задняя панель коммутатора, а также показаны аппаратные подключения.

3.1 Подключения на передней панели

Передняя панель коммутатора показана на рисунке ниже.

Рисунок 8 Передняя панель: ES-2024A

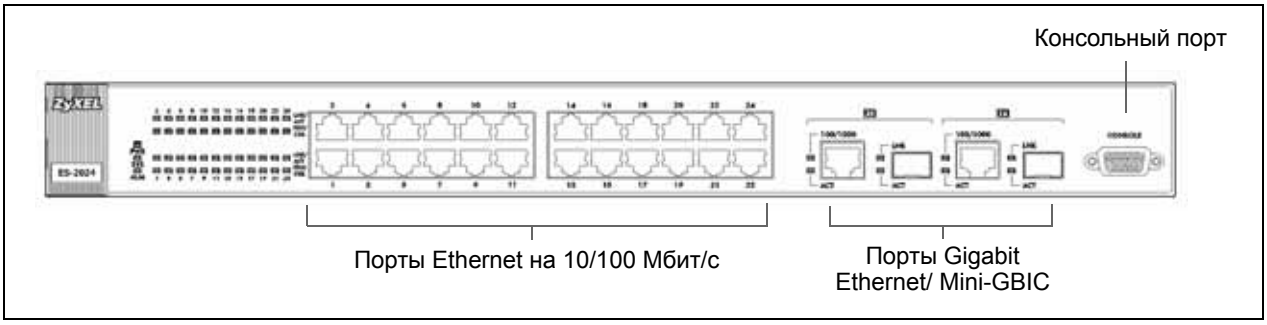
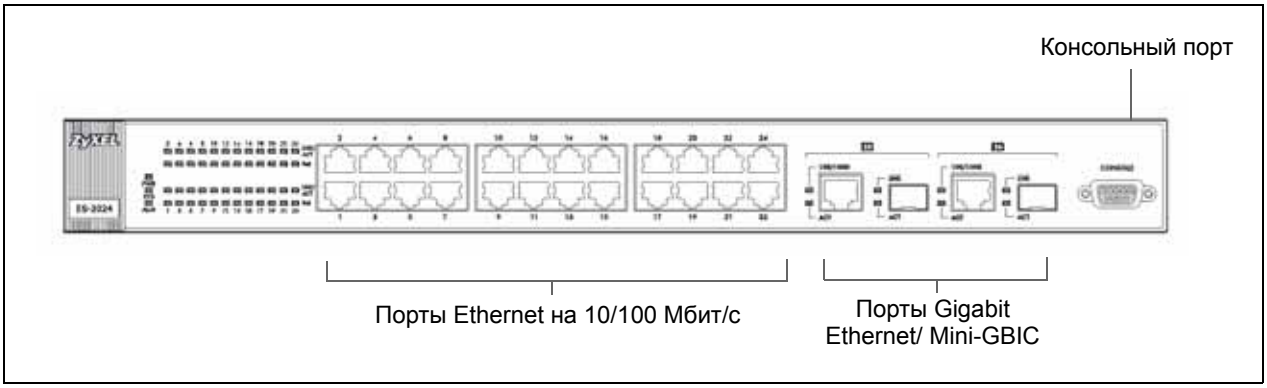


Рисунок 9 Передняя панель: ES-2024PWR



Назначение портов на передней панели описано в следующей таблице.

Таблица 1 Передняя панель

ПОЛЕ	ОПИСАНИЕ
Консольный порт	К этому порту следует подключаться только тогда, когда требуется настроить коммутатор с помощью интерфейса командной строки через консольный порт.
24 порта Ethernet на 10/100 Мбит/с с разъемами RJ-45	К этим портам можно подключать компьютеры, концентраторы, Ethernet-коммутаторы или маршрутизаторы.
Порты Gigabit Ethernet/ Mini-GBIC	Порты Gigabit Ethernet подключаются к высокоскоростным магистральным Ethernet-коммутаторам или используются для последовательного соединения нескольких коммутаторов. Кроме того, в слоты можно вставить трансиверы mini-GBIC для подключения к магистральным Ethernet-коммутаторам посредством оптоволокна.

3.1.1 Консольный порт

Для локального управления можно использовать компьютер с установленной на нем программой-эмулятором терминала, настроенной со следующими параметрами:

- Эмуляция терминала VT100
- Скорость 9600 бод
- Четность – нет, 8 бит данных, 1 стоп-бит
- Управление потоком – нет

Подключите 9-пиновый разъем типа «папа» консольного кабеля к консольному порту коммутатора. Подключите другой конец кабеля с разъемом типа «мама» к последовательному порту (COM1, COM2 или другому COM-порту) компьютера.

3.1.2 Порты Ethernet

Данный коммутатор оснащен 24 портами Ethernet на 10/100 Мбит/с с функциями автосогласования и автоматического определения типа кабеля. Порты Fast Ethernet на 10/100 Мбит/с могут работать на скорости 10 Мбит/с или 100 Мбит/с в полудуплексном или дуплексном режиме.

Коммутатор оснащен двумя парами портов Gigabit Ethernet/mini-GBIC. Порты mini-GBIC имеют приоритет перед портами Gigabit Ethernet. Это означает, что если порт mini-GBIC и соответствующий ему порт Gigabit Ethernet подключены одновременно, то порт Gigabit Ethernet работать не будет. Скорость на портах Gigabit Ethernet/mini-GBIC может быть либо 100 Мбит/с, либо 1000 Мбит/с, а режим – либо полудуплексным (на скорости 100 Мбит/с), либо дуплексным.

Порт с функцией автосогласования может определять и настраивать оптимальную скорость (10/100 Мбит/с) и режим дуплекса (полудуплекс или дуплекс) канала Ethernet для подключенного устройства.

Порт с функцией автоматического определения типа кабеля (автоматического выбора режима MDI/MDI-X) позволяет использовать для подключения как стандартный (прямой), так и кроссоверный (перекрещенный) кабели Ethernet.

3.1.2.1 Настройки Ethernet по умолчанию

По умолчанию для портов Ethernet коммутатора установлены следующие заводские настройки:

- Скорость: Автосогласование
- Режим дуплекса: Автосогласование
- Управление потоком: Нет

3.1.3 Слоты Mini-GBIC

Эти слоты предназначены для трансиверов mini-GBIC (конвертеров гигабитного интерфейса). Трансивер – это устройство, совмещающее в себе функции передатчика и приемника. Трансиверы не входят в комплект поставки коммутатора. Разрешается использовать только трансиверы, отвечающие требованиям SFP Tranciever MultiSource Agreement (MSA). Более подробную информацию можно найти в спецификации INF-8074i Rev 1.0 комитета SFF.

Коммутатор оснащен двумя парами портов Gigabit Ethernet/mini-GBIC. Порты mini-GBIC имеют приоритет перед портами Gigabit Ethernet. Это означает, что если порт mini-GBIC и соответствующий ему порт Gigabit Ethernet подключены одновременно, то порт Gigabit Ethernet работать не будет.

Трансиверы можно менять во время работы коммутатора. Для подключения к Ethernet-коммутаторам с различными типами оптоволоконных разъемов можно пользоваться различными типами трансиверов.

- Тип: Интерфейс подключения SFP
- Скорость подключения: 1 гигабит в секунду (1 Гбит/с)

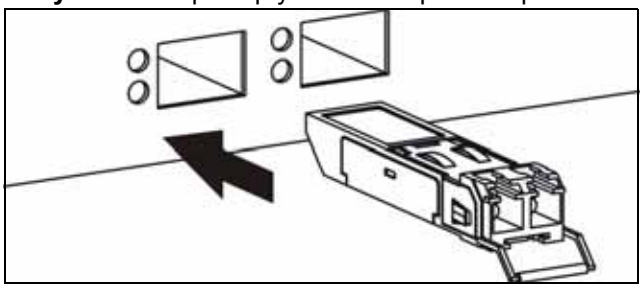
Во избежание возможной травмы глаз не смотрите в разъемы работающего оптоволоконного модуля.

3.1.3.1 Установка трансивера

Для установки трансивера mini-GBIC (SFP-модуля) выполните следующие действия.

1. Вставьте трансивер в слот открытой секцией печатной платы вниз.

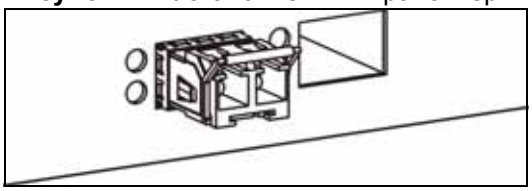
Рисунок 10 Пример установки трансивера



2. Надавите на трансивер, пока он не защелкнется на месте.

3 Данный коммутатор автоматически обнаружит установленный трансивер. Проверьте состояние светодиодных индикаторов, чтобы убедиться, что он работает.

Рисунок 11 Установленный трансивер

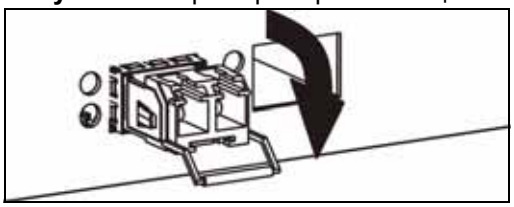


3.1.3.2 Удаление трансивера

Для удаления трансивера mini-GBIC (SFP-модуля) выполните следующие действия.

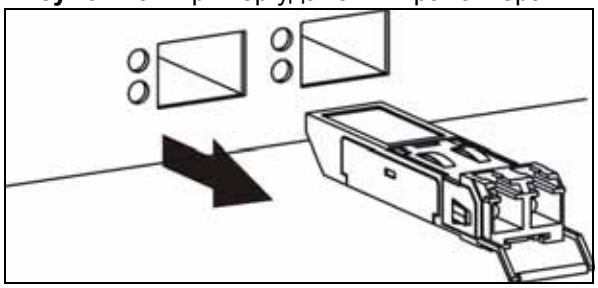
1 Откройте защелку трансивера (их вид может различаться).

Рисунок 12 Пример открытия защелки трансивера



2 Выньте трансивер из слота.

Рисунок 13 Пример удаления трансивера



3.2 Задняя панель

Задняя панель коммутатора показана на рисунке ниже. Разъем для шнура питания находится на задней панели.

Рисунок 14 Задняя панель

3.2.1 Разъем питания

Убедитесь, что параметры питающей сети соответствуют указанным на панели.

Для подключения питания к коммутатору вставьте разъем типа «мама» шнура питания в розетку на задней панели. Подключите другой конец шнура питания к источнику питания.

3.3 Индикаторы

Светодиодные индикаторы находятся на передней панели. Индикаторы на передней панели описаны в следующей таблице.

Таблица 2 Индикаторы

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
PWR	Зеленый	Горит	Система работает.
		Не горит	Система не работает.
SYS	Зеленый	Мигает	Система перезагружается и выполняет самодиагностику.
		Горит	Система включена и функционирует нормально.
		Не горит	Питание отключено или система не готова / работает с ошибками.
ALM	Красный	Горит	Обнаружен сбой оборудования.
		Не горит	Система работает нормально.
Порты Ethernet			
LNK/ACT	Желтый	Мигает	Осуществляется передача/прием данных на скорости 10/100 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 10/100 Мбит/с.
		Не горит	Соединение с сетью Ethernet не установлено.
FDX/COL (ES-2024A)	Желтый	Мигает	Порт Ethernet работает в полудуплексном режиме, имеют место коллизии; чем больше коллизий, тем чаще мигает индикатор.
		Горит	Порт Ethernet работает в дуплексном режиме.
		Не горит	Порт Ethernet работает в полудуплексном режиме, коллизии отсутствуют.
POE (ES-2024PWR)	Желтый	Горит	На порт подается питание.
		Не горит	Питание на порт не подается.
Порты Gigabit Ethernet			
100/1000	Зеленый	Горит	Установлено соединение с сетью Ethernet на скорости 1000 Мбит/с.
	Желтый	Горит	Установлено соединение с сетью Ethernet на скорости 100 Мбит/с.
		Не горит	Соединение с сетью Ethernet не установлено.
ACT	Зеленый	Мигает	Осуществляется прием или передача данных через порт.
		Горит	Установлено соединение с сетью Ethernet, но данные не принимаются и не передаются.
		Не горит	Соединение с сетью Ethernet не установлено.

Таблица 2 Индикаторы (продолжение)

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
Порты mini-GBIC			
LNK	Зеленый	Горит	Соединение установлено успешно.
		Не горит	Ethernet-устройство к порту не подключено.
ACT	Зеленый	Мигает	Осуществляется прием или передача данных через порт.
		Не горит	Данные через порт не принимаются и не передаются.

Часть II
Основные настройки

4

Web-конфигуратор

В данном разделе описаны настройки и функции Web-конфигуратора.

4.1 Введение

Web-конфигуратор – это интерфейс управления на основе HTML, который позволяет легко настраивать и управлять коммутатором через Интернет-браузер. Следует использовать программы Internet Explorer 6.0 и более поздних версий, или Netscape Navigator 7.0 и более поздних версий. Рекомендованное разрешение экрана – 1024 на 768 пикселей.

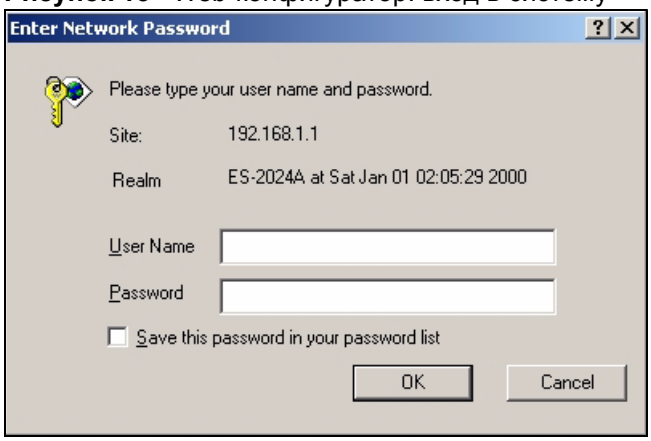
Для использования Web-конфигуратора нужно разрешить:

- Всплывающие окна браузера на устройстве. Блокировка всплывающих окон браузера по умолчанию включена в операционной системе Windows XP SP (Service Pack) 2.
- JavaScript (по умолчанию включен).
- Разрешения Java (по умолчанию включены).

4.2 Вход в систему

1. Запустите Web-браузер.
2. Введите «http://» и IP-адрес коммутатора (например, адрес по умолчанию – 192.168.1.1) в поле адреса. Нажмите [ENTER].
3. Появится экран ввода имени и пароля. Имя пользователя по умолчанию – **admin**, а соответствующий ему пароль по умолчанию – **1234**. Дата и время будут показаны так, как на рисунке, если вы не настроили сервер времени и не ввели дату и время в меню **General Setup**.

Рисунок 15 Web-конфигуратор: вход в систему



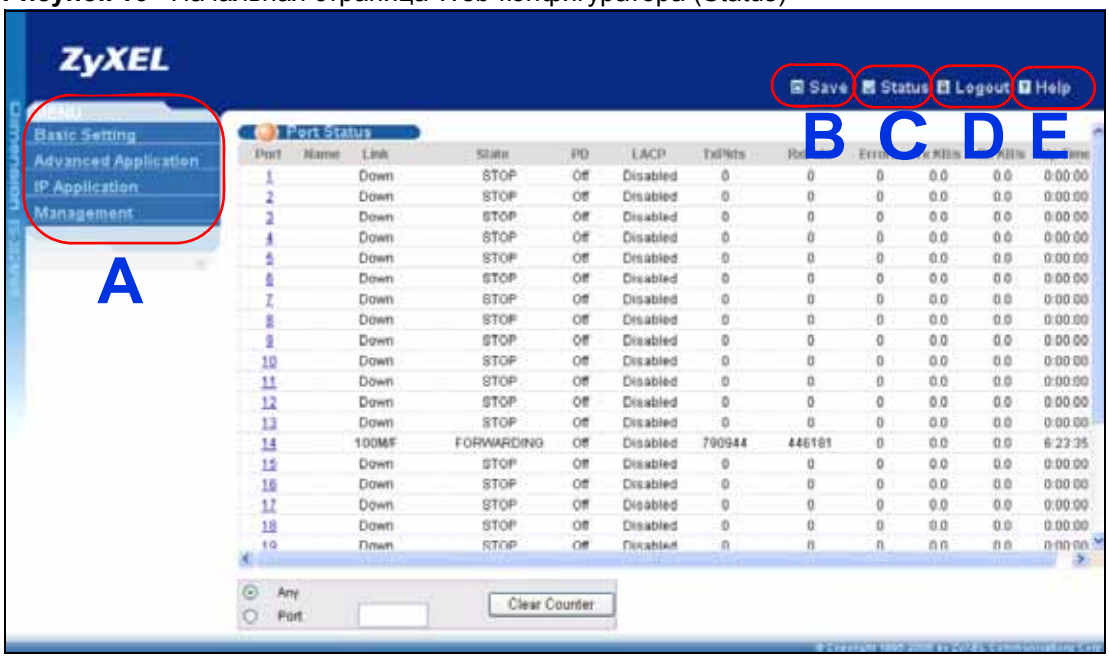
4 Нажмите **OK**, чтобы попасть на начальный экран Web-конфигуратора.

4.3 Окно состояния (Status)

После получения доступа к Web-конфигуратору первым отображается экран **Status**.

На приведенном ниже рисунке показаны элементы навигации по экрану Web-конфигуратора.

Рисунок 16 Начальная страница Web-конфигуратора (Status)



A – Нажатие на пункты меню раскрывает ссылки на пункты подменю; выбор одного из пунктов подменю открывает соответствующий экран в основном окне.

B, **C**, **D**, **E** – С помощью этих быстрых ссылок можно выполнять определенные действия независимо от текущего экрана.

B – Нажатие на данную ссылку вызывает сохранение конфигурации в энергонезависимой памяти коммутатора. Содержимое энергонезависимой памяти записывается в файл конфигурации, который используется коммутатором для загрузки, и не изменяется даже при отключении питания коммутатора. Более подробную информацию о сохранении настроек в определенный файл конфигурации можно найти в разд. 26.3 на стр. 214.

C – Нажатие на данную ссылку вызывает переход на страницу состояния коммутатора.

D – Нажатие на данную ссылку вызывает выход из Web-конфигуратора.

E – Нажатие на данную ссылку открывает страницы справки. На страницах справки приводятся описания всех экранов настройки.

Чтобы открыть список ссылок в подменю, нажмите на основную ссылку в панели навигации.

Таблица 3 Обзор подменю панели навигации

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
			

Экраны различных подменю Web-конфигуратора перечислены в следующей таблице..

Таблица 4 Содержание экранов подменю Web-конфигуратора

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
System Info (Информация о системе) General Setup (Общие настройки) Switch Setup (Настройка коммутатора) IP Setup (Настройка протокола IP) Port Setup (Настройки портов)	VLAN Status (Состояние VLAN) VLAN Port Setting (Настройки портов VLAN) Static VLAN (Статические VLAN) VLAN Detail (Подробная информация о сети VLAN) Static MAC Forwarding (Пересылка на основе статических MAC-адресов) Filtering (Фильтрация) Spanning Tree Protocol Status (Состояние протокола STP) Configuration (Настройка) RSTP MSTP Bandwidth Control (Управление пропускной способностью) Broadcast Storm Control (Контроль широковещательных штормов) Mirroring (Зеркальное копирование) Link Aggregation Status (Состояние агрегации каналов) Link Aggregation Setting (Настройка агрегации каналов) Ling Aggregation Control Protocol (Протокол LACP) Port Authentication (Аутентификация портов) 802.1x Port Security (Средства безопасности портов) Queuing Method (Метод организации очередей)	Static Routing (Статические маршруты) DiffServ (Дифференцированное обслуживание) DSCP Setting (Настройки DSCP) DHCP Status (Состояние DHCP) DHCP Relay (Ретрансляция DHCP) VLAN Setting (Настройки VLAN)	Maintenance (Обслуживание) Firmware Upgrade (Обновление встроенного программного обеспечения) Restore Configuration (Восстановление конфигурации) Backup Configuration (Резервное копирование конфигурации) Load Factory Default (Загрузка заводских настроек по умолчанию) Save Configuration (Сохранение конфигурации) Reboot System (Перезагрузка системы) Access Control (Контроль доступа) SNMP (Протокол SNMP) Trap Group (Группы «ловушек») Logins (Пользователи и пароли) Service Access Control (Контроль доступа к службам) Remote Management (Удаленное управление) Diagnostic (Диагностика) Syslog Setup (Настройки системного журнала) Syslog Server Setup (Настройка сервера syslog)

Таблица 4 Содержание экранов подменю Web-конфигуратора (продолжение)

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
	Multicast Status (Состояние мультивещания) Multicast Setting (Настройка мультивещания) IGMP Snooping VLAN (VLAN отслеживания многоадресного трафика IGMP) IGMP Filtering Profile (Профиль фильтрации IGMP) MVR (Регистрация VLAN-сети мультивещания) Group Configuration (Настройка групп) Authentication and Accounting (Аутентификация и учет) RADIUS Server Setup (Настройка сервера RADIUS) TACACS+ Server Setup (Настройка сервера TACACS+) Auth and Acct Setup (Настройка аутентификации и учета) IP Source Guard (Защита от подмены IP-адресов) IP Source Guard Static Binding (Статическая привязка для защиты от подмены IP-адресов) ARP Inspection Status (Состояние инспекции ARP-пакетов) ARP Inspection Log Status (Состояние журнала инспекции ARP-пакетов) ARP Inspection Configure (Настройка инспекции ARP-пакетов) ARP Inspection Port Configure (Настройка портов для инспекции ARP-пакетов) ARP Inspection VLAN Configure (Настройка сети VLAN для инспекции ARP-пакетов) Loop Guard (Защита от образования петель)		Clustering Management Status (Состояние управления кластерами) Clustering Management Configuration (Настройка управления кластерами) MAC Table (Таблица MAC-адресов) ARP Table (Таблица ARP) Configure Clone (Настройка клонирования)

Пункты меню навигационной панели описаны в следующей таблице.

Таблица 5 Пункты меню навигационной панели

ПУНКТ	ОПИСАНИЕ
Basic setting (Основные настройки)	
System Info (Информация о системе)	Этот пункт открывает экран общей информации о системе и мониторинга аппаратного обеспечения.
General Setup (Общие настройки)	Этот пункт открывает экран, позволяющий настроить общую идентификационную информацию о коммутаторе.
Switch Setup (Настройка коммутатора)	Этот пункт открывает экран, позволяющий настроить глобальные параметры коммутатора, такие как тип VLAN, получение таблицы MAC-адресов, протокол GARP и приоритеты очередности.
IP Setup (Настройка протокола IP)	Этот пункт открывает экран, позволяющий настроить IP-адрес и маску подсети (необходимые для управления коммутатором), а также сервер DNS (сервер доменных имен) и домены IP-маршрутизации.
Port Setup (Настройки портов)	Этот пункт открывает экраны, позволяющие настроить отдельные порты коммутатора.
Advanced application (Расширенные приложения)	
VLAN (Виртуальные локальные сети)	Этот пункт открывает экраны, позволяющие настроить виртуальные локальные сети на основе портов или стандарта 802.1Q (в зависимости от того, что было выбрано в меню **Switch Setup**).
Static MAC Forwarding (Пересылка на основе статических MAC-адресов)	Этот пункт открывает экраны, позволяющие настроить статические MAC-адреса для каждого из портов. Такие статические MAC-адреса не имеют срока действия.
Filtering (Фильтрация)	Этот пункт открывает экран, позволяющий настроить правила фильтрации.
Spanning Tree Protocol (Протокол покрывающего дерева)	Этот пункт открывает экраны, позволяющие настроить протоколы RSTP/MSTP для предотвращения петель в сети.
Bandwidth Control (Управление пропускной способностью)	Этот пункт открывает экраны, позволяющие настроить пределы пропускной способности от одного или нескольких начальных пунктов к одному или нескольким указанным пунктам назначения.
Broadcast Storm Control (Контроль широковещательных штормов)	Этот пункт открывает экран, позволяющий настроить фильтры широковещательной передачи.
Mirroring (Зеркальное копирование)	Этот пункт открывает экраны, позволяющие настроить копирование трафика от одного или нескольких портов на другой порт, чтобы можно было проверить трафик на первом порту, не вмешиваясь в его поток.
Link Aggregation (Агрегация каналов)	Этот пункт открывает экран, позволяющий логически объединить несколько физических каналов в один логический канал большей пропускной способности.
Port Authentication (Аутентификация портов)	Этот пункт открывает экран, позволяющий настроить аутентификацию портов на основе IEEE 802.1x.
Port Security (Средства безопасности портов)	Этот пункт открывает экран, позволяющий включить получение таблицы MAC-адресов и установить максимальное количество MAC-адресов, которые может запомнить порт.

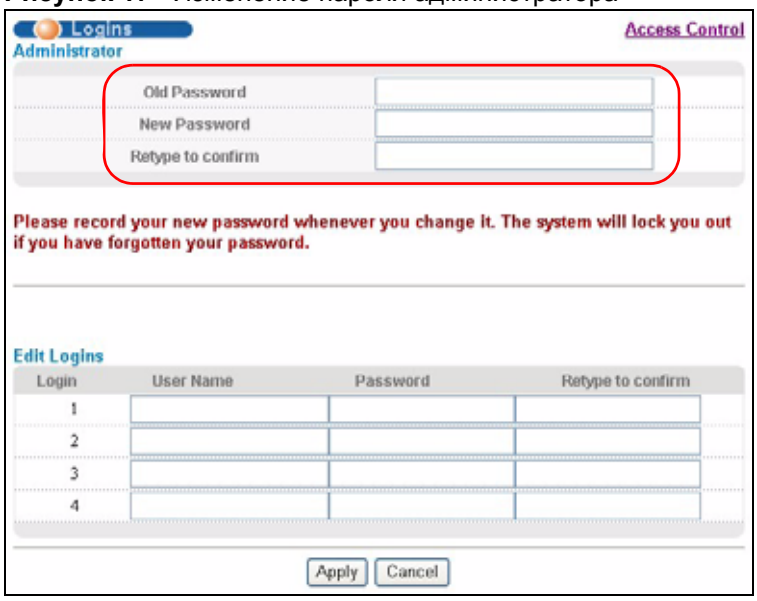
Таблица 5 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
Queuing Method (Метод организации очередей)	Этот пункт открывает экран, позволяющий настроить организацию очередей, а также установить соответствующие значения весов.
Multicast (Мультивещание)	Этот пункт открывает экран, позволяющий настроить различные функции мультивещания и создать VLAN-сети мультивещания.
Auth and Acct (Аутентификация и учет)	Этот пункт открывает экран, позволяющий настроить различные функции аутентификации и учета с использованием внешних серверов. В качестве таких внешних серверов могут выступать серверы RADIUS (Remote Authentication Dial-In User Service) или TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard (Защита от подмены IP-адресов)	Этот пункт открывает экран, позволяющий настроить фильтрацию несанкционированных ARP-пакетов в вашей сети.
Loop Guard (Защита от образования петель)	Этот пункт открывает экран, позволяющий настроить защиту от образования сетевых петель на границе сети.
IP Application (IP-приложения)	
Static Routing (Статические маршруты)	Этот пункт открывает экраны, позволяющие настроить статические маршруты. Статический маршрут указывает коммутатору, куда следует направлять IP-трафик, посредством ручной настройки параметров протокола TCP/IP.
DiffServ (Дифференцированное обслуживание)	Этот пункт открывает экраны, позволяющие включить DiffServ и определить отображения между битами DSCP и IEEE 802.1p.
DHCP (Протокол DHCP)	Этот пункт открывает экран, позволяющий настроить протокол DHCP.
Management (Управление)	
Maintenance (Обслуживание)	Этот пункт открывает экраны, позволяющие работать с файлами конфигурации и встроенного программного обеспечения, а также осуществлять перезагрузку системы.
Access Control (Контроль доступа)	Этот пункт открывает экраны, позволяющие изменить имя входа и пароль доступа к системе, а также настроить протокол SNMP и удаленное управление.
Diagnostic (Диагностика)	Этот пункт открывает экраны, позволяющие просматривать системные журналы и тестировать порты.
Syslog (Системный журнал)	Этот пункт открывает экраны, позволяющие настраивать системные журналы и сервер системного журнала.
Cluster Management (Управление кластерами)	Этот пункт открывает экран, позволяющий настроить управление кластерами и просмотреть его состояние.
MAC Table (Таблица MAC-адресов)	Этот пункт открывает экран, позволяющий просматривать MAC-адреса (и типы) устройств, подключенных к каким-либо портам, а также идентификаторы виртуальных локальных сетей VLAN ID.
ARP Table (Таблица ARP)	Этот пункт открывает экран, позволяющий просмотреть таблицу соответствия MAC-адресов и IP-адресов.
Configure Clone (Настройка клонирования)	Данный пункт открывает экран, позволяющий скопировать настройки одного из портов на другие порты.

4.3.1 Изменение пароля

После первого входа в систему рекомендуется изменить пароль администратора по умолчанию. Нажмите **Management** > **Access Control > Logins**, чтобы отобразить следующий экран.

Рисунок 17 Изменение пароля администратора



4.4 Сохранение конфигурации

Закончив изменение настроек на экране, нажмите **Apply** для сохранения изменений в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

Чтобы сохранить конфигурацию в энергонезависимой памяти, нажмите на ссылку **Save** в правом верхнем углу Web-конфигуратора. Под энергонезависимой памятью коммутатора понимается память, содержимое которой сохраняется даже при отключении питания коммутатора.

После завершения сеанса настройки обязательно воспользуйтесь ссылкой **Save**.

4.5 Блокировка коммутатора

Выполнение любого из следующих действий приводит к блокированию возможности внутриполосного управления коммутатором (управления через порты передачи данных) для всех пользователей:

1. Удаление виртуальной локальной сети управления (по умолчанию – VLAN 1).
2. Удаление всех виртуальных локальных сетей на основе портов, членом которых является порт CPU. «Порт CPU» – это управляющий порт коммутатора.
3. Установка фильтрации всего трафика для порта CPU.
4. Отключение всех портов.
5. Ошибка в текстовом конфигурационном файле.
6. Утрата пароля и/или IP-адреса.
7. Запрет доступа к коммутатору для всех служб.
8. Изменение номера порта службы и его утрата.

Соблюдайте осторожность, чтобы не заблокировать доступ к коммутатору для себя и всех остальных пользователей.

4.6 Сброс коммутатора

Если коммутатор оказался заблокирован для вас (и остальных пользователей), или вы забыли пароль администратора, потребуется загрузить файл конфигурации по умолчанию или сбросить коммутатор, чтобы он вернулся к заводским настройкам по умолчанию.

4.6.1 Загрузка файла конфигурации

При загрузке файла конфигурации с заводскими настройками имеющийся файл конфигурации заменяется файлом с заводскими настройками. При этом все предыдущие настройки будут сброшены, а скорость консольного порта вернется к стандартным параметрам (9600 бод, 8 бит данных, четности нет, 1 стоп-бит, управление потоком отключено). Кроме того, будет установлен пароль «1234»и IP-адрес 192.168.1.1.

Для загрузки файла конфигурации сделайте следующее:

1. Подключитесь к консольному порту с помощью программы-эмулятора терминала, установленной на компьютере. Более подробную информацию можно найти в разд. 3.1.1 на стр. 40.
2. Отключите и включите снова питание коммутатора, чтобы начать сессию. При повторном включении питания коммутатора вы увидите начальный экран.
3. Получив сообщение «`Press any key to enter Debug Mode within 3 seconds...`», нажмите любую клавишу для входа в режим отладки.
4. Наберите команду `atlc` после сообщения «`Enter Debug Mode`».
5. Дождитесь сообщения «`Starting XMODEM upload`», после чего активируйте режим загрузки XMODEM на своем терминале.
6. После загрузки файла конфигурации наберите команду `atgo` для перезагрузки коммутатора.

Пример показан ниже.

Рисунок 18 Сброс коммутатора: через консольный порт

```
Bootbase Version: V1.07 | 04/20/2005 13:38:02
RAM: Size = 32768 Kbytes
FLASH: AMD 32M *1

ZyNOS Version: V3.70(TX.0)| 07/11/2006 19:59:04
Press any key to enter debug mode within 3 seconds.
.................
Enter Debug Mode
sysname> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCC
Total  49152 bytes received.
Erasing..
.............................................................
OK
sysname> atgo
```

Теперь коммутатор перезагружен с файлом настроек по умолчанию, включая пароль «1234».

4.7 Выход из Web-конфигуратора

Чтобы выйти из Web-конфигуратора, нажмите **Logout** на экране. Для повторного входа после выхода необходимо будет заново ввести пароль. Данное действие рекомендуется выполнить после окончания сеанса управления по соображениям безопасности.

Рисунок 19 Web-конфигуратор: экран выхода

4.8 Помощь

Страница онлайновой справки по Web-конфигуратору содержит описания отдельных экранов, а также дополнительную информацию.

Чтобы получить в режиме онлайн описание конкретного экрана, выберите пункт **Help** на соответствующем экране Web-конфигуратора.

5

Пример первичной настройки

В данной главе описаны настройки коммутатора на примере конкретной сети.

5.1 Обзор

Первичная настройка включает в себя следующие шаги:

- Создание виртуальной локальной сети VLAN
- Определение идентификаторов VLAN для портов
- Настройка IP-адреса управления для коммутатора

Перед началом работы необходимо выполнить вход в Web-конфигуратор.

1. Подключите компьютер к любому Ethernet-порту коммутатора. Убедитесь, что компьютер находится в той же подсети, что и коммутатор.
2. Откройте Web-браузер и введите в строке адреса 192.168.1.1 (IP-адрес по умолчанию), чтобы получить доступ к Web-конфигуратору.

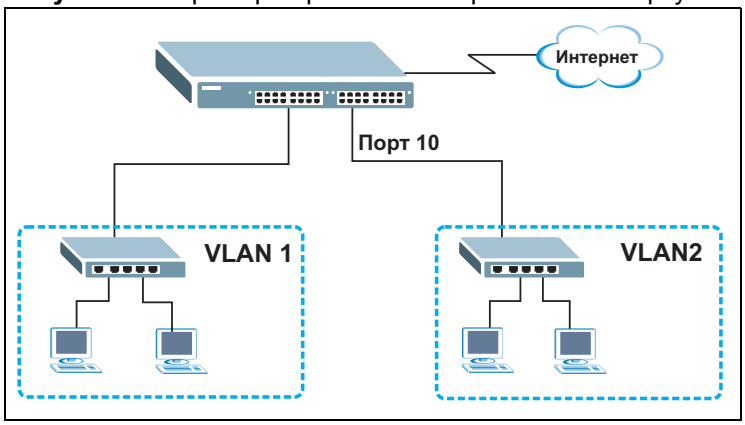
Дополнительную информацию можно найти в разд. 4.2 на стр. 47.

5.1.1 Создание виртуальной локальной сети VLAN

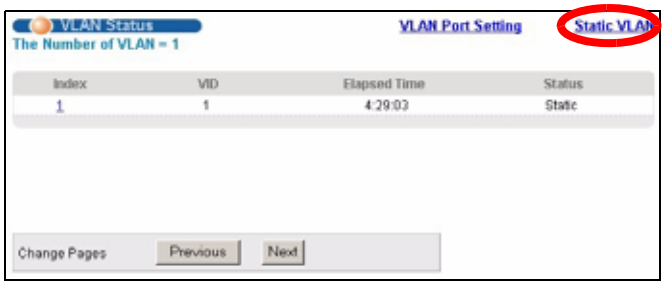
Виртуальные локальные сети ограничивают широковещательные кадры той группой VLAN, к которой принадлежит порт(ы). Для этого можно использовать виртуальные локальные сети на основе портов или статические виртуальные локальные сети на основе тегов с фиксированными портами-членами.

В данном примере порт 10 конфигурируется в качестве члена виртуальной локальной сети VLAN 2.

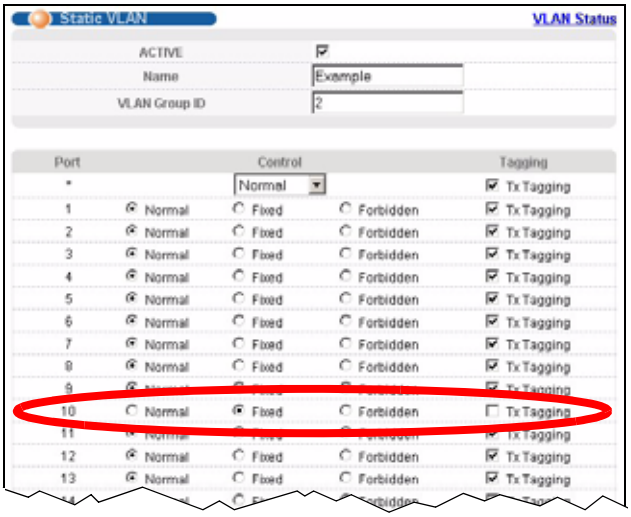
Рисунок 20 Пример первичной настройки сети: виртуальная локальная сеть



1 Выберите в навигационной панели **Advanced Application** и **VLAN**, затем выберите пункт **Static VLAN**.



2 На экране **Static VLAN** выберите **ACTIVE**, введите имя-описание в поле **Name** и введите 2 в поле **VLAN Group ID** для сети **VLAN2**.



Поле **VLAN Group ID** на этом экране и поле **VID** на экране меню **IP Setup** относятся к одному и тому же идентификатору виртуальной локальной сети VLAN ID.

3 Поскольку сеть **VLAN2** подключена к порту 10 коммутатора, выберите пункт **Fixed**, чтобы назначить порт 10 постоянным членом только этой VLAN.

4 Чтобы не поддерживающие идентификаторы VLAN устройства (например, компьютеры и концентраторы) правильно принимали кадры, снимите выделение с

переключателя **TX Tagging** – тогда коммутатор будет удалять теги VLAN перед отправкой.

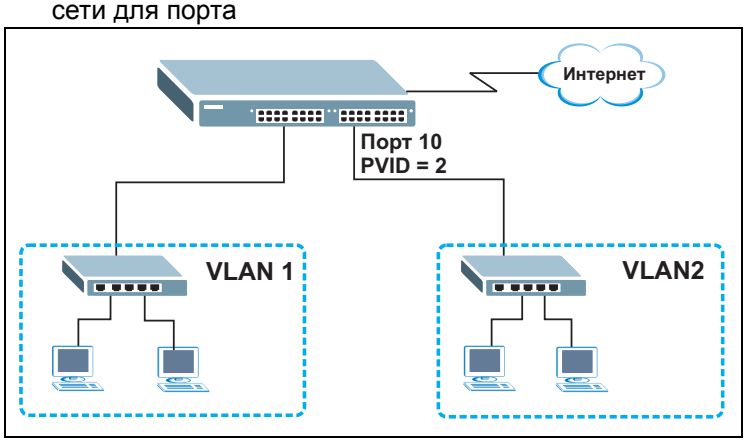
5 Нажмите **Add** для создания статической сети VLAN и затем на кнопку **Save**, чтобы сохранить настройки.

5.1.2 Назначение идентификатора виртуальной локальной сети VID для порта

Идентификатор виртуальной локальной сети для порта (PVID) используется для добавления тегов к кадрам без тегов, поступающим на этот порт, чтобы такие кадры направлялись в ту группу VLAN, которую определяет тег.

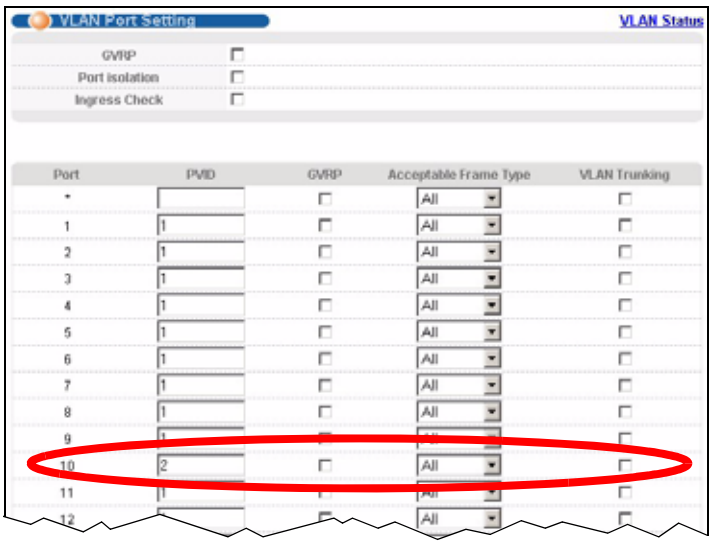
В данном примере необходимо установить 2 в качестве идентификатора VID для порта 10, чтобы все непомеченные тегами кадры, принятые через этот порт, отправлялись в виртуальную локальную сеть VLAN 2.

Рисунок 21 Пример первичной настройки сети: идентификатор виртуальной локальной сети для порта



1 Выберите в навигационной панели **Advanced Applications** и **VLAN**. Затем выберите пункт **VLAN Port Setting**.

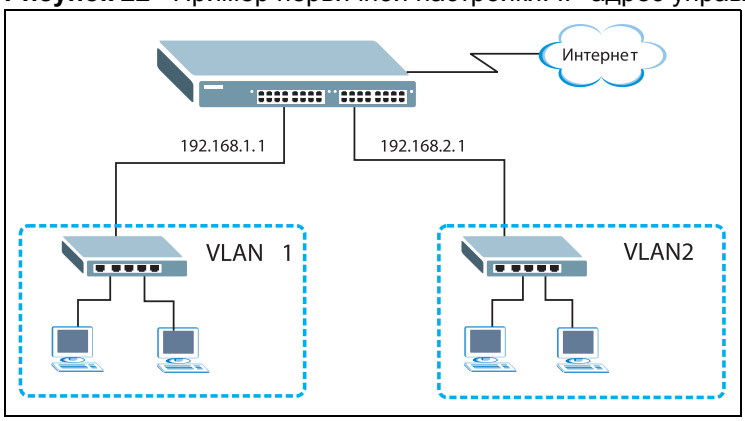
2 Введите 2 в поле **PVID** для порта 10 и нажмите **Apply**, чтобы применить настройку порта VLAN. Чтобы сохранить настройки, нажмите **Save**.



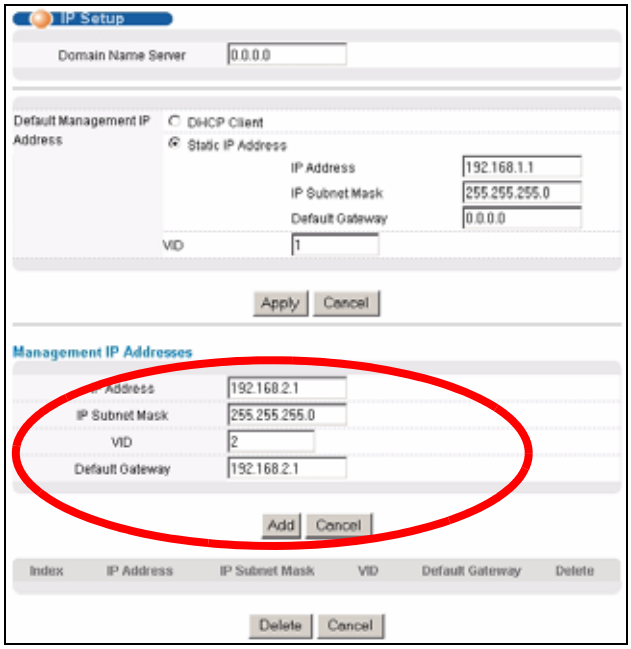
5.1.3 Настройка IP-адреса управления для коммутатора

По умолчанию в качестве IP-адреса управления коммутатором устанавливается адрес 192.168.1.1. Имеется возможность установить другой IP-адрес из другой подсети. Пример показан на рисунке.

Рисунок 22 Пример первичной настройки: IP-адрес управления



1. Выберите в навигационной панели **Basic Setting** и **IP Setup**.
2. Введите нужную информацию на экране **IP Setup**.
   Для сети **VLAN2** введите IP-адрес 192.168.2.1 и маску подсети 255.255.255.0.
3. В поле **VID** введите идентификатор группы VLAN, к которой должен принадлежать этот IP-адрес управления. Это должно быть то же значение, которое было введено в поле VLAN ID на экране меню **Static VLAN**.
4. Нажмите **Add**.



6

Состояние системы и статистика портов

В данной главе описаны экраны состояния системы (начальная страница Web-конфигуратора) и детальной информации по портам.

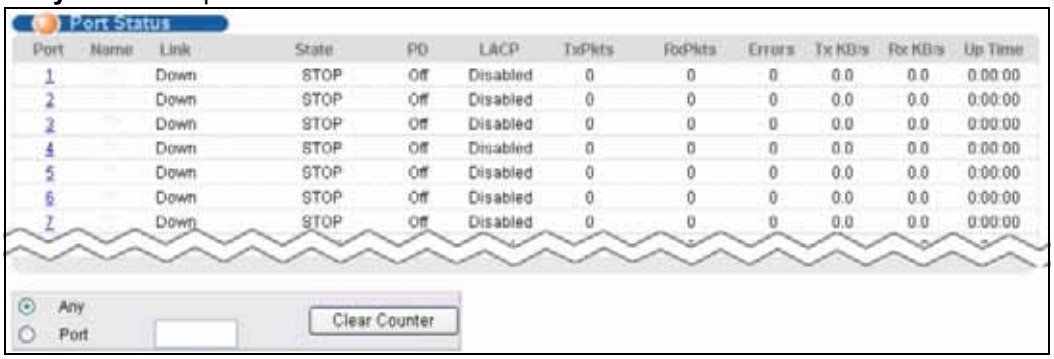
6.1 Обзор

Начальная страница Web-конфигуратора содержит сводную статистику по портам со ссылками на каждый порт, позволяющими отобразить детальную статистику каждого порта.

6.2 Сводная информация о состоянии портов

Для просмотра статистики по портам нажмите **Status** на любом из экранов Web-конфигуратора, чтобы отобразить окно **Status**, как показано на иллюстрации.

Рисунок 23 Экран Status



Поля экрана описаны в следующей таблице.

Таблица 6 Экран Status

ПОЛЕ	ОПИСАНИЕ
Port	Номер Ethernet-порта. Нажмите на номер порта, чтобы отобразить экран подробной статистики порта **Port Details** (см. рис. 24 на стр. 63).
Name	Имя, назначенное данному порту на экране **Basic Setting**, **Port Setup**.

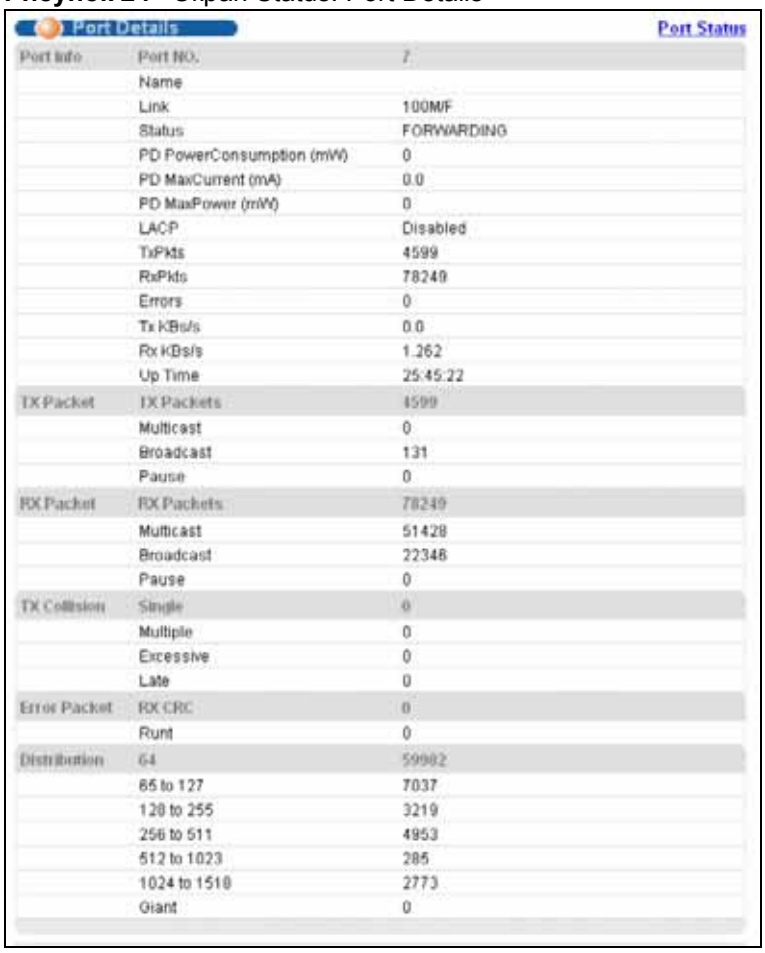
Таблица 6 Экран Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
Link	В этом поле отображается скорость (**10M** для 10 Мбит/с, **100M** для 100 Мбит/с или **1000M** для 1000 Мбит/с) и режим дуплекса (**F** для дуплекса или **H** для полудуплекса). Кроме того, в поле отображается тип кабеля (**Copper** для витой пары или **Fiber** для оптоволокна) для комбинированных портов.
State	Если активирован протокол покрывающего дерева STP, в этом поле отображается состояние порта по протоколу STP (дополнительную информацию можно найти в разд. 11.1.3 на стр. 103). Если протокол STP отключен, в этом поле отображается **FORWARDING** в случае установленного соединения и **STOP** в противном случае.
PD (только на модели PWR)	В данном поле отображается текущее значение мощности, потребляемой подключенными к данному порту устройствами в случае использования функции питания устройств по витой паре (PoE) от коммутатора.
LACP	В этом поле отображается состояние протокола LACP (протокол управления агрегацией каналов) – включен он или нет на данном порту.
TxPkts	В этом поле отображается количество переданных этим портом кадров.
RxPkts	В этом поле отображается количество принятых этим портом кадров.
Errors	В этом поле отображается количество принятых этим портом кадров с ошибками.
Tx KB/s	В этом поле отображается количество переданных этим портом килобайт в секунду.
Rx KB/s	В этом поле отображается количество принятых этим портом килобайт в секунду.
Up Time	В этом поле отображается полное количество часов, минут и секунд, в течение которых порт работал.
Clear Counter	Чтобы сбросить статистику для отдельного порта, введите номер соответствующего порта и нажмите кнопку **Clear Counter**; чтобы сбросить статистику для всех портов – выберите **Any** и также нажмите кнопку **Clear Counter**.

6.2.1 Экран Status: Port Details

Чтобы отобразить статистику по отдельному порту, выберите номер в столбце **Port** на экране **Status**. Этот экран используется для отображения состояния и подробных данных о работе отдельного порта коммутатора.

Рисунок 24 Экран Status: Port Details



Поля экрана описаны в следующей таблице.

Таблица 7 Экран Status > Port Details

ПОЛЕ	ОПИСАНИЕ
Port Info	
Port NO.	В этом поле отображается номер порта.
Name	В этом поле отображается имя порта.
Link	В этом поле отображается скорость (**10M** для 10 Мбит/с, **100M** для 100 Мбит/с или **1000M** для 1000 Мбит/с) и режим дуплекса (**F** для дуплекса или **H** для полудуплекса). Кроме того, в поле отображается тип кабеля (**Copper** для витой пары или **Fiber** для оптоволокна).
Status	Если активирован протокол покрывающего дерева STP, в этом поле отображается состояние порта по протоколу STP (дополнительную информацию можно найти в разд. 11.1.3 на стр. 103). Если протокол STP отключен, в этом поле отображается FORWARDING в случае установленного соединения и STOP в противном случае.
PD PowerConsumption	Данное поле имеется только на модели PWR. В данном поле отображается текущее значение мощности, потребляемой подключенными к данному порту устройствами в случае использования функции питания устройств по витой паре (PoE) от коммутатора.

Таблица 7 Экран Status > Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
PD MaxCurrent	Данное поле имеется только на модели PWR. В данном поле отображается максимальное значение тока, потребляемого подключенными к данному порту устройствами в случае использования функции питания устройств по витой паре (PoE) от коммутатора.
PD MaxPower	Данное поле имеется только на модели PWR. В данном поле отображается максимальное значение мощности, потребляемой подключенными к данному порту устройствами в случае использования функции питания устройств по витой паре (PoE) от коммутатора.
LACP	В этом поле указано, включен ли для данного порта протокол LACP.
TxPkts	В этом поле отображается количество переданных этим портом кадров.
RxPkts	В этом поле отображается количество принятых этим портом кадров.
Errors	В этом поле отображается количество принятых этим портом кадров с ошибками.
Tx KB/s	В этом поле отображается количество переданных этим портом килобайт в секунду.
Rx KB/s	В этом поле отображается количество принятых этим портом килобайт в секунду.
Up Time	В этом поле отображается полное время, в течение которого поддерживалось соединение.
Tx Packet В следующих полях отображается подробная информация о переданных пакетах.	
TX Packets	В этом поле отображается количество переданных цельных пакетов (одноадресных, мультивещательных, широковещательных).
Multicast	В этом поле отображается количество переданных цельных мультивещательных пакетов.
Broadcast	В этом поле отображается количество переданных цельных широковещательных пакетов.
Pause	В этом поле отображается количество переданных пакетов 802.3x типа Pause.
Rx Packet В следующих полях отображается подробная информация о принятых пакетах.	
RX Packets	В этом поле отображается количество принятых цельных пакетов (одноадресных, мультивещательных, широковещательных).
Multicast	В этом поле отображается количество принятых цельных мультивещательных пакетов.
Broadcast	В этом поле отображается количество принятых цельных широковещательных пакетов.
Pause	В этом поле отображается количество принятых пакетов 802.3x типа Pause.
TX Collision В следующих полях отображается информация о коллизиях в процессе передачи.	
Single	Количество успешно переданных пакетов, передача которых была запрещена в точности одиночной коллизией.
Multiple	Количество успешно переданных пакетов, передача которых была запрещена несколькими коллизиями.
Excessive	Количество пакетов, передача которых оказалась невозможна из-за избыточного количества коллизий. Под избыточным количеством коллизий понимается максимальное количество коллизий, после которого сбрасывается счетчик попыток повторной передачи.

Таблица 7 Экран Status > Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
Late	Количество зафиксированных с опозданием коллизий, то есть коллизий, обнаруженных после передачи как минимум 512 бит пакета.
Error Packet	В следующих полях отображается подробная информация о принятых пакетах с ошибками.
RX CRC	В этом поле отображается количество пакетов, принятых с ошибкой (ошибками) циклического избыточного кода CRC.
Runt	В этом поле отображается количество принятых пакетов, оказавшихся слишком короткими (менее 64 октетов), включая пакеты с ошибками CRC.
Distribution	
64	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет 64 октета.
65-127	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 65 до 127 октетов.
128-255	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 128 до 255 октетов.
256-511	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 256 до 511 октетов.
512-1023	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 512 до 1023 октетов.
1024-1518	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 1024 до 1518 октетов.
Giant	В этом поле отображается количество пакетов, отброшенных из-за превышения максимального размера кадра.

7

Основные настройки

В данной главе описаны настройки экранов **System Info (Информация о системе)**, **General Setup (Общие настройки)**, **Switch Setup (Настройка коммутатора)**, **IP Setup (Настройка протокола IP)** и **Port Setup (Настройки портов)**.

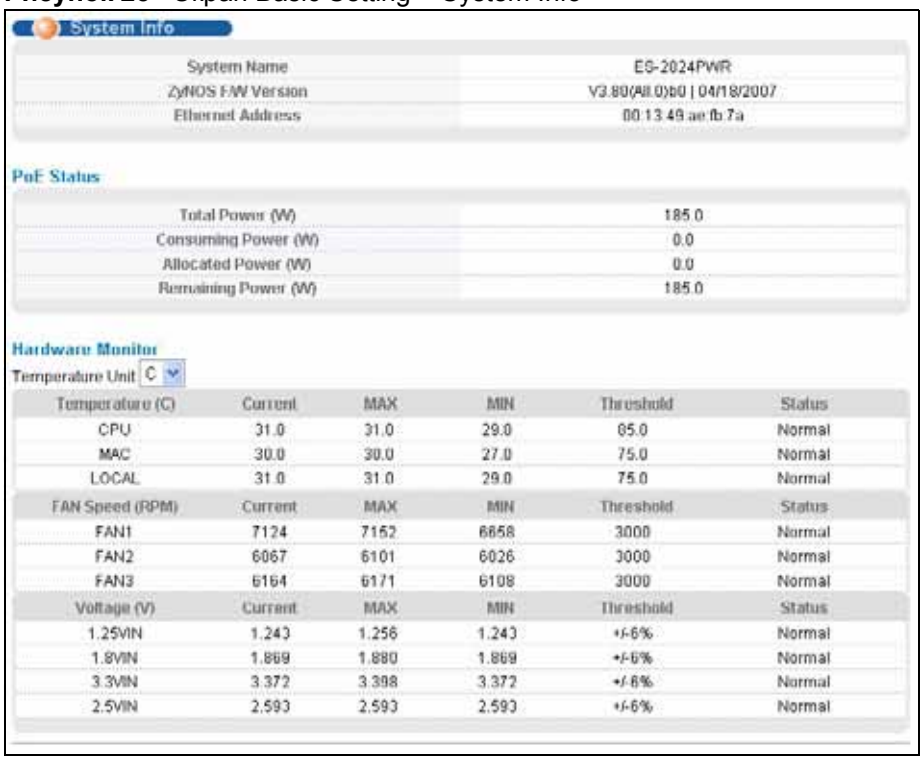
7.1 Обзор

На экране **System Info** отображается общая информация о коммутаторе (например, номер версии встроенного программного обеспечения), а также получаемые путем опроса параметры аппаратного обеспечения (например, скорость вращения вентиляторов). На экране **General Setup** можно настроить общую идентификационную информацию о коммутаторе. Кроме того, на экране **General Setup** можно вручную установить время или выбрать режим получения даты и времени с внешнего сервера при включении коммутатора. Тогда в системных журналах коммутатора будет отображаться реальное время. На экране **Switch Setup** можно установить и настроить глобальные функции коммутатора. На экране **IP Setup** можно настроить IP-адрес коммутатора в каждом из доменов маршрутизации, маску (маски) подсети и адрес сервера DNS для управления коммутатором.

7.2 Информация о системе

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting** > **System Info**. Здесь можно узнать версию встроенного программного обеспечения, а также отслеживать температуру, скорость вращения вентиляторов и напряжение коммутатора.

Рисунок 25 Экран Basic Setting > System Info



Поля экрана описаны в следующей таблице.

Таблица 8 Экран Basic Setting > System Info

ПОЛЕ	ОПИСАНИЕ
System Name	В этом поле отображается имя-описание коммутатора, с помощью которого его можно идентифицировать.
ZyNOS F/W Version	В этом поле отображается номер версии текущего встроенного программного обеспечения коммутатора, в том числе дата его создания.
Ethernet Address	В этом поле отображается MAC-адрес коммутатора для сети Ethernet.
PoE Status (Данный раздел имеется только в модели PWR)	
Total Power	В этом поле отображается суммарная мощность, которую коммутатор может направить на подключенные к портам PoE устройства, поддерживающие питание по витой паре (PoE).
Consuming Power	В этом поле отображается мощность, подаваемая в настоящее время коммутатором на подключенные устройства с поддержкой PoE.
Allocated Power	В этом поле отображается суммарная мощность, зарезервированная коммутатором для питания устройств после опроса подключенных устройств с поддержкой PoE.
Remaining Power	В этом поле отображается мощность, которую может дополнительно подать коммутатор для питания устройств по витой паре. Примечание: Для питания устройства коммутатору требуется запас мощности минимум в 16 Вт; даже если устройство PoE запрашивает меньшую мощность.

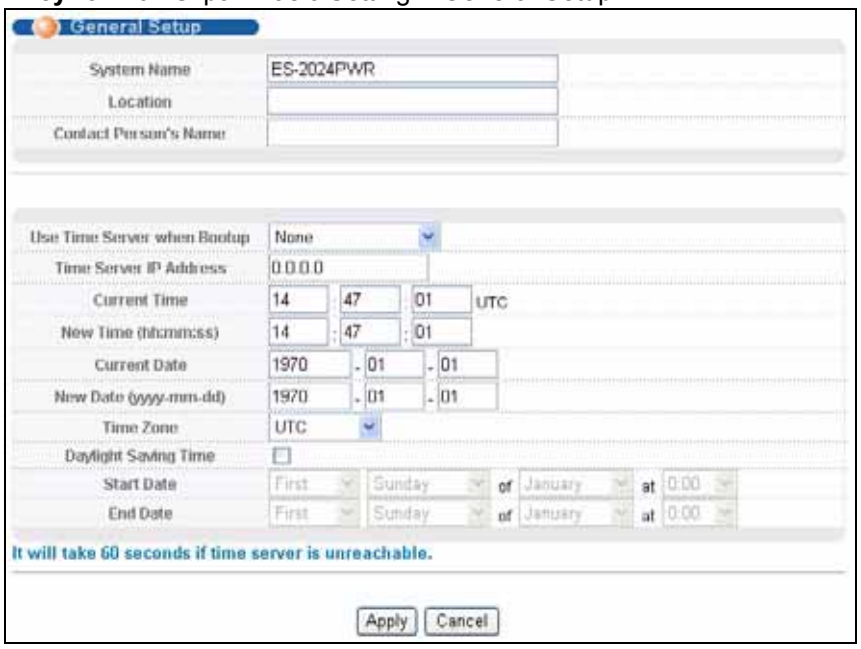
Таблица 8 Экран Basic Setting > System Info (продолжение)

ПОЛЕ	ОПИСАНИЕ
Hardware Monitor	
Temperature Unit	Предусмотренные в коммутаторе датчики температуры позволяют обнаруживать и сообщать о повышении температуры выше установленного порогового значения. В этом поле можно выбрать единицы измерения температуры (градусы по Цельсию – Centigrade, или градусы по Фаренгейту – Fahrenheit).
Температура:	Поля **MAC**, **CPU** and **LOCAL** указывают расположение датчиков температуры на печатной плате коммутатора.
Current	В этом поле отображается текущая температура, измеренная данным датчиком.
MAX	В этом поле отображается максимальная температура, измеренная данным датчиком.
MIN	В этом поле отображается минимальная температура, измеренная данным датчиком.
Threshold	В этом поле отображается верхний лимит температуры для данного датчика.
Status	Если температура не превышает порогового значения, в этом поле указывается **Normal**, в противном случае – **Error**.
Fan Speed (RPM)	Для соблюдения надлежащего теплового режима устройства огромное значение имеет правильная работа вентиляторов (наряду с хорошо вентилируемым, охлаждаемым помещением). В каждом из вентиляторов имеется датчик, который обнаруживает и сообщает о понижении скорости работы вентилятора ниже указанного порогового значения.
Current	В этом поле отображается текущая скорость вентилятора в оборотах в минуту (RPM).
MAX	В этом поле отображается максимальная измеренная скорость вентилятора в оборотах в минуту (RPM).
MIN	В этом поле отображается минимальная измеренная скорость вентилятора в оборотах в минуту (RPM). Если скорость слишком низкая и не поддается измерению (меньше 2000 об/мин), в этом поле указывается «<41».
Threshold	В этом поле отображается минимальная допустимая скорость работы вентилятора.
Status	Если скорость вентилятора выше установленного минимального значения, в этом поле указывается **Normal**. Если скорость вентилятора ниже установленного минимума, в этом поле указывается **Error**.
Voltage (V)	Для каждого значения напряжения в блоке питания имеется датчик, который способен обнаруживать и сообщать о выходе напряжения из допустимого диапазона.
Current	Текущее значение напряжения.
MAX	В этом поле отображается максимальное напряжение, измеренное в данной точке.
MIN	В этом поле отображается минимальное напряжение, измеренное в данной точке.
Threshold	В этом поле отображается допустимый процент отклонения напряжения от номинала, при котором коммутатор будет по-прежнему работать.
Status	Если напряжение в данной точке находится в допустимом диапазоне, в этом поле отображается **Normal**; в противном случае отображается **Error**.

7.3 Общие настройки

На этом экране можно сконфигурировать общие параметры, такие как имя системы и время.Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting** и **General Setup**.

Рисунок 26 Экран Basic Setting > General Setup



Поля экрана описаны в следующей таблице.

Таблица 9 Экран Basic Setting > General Setup

ПОЛЕ	ОПИСАНИЕ
System Name	Выберите имя-описание, с помощью которого можно будет идентифицировать коммутатор. Максимальная длина имени – 64 печатных символа; пробелы допускаются.
Location	Введите адрес географического местоположения коммутатора. В поле можно ввести до 32 символов в английской раскладке; пробелы допускаются.
Contact Person's Name	Введите имя ответственного лица для данного коммутатора. В поле можно ввести до 32 символов в английской раскладке; пробелы допускаются.
Use Time Server when Bootup	Укажите протокол службы времени, используемый вашим сервером времени. Не все серверы времени поддерживают все протоколы, поэтому нужный протокол, возможно, придется подбирать методом проб и ошибок. Основные различия между ними заключаются в формате времени. При выборе формата **Daytime (RFC 867)** коммутатор отображает день, месяц, год и время без учета поправки для часового пояса. При использовании этого формата рекомендуется использовать сервер времени, находящийся в вашем географическом часовом поясе. Формат **Time (RFC-868)** представляет собой 4-байтное целое, соответствующее общему количеству секунд с 0:0:0 1970/1/1. Формат **NTP (RFC-1305)** аналогичен формату Time (RFC-868). По умолчанию установлено значение **None**. Время вводится вручную. Каждый раз при включении коммутатора время и дата сбрасываются на 1970-1-1 0:0:0.

Таблица 9 Экран Basic Setting > General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Time Server IP Address	Введите IP-адрес сервера времени. Данный коммутатор будет искать сервер времени не более 60 секунд. При выборе недоступного сервера времени этот экран будет заблокирован на 60 секунд. Подождите.
Current Time	В этом поле отображается время, соответствующее моменту открытия этого меню (или его обновления).
New Time (hh:min:ss)	Введите новое время в формате «часы, минуты, секунды». После нажатия на **Apply** в поле **Current Time** появится новое время.
Current Date	В этом поле отображается дата, соответствующая моменту открытия этого меню.
New Date (yyyy-mm-dd)	Введите новую дату в формате «год, месяц, день». После нажатия на **Apply** в поле **Current Date** появится новая дата.
Time Zone	Выберите в ниспадающем списке разницу во времени между поясом UTC (всеобщее скоординированное время, ранее известное как GMT или время по Гринвичу) и вашим часовым поясом.
Daylight Saving Time	Период летнего времени – период с поздней весны до начала осени, когда во многих странах принято переводить часы на один час вперед в целях более рационального использования светлого времени суток по вечерам. При использовании летнего времени необходимо установить данный переключатель.
Start Date	Укажите день и час, когда начинается действие летнего времени (в случае выбора переключателя **Daylight Saving Time**). Время отображается в 24-часовом формате. Ниже приводится несколько примеров: Действие летнего времени в большинстве Соединенных Штатов начинается со второго воскресенья марта. В каждом из часовых поясов Соединенных Штатов летнее время вступает в силу в 2:00 по местному времени. Таким образом, для Соединенных Штатов необходимо выбрать **Second** (второе), **Sunday** (воскресенье), **March** (марта) и **2:00**. В странах Европейского Союза действие летнего времени начинается в последнее воскресенье марта. Во всех часовых поясах Европейского Союза летнее время вводится одномоментно (в 01:00 по Гринвичу или всеобщему скоординированному времени). Таким образом, для Европейского Союза необходимо выбрать **Last** (последнее), **Sunday** (воскресенье), **March** (март), а содержимое последнего поля зависит от конкретного часового пояса. Например, для Германии необходимо выбрать **2:00**, так как часовой пояс Германии соответствует +1 часу относительно Гринвича (GMT+1).
End Date	Укажите день и час, когда прекращается действие летнего времени (в случае выбора переключателя **Daylight Saving Time**). Время отображается в 24-часовом формате. Ниже приводится несколько примеров: Действие летнего времени в большинстве Соединенных Штатов прекращается с первого воскресенья ноября. В каждом из часовых поясов Соединенных Штатов летнее время отменяется в 2:00 по местному времени. Таким образом, для Соединенных Штатов необходимо выбрать **First** (первое), **Sunday** (воскресенье), **November** (ноября) и **2:00**. В странах Европейского Союза действие летнего времени прекращается в последнее воскресенье октября. Во всех часовых поясах Европейского Союза летнее время отменяется одномоментно (в 01:00 по Гринвичу или всеобщему скоординированному времени). Таким образом, для Европейского Союза необходимо выбрать **Last** (последнее), **Sunday** (воскресенье), **October** (октября), а содержимое последнего поля зависит от конкретного часового пояса. Например, для Германии необходимо выбрать **2:00**, так как часовой пояс Германии соответствует +1 часу относительно Гринвича (GMT+1).

Таблица 9 Экран Basic Setting > General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

7.4 Введение в виртуальные локальные сети (VLAN)

Виртуальные локальные сети (VLAN, Virtual Local Area Network) позволяют разделить одну физическую сеть на несколько логических. Устройства в логической сети принадлежат к одной группе. Устройство может принадлежать к нескольким группам. При использовании сетей VLAN устройство не может отправлять или принимать данные от устройств, не принадлежащих к той же группе (группам); такой трафик должен проходить через маршрутизатор.

При использовании в бизнес-центрах с несколькими арендаторами виртуальные локальные сети VLAN – важнейший компонент обеспечения изоляции и безопасности абонентов сети. При условии надлежащей настройки виртуальные локальные сети не позволяют какому-либо пользователю получить доступ к ресурсам, принадлежащим другому пользователю в той же локальной сети, то есть пользователь не увидит принтеры и жесткие диски другого пользователя в том же здании.

Кроме того, виртуальные локальные сети повышают производительность сети за счет ограничения широковещательной рассылки сравнительно небольшими и легко управляемыми логическими широковещательными доменами. В традиционных коммутируемых средах все широковещательные пакеты направляются на все без исключения порты. При использовании виртуальных локальных сетей широковещательные пакеты рассылаются лишь в конкретном широковещательном домене.

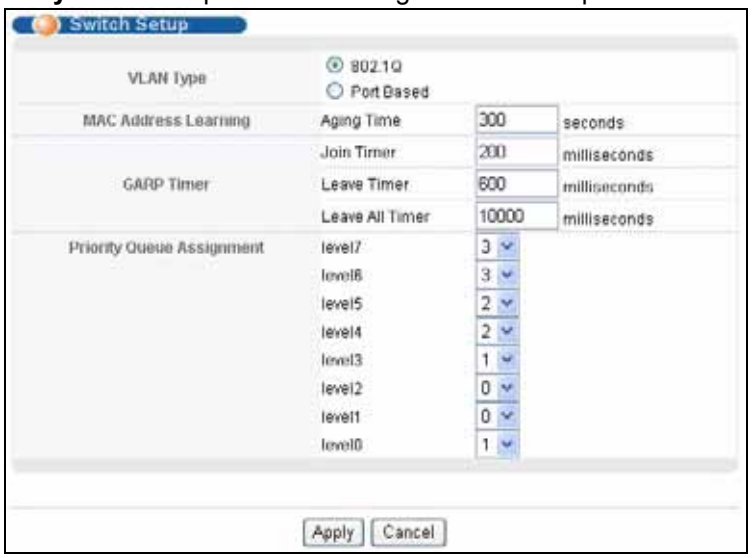
Механизм поддержки виртуальных локальных сетей VLAN работает только в одном направлении; им контролируется только исходящий трафик.

Информацию о виртуальных локальных сетях на основе портов и на основе тегов 802.1Q можно найти в гл. 8 на стр. 83.

7.5 Экран Switch Setup

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting** и **Switch Setup**. Экраны настройки виртуальных локальных сетей VLAN изменяются в зависимости о того, какой пункт выбран в поле **VLAN Type**: **802.1Q** или **Port Based**. Информацию по виртуальным локальным сетям можно найти в соответствующей главе.

Рисунок 27 Экран Basic Setting > Switch Setup



Поля экрана описаны в следующей таблице.

Таблица 10 Экран Basic Setting > Switch Setup

ПОЛЕ	ОПИСАНИЕ
VLAN Type	Выберите **802.1Q** или **Port Based**. Экран **VLAN Setup** изменится в зависимости от того, какой тип виртуальных локальных сетей VLAN выбран на этом экране: **802.1Q** или **Port Based**. Дополнительную информацию можно найти в гл. 8 на стр. 83.
MAC Address Learning	Функция получения (запоминания) MAC-адресов снижает объем исходящего широковещательного трафика. Получение MAC-адресов работает только на активных портах.
Aging Time	Введите время от 10 до 3000 секунд. Это период, в течение которого все динамически полученные MAC-адреса хранятся в таблице MAC-адресов. По его истечении они устаревают и должны быть получены заново.
GARP Timer: Коммутаторы присоединяются к виртуальным локальным сетям VLAN путем передачи декларации. Декларация представляет собой передачу сообщения **Join** с использованием протокола GARP. Декларации отменяются путем передачи сообщения **Leave**. Сообщение **Leave All** отменяет все декларации. Таймеры GARP определяют значения тайм-аута для декларации. Более подробную информацию можно найти в главе о VLAN.	
Join Timer	Параметр Join Timer определяет длительность таймера Join Period для протокола регистрации VLAN по GARP (GVRP) в миллисекундах. У каждого порта имеется таймер **Join Period**. Допустимый диапазон значений параметра **Join Time** – от 100 до 65 535 миллисекунд; по умолчанию это значение равно 200 миллисекундам. Более подробную информацию можно найти в главе о VLAN.

Таблица 10 Экран Basic Setting > Switch Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Leave Timer	Параметр Leave Time определяет длительность таймера **Leave Period** для протокола GVRP в миллисекундах. У каждого порта имеется отдельный таймер **Leave Period**. Значение параметра Leave Time должно быть в два раза больше параметра **Join Timer**; по умолчанию оно равно 600 миллисекундам.
Leave All Timer	Параметр Leave All Timer определяет длительность таймера Leave All Period для протокола GVRP в миллисекундах. У каждого порта имеется отдельный таймер Leave All Period. Значение параметра Leave All Timer должно больше параметра Leave Timer.
Priority Queue Assignment Стандарт IEEE 802.1p различает до 8 отдельных типов трафика путем добавления в кадр MAC-уровня тега, содержащего биты определения класса обслуживания. Кадры без явного тега приоритета получают на входящем порту приоритет по умолчанию. Следующие поля используются для определения соответствия между уровнями приоритетов и физическими очередями. У коммутатора имеется четыре физических очереди, которые можно поставить в соответствие 8 уровням приоритета. Трафик, попадающий в очередь с большим номером, проходит через коммутатор быстрее, тогда как трафик в очередях с меньшим номером может быть отброшен при перегрузке в сети.	
Уровень приоритета (следующие описания относятся к типам трафика, описанным в стандарте IEEE 802.1d (в него входит стандарт 802.1p)).	
Level 7	Обычно используется для трафика сетевого управления, например, сообщений настройки маршрутизаторов.
Level 6	Обычно используется для голосового трафика, который особенно чувствителен к джиттеру (джиттер – колебания времени задержки).
Level 5	Обычно используется для видеотрафика, которому требуется высокая пропускная способность и который также чувствителен к джиттеру.
Level 4	Обычно используется для трафика с контролируемой нагрузкой и высокой чувствительностью к задержкам, например, транзакций SNA.
Level 3	Обычно используется для трафика, доставляемого по принципу «максимума усилий», то есть более высокого класса, чем доставляемого по принципу «наибольших усилий». Сюда может входить важный бизнес-трафик, для которого допустимы небольшие задержки.
Level 2	Для трафика, доставляемого при наличии «лишней пропускной способности».
Level 1	Обычно используется для некритического, «фонового» трафика, например, для передачи больших объемов данных, которые разрешены, но не должны мешать другим приложениям и пользователям.
Level 0	Обычно используется для трафика, доставляемого по принципу «наибольших усилий».
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

7.6 Настройки протокола IP

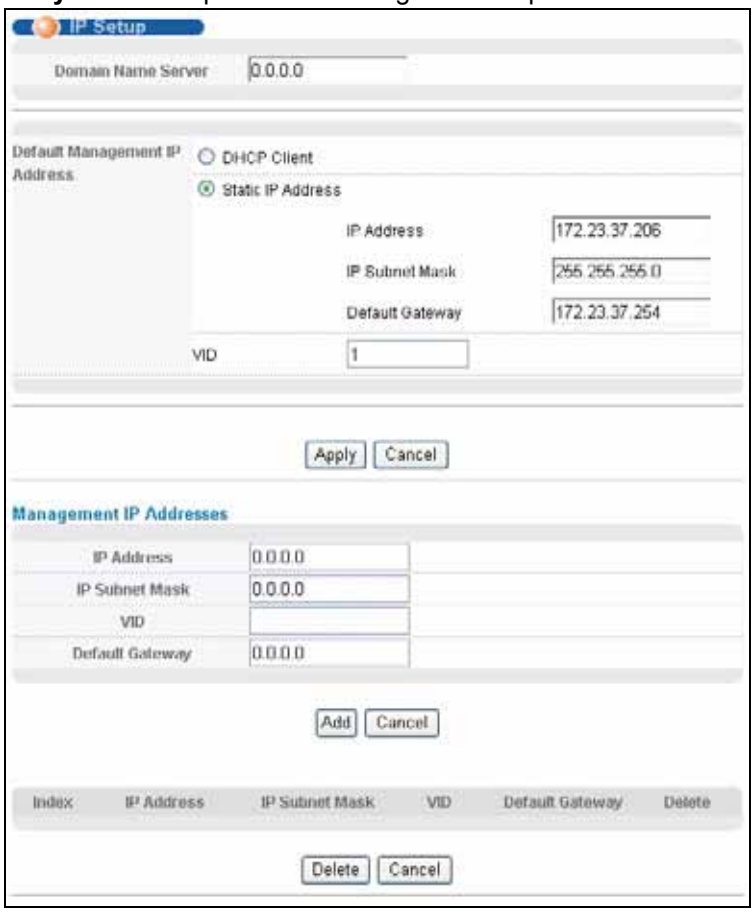
Экран **IP Setup** используется для настройки шлюза по умолчанию, сервера DNS по умолчанию и добавления IP-доменов.

7.6.1 IP-интерфейсы

Для управления через сеть коммутатору должен быть назначен IP-адрес. По умолчанию используется IP-адрес 192.168.1.1. Маска подсети определяет, какую часть в IP-адресе занимает номер сети. По умолчанию используется маска 255.255.255.0.

Можно настроить IP-адреса для доступа и управления коммутатором через порты, принадлежащее определенным виртуальным локальным сетям VLAN. Информацию о количестве поддерживаемых IP-адресов можно найти в табл. 99 на стр. 268.

Рисунок 28 Экран Basic Setting > IP Setup



Поля экрана описаны в следующей таблице.

Таблица 11 Экран Basic Setting > IP Setup

ПОЛЕ	ОПИСАНИЕ
Domain Name Server	Сервер DNS (системы доменных имен) определяет соответствие между доменным именем и IP-адресом, и наоборот. Введите IP-адрес сервера DNS, чтобы вместо IP-адресов можно было использовать доменные имена.
Default Management IP Address В этих полях можно настроить IP-адрес управления по умолчанию.	
DHCP Client	Выберите эту опцию, если у вас имеется DHCP-сервер, который может назначить коммутатору IP-адрес и маску подсети, IP-адрес шлюза по умолчанию и IP-адрес сервера DNS.

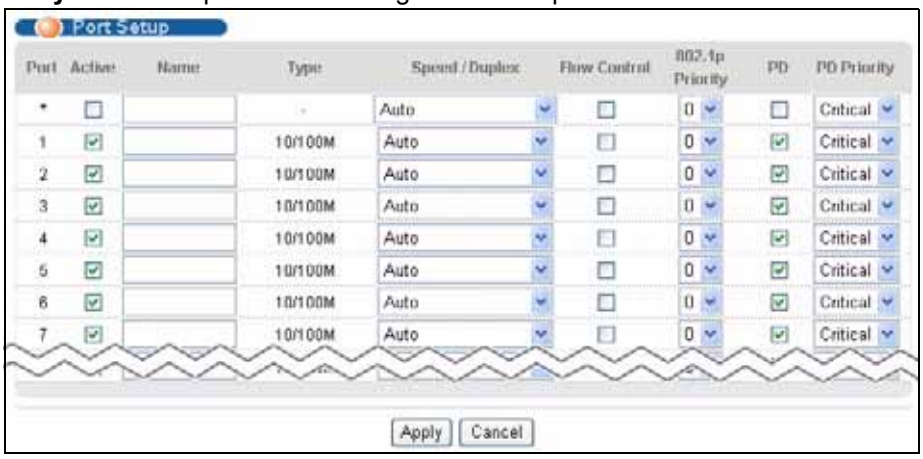
Таблица 11 Экран Basic Setting > IP Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Static IP Address	Выберите эту опцию, если у вас нет DHCP-сервера или вы хотите назначить коммутатору статический IP-адрес. При выборе этой опции нужно заполнить следующие поля.
IP Address	Введите IP-адрес коммутатора в виде десятичных чисел, разделенных точками, например 192.168.1.1.
IP Subnet Mask	Введите IP-маску подсети коммутатора в виде десятичных чисел, разделенных точками, например 255.255.255.0.
Default Gateway	Введите IP-адрес исходящего шлюза по умолчанию в виде десятичных чисел, разделенных точками, например 192.168.1.254.
VID	Введите идентификационный номер VLAN, связанный с IP-адресом коммутатора. Этот идентификатор VLAN центрального процессора (CPU) используется только для управления. По умолчанию используется номер «1». По умолчанию все порты являются фиксированными членами этой «VLAN управления», чтобы устройством можно было управлять с любого порта. Если порт не является членом этой VLAN, то пользователи этого порта не получат доступ к устройству. При получении доступа к коммутатору, убедитесь, что порт, через который происходит подключение, является членом VLAN управления.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы сбросить поля к предыдущим значениям.
Management IP Addresses В этих полях настраиваются дополнительные IP-адреса управления.	
IP Address	Введите IP-адрес для управления коммутатором членами VLAN, указанной в поле **VID** ниже.
IP Subnet Mask	Введите IP-маску подсети в виде десятичных чисел, разделенных точками. Например, 255.255.255.0.
VID	Введите идентификационный номер VLAN.
Default Gateway	Введите IP-адрес исходящего шлюза по умолчанию в виде десятичных чисел, разделенных точками, например 192.168.1.254.
Add	Нажмите **Add**, чтобы добавить новое правило для коммутатора. После этого он появится в итоговой таблице внизу экрана. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы сбросить поля к предыдущим значениям.
Index	В этом поле отображается порядковый номер записи.
IP Address	В этом поле отображается IP-адрес управления коммутатором.
IP Subnet Mask	В этом поле отображается маска подсети для соответствующего IP-адреса.
VID	В этом поле отображается идентификационный номер VLAN.
Default Gateway	В этом поле отображается IP-адрес шлюза по умолчанию.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

7.7 Настройки портов

Настройки портов коммутатора осуществляются на этом экране. Чтобы открыть экран настроек порта, выберите в навигационной панели **Basic Setting** > **Port Setup**.

Рисунок 29 Экран Basic Setting > Port Setup



Поля экрана описаны в следующей таблице.

Таблица 12 Экран Basic Setting > Port Setup

ПОЛЕ	ОПИСАНИЕ
Port	Порядковый номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить порт. По умолчанию все порты включены. Передача данных происходит только через включенные порты.
Name	Введите имя-описание для идентификации порта. В поле можно ввести до 64 алфавитно-цифровых символов. Примечание: Из-за ограниченного места на некоторых экранах Web-конфигуратора имя порта может отображаться не полностью.
Type	В этом поле используется обозначение **10/100M** для подключений Ethernet/Fast Ethernet и **10/100/1000M** – для подключений Gigabit Ethernet.

Таблица 12 Экран Basic Setting > Port Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Speed/Duplex	Выберите скорость и режим дуплекса для Ethernet-соединения на этом порту. Возможны значения **Auto** (автосогласование), **10M/Half Duplex** (10 Мбит/с, полудуплекс), **10M/Full Duplex** (10 Мбит/с, дуплекс), **100M/Half Duplex** (100 Мбит/с, полудуплекс), **100M/Full Duplex** (100 Мбит/с, дуплекс) и **1000M/Full Duplex** (1000 Мбит/с, дуплекс) (только для портов Gigabit Ethernet). Значение **Auto** (автосогласование) позволяет порту автоматически согласовать с подключенным портом и выбрать скорость соединения и режим дуплекса, которые поддерживают оба порта. Когда автосогласование включено, порт коммутатора автоматически обменивается данными с портом на другой стороне и сам выбирает скорость соединения и режим дуплекса. Если порт на другой стороне не поддерживает автосогласование, или на нем эта функция отключена, коммутатор определяет скорость по сигналу в кабеле и выставляет полудуплексный режим. Когда функция автосогласования отключена, при подключении порт использует заранее определенную скорость и режим дуплекса. Таким образом, чтобы соединение произошло, у порта на другой стороне должны быть точно такие же параметры, что и у порта коммутатора.
Flow Control	Концентрация трафика на порту вызывает падение пропускной способности и перегружает буферную память, из-за чего происходит отбрасывание пакетов и потеря кадров. Функция управления потоком (**Flow Control**) используется для регулирования передачи сигналов в зависимости от пропускной способности принимающего порта. Данный коммутатор использует управление потоком по стандарту IEEE 802.3x в дуплексном режиме и управление потоком методом обратного давления (противодавления) в полудуплексном режиме. Управление потоком по стандарту IEEE 802.3x в дуплексном режиме подразумевает отправку сигнала паузы на передающий порт, что позволяет приостановить передачу при переполнении буфера принимающего порта. Управление потоком методом обратного давления обычно применяется в полудуплексном режиме и предполагает отправку на передающий порт сигнала коллизии (имитацию состояния коллизии), из-за чего передающий порт на некоторое время приостанавливает передачу. Чтобы включить эту функцию, установите переключатель **Flow Control**.
802.1p Priority	Это значение приоритета добавляется к входящим кадрам, не имеющим тега приоритета очередности (802.1p).Дополнительную информацию можно найти в описании поля **Priority Queue Assignment** в табл. 10 на стр. 73.
PD	Данное поле предусмотрено только в модели PWR, причем для гигабитных портов и портов mini-GBIC оно недоступно. Питаемым устройством (powered device, PD) называется устройство (например, точка доступа или коммутатор), поддерживающее стандарт питания по витой паре PoE, благодаря чему оно может получать питание от другого устройства через порт Ethernet на 10/100 Мбит/с. Установите переключатель для тех портов, через которые необходимо разрешить питание коммутатором подключенных устройств.
PD Priority	Данное поле предусмотрено только в модели PWR, причем для гигабитных портов и портов mini-GBIC оно недоступно. Если совокупная мощность, запрошенная питаемыми устройствами, превышает максимальную мощность коммутатора, которую он способен отдавать для питания устройств по витой паре, питание будет направляться коммутатором на те порты, для которых с помощью данного поля установлен более высокий приоритет. Самый высокий приоритет имеют порты, обозначенные как **Critical**. Между портами с приоритетом **High** резерв мощности будет распределяться коммутатором после того, как питание будет обеспечено по всем портам с приоритетом **Critical**. Между портами с приоритетом **Low** резерв мощности будет распределяться коммутатором после того, как питание будет обеспечено по всем портам с приоритетами **Critical** и **High**.

Таблица 12 Экран Basic Setting > Port Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

Часть III
Расширенные настройки

8

Виртуальные локальные сети (VLAN)

Тип отображаемого экрана зависит от того, какой тип VLAN (параметр **VLAN Type**) был выбран на экране настроек коммутатора (**Switch Setup**). В данной главе рассматривается конфигурирование виртуальных локальных сетей на основе тегов (стандарт 802.1Q) и виртуальных локальных сетей на основе портов.

8.1 Введение в виртуальные локальные сети на основе тегов (согласно IEEE 802.1Q)

В виртуальных локальных сетях на основе тегов для определения принадлежности кадра к определенной VLAN на мостах используется явный тег (идентификатор VLAN) в MAC-заголовке – такие теги не привязаны к коммутатору, на котором были созданы. Виртуальные локальные сети могут создаваться статически (вручную) или динамически с помощью протокола динамической регистрации VLAN по GARP (GVRP). Идентификатор VLAN ассоциирует кадр с конкретной сетью VLAN и предоставляет информацию, которая необходима коммутаторам для обработки кадра при его прохождении по сети. Кадр с тегом на четыре байта больше кадра без тега и включает в себя два байта TPID (идентификатор протокола тега, он находится в поле типа/длины Ethernet-кадра) и два байта TCI (контрольная информация тега, начинается после поля адреса источника в Ethernet-кадре).

Однобитный флаг CFI (индикатор канонического формата) для Ethernet-коммутаторов всегда устанавливается равным нулю. Если у кадра, полученного через Ethernet-порт, флаг CFI равен 1, то этот кадр нельзя передать «как есть» на порт без тега. Оставшиеся 12 бит определяют идентификатор VLAN, поэтому максимально возможное количество сетей VLAN составляет 4 096. Следует иметь в виду, что уровень приоритета пользователя и идентификатор VLAN не зависят друг от друга. Кадр с идентификатором VLAN (VID), равным нулю (0), называется кадром приоритета. В таком кадре значение имеет только уровень приоритета, а в качестве идентификатора VID кадру назначается идентификатор VID по умолчанию входящего порта. Из 4096 возможных идентификаторов VLAN значение VID, равное нулю, используется для идентификации кадров приоритета, а значение 4095 (FFF) зарезервировано, поэтому максимальное количество конфигураций VLAN составляет 4094.

TPID 2 байта	Приоритет пользователя 3 бита	CFI 1 бит	VLAN ID 12 бит

8.1.1 Пересылка кадров с тегами и без тегов

Через каждый порт коммутатора могут проходить как кадры с тегами, так и кадры без тегов. Чтобы переслать кадр с коммутатора с поддержкой VLAN на основе 802.1Q на коммутатор без поддержки таких VLAN, коммутатор сначала определяет, куда требуется переслать этот кадр, а потом удаляет тег VLAN. Чтобы переслать кадр с коммутатора без поддержки VLAN на основе 802.1Q на коммутатор, поддерживающий такие VLAN, коммутатор сначала определяет, куда требуется переслать этот кадр, а потом вставляет тег VLAN, содержащий идентификатор VLAN по умолчанию входящего порта. В качестве PVID по умолчанию используется VLAN 1 для всех портов, но эту установку можно изменить.

Широковещательные кадры (а также кадры мультивещания для известной системе группы мультивещания) дублируются только на те порты, которые входят в группу VID (за исключением самого входящего порта), ограничивая таким образом широковещание конкретным доменом.

8.2 Автоматическая регистрация VLAN

Для автоматической регистрации членов VLAN коммутаторами используются протоколы GARP и GVRP.

8.2.1 Протокол GARP

Протокол GARP (Протокол регистрации по общим атрибутам) позволяет коммутаторам в сети регистрировать и снимать регистрацию значений атрибутов на других устройствах с поддержкой GARP внутри локальных сетей на основе мостов. GARP – это протокол, предоставляющий общий механизм работы для протоколов, которые имеют более конкретное применение, таких как протокол GVRP.

8.2.1.1 Таймеры GARP

Коммутаторы присоединяются к виртуальным локальным сетям VLAN путем передачи декларации. Декларация представляет собой передачу сообщения Join с использованием протокола GARP. Декларации отменяются путем передачи сообщения Leave. Сообщение Leave All отменяет все декларации. Таймеры GARP определяют значения тайм-аута для декларации.

8.2.2 Протокол GVRP

GVRP (GARP VLAN Registration Protocol, протокол регистрации VLAN по GARP) является протоколом регистрации, который определяет способ регистрации коммутаторами необходимых членов VLAN на портах в сети. Включение этой функции разрешает создание групп VLAN за пределами локального коммутатора.

Общая терминология сетей VLAN на основе IEEE 802.1Q описана в следующей таблице.

Таблица 13 Терминология сетей VLAN на основе IEEE 802.1Q

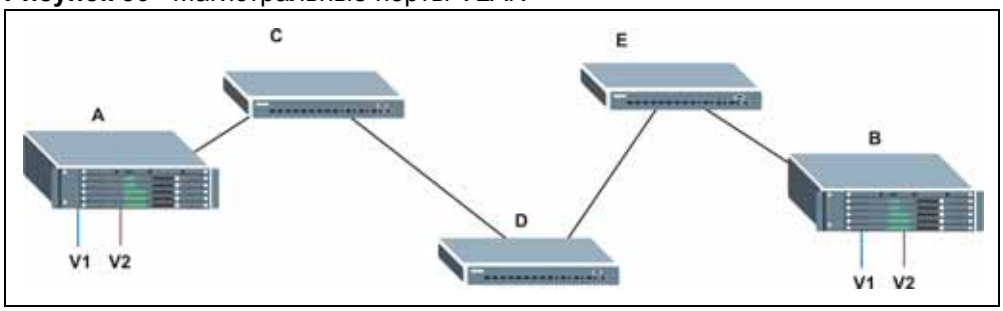
ПАРАМЕТРЫ VLAN	ТЕРМИН	ОПИСАНИЕ
Тип VLAN	Постоянная VLAN	Статическая виртуальная локальная сеть VLAN, созданная вручную.
	Динамическая VLAN	Сеть VLAN, настроенная в процессе регистрации/ дерегистрации протоколом GVRP.
Административный контроль над VLAN	Фиксированная регистрация	Порты с фиксированной регистрацией являются постоянными членами VLAN.
	Регистрация запрещена	Портам с запрещенной регистрацией запрещено присоединяться к указанной VLAN.
	Нормальная регистрация	Порты динамически присоединяются к VLAN с использованием протокола GVRP.
Управление тегами VLAN	С тегами	Порты, принадлежащие к данной VLAN, добавляют теги ко всем передаваемым исходящим кадрам.
	Без тегов	Порты, принадлежащие к данной VLAN, не добавляют теги ко всем передаваемым исходящим кадрам.
Порт VLAN	Идентификатор порта VLAN	Идентификатор VLAN, назначаемый получаемым через этот порт кадрам без тегов.
	Acceptable Frame Type	Можно выбрать один из режимов – принимать ли на порт входящие кадры как с тегами, так и без тегов, принимать только кадры с тегами или только кадры без тегов.
	Фильтрация входящих кадров	Если этот параметр включен, коммутатор отбрасывает входящие кадры для VLAN, членом которых не является данный порт.

8.3 Магистральные порты VLAN

Включение параметра **VLAN Trunking** для порта позволяет разрешить прохождение через этот порт кадров, принадлежащих неизвестным группам VLAN. Это полезно, если требуется настроить группы VLAN на конечных устройствах без необходимости настраивать те же группы на промежуточных устройствах.

См. следующий рисунок. Предположим, что требуется создать группы VLAN 1 и 2 (V1 и V2) на устройствах A и B. Без функции магистральных соединений VLAN (**VLAN Trunking**) необходимо будет настроить группы VLAN 1 и 2 на всех промежуточных коммутаторах C, D и E; в противном случае они будут отбрасывать кадры с тегами неизвестных групп VLAN. Однако, если на порту(портах) каждого промежуточного коммутатора будет включен параметр **VLAN Trunking**, то группы VLAN нужно будет создать только на конечных устройствах (A и B). Устройства C, D и E автоматически позволят кадрам с тегами групп VLAN 1 и 2 (то есть групп VLAN, о которых этим устройствам не известно) проходить через свои магистральные порты VLAN.

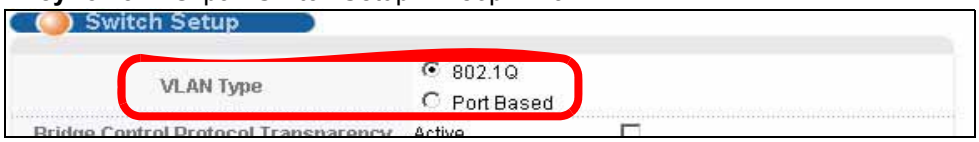
Рисунок 30 Магистральные порты VLAN



8.4 Выбор типа VLAN

Тип VLAN выбирается на экране **Basic Setting > Switch Setup**.

Рисунок 31 Экран Switch Setup: выбор типа VLAN



8.5 Статические VLAN

Статические виртуальные локальные сети используется, если входящий через порт кадр должен быть

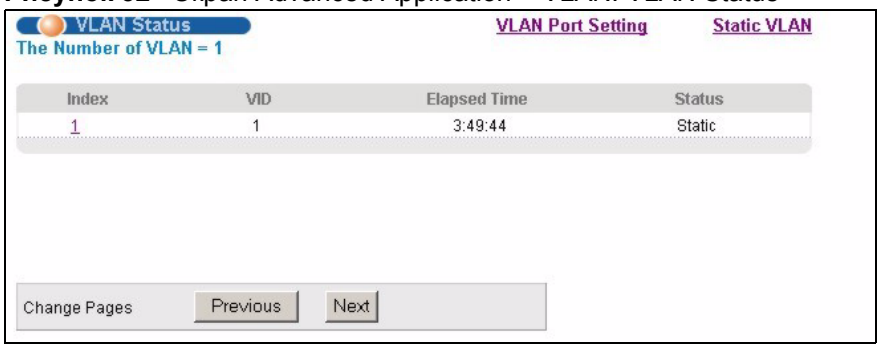
- отправлен в группу VLAN обычным образом, в зависимости от его тега VLAN.
- отправлен в группу независимо от того, имеется у него тег VLAN или нет.
- заблокирован от направления в группу VLAN независимо от его тега VLAN.

Кроме того, имеется возможность добавлять ко всем исходящим кадрам (ранее не имевшим тегов), отправляемым через порт, указанный идентификатор VLAN.

8.5.1 Состояние статической VLAN

Дополнительную информацию о статических VLAN можно найти в разд. 8.1 на стр. 83.Чтобы отобразить показанный ниже экран **VLAN Status**, выберите в навигационной панели **Advanced Application** > **VLAN**.

Рисунок 32 Экран Advanced Application > VLAN: VLAN Status



Поля экрана описаны в следующей таблице.

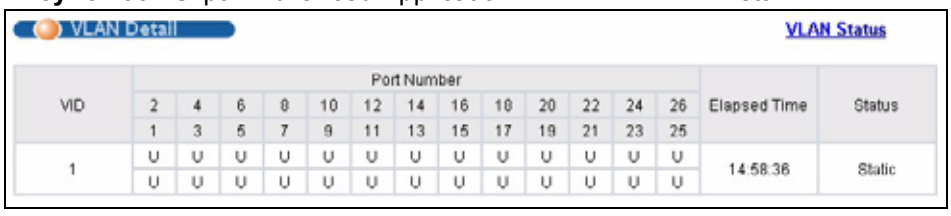
Таблица 14 Экран Advanced Application > VLAN: VLAN Status

ПОЛЕ	ОПИСАНИЕ
The Number of VLAN	Количество виртуальных локальных сетей (VLAN), настроенных на коммутаторе.
Index	Порядковый номер VLAN. Нажатие на порядковом номере позволяет отобразить более подробную информацию о сети VLAN.
VID	Идентификационный номер VLAN, определенный ранее на экране **Static VLAN**.
Elapsed Time	В этом поле отображается время, в течение которого была зарегистрирована обычная VLAN или настроена статическая VLAN.
Status	В этом поле указано, каким образом VLAN была настроена на коммутаторе; **Dynamic** – с использованием протокола GVRP, **Static** – добавлена в качестве постоянной записи или **Other** – добавлена другим способом, например, с использованием механизма регистрации VLAN-сети мультивещания (MVR).
Change Pages	Нажмите **Previous** или **Next**, чтобы отобразить предыдущий/следующий экран, если информация о состоянии не помещается на одном экране.

8.5.2 Подробная информация о статической VLAN

На этом экране отображается подробные настройки портов и информация о состоянии группы VLAN. Дополнительную информацию о статических VLAN можно найти в разд. 8.1 на стр. 83. Чтобы отобразить экран подробной информации о сети VLAN, нажмите на порядковом номере сети на экране **VLAN Status**.

Рисунок 33 Экран Advanced Application > VLAN > VLAN Detail



Поля экрана описаны в следующей таблице.

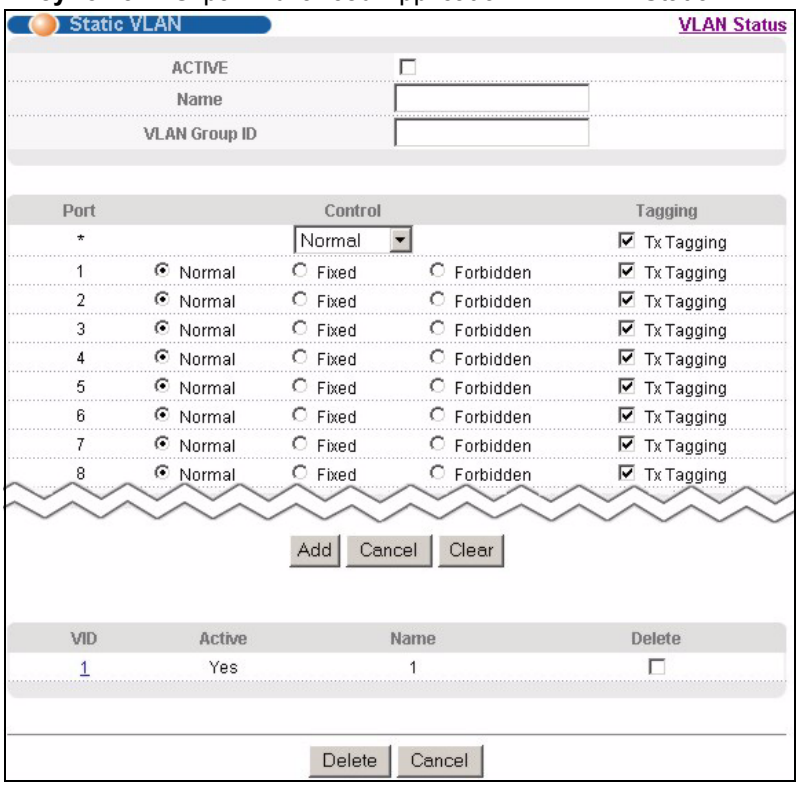
Таблица 15 Экран Advanced Application > VLAN > VLAN Detail

ПОЛЕ	ОПИСАНИЕ
VLAN Status	Нажатие на этой ссылке позволяет перейти к экрану **VLAN Status**.
VID	Идентификационный номер VLAN, определенный ранее на экране **Static VLAN**.
Port Number	В этом столбце отображаются порты, участвующие в VLAN. Порт с тегом обозначается буквой **T**, порт без тега – буквой **U**, а порты, не являющиеся членами VLAN – знаком «**–**».
Elapsed Time	В этом поле отображается время, в течение которого была зарегистрирована обычная VLAN или настроена статическая VLAN.
Status	В этом поле указано, каким образом VLAN была настроена на коммутаторе; **Dynamic** – с использованием протокола GVRP, **Static** – добавлена в качестве постоянной записи или **Other** – добавлена другим способом, например, с использованием механизма регистрации VLAN-сети мультивещания (MVR).

8.5.3 Настройка статической VLAN

На этом экране можно настроить и просмотреть параметры сети VLAN на основе 802.1Q коммутатора. Дополнительную информацию о статических VLAN можно найти в разд. 8.1 на стр. 83. Для настройки статической VLAN нажмите **Static VLAN** на экране **VLAN Status**. Откроется экран меню, показанный ниже.

Рисунок 34 Экран Advanced Application > VLAN > Static VLAN



Поля экрана описаны в следующей таблице.

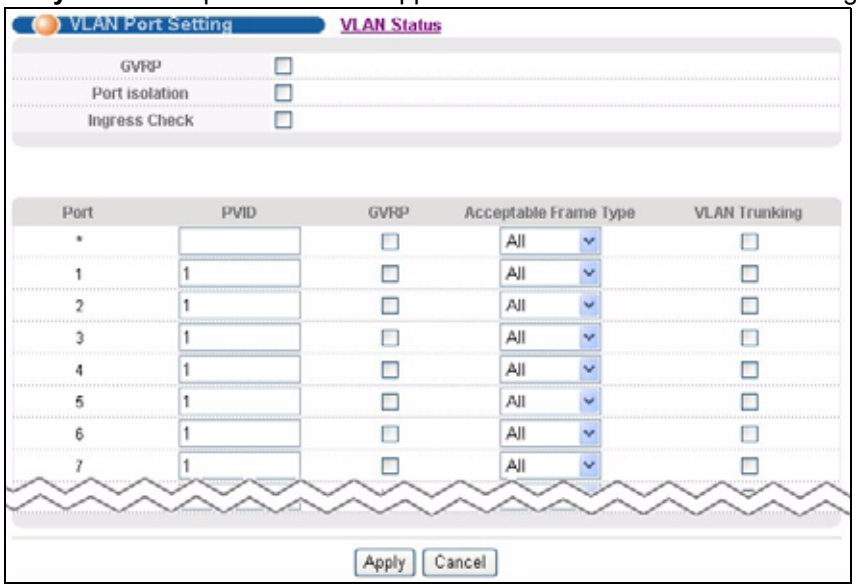
Таблица 16 Экран Advanced Application > VLAN > Static VLAN

ПОЛЕ	ОПИСАНИЕ
ACTIVE	Установите этот переключатель, чтобы включить настройки VLAN.
Name	Введите имя-описание VLAN, с помощью которого ее можно идентифицировать. Максимальная длина имени – 64 печатных символа; пробелы допускаются.
VLAN Group ID	Введите идентификатор VLAN для данной статической записи; допустимое значение находится в диапазоне от 1 до 4094.
Port	Номер порта – определяет настраиваемый порт.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Control	Выберите **Normal**, если порт должен присоединяться к данной группе VLAN динамически с использованием протокола GVRP. Данный параметр выбран по умолчанию. Выберите **Fixed**, если порт должен стать постоянным членом данной группы VLAN. Выберите **Forbidden**, чтобы запретить порту присоединяться к данной группе VLAN.
Tagging	Установите переключатель **TX Tagging**, чтобы порт добавлял теги ко всем исходящим кадрам, отправляемым с идентификатором этой группы VLAN.
Add	Нажмите **Add**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Clear	Нажмите **Clear**, чтобы начать настройку на этом экране заново.
VID	В этом поле отображается идентификационный номер группы VLAN. Нажмите на этот номер, чтобы редактировать настройки VLAN.
Active	В этом поле отображается текущее состояние настроек VLAN – включены (**Yes**) или отключены (**No**).
Name	В этом поле отображается имя-описание группы VLAN.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

8.5.4 Настройка порта VLAN

Для настройки параметров статической VLAN (на основе IEEE 802.1Q) для порта используется экран VLAN Port Setting. Дополнительную информацию о статических VLAN можно найти в разд. 8.1 на стр. 83.Нажмите на ссылке **VLAN Port Setting** на экране **VLAN Status**.

Рисунок 35 Экран Advanced Application > VLAN > VLAN Port Setting



Поля экрана описаны в следующей таблице.

Таблица 17 Экран Advanced Application > VLAN > VLAN Port Setting

ПОЛЕ	ОПИСАНИЕ
GVRP	GVRP (GARP VLAN Registration Protocol, протокол регистрации VLAN по GARP) является протоколом регистрации, который определяет способ регистрации коммутаторами необходимых членов VLAN на портах в сети. Включение этой функции разрешает создание групп VLAN за пределами локального коммутатора.
Port Isolation	С помощью параметра изоляции портов **Port Isolation** можно запретить каждому из портов обмениваться данными друг с другом – обмен будет разрешен только с портом управления CPU и гигабитными портами каскадирования. Этот вариант является самым ограничивающим, но в то же время и самым безопасным.
Ingress Check	Установите этот переключатель, если необходимо включить фильтрацию входящих кадров на коммутаторе. Снимите выделение с переключателя, если требуется отключить фильтрацию входящих кадров на коммутаторе.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
PVID	Введите номер от 1 до 4094 в качестве идентификатора VLAN для порта.
GVRP	Установите этот переключатель, чтобы включить на этом порту протокол GVRP.

Таблица 17 Экран Advanced Application > VLAN > VLAN Port Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
Acceptable Frame Type	Укажите тип кадров, разрешенных для данного порта. Можно выбрать значение **All** или **Tag Only**. Выбор **All** в ниспадающем списке разрешает прием через этот порт как кадров с тегами, так и кадров без тегов. Это значение выбрано по умолчанию. Выбор **Tag Only** разрешает прием через этот порт только кадров с тегами. Все кадры без тегов будут отброшены.
VLAN Trunking	Установите переключатель **VLAN Trunking** для портов, подключенных к другим коммутаторам или маршрутизаторам (но не для портов, напрямую подключенных к конечным пользователям), чтобы разрешить прохождение через коммутатор кадров, принадлежащих к неизвестным группам VLAN.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

8.6 Настройка VLAN на основе портов

Виртуальные локальные сети на основе портов – это такие VLAN, в которых решение о пересылке пакета принимается на основе MAC-адреса назначения и связанного с ним порта.

Для VLAN на основе портов требуется разрешение исходящей передачи для всех портов. Таким образом, чтобы позволить двум пользователям общаться друг с другом, например, между конференц-залами в отеле, необходимо разрешить исходящую передачу данных для обоих портов.

VLAN на основе портов действуют только на том коммутаторе, на котором они были созданы.

При активировании VLAN на основе портов коммутатор по умолчанию назначает ей идентификатор 1. Изменить его нельзя.

На тех экранах (например, **IP Setup** и **Filtering**), где требуется ввести идентификатор VLAN, в качестве такого идентификатора следует вводить 1.

Экран настройки VLAN на основе портов показан на следующем рисунке. В состав VLAN входит управляющий порт **CPU** и все Ethernet-порты.

8.6.1 Настройка VLAN на основе портов

Выберите **Port Based** в качестве типа VLAN (**VLAN Type**) на экране **Switch Setup**, затем нажмите **VLAN** в навигационной панели. Появится следующий экран.

Рисунок 36 Экран Advanced Application > VLAN: Port Based VLAN Setup (All Connected)

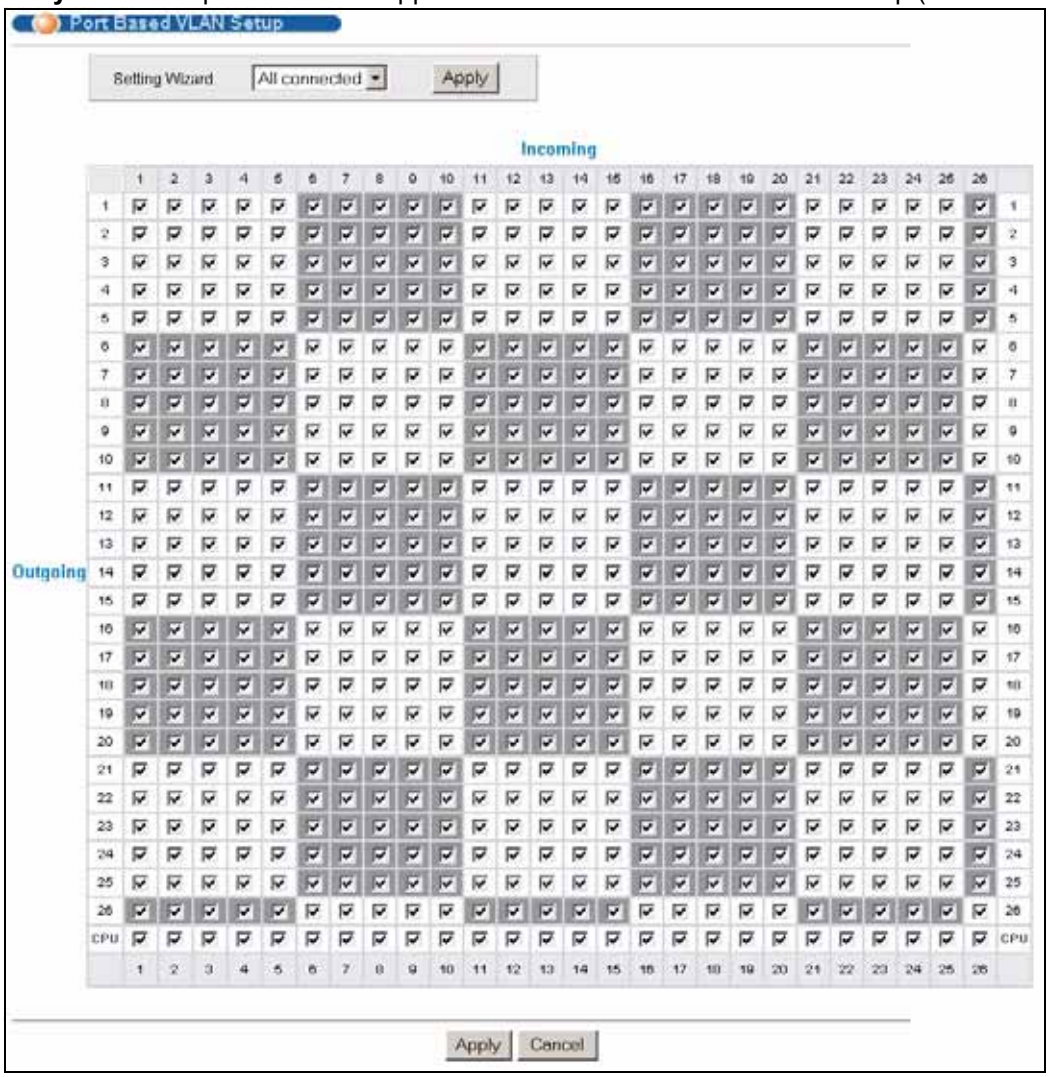
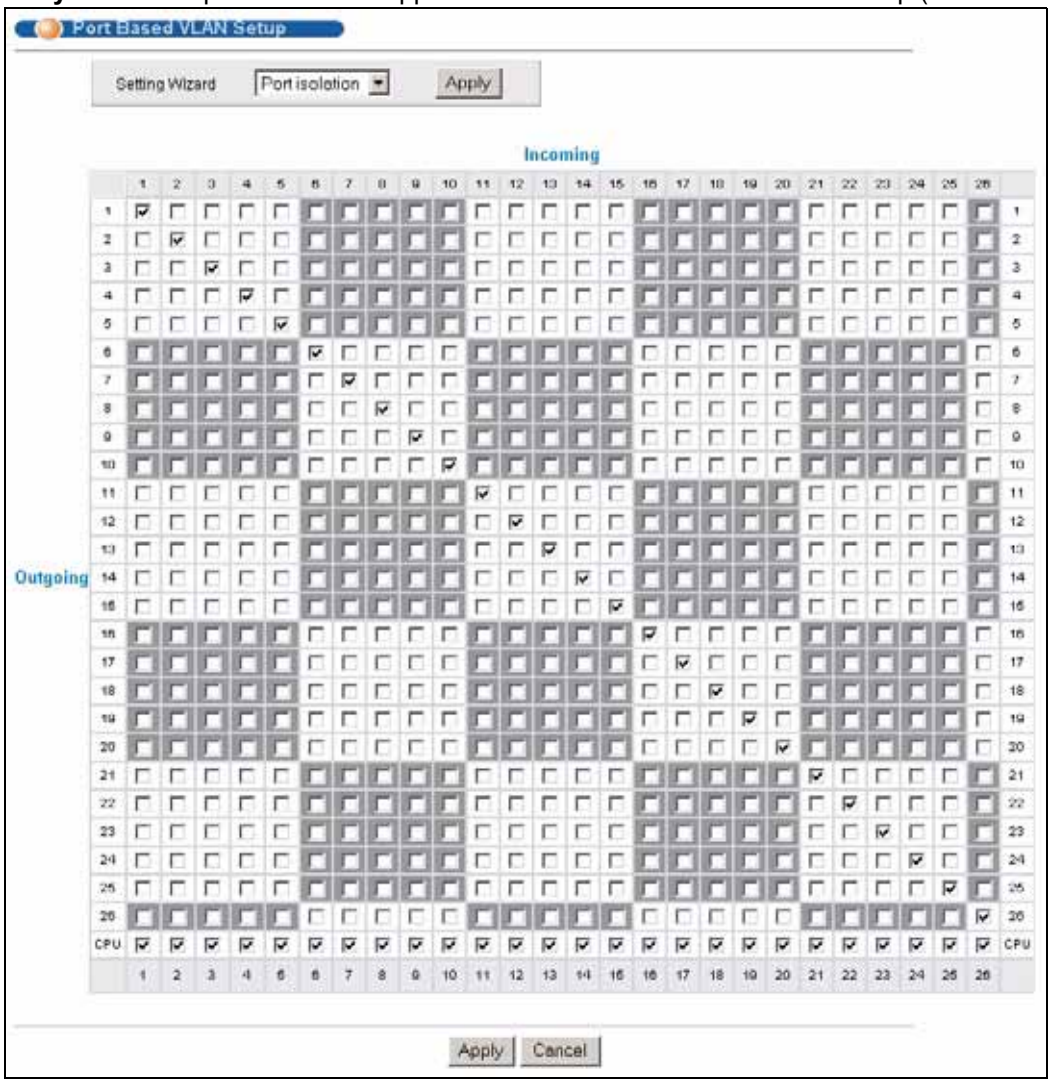


Рисунок 37 Экран Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



Поля экрана описаны в следующей таблице.

Таблица 18 Экран Advanced Application > VLAN: Port Based VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Setting Wizard	Выберите значение **All connected** или **Port isolation**. Значение **All connected** означает, что все порты могут обмениваться данным друг с другом, то есть виртуальных локальных сетей нет. Выбраны все входящие и исходящие порты. Этот вариант наиболее гибок, но в то же время наименее безопасен. Значение **Port isolation** означает, что каждый порт может обмениваться данными только с управляющим портом CPU, и не может с остальными портами. При этом будут выбраны все входящие порты, а из исходящих – только порт CPU. Этот вариант является самым ограничивающим, но в то же время и самым безопасным. Сделав выбор, нажмите кнопку **Apply** (она находится в правой верхней части экрана), чтобы отобразить экраны в том виде, как указано выше. Вы можете вносить изменения в эти настройки, добавляя или удаляя входящие или исходящие порты, но тогда необходимо нажимать кнопку **Apply** в нижней части экрана.
Incoming	Входящие порты; входящий порт – это тот порт, через который пакет данных попадает в коммутатор. Чтобы позволить двум абонентским портам общаться друг с другом, оба порта необходимо определить как входящие. Числа в верхнем ряду относятся к входящим портам, а соответствующие им исходящие порты перечислены слева. Порт **CPU** – это управляющий порт коммутатора. По умолчанию он входит в виртуальную локальную сеть со всеми Ethernet-портами. Если в состав этой VLAN не входит какой-либо из портов, то управлять коммутатором через этот порт нельзя.
Outgoing	Исходящие порты; исходящий порт – это тот порт, через который пакет данных покидает коммутатор. Чтобы позволить двум абонентским портам общаться друг с другом, оба порта необходимо определить как исходящие. Порт **CPU** – это управляющий порт коммутатора. По умолчанию он входит в виртуальную локальную сеть со всеми Ethernet-портами. Если в состав этой VLAN не входит какой-либо из портов, то управлять коммутатором через этот порт нельзя.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

9

Настройка пересылки на основе статических MAC-адресов

Описанные ниже экраны используются для настройки пересылки на основе статических MAC-адресов.

9.1 Обзор

В данной главе рассказывается о настройке правил пересылки на основе MAC-адресов устройств в вашей сети.

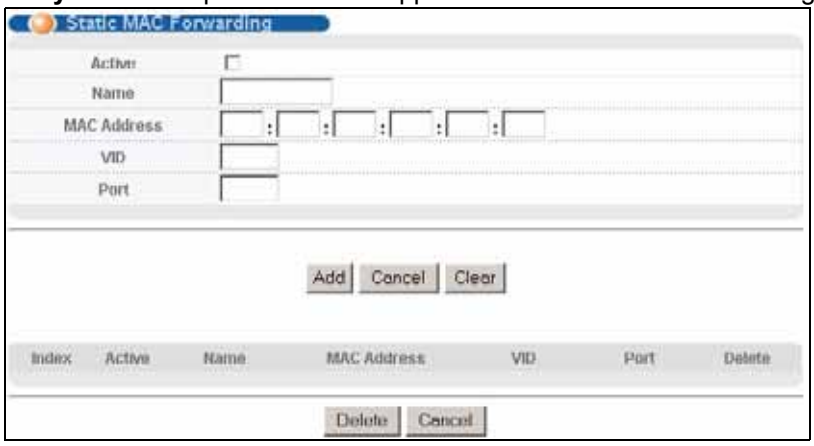
9.2 Настройка пересылки на основе статических MAC-адресов

Статический MAC-адрес – это адрес, вручную внесенный в таблицу MAC-адресов. Статические MAC-адреса не имеют срока действия. При настройке правил для статических MAC-адресов для порта определяются статические MAC-адреса. Это позволяет снизить объемы широковещательного трафика.

Пересылка на основе статических MAC-адресов вместе со средствами безопасности портов позволяют разрешить доступ к коммутатору только тем компьютерам, MAC-адреса которых указаны в таблице MAC-адресов для порта. Более подробную информацию о средствах безопасности портов можно найти в гл. 17 на стр. 139.

Чтобы отобразить показанный ниже экран настройки, выберите в навигационной панели **Advanced Applications > Static MAC Forwarding**.

Рисунок 38 Экран Advanced Application > Static MAC Forwarding



Поля экрана описаны в следующей таблице.

Таблица 19 Экран Advanced Application > Static MAC Forwarding

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить правило. Правило можно временно отключить, не удаляя его, если снять выделение с этого переключателя.
Name	Введите имя-описание, по которому можно будет идентифицировать это правило пересылки на основе статических MAC-адресов.
MAC Address	Введите MAC-адрес в соответствующем формате, то есть шесть пар шестнадцатеричных чисел. Примечание: Статические MAC-адреса не имеют срока действия.
VID	Введите идентификационный номер VLAN.
Port	Введите номер порта, на который будет направляться трафик для MAC-адреса, введенного в предыдущем поле.
Add	Нажмите **Add**, чтобы сохранить правило в оперативной памяти коммутатора. Это правило будет утеряно в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Clear	Нажмите **Clear**, чтобы начать настройку на этом экране заново.
Index	Нажмите на порядковый номер, чтобы изменить правило пересылки на основе статических MAC-адресов для данного порта.
Active	В этом поле указано, активно данное правило пересылки на основе статических MAC-адресов (**Yes**) или нет (**No**). Правило можно временно отключить, не удаляя его.
Name	Введите имя-описание, по которому можно будет идентифицировать это правило пересылки на основе статических MAC-адресов.
MAC Address	В этом поле отображается MAC-адрес, а также идентификационный номер VLAN, к которой принадлежит MAC-адрес.
VID	В этом поле отображается идентификационный номер группы VLAN.
Port	В этом поле отображается порт, на который будет направляться трафик для MAC-адреса, указанного в соседнем поле.

Таблица 19 Экран Advanced Application > Static MAC Forwarding (продолжение)

ПОЛЕ	ОПИСАНИЕ
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

10

Фильтрация

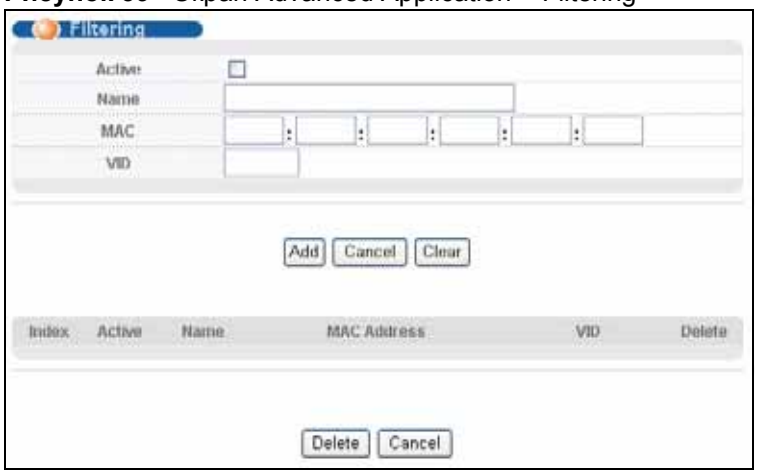
В этой главе описана фильтрация MAC-адресов на портах.

10.1 Настройка правила фильтрации

Фильтрация позволяет отсеивать трафик, проходящий через коммутатор, на основе MAC-адреса источника и идентификатора группы VLAN.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Filtering**.

Рисунок 39 Экран Advanced Application > Filtering



Поля экрана описаны в следующей таблице.

Таблица 20 Экран Advanced Application > Filtering

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить правило. Правило можно временно отключить, не удаляя его, если снять выделение с этого переключателя.
Name	Введите имя-описание (до 32 отображаемых символов в английской раскладке) для этого правила. Оно будет использоваться только для идентификации.
MAC	Введите MAC-адрес в соответствующем формате, то есть шесть пар шестнадцатеричных чисел.
VID	Введите идентификационный номер группы VLAN.

Таблица 20 Экран Advanced Application > Filtering (продолжение)

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите **Add**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	В этом поле отображается порядковый номер правила. Нажмите на этот номер, чтобы изменить настройки.
Active	В этом поле отображается **Yes**, если правило активно, и **No**, если правило отключено.
Name	В этом поле отображается имя-описание для данного правила. Оно будет использоваться только для идентификации.
MAC Address	В этом поле отображается MAC-адрес, а также идентификационный номер VLAN, к которой принадлежит MAC-адрес.
VID	В этом поле отображается идентификационный номер группы VLAN.
Delete	В столбце **Delete** установите переключатели правил, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей в столбце **Delete**.

11

Протокол покрывающего дерева

Данный коммутатор поддерживает протокол покрывающего дерева (STP), быстрый протокол покрывающего дерева (RSTP) и протокол нескольких экземпляров покрывающего дерева (MSTP), как это определено в следующих стандартах.

- IEEE 802.1d – протокол покрывающего дерева
- IEEE 802.1w – быстрый протокол покрывающего дерева
- IEEE 802.1s – протокол нескольких экземпляров покрывающего дерева

Данный коммутатор также позволяет настроить несколько конфигураций STP (несколько деревьев). После этого порты могут быть отнесены к различным деревьям.

11.1 Обзор протоколов STP/RSTP

Протокол (R)STP обнаруживает и разрывает сетевые петли и обеспечивает наличие запасных каналов между коммутаторами, мостами или маршрутизаторами. Он позволяет коммутатору взаимодействовать с другими устройствами, поддерживающими протокол (R)STP, благодаря чему достигается наличие только одного пути между любыми двумя станциями в сети.

Данный коммутатор поддерживает быстрый протокол покрывающего дерева RSTP, определенный стандартом IEEE 802.1w. Он обеспечивает более быструю сходимость покрывающего дерева по сравнению с STP (и в то же время обратно совместим с мостами, поддерживающими только протокол STP). При использовании RSTP информация об изменении топологии непосредственно распространяется по всей сети от устройства, вызвавшего изменение топологии. При использовании STP для этого требуется большее время, так как устройство, вызвавшее изменение топологии, прежде всего уведомляет об этом корневой мост, который в свою очередь распространяет изменение по сети. Как в RSTP, так и в STP осуществляется удаление ненужных полученных адресов из базы данных фильтрации. При использовании RSTP порт может находиться в состояниях Discarding, Learning и Forwarding.

В данном руководстве пользователя упоминание «STP» относится как к протоколу STP, так и к протоколу RSTP.

11.1.1 Терминология STP

Корневой мост – это основание покрывающего дерева.

Стоимость пути – это стоимость передачи кадра в локальную сеть через этот порт. Стоимость рекомендуется назначать в зависимости от скорости канала, к которому подключен порт. Чем медленнее канал, тем выше стоимость.

Таблица 21 Стоимость путей протокола STP

	СКОРОСТЬ КАНАЛА	РЕКОМЕНДУЕМОЕ ЗНАЧЕНИЕ	РЕКОМЕНДУЕМЫЙ ДИАПАЗОН	ДОПУСТИМЫЙ ДИАПАЗОН
Стоимость пути	4 Мбит/с	250	От 100 до 1000	От 1 до 65 535
Стоимость пути	10 Мбит/с	100	От 50 до 600	От 1 до 65 535
Стоимость пути	16 Мбит/с	62	От 40 до 400	От 1 до 65 535
Стоимость пути	100 Мбит/с	19	От 10 до 60	От 1 до 65 535
Стоимость пути	1 Гбит/с	4	От 3 до 10	От 1 до 65 535
Стоимость пути	10 Гбит/с	2	От 1 до 5	От 1 до 65 535

На каждом мосту корневым портом является порт, через который данный мост осуществляет связь с корнем. Таким портом на данном коммутаторе является порт с наименьшей стоимостью пути к корню. Если корневого порта нет, то данный коммутатор считается корневым мостом сети покрывающего дерева.

Для каждого сегмента локальной сети выбирается назначенный мост. Среди всех мостов, подключенных к локальной сети, этот мост имеет наименьшую стоимость пути к корню.

11.1.2 Как работает протокол STP

После того, как мост с помощью протокола STP определяет покрывающее дерево с наименьшей стоимостью пути, он активирует корневой порт и порты, назначенные для подключенных локальных сетей, а также отключает все остальные порты, принимающие участие в покрывающем дереве. Сетевые пакеты, таким образом, направляются только через подключенные порты, что исключает возможность возникновения сетевых петель.

Коммутаторы, поддерживающие протокол STP, периодически обмениваются блоками данных мостового протокола (BPDU). При изменении топологии локальной сети, соединенной мостами, создается новое покрывающее дерево.

После создания стабильной сетевой топологии все мосты ожидают блоков BPDU типа Hello от корневого моста. Если мост не получает блока данных Hello по истечении заранее определенного интервала (Max Age), то он понимает это как отсутствие канала к корневому мосту. Тогда этот мост предпринимает попытки связаться с другими мостами, чтобы перенастроить сеть и создать новую действующую сетевую топологию.

11.1.3 Состояния портов по протоколу STP

В целях устранения зацикливания пакетов протокол STP назначает порту одно из пяти состояний. Для предотвращения появления кратковременных петель не разрешается переключение порта моста из состояния блокировки непосредственно в состояние пересылки.

Таблица 22 Состояния портов по протоколу STP

СОСТОЯНИЕ ПОРТА	ОПИСАНИЕ
Disabled	Протокол STP отключен (по умолчанию).
Blocking	Принимаются и обрабатываются только пакеты BPDU настройки и управления.
Listening	Принимаются и обрабатываются все пакеты BPDU. Примечание: Состояние «Listening» не используется в RSTP.
Learning	Принимаются и обрабатываются все пакеты BPDU. Кадры информации направляются процессу получения (запоминания), но не пересылаются.
Forwarding	Принимаются и обрабатываются все пакеты BPDU. Все кадры информации принимаются и пересылаются.

11.1.4 Протокол MSTP

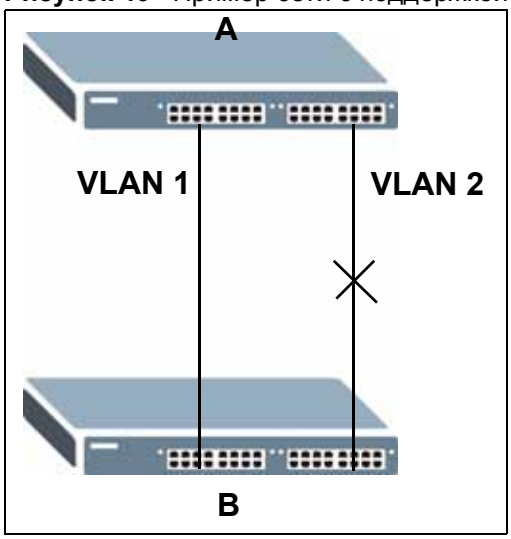
Протокол нескольких экземпляров покрывающего дерева MSTP (IEEE 802.1s) обратно совместим с протоколами STP/RSTP и устраняет ограничения, характерные для существующих протоколов STP и RSTP за счет реализации следующих функций:

- Одно общее и внутреннее покрывающее дерево (Common and Internal Spanning Tree, CIST), представляющее структуру связности всей сети.
- Группировка нескольких мостов (или коммутирующих устройств) в регионы, которые рассматриваются сетью как один мост.
- Связывание VLAN с конкретным экземпляром покрывающего дерева (MSTI). Благодаря MSTI можно использовать одно и то же покрывающее дерево для нескольких сетей VLAN.
- Возможность балансировки нагрузки благодаря использованию для трафика различных VLAN конкретных путей в регионе.

11.1.4.1 Пример сети с поддержкой MSTP

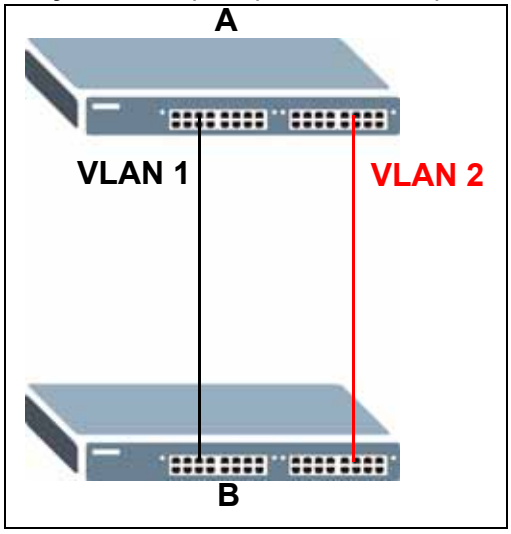
На приведенном ниже рисунке показан пример сети, в которой на двух коммутаторах настроены две сети VLAN. В случае использования на коммутаторах протокола STP или RSTP канал для VLAN 2 будет заблокирован, так как протоколы STP и RSTP допускают наличие только одного канала и блокируют избыточные каналы.

Рисунок 40 Пример сети с поддержкой STP/RSTP



При использовании MSTP сети VLAN 1 и 2 можно связать с различными экземплярами покрывающего дерева в сети. Таким образом, трафик для двух сетей VLAN будет проходить по различным путям. Пример сети с использованием протокола MSTP показан на следующем рисунке.

Рисунок 41 Пример сети с поддержкой MSTP



11.1.4.2 Регион MST

Регионом MST называется логическая группа нескольких сетевых устройств, которая для остальной сети представляется в виде одного устройства. Каждое из устройств с поддержкой MSTP может принадлежать только одному региону MST. При поступлении блоков BPDU в регион MST стоимость внешнего пути (или путей, выходящих из данного региона) увеличивается на единицу. Стоимость внутреннего пути (или путей внутри данного региона) увеличивается на единицу при прохождении блока BPDU через регион.

На устройствах, принадлежащие одному региону MST, настраиваются одинаковые идентификационные параметры MSTP. Сюда входят следующие параметры:

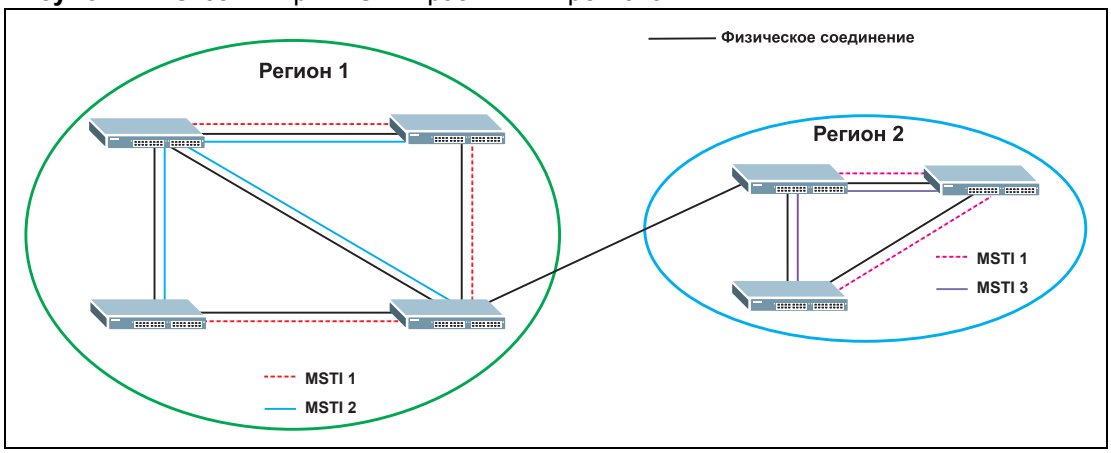
- Имя региона MST
- Номер версии в качестве уникального номера региона MST
- Связывание VLAN с конкретным экземпляром MST

11.1.4.3 Экземпляр MST

Экземпляром MST (MSTI) называется экземпляр покрывающего дерева. Для VLAN можно определить работу с использованием конкретного MSTI. Каждый созданный экземпляр MSTI идентифицируется по уникальному номеру (также называемому идентификатором MST ID), известному внутри региона. Таким образом, MSTI не охватывает несколько регионов MST.

Пример с двумя регионами MST показан на следующем рисунке. В регионах 1 и 2 имеется 2 экземпляра покрывающего дерева.

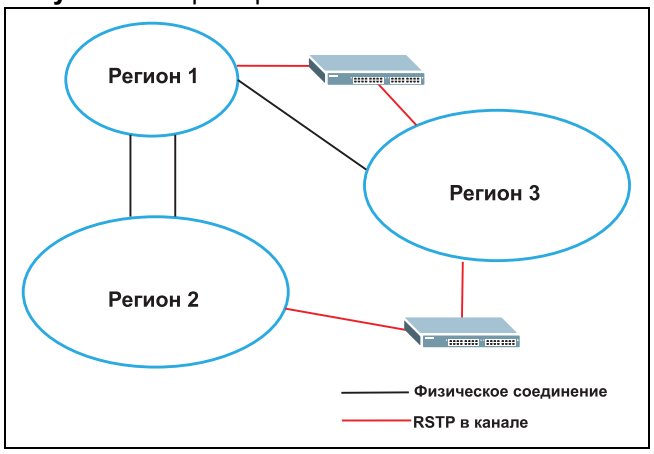
Рисунок 42 Экземпляры MSTI в различных регионах



11.1.4.4 Общее и внутреннее покрывающее дерево (CIST)

CIST представляет структуру связности всей сети в целом и является эквивалентом покрывающего дерева протоколов STP/RSTP. CIST представляет собой используемый по умолчанию экземпляр MST (MSTID 0). Все виртуальные локальные сети VLAN, которые не связаны с конкретным экземпляром MST, связаны с CIST. В сети с поддержкой MSTP имеется только одного дерево CIST, которое охватывает регионы MST и отдельные устройства с поддержкой протокола покрывающего дерева. Сеть может включать в себя несколько регионов MST и другие сегменты, в которых используется RSTP.

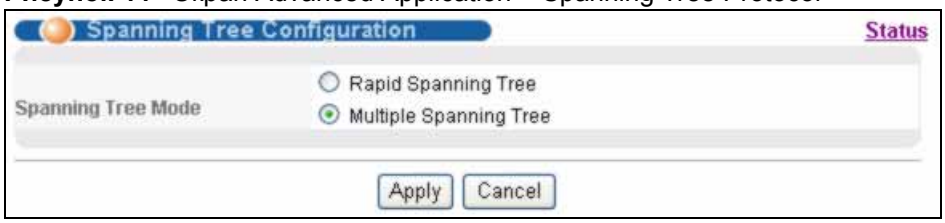
Рисунок 43 Пример сети с использованием MSTP и традиционного протокола RSTP



11.2 Экран настройки протокола покрывающего дерева

На этом экране можно выбрать режим STP для коммутатора. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > Spanning Tree Protocol > Configuration**.

Рисунок 44 Экран Advanced Application > Spanning Tree Protocol

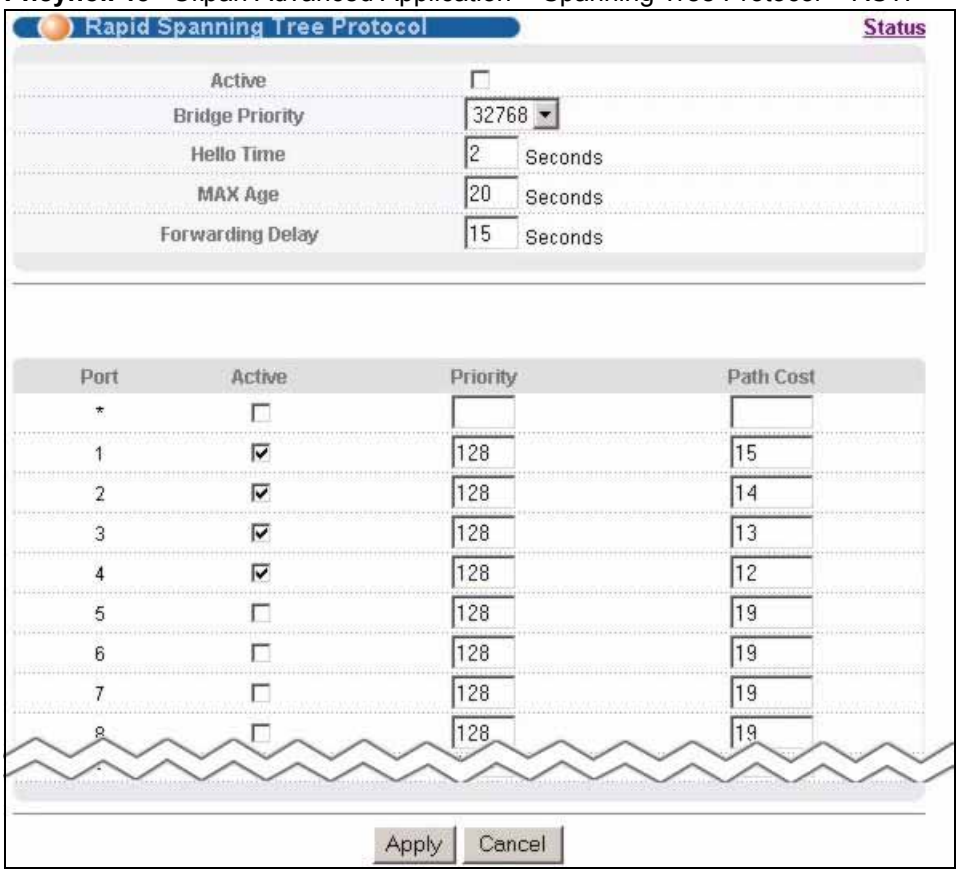


Выберите режим STP, который необходимо установить на коммутаторе.

11.3 Настройка быстрого протокола покрывающего дерева

Данный экран используется для настройки RSTP; более подробную информацию о RSTP можно найти в разд. 11.1 на стр. 101. Нажмите на **RSTP** на экране **Advanced Application** > **Spanning Tree Protocol**.

Рисунок 45 Экран Advanced Application > Spanning Tree Protocol > RSTP



Поля экрана описаны в следующей таблице.

Таблица 23 Экран Advanced Application > Spanning Tree Protocol > RSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите **Status**, чтобы отобразить экран состояния **RSTP Status** (см. рис. 46 на стр. 109).
Active	Установите этот переключатель, чтобы включить протокол RSTP. Снимите выделение с переключателя, если необходимо отключить RSTP.
Bridge Priority	Приоритет моста используется для определения корневого коммутатора, корневого порта и назначенного порта. Коммутатор с наивысшим приоритетом (наименьшее числовое значение) становится корневым коммутатором протокола STP. Если у всех коммутаторов одинаковый приоритет, то корневым становится коммутатором с наименьшим MAC-адресом. Выберите значение в ниспадающем списке. Чем меньшее числовое значение будет выбрано, тем выше будет приоритет у этого моста. Параметр Bridge Priority определяет корневой мост, который, в свою очередь, определяет параметры Hello Time, Max Age и Forwarding Delay.
Hello Time	Временной интервал в секундах между конфигурационными сообщениями BPDU (блоки данных мостового протокола), генерируемыми корневым коммутатором. Диапазон допустимых значений – от 1 до 10 секунд.

Таблица 23 Экран Advanced Application > Spanning Tree Protocol > RSTP

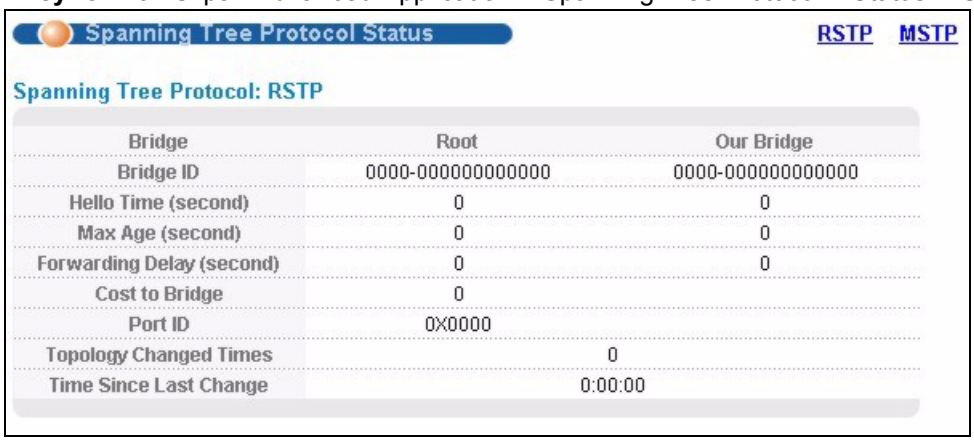
ПОЛЕ	ОПИСАНИЕ
Max Age	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая сообщений BPDU, прежде чем он предпримет попытку произвести настройку заново. Все порты коммутатора (за исключением назначенных портов) должны получать сообщения BPDU через регулярные промежутки времени. Любой порт с устаревшей информацией протокола STP (содержащейся в последнем сообщении BPDU) становится назначенным портом для подключенной локальной сети. Если это корневой порт, то новый корневой порт выбирается из портов коммутатора, подключенных к сети. Диапазон допустимых значений – от 6 до 40 секунд.
Forwarding Delay	Временной интервал (в секундах), в течение которого корневой ожидает, прежде чем сменить состояния. Эта задержка необходима для того, чтобы коммутатор успел получить информацию о топологии прежде, чем он начнет пересылать кадры. Кроме того, каждому порту требуется время для получения информации о конфликтах, которая может заставить его вернуться в состояние блокировки; в противном случае могут возникнуть временные петли данных. Диапазон допустимых значений – от 4 до 30 секунд. Как правило: Примечание: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить на этом порту протокол RSTP.
Priority	Здесь можно определить приоритет для каждого из портов. Уровень приоритета определяет, какой из портов нужно отключить, когда на нескольких портах коммутатора образуется петля. Порты с более высоким значением приоритета отключаются первыми. Допустимый диапазон значений – от 0 до 255, по умолчанию устанавливается уровень приоритета 128.
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – дополнительную информацию можно найти в табл. 21 на стр. 102.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

11.4 Состояние быстрого протокола покрывающего дерева

Чтобы отобразить следующий экран состояния, нажмите в навигационной панели **Advanced Application** > **Spanning Tree Protocol**. Более подробную информацию о RSTP можно найти в разд. 11.1 на стр. 101.

Данный экран доступен лишь в том случае, если на коммутаторе был включен протокол RSTP.

Рисунок 46 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP



Поля экрана описаны в следующей таблице.

Таблица 24 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP

ПОЛЕ	ОПИСАНИЕ
Bridge	**Root** относится к основанию покрывающего дерева (корневой мост). **Our Bridge** – данный коммутатор. Данный коммутатор также может быть корневым мостом.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях **Root** и **Our Bridge** указывается один и тот же идентификатор.
Hello Time (second)	Временной интервал (в секундах), в течение которого корневой коммутатор передает конфигурационное сообщение. Значения параметров Hello Time, Max Age и Forwarding Delay определяет корневой мост.
Max Age (second)	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая конфигурационного сообщения, прежде чем он предпримет попытку произвести настройку заново.
Forwarding Delay (second)	Время (в секундах), в течение которого корневой коммутатор ожидает перед сменой состояний (то есть от Listening к Learning и затем к Forwarding). Примечание: Состояние «Listening» не используется в RSTP.
Cost to Bridge	Стоимость пути от корневого порта на данном коммутаторе к корневому коммутатору.
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем покрывающего дерева.

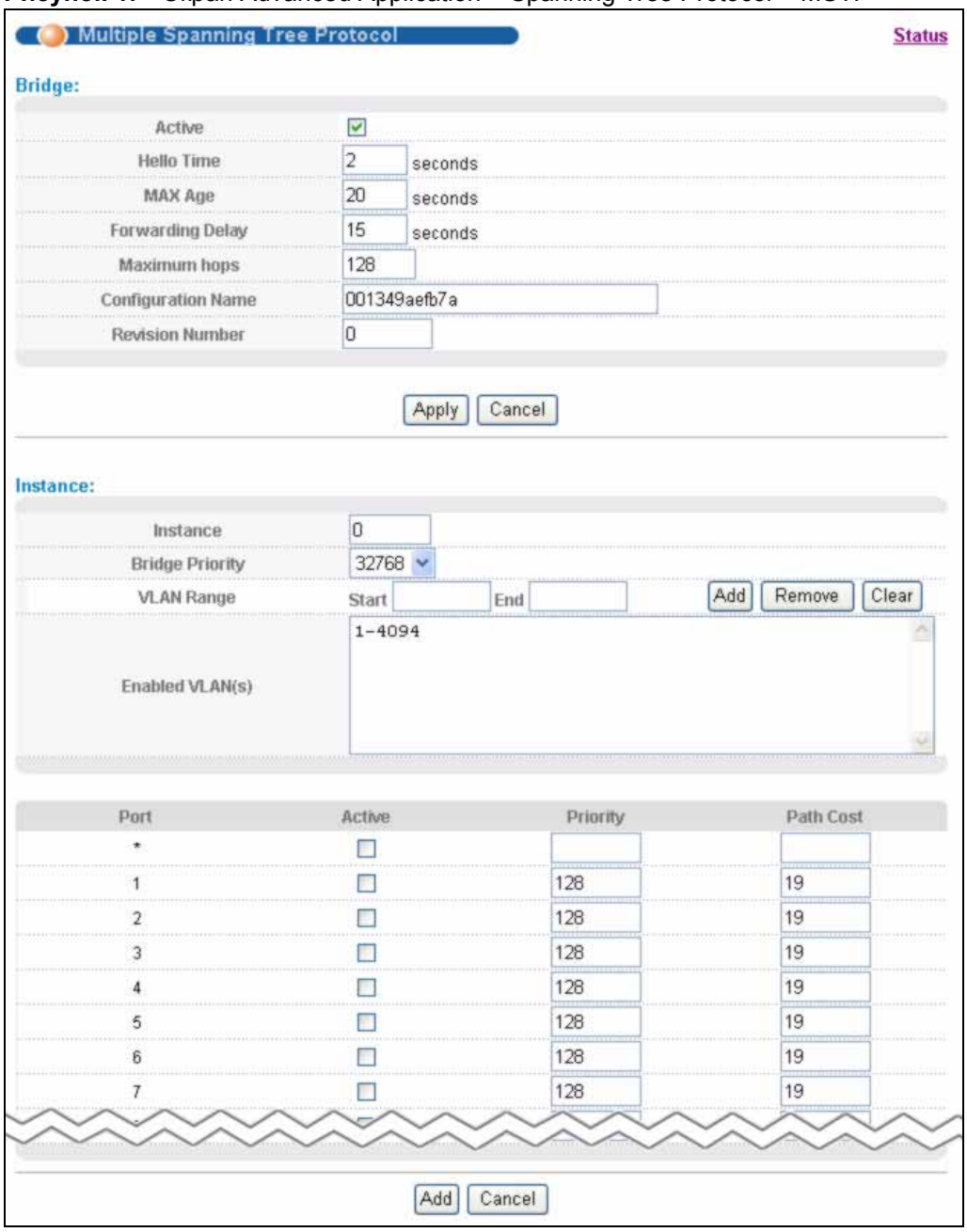
Таблица 24 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP

ПОЛЕ	ОПИСАНИЕ
Topology Changed Times	Количество смен конфигурации покрывающего дерева.
Time Since Last Change	Время, прошедшее с последней смены конфигурации покрывающего дерева.

11.5 Настройка протокола MSTP

Чтобы настроить протокол MSTP, нажмите на **MSTP** на экране **Advanced Application** > **Spanning Tree Protocol**. Более подробную информацию о MSTP можно найти в разд. 11.1.4 на стр. 103.

Рисунок 47 Экран Advanced Application > Spanning Tree Protocol > MSTP



Поля экрана описаны в следующей таблице.

Таблица 25 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите **Status**, чтобы отобразить экран состояния **MSTP Status** (см. рис. 48 на стр. 114).
Active	Установите этот переключатель, если необходимо включить протокол MSTP на коммутаторе. Снимите выделение с переключателя, если требуется отключить протокол MSTP на коммутаторе.

Таблица 25 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
Hello Time	Временной интервал в секундах между конфигурационными сообщениями BPDU (блоки данных мостового протокола), генерируемыми корневым коммутатором. Диапазон допустимых значений – от 1 до 10 секунд.
MAX Age	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая сообщений BPDU, прежде чем он предпримет попытку произвести настройку заново. Все порты коммутатора (за исключением назначенных портов) должны получать сообщения BPDU через регулярные промежутки времени. Любой порт с устаревшей информацией протокола STP (содержащейся в последнем сообщении BPDU) становится назначенным портом для подключенной локальной сети. Если это корневой порт, то новый корневой порт выбирается из портов коммутатора, подключенных к сети. Диапазон допустимых значений – от 6 до 40 секунд.
Forwarding Delay	Временной интервал (в секундах), в течение которого корневой ожидает, прежде чем сменить состояния. Эта задержка необходима для того, чтобы коммутатор успел получить информацию о топологии прежде, чем он начнет пересылать кадры. Кроме того, каждому порту требуется время для получения информации о конфликтах, которая может заставить его вернуться в состояние блокировки; в противном случае могут возникнуть временные петли данных. Диапазон допустимых значений – от 4 до 30 секунд. Как правило: Примечание: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)
Maximum hops	Введите количество переходов (от 1 до 255) в регионе MSTP, после которого блок данных BPDU будет отбрасываться, и информация порта будет считаться устаревшей.
Configuration Name	Введите имя-описание (до 32 символов) для региона MST.
Revision Number	Введите идентификационный номер конфигурации региона. Этот номер должен быть одинаковым на всех устройствах, принадлежащих одному региону.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Instance	В этом разделе определяются параметры MSTI (экземпляра покрывающего дерева).
Instance	Введите номер, используемый для идентификации данного экземпляра MST на коммутаторе. Данный коммутатор поддерживает номера экземпляров в диапазоне 0-16.
Bridge Priority	Укажите приоритет коммутатора для конкретного экземпляра покрывающего дерева. Чем меньше это значение, тем с большей вероятностью коммутатор будет выбран в качестве корневого моста в рамках данного экземпляра покрывающего дерева=. В качестве приоритета допускается использовать значения от 0 до 61440 с шагом 4096 (т.е. значения 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 и 61440).

Таблица 25 Экран Advanced Application > Spanning Tree Protocol > MSTP

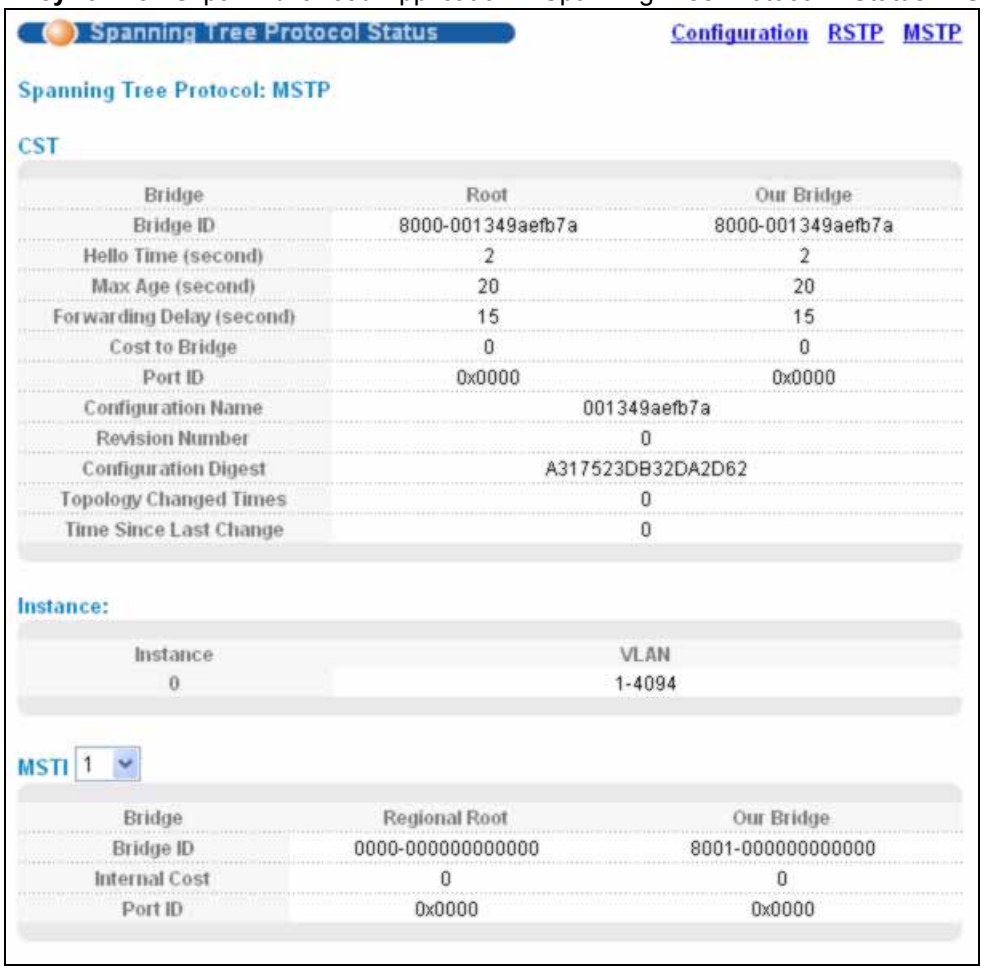
ПОЛЕ	ОПИСАНИЕ
VLAN Range	Введите начальный идентификатор диапазона идентификаторов VLAN, который необходимо добавить или удалить из области редактирования диапазонов VLAN, в поле **Start**. Введите конечный идентификатор диапазона идентификаторов VLAN, который необходимо добавить или удалить из области редактирования диапазонов VLAN, в поле **End**. Затем нажмите: • **Add** – чтобы добавить данный диапазон идентификаторов VLAN к списку связанных с данным экземпляром MST. • **Remove** – чтобы удалить данный диапазон идентификаторов VLAN из списка связанных с данным экземпляром MST. • **Clear** – чтобы удалить все сети VLAN из списка связанных с данным экземпляром MST.
Enabled VLAN(s)	В данном поле отображаются сети VLAN, связанные с данным экземпляром MST.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите данный переключатель, чтобы добавить данный порт к данному экземпляру MST.
Priority	Здесь можно определить приоритет для каждого из портов. Уровень приоритета определяет, какой из портов нужно отключить, когда на нескольких портах коммутатора образуется петля. Порты с более высоким значением приоритета отключаются первыми. Допустимый диапазон значений – от 0 до 255, по умолчанию устанавливается уровень приоритета 128.
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – дополнительную информацию можно найти в табл. 21 на стр. 102.
Add	Нажмите **Add**, чтобы сохранить данный экземпляр MST в оперативной памяти коммутатора. Это изменение будет утеряно в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Instance	В этом поле отображается идентификатор экземпляра MST.
VLAN	В данном поле отображается идентификатор VID (или диапазоны идентификаторов VID), связанные с данным экземпляром MST.
Active Port	В данном поле отображаются порты, включенные в данный экземпляр MST.
Delete	В столбце **Delete** установите переключатели правил, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

11.6 Состояние протокола MSTP

Чтобы отобразить следующий экран состояния, нажмите в навигационной панели **Advanced Application** > **Spanning Tree Protocol**. Более подробную информацию о MSTP можно найти в разд. 11.1.4 на стр. 103.

Данный экран доступен лишь в том случае, если на коммутаторе был включен протокол MSTP.

Рисунок 48 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP



Поля экрана описаны в следующей таблице.

Таблица 26 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

ПОЛЕ	ОПИСАНИЕ
Configuration	Нажмите **Configuration**, чтобы выбрать нужный режим STP. Для изменения настроек MSTP коммутатора нажмите на **MSTP**.
CST	В данном разделе описываются настройки общего покрывающего дерева.

Таблица 26 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

ПОЛЕ	ОПИСАНИЕ
Bridge	**Root** относится к основанию покрывающего дерева (корневой мост). **Our Bridge** – данный коммутатор. Данный коммутатор также может быть корневым мостом.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях **Root** и **Our Bridge** указывается один и тот же идентификатор.
Hello Time (second)	Временной интервал (в секундах), в течение которого корневой коммутатор передает конфигурационное сообщение.
Max Age (second)	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая конфигурационного сообщения, прежде чем он предпримет попытку произвести настройку заново.
Forwarding Delay (second)	Время (в секундах), в течение которого корневой коммутатор ожидает перед сменой состояний (то есть от Listening к Learning и затем к Forwarding).
Cost to Bridge	Стоимость пути от корневого порта на данном коммутаторе к корневому коммутатору.
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем покрывающего дерева.
Configuration Name	В этом поле отображается имя конфигурации для данного региона MST.
Revision Number	В этом поле отображается номер версии для данного региона MST.
Configuration Digest	Кодификация конфигурации генерируется на основе информации о связывании VLAN-MSTI. В данном поле отображается состоящая из 16 октетов сигнатура, которая включается в блоки BPDU протокола MSTP. Кодификация отображается в данном поле лишь в том случае, если в системе включен протокол MSTP.
Topology Changed Times	Количество смен конфигурации покрывающего дерева.
Time Since Last Change	Время, прошедшее с последней смены конфигурации покрывающего дерева.
Instance:	В данных полях отображается информация о связывании MSTI с VLAN. Другими словами, какие виртуальные локальные сети работают в каждом из экземпляров покрывающего дерева.
Instance	В этом поле отображается идентификатор MSTI ID.
VLAN	В этом поле отображаются сети VLAN, связанные с указанным MSTI.
MSTI	Выберите экземпляр MST, настройки которого необходимо отобразить.
Bridge	**Root** определяет основание экземпляра покрывающего дерева MST. **Our Bridge** – данный коммутатор. Данный коммутатор также может быть корневым мостом.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях **Root** и **Our Bridge** указывается один и тот же идентификатор.
Internal Cost	Стоимость пути от корневого порта в данном экземпляре MST к корневому коммутатору региона.
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем экземпляра MST.

12

Управление пропускной способностью

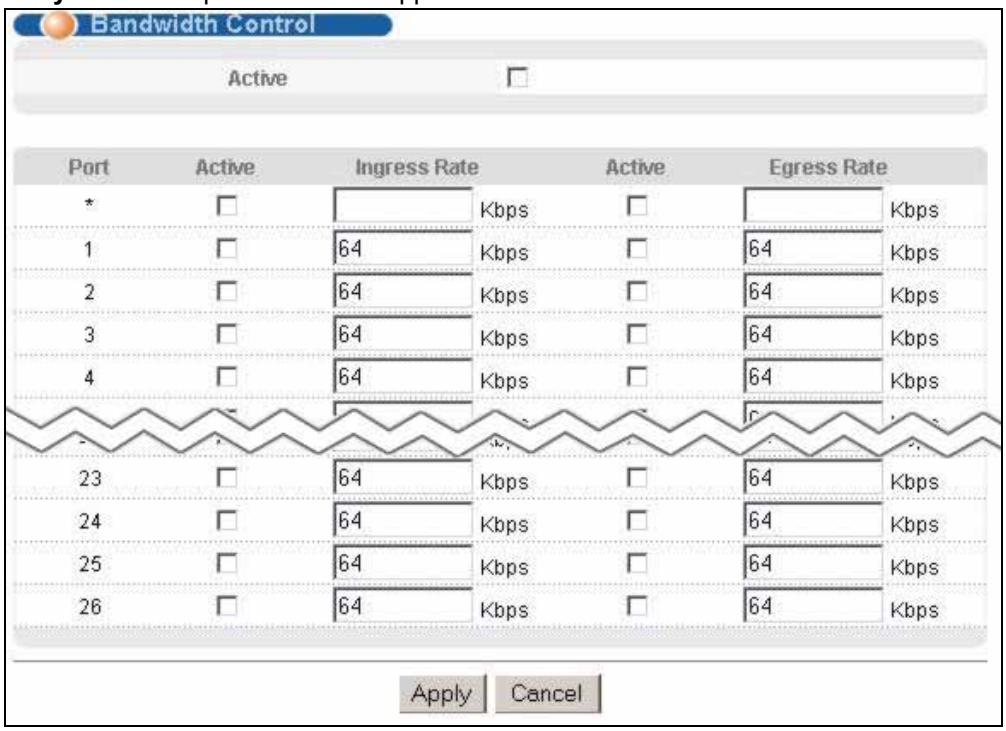
В данной главе рассказывается, как ограничить максимальную пропускную способность с помощью меню **Bandwidth Control**.

12.1 Настройка управления пропускной способностью

Управление пропускной способностью подразумевает определение максимальной разрешенной пропускной способности для входящего и/или исходящего потоков трафика через порт.

Чтобы открыть показанный ниже экран, выберите в навигационной панели **Advanced Application > Bandwidth Control**.

Рисунок 49 Экран Advanced Application > Bandwidth Control



Поля экрана описаны в следующей таблице.

Таблица 27 Экран Advanced Application > Bandwidth Control

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить управление пропускной способностью на коммутаторе.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы активировать ограничение скорости входящего трафика на данном порту.
Ingress Rate	Укажите максимальную разрешенную пропускную способность в килобитах в секунду (кбит/с) для входящего потока трафика через этот порт. При вводе значения в диапазоне от 64 до 1728 коммутатор автоматически округлит его в меньшую сторону до ближайшего числа, кратного 64. Если ввести значение в диапазоне от 1729 до 1999, скорость будет автоматически выставлена равной 1792. При вводе значения в диапазоне от 2000 до 103999 коммутатор автоматически округлит его в меньшую сторону до ближайшего числа, кратного 1000. На портах Gigabit Ethernet/mini-GBIC для значений в диапазоне от 104 000 до 1 000 000 коммутатор округляет значение скорости в меньшую сторону до ближайшего числа, кратного 8000.
Active	Установите этот переключатель, чтобы включить на этом порту ограничение скорости исходящего трафика.
Egress Rate	Укажите максимальную разрешенную пропускную способность в килобитах в секунду (кбит/с) для исходящего потока трафика через этот порт. При вводе значения в диапазоне от 64 до 1728 коммутатор автоматически округлит его в меньшую сторону до ближайшего числа, кратного 64. Если ввести значение в диапазоне от 1729 до 1999, скорость будет автоматически выставлена равной 1792. При вводе значения в диапазоне от 2000 до 103999 коммутатор автоматически округлит его в меньшую сторону до ближайшего числа, кратного 1000. На портах Gigabit Ethernet/mini-GBIC для значений в диапазоне от 104 000 до 1 000 000 коммутатор округляет значение скорости в меньшую сторону до ближайшего числа, кратного 8000.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

13

Контроль широковещательных штормов

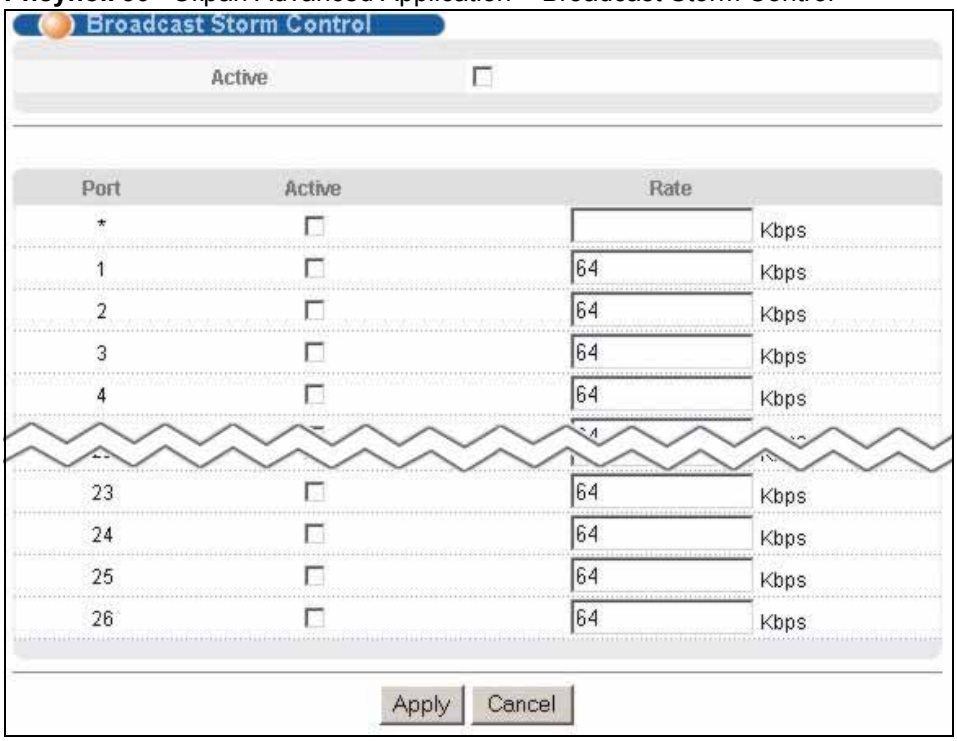
В этой главе описывается функция контроля широковещательных штормов и порядок ее настройки.

13.1 Настройка функции контроля широковещательных штормов

Функция контроля широковещательных штормов ограничивает количество широковещательных пакетов, пакетов мультивещания и DLF-пакетов (destination lookup failure), которые могут быть приняты за секунду времени через порты коммутатора. При достижении максимального допустимого количества широковещательных пакетов, пакетов мультивещания и/или DLF-пакетов все последующие пакеты отбрасываются. Включение этой функции позволяет снизить объем широковещательных пакетов, пакетов мультивещания и DLF-пакетов, поступающих в сеть. Имеется возможность ограничить для каждого порта количество пакетов каждого отдельного типа.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Broadcast Storm Control**.

Рисунок 50 Экран Advanced Application > Broadcast Storm Control



Поля экрана описаны в следующей таблице.

Таблица 28 Экран Advanced Application > Broadcast Storm Control

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить контроль широковещательного трафика на коммутаторе. Снимите выделение с переключателя, если необходимо отключить эту функцию.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить контроль широковещательных штормов на данном порту. Снимите выделение с переключателя, если необходимо отключить эту функцию.
Rate	Укажите, какой объем трафика должен принимать порт, в килобитах в секунду (кбит/с). При вводе значения в диапазоне от 64 до 1728 коммутатор автоматически округлит его в меньшую сторону до ближайшего числа, кратного 64. Если ввести значение в диапазоне от 1729 до 1999, скорость будет автоматически выставлена равной 1792. При вводе значения в диапазоне от 2000 до 103999 коммутатор автоматически округлит его в меньшую сторону до ближайшего числа, кратного 1000. На портах Gigabit Ethernet/mini-GBIC для значений в диапазоне от 104 000 до 1 000 000 коммутатор округляет значение скорости в меньшую сторону до ближайшего числа, кратного 8000.

Таблица 28 Экран Advanced Application > Broadcast Storm Control (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

14

Зеркальное копирование

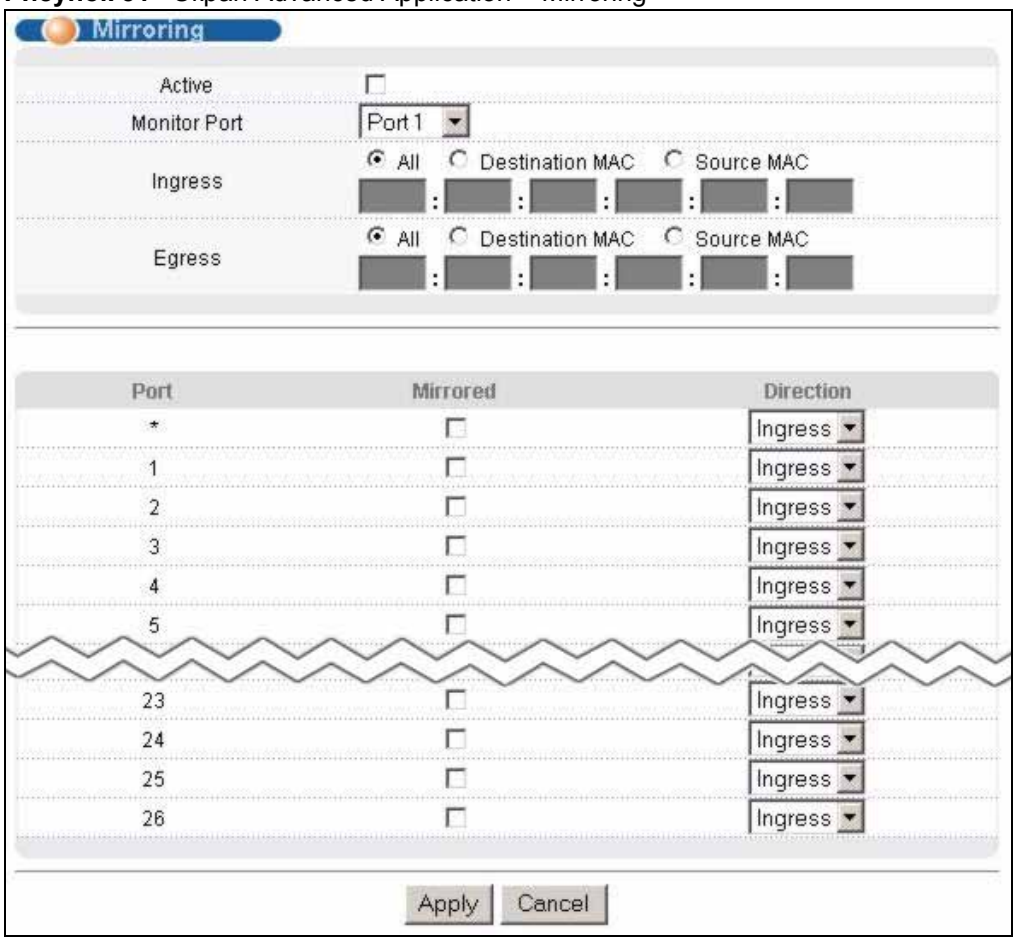
В данной главе описаны экраны настройки зеркального копирования портов.

14.1 Настройка зеркального копирования портов

Зеркальное копирование портов позволяет копировать трафик на контрольный порт (тот, на который копируется трафик), чтобы можно было анализировать трафик на контролируемом порту, не вмешиваясь в поток.

Чтобы отобразить экран настроек зеркального копирования **Mirroring**, выберите в навигационной панели **Advanced Application** > **Mirroring**. Этот экран позволяет выбрать контрольный порт и определить поток трафика, который будет копироваться на контрольный порт.

Рисунок 51 Экран Advanced Application > Mirroring



Поля экрана описаны в следующей таблице.

Таблица 29 Экран Advanced Application > Mirroring

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, если необходимо включить фильтрацию зеркального копирования портов на коммутаторе. Снимите выделение с переключателя, если необходимо отключить эту функцию.
Monitor Port	Контрольный порт – это порт, на который копируется трафик с целью его анализа без вмешательства в поток трафика на исходном порту (портах). Введите номер контрольного порта.
Ingress	Имеется возможность выбрать копирование всего входящего трафика или трафика, приходящего на заданный MAC-адрес или с заданного MAC-адреса. Выберите **All**, чтобы копировать весь входящий трафик с копируемого порта (портов). Выберите **Destination MAC**, чтобы копировать трафик, приходящий на копируемый порт (порты) и предназначенный для заданного MAC-адреса. Введите в соответствующих полях MAC-адрес назначения. Выберите **Source MAC**, чтобы копировать трафик, приходящий на копируемый порт (порты) с заданного MAC-адреса. Введите в соответствующих полях MAC-адрес источника.

Таблица 29 Экран Advanced Application > Mirroring (продолжение)

ПОЛЕ	ОПИСАНИЕ
Egress	Имеется возможность выбрать копирование всего исходящего трафика или трафика, приходящего на заданный MAC-адрес или с заданного MAC-адреса. Выберите **All**, чтобы копировать весь исходящий трафик с копируемого порта (портов). Выберите **Destination MAC**, чтобы копировать трафик, выходящий из копируемого порта (портов) и предназначенный для заданного MAC-адреса. Введите в соответствующих полях MAC-адрес назначения. Выберите **Source MAC**, чтобы копировать трафик, выходящий из копируемого порта (портов) с заданного MAC-адреса. Введите в соответствующих полях MAC-адрес источника.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Mirrored	Выберите эту опцию, чтобы копировать трафик на порту.
Direction	Выберите направление трафика для зеркального копирования из ниспадающего списка. Выбрать можно **Egress** (исходящий), **Ingress** (входящий) или **Both** (весь трафик).
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

15

Агрегация каналов

В этой главе рассказывается о логическом объединении (агрегации) нескольких физических каналов в один логический канал большей пропускной способности.

15.1 Обзор агрегации каналов

Агрегация (группирование) каналов – это объединение нескольких физических портов в один логический канал большей пропускной способности. Объединить несколько портов в один канал можно в том случае, если, например, дешевле использовать несколько каналов меньшей скорости, чем не на полную мощность загружать высокоскоростной, но более дорогой канал с одним портом.

Однако, чем больше портов будут подвергнуты агрегации, тем меньше доступных портов останется. Группой портов называется единый логический канал, объединяющий несколько портов.

Для формирования группы портов начальный порт каждой группы должен быть физически подключен.

Данный коммутатор поддерживает как статическую, так и динамическую агрегацию каналов.

В надлежащим образом спланированной сети рекомендуется использовать только статическую агрегацию каналов. Это обеспечивает более высокую стабильность сети и управление группами портов на коммутаторе.

Пример использования статического группирования портов можно найти в разд. 15.6 на стр. 132.

15.2 Динамическая агрегация каналов

Поддержка статического и динамического группирования портов осуществляется коммутатором в соответствии со стандартом IEEE 802.3ad (протокол LACP).

Данный коммутатор поддерживает стандарт агрегации каналов IEEE802.3ad. Этот стандарт описывает протокол управления агрегацией каналов (LACP) – протокол, обеспечивающий динамическое создание и управление группами портов

При включении агрегации каналов по протоколу LACP на одном из портов этот порт может начать процесс автоматического согласования групп портов с устройством на другом конце. Протокол LACP также поддерживает избыточность портов, то есть если работающий порт выйдет из строя, то один из «резервных» портов начнет работать без вмешательства пользователя. Следует иметь в виду, что:

- Все порты должны быть подключены по схеме «точка-точка» к одному и тому же Ethernet-коммутатору, а также сконфигурированы в группу с использованием протокола LACP.
- Протокол LACP работает только на дуплексных каналах.
- Все порты, принадлежащие к одной группе, должны иметь одинаковый тип среды передачи, скорость, режим дуплекса и настройки управления потоком.

Настраивать группы портов или протокол LACP следует до подключения Ethernet-коммутатора, во избежание появления петель в сетевой топологии.

15.2.1 Идентификатор агрегации каналов

Идентификатор агрегации протокола LACP включает в себя[1]:

Таблица 30 Идентификатор агрегации каналов: локальный коммутатор

ПРИОРИТЕТ СИСТЕМЫ	MAC-АДРЕС	КЛЮЧ	ПРИОРИТЕТ ПОРТА	НОМЕР ПОРТА
0000	00-00-00-00-00	0000	00	0000

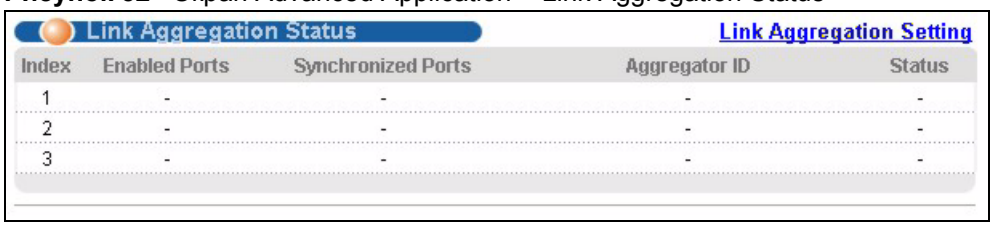
Таблица 31 Идентификатор агрегации каналов: коммутатор-партнер

ПРИОРИТЕТ СИСТЕМЫ	MAC-АДРЕС	КЛЮЧ	ПРИОРИТЕТ ПОРТА	НОМЕР ПОРТА
0000	00-00-00-00-00	0000	00	0000

15.3 Состояние агрегации каналов

Выберите в навигационной панели **Advanced Application** > **Link Aggregation**. По умолчанию появится экран **Link Aggregation Status**. Дополнительную информацию можно найти в разд. 15.1 на стр. 127.

Рисунок 52 Экран Advanced Application > Link Aggregation Status



1. Уровень приоритета порта и номер порта равны нулю, так как это агрегационный идентификатор для всей группы, а не отдельного порта.

Поля экрана описаны в следующей таблице.

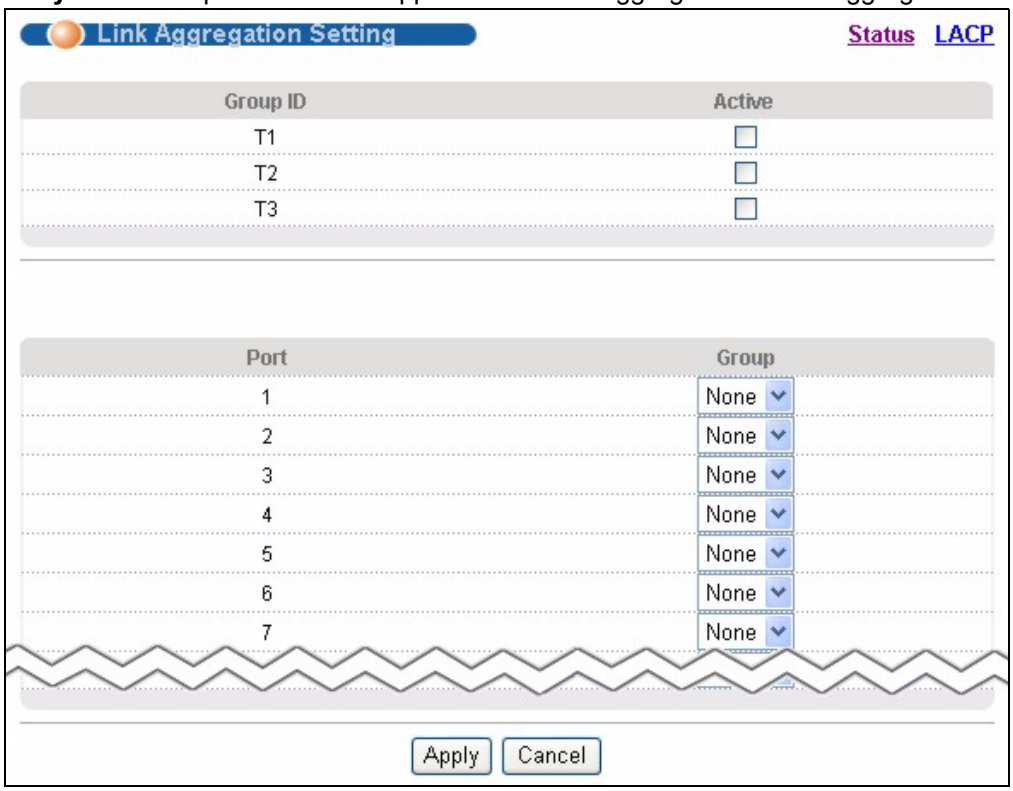
Таблица 32 Экран Advanced Application > Link Aggregation Status

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается идентификатор группы, который определяет группу портов, то есть логический канал, объединяющий несколько портов.
Enabled Ports	Порты, настроенные в меню **Link Aggregation** как члены группы портов.
Synchronized Ports	Порты, в данный момент передающие данные как единый канал в этой группе портов.
Aggregator ID	Идентификатор агрегации каналов включает в себя: приоритет системы, MAC-адрес, ключ, приоритет порта и номер порта. Более подробную информацию об этом поле можно найти в разд. 15.2.1 на стр. 128.
Status	В этом поле отображается способ добавления указанных портов в группу портов. Возможные значения: • **Static** – если порты настроены в качестве статических членов группы портов. • **LACP** – если порты были присоединены к группе портов посредством LACP.

15.4 Настройка агрегации каналов

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Link Aggregation > Link Aggregation Setting**. Дополнительную информацию об агрегации каналов можно найти в разд. 15.1 на стр. 127.

Рисунок 53 Экран Advanced Application > Link Aggregation > Link Aggregation Setting



Поля экрана описаны в следующей таблице.

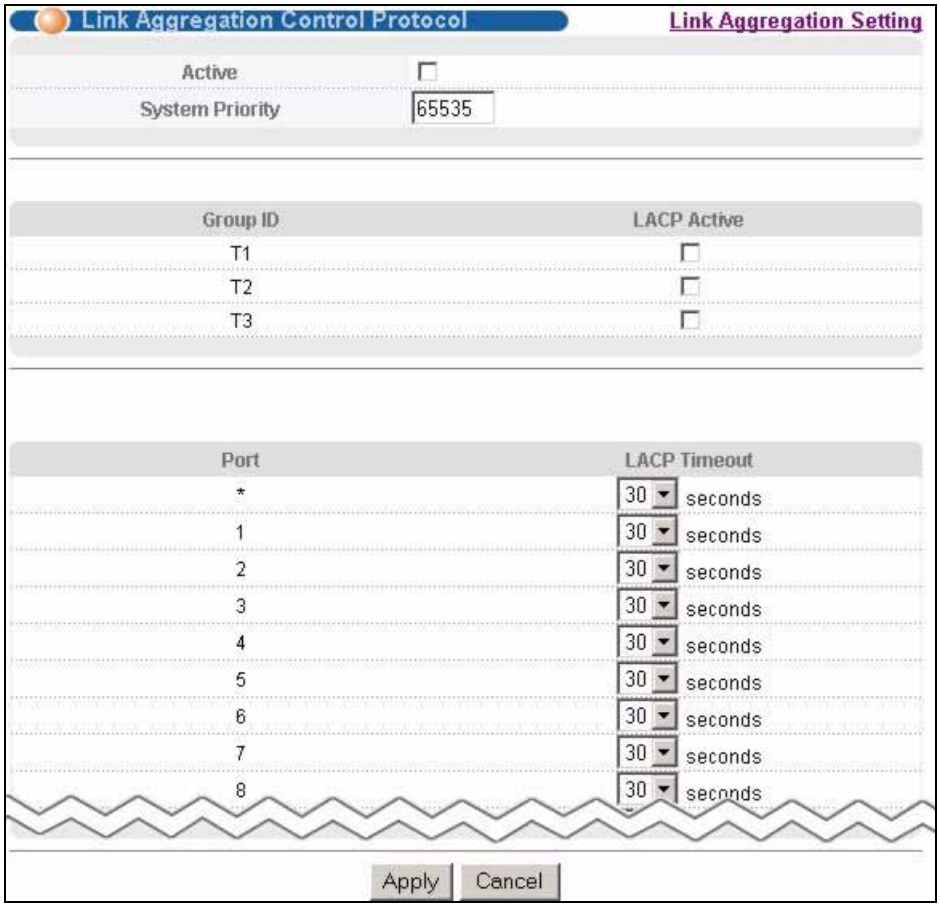
Таблица 33 Экран Advanced Application > Link Aggregation > Link Aggregation Setting

ПОЛЕ	ОПИСАНИЕ
Link Aggregation Setting	При включении статической агрегации каналов все настройки производятся на данном экране.
Group ID	В этом поле указан идентификатор группы агрегации каналов, то есть логического канала, объединяющего несколько портов.
Active	Установите этот переключатель, чтобы активировать группу портов.
Port	В этом поле отображается номер порта.
Group	Выберите группу портов, к которой принадлежит порт.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

15.5 Протокол управления агрегацией каналов LACP

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP**. Дополнительную информацию о динамической агрегации каналов можно найти в разд. 15.2 на стр. 127.

Рисунок 54 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



Поля экрана описаны в следующей таблице.

Таблица 34 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

ПОЛЕ	ОПИСАНИЕ
Link Aggregation Control Protocol	Примечание: Настройки на данном экране следует производить только при включении динамической агрегации каналов.
Active	Установите этот переключатель, чтобы включить протокол LACP.
System Priority	Приоритет системы протокола LACP – это число от 1 до 65 535. Коммутатор с наименьшим приоритетом системы (и наименьшим номером порта, если значения приоритета системы одинаковы) становится «сервером» протокола LACP. «Сервер» LACP управляет работой протокола LACP. Введите номер для установки приоритета активного порта, использующего протокол LACP. Чем меньше номер, тем выше уровень приоритета.
Group ID	В этом поле указан идентификатор группы агрегации каналов, то есть логического канала, объединяющего несколько портов.
LACP Active	Установите этот переключатель, чтобы включить протокол LACP для группы.
Port	В этом поле отображается номер порта.

Таблица 34 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (продолжение)

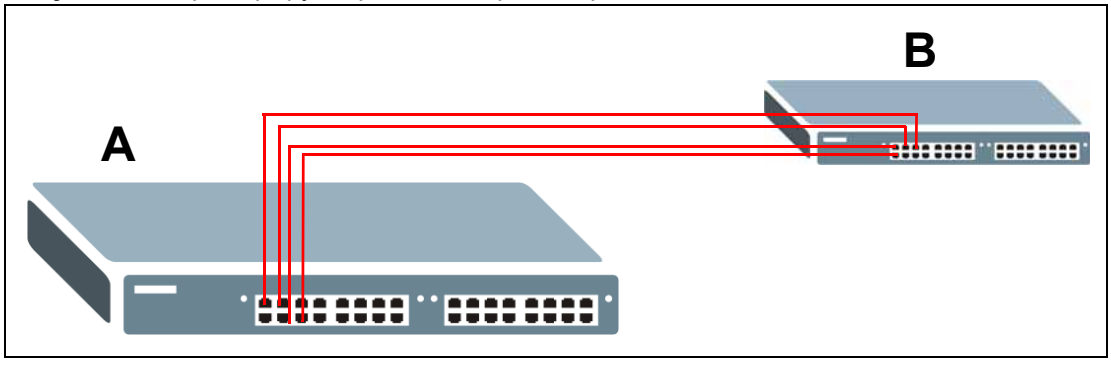
ПОЛЕ	ОПИСАНИЕ
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
LACP Timeout	Тайм-аут, определяющий временной промежуток от одного обмена пакетами LACP между отдельными портами до другого (в целях проверки работоспособности портов-партнеров в группе портов). Если порт не ответил после трех попыток, то он считается «отключенным» и удаляется из группы. Для загруженных сгруппированных каналов следует использовать короткий интервал (одна секунда), чтобы обеспечить скорейшее удаление отключенных портов из группы. Выберите значение (1 секунда или 30 секунд).
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

15.6 Пример статического группирования портов

В данном примере показано создание статической группы портов для портов 2-5.

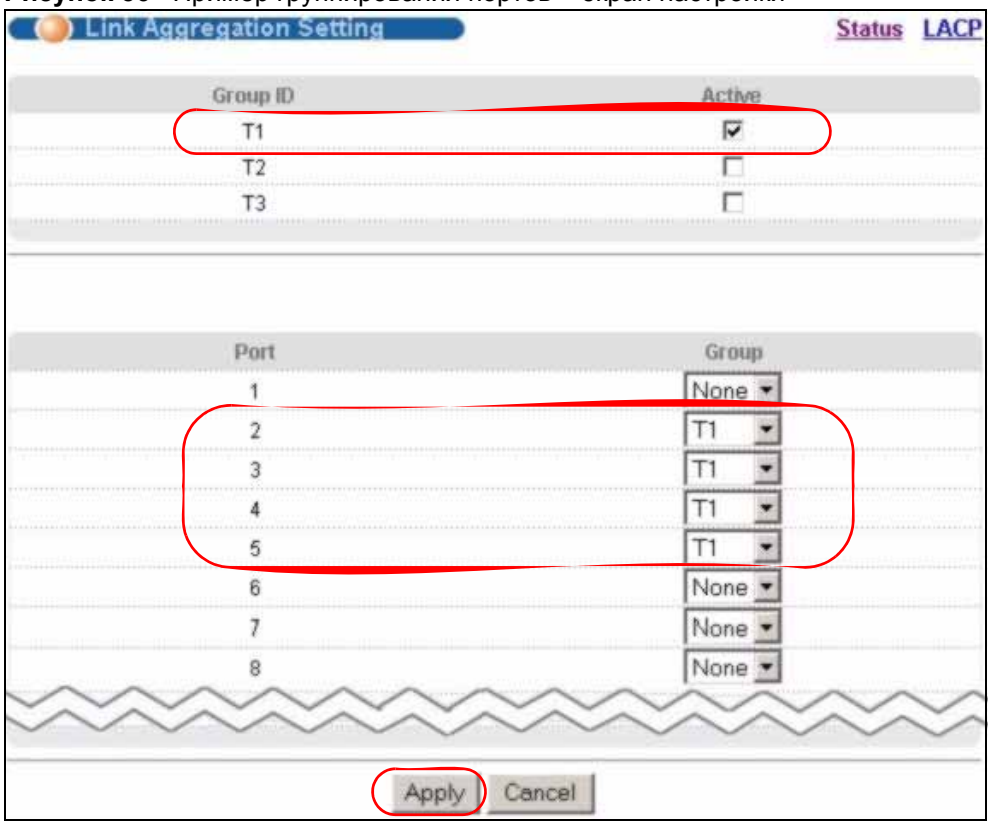
1 **Выполните физические подключения** – подключите все порты, которые должны войти в группу, к одному и тому же пункту назначения. На приведенном ниже рисунке показано подключение портов 2-5 коммутатора **A** к коммутатору **B**.

Рисунок 55 Пример группирования портов – физические подключения



2 **Настройте статическую группу портов** – нажмите **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting**. На этом экране активируйте группу портов **T1** и выберите порты, которые должны быть включены в эту группу, как показано на следующем рисунке. После этого нажмите **Apply**.

Рисунок 56 Пример группирования портов – экран настройки



На этом настройка группы портов 1 (**T1**) завершена; переходить на какие-либо другие экраны не требуется.

16

Аутентификация портов

В данной главе описаны методы аутентификации IEEE 802.1x.

16.1 Обзор аутентификации портов

Механизм аутентификации портов позволяет проверять права доступа клиентов к портам коммутатора с использованием внешнего сервера (сервера аутентификации). Данный коммутатор поддерживает стандарт аутентификации **IEEE 802.1x**[2], который предусматривает проверку прав доступа к портам на сервере аутентификации с использованием имени пользователя и пароля, предоставленных пользователями.

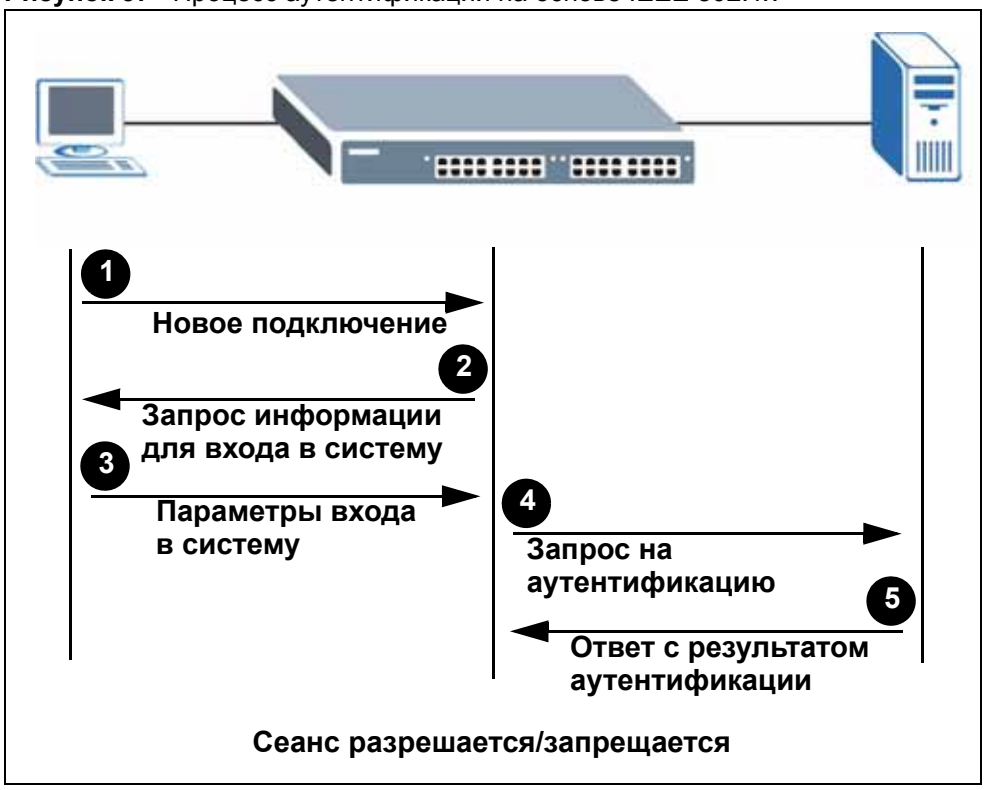
Проверка прав пользователя при такой аутентификации осуществляется с использованием протокола RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139). Дополнительную информацию о настройках сервера RADIUS можно найти в разд. 20.1.2 на стр. 164.

16.1.1 Аутентификация на основе IEEE 802.1x

Процесс проверки прав пользователя, подключающегося к порту с активированным механизмом аутентификации IEEE 802.1x, показан на следующем рисунке. Данный коммутатор запрашивает у клиента информацию для входа в систему в виде имени пользователя и пароля. После получения от клиента параметров входа в систему коммутатор отправляет запрос на аутентификацию на сервер RADIUS. Сервер RADIUS проверяет, обладает ли данный клиент правом доступа к данному порту.

2. На момент написания данного руководства стандарт IEEE 802.1x поддерживался не всеми операционными системами. Обратитесь к документации по операционной системе. Если операционная система не поддерживает стандарт 802.1x, может потребоваться установка программного обеспечения клиента 802.1x.

Рисунок 57 Процесс аутентификации на основе IEEE 802.1x



16.2 Настройка аутентификации портов

Чтобы включить аутентификацию портов, прежде всего необходимо активировать используемый метод или используемые методы аутентификации (как на коммутаторе, так и на портах), а затем настроить параметры сервера RADIUS на экране **Auth and Acct > Radius Server Setup**.

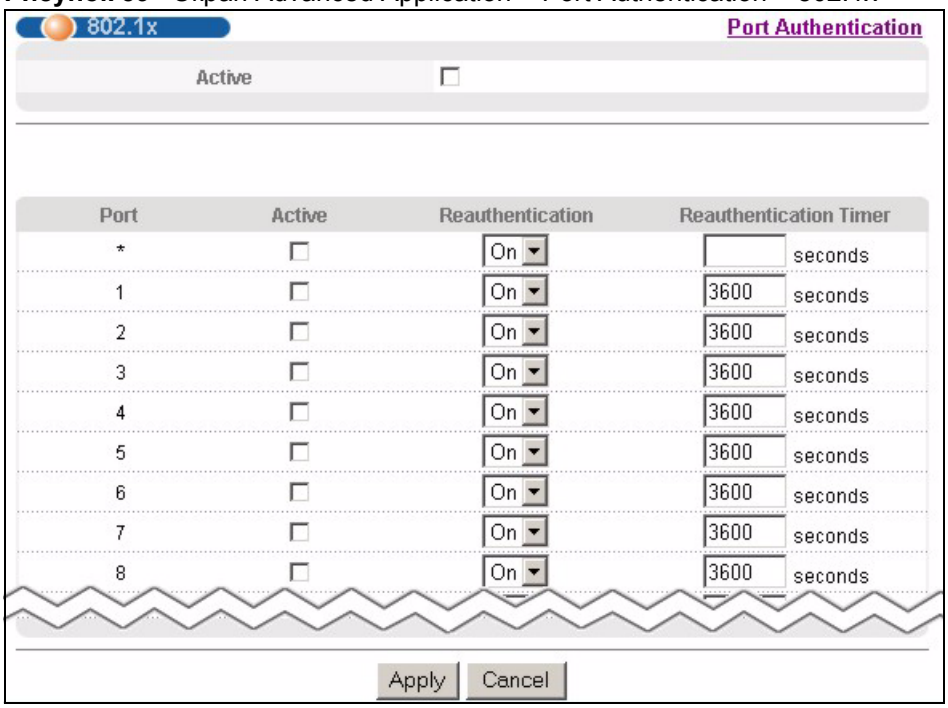
Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Port Authentication**.

Рисунок 58 Экран Advanced Application > Port Authentication

16.2.1 Включение функций безопасности стандарта IEEE 802.1x

С помощью данного экрана можно активировать функции безопасности стандарта IEEE 802.1x. На экране **Port Authentication** нажмите **802.1x**, чтобы отобразить показанный ниже экран настройки.

Рисунок 59 Экран Advanced Application > Port Authentication > 802.1x



Поля экрана описаны в следующей таблице.

Таблица 35 Экран Advanced Application > Port Authentication > 802.1x

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы разрешить аутентификацию по стандарту 802.1x на коммутаторе. Примечание: Прежде чем приступать к настройке службы аутентификации по стандарту 802.1x на каждом порту, необходимо включить ее на коммутаторе.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы разрешить аутентификацию по стандарту 802.1x на этом порту. Прежде чем активировать аутентификацию по стандарту 802.1x на каждом порту, необходимо включить ее на коммутаторе.
Reauthentication	Укажите, требуется ли пользователю периодически вводить заново свое пользовательское имя и пароль, чтобы оставаться подключенным к порту.
Reauthentication Timer	Укажите, как часто клиенту требуется вводить заново свое имя пользователя и пароль, чтобы оставаться подключенным к порту.

Таблица 35 Экран Advanced Application > Port Authentication > 802.1x (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

17

Средства безопасности портов

В данной главе описана настройка функций безопасности портов.

17.1 Обзор средств безопасности портов

Средства безопасности портов позволяют разрешить прохождение через порт коммутатора только пакетов с динамически полученными MAC-адресами и/или настроенными статическими MAC-адресами. Информацию о настройке пересылки на основе статических MAC-адресов можно найти в гл. 9 на стр. 95.

Для обеспечения максимальной безопасности порта необходимо отключить получение MAC-адресов и настроить для порта статический MAC-адрес (или MAC-адреса). По умолчанию функция получения MAC-адресов остается активированной, даже если средства безопасности портов не включены.

Функционально в коммутаторе предусмотрено три возможных результата работы средств безопасности портов. Для портов коммутатора можно настроить:

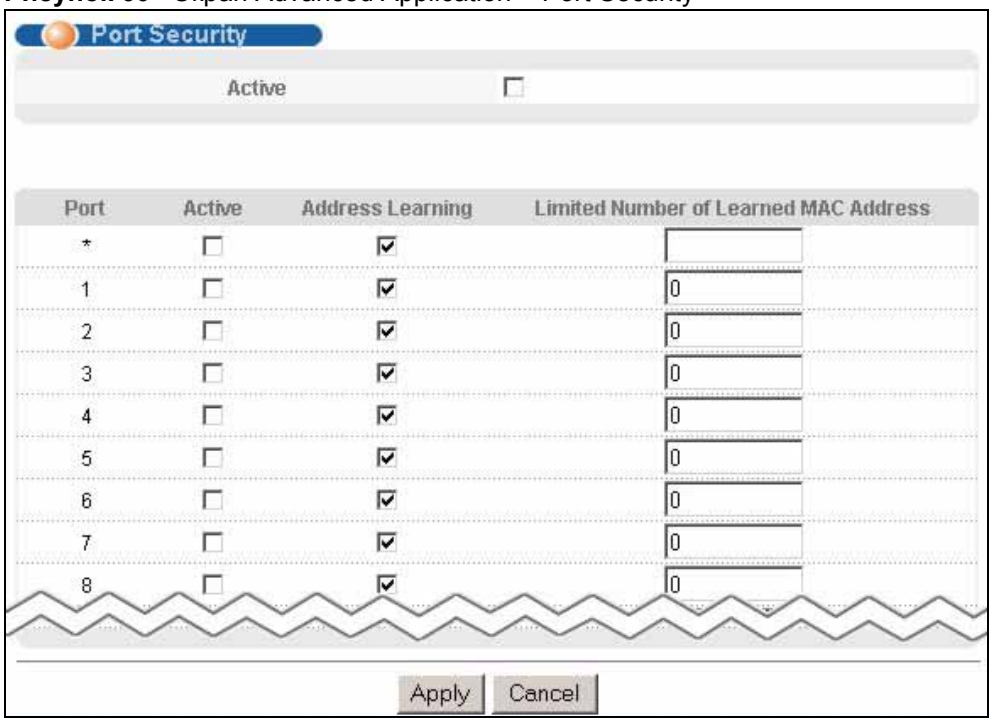
- Пересылку всех пакетов и получение (запоминание) всех MAC-адресов.
- Отбрасывание всех пакетов от неизвестных MAC-адресов и запрет на получение MAC-адресов.
- Отбрасывание всех пакетов от неизвестных MAC-адресов и получение ограниченного числа MAC-адресов.

Для средств безопасности портов коммутатором поддерживаются пять возможных конфигураций. Поддерживаемые конфигурации и примеры приводятся в разд. 17.3 на стр. 141.

17.2 Настройка средств безопасности портов

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Port Security**.

Рисунок 60 Экран Advanced Application > Port Security



Поля экрана описаны в следующей таблице.

Таблица 36 Экран Advanced Application > Port Security

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить средства безопасности портов на коммутаторе.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить средства безопасности для данного порта. Данный коммутатор пересылает пакеты, MAC-адрес(а) которых содержится в таблице MAC-адресов для этого порта. Пакеты с другими MAC-адресами отбрасываются. Снимите выделение с переключателя, если необходимо отключить эту функцию. Данный коммутатор будет пересылать все пакеты через этот порт.
Address Learning	Функция получения MAC-адресов снижает объем исходящего широковещательного трафика. Запоминание MAC-адресов через порт происходит лишь в том случае, если сам порт включен (на экране **Basic Settings**, **Port Setup**) и для него включено получение MAC-адресов.

Таблица 36 Экран Advanced Application > Port Security (продолжение)

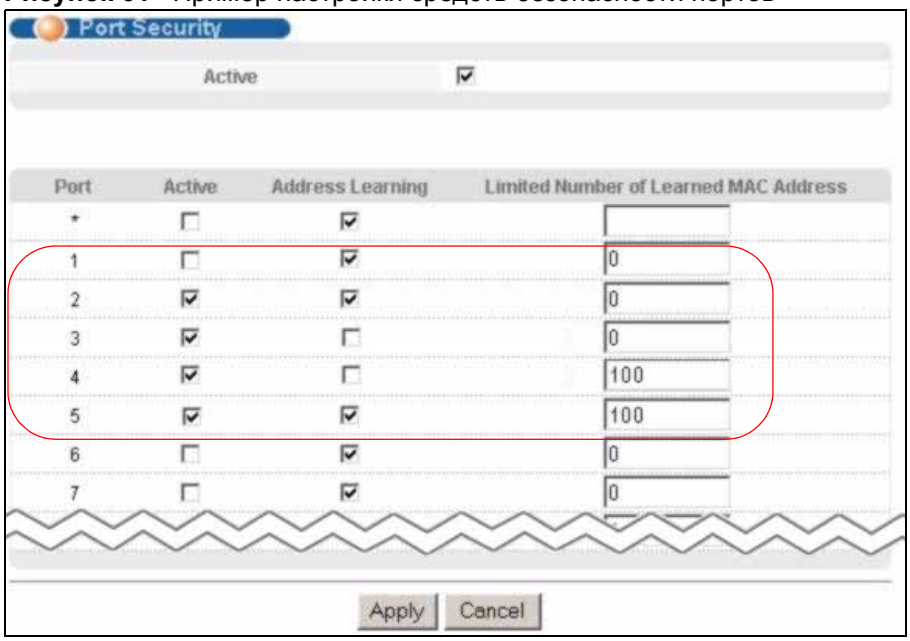
ПОЛЕ	ОПИСАНИЕ
Limited Number of Learned MAC Address	Это поле используется для ограничения допустимого количества (динамически) полученных MAC-адресов для порта. Например, если указать в этом поле для порта 2 значение «5», то в каждый момент времени одновременно получить доступ к порту 2 смогут лишь устройства с пятью полученными MAC-адресами. Шестому устройству придется ждать, пока один из этих пяти полученных MAC-адресов устареет. Параметр устаревания MAC-адресов можно определить в меню **Switch Setup**. Допустимый диапазон значений составляет от 0 до 8192. «0» означает отключение ограничений на количество запоминаемых адресов.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

17.3 Пример настройки средств безопасности портов

Следующий пример демонстрирует различные настройки и результаты работы различных конфигураций средств безопасности портов. Для портов с 1 по 5 установлены следующие настройки:

- Порт 1 – Пересылка всех пакетов и получение (запоминание) всех MAC-адресов.
- Порт 2 – Пересылка всех пакетов и получение (запоминание) всех MAC-адресов.
- Порт 3 – Отбрасывание всех пакетов от неизвестных MAC-адресов и запрет на получение MAC-адресов.
- Порт 4 – Отбрасывание всех пакетов от неизвестных MAC-адресов и запрет на получение MAC-адресов.
- Порт 5 – Отбрасывание всех пакетов от неизвестных MAC-адресов и пересылка пакетов от максимум 100 запомненных MAC-адресов.

Рисунок 61 Пример настройки средств безопасности портов



Возможные комбинации настроек и результаты их работы сведены в следующей таблице.

Таблица 37 Пример настройки средств безопасности портов

ПОРТ	НАСТРОЙКИ			РЕЗУЛЬТАТ
	ВКЛЮЧЕНИЕ СРЕДСТВ БЕЗОПАСНОСТИ	ВКЛЮЧЕНИЕ ЗАПОМИНАНИЯ АДРЕСОВ	ОГРАНИЧЕНИЕ КОЛ-ВА ЗАПОМИНАЕМЫХ MAC-АДРЕСОВ	
1		X	0 (без ограничений)	Пересылка всех пакетов, получение (запоминание) всех MAC-адресов.
2	X	X	0 (без ограничений)	Пересылка всех пакетов, получение (запоминание) всех MAC-адресов.
3	X		0 (без ограничений)	Отбрасывание всех пакетов от неизвестных MAC-адресов, запрет на получение MAC-адресов.
4	X		100	Отбрасывание всех пакетов от неизвестных MAC-адресов, запрет на получение MAC-адресов.
5	X	X	100	Отбрасывание пакетов от неизвестных MAC-адресов, запоминание максимум 100 MAC-адресов.

18

Метод организации очередей

В данной главе описаны поддерживаемые методы организации очередей.

18.1 Обзор методов организации очередей

Организация очередей помогает решить проблему снижения производительности в случаях перегрузки сети. Для настройки алгоритмов организации очередей для исходящего трафика используется меню **Queuing Method**. Дополнительную информацию можно также найти в описании меню **Priority Queue Assignment** на экране **Switch Setup** и **802.1p Priority** на экране **Port Setup**.

Алгоритмы организации очередей позволяют коммутаторам поддерживать раздельные очереди для пакетов от каждого отдельного источника или потока, а также предотвращать присвоение всей пропускной способности одним источником.

Таблица 38 Приоритет физической очереди

ОЧЕРЕДЬ	ПРИОРИТЕТ
Q3	4 (высший)
Q2	3
Q1	2
Q0	1 (низший)

18.1.1 Строгая очередь приоритетов (SPQ)

Алгоритм строгой очереди приоритетов SPQ обрабатывает очереди на основании только уровня приоритета. При поступлении трафика на коммутатор трафик с наивысшим уровнем приоритета (Q7) передается первым. Когда эта очередь заканчивается, начинает передаваться трафик со следующим уровнем приоритета Q6, пока эта очередь также не закончится, после чего начинает передаваться трафик с уровнем приоритета Q5, и так далее. Если очереди для трафика с высоким приоритетом никогда не заканчиваются, то трафик с низким приоритетом может не пройти через коммутатор. Алгоритм SPQ не может автоматически приспосабливаться к изменяющимся требованиям сети.

18.1.2 Взвешенное циклическое обслуживание (WRR)

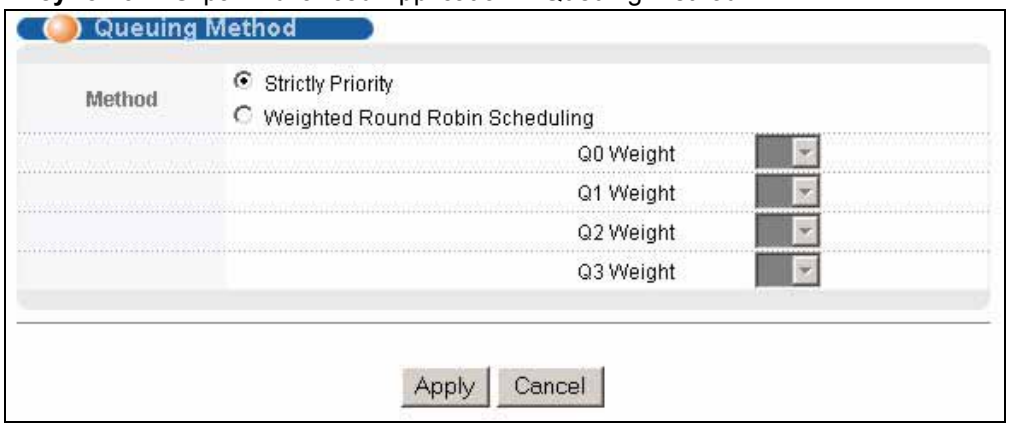
Алгоритм циклического обслуживания обрабатывает очереди по кругу и запускается только тогда, когда на порт приходит больше трафика, чем он может принять. Очереди выделяется некоторая доля пропускной способности вне зависимости от объема трафика, приходящего на этот порт. Затем эта очередь смещается в конец списка. Следующей очереди выделяется аналогичная доля пропускной способности, затем эта очередь тоже перемещается в конец списка; и так далее, в зависимости от количества используемых очередей. Алгоритм циклически повторяется, пока очередь не опустеет.

Алгоритм взвешенного циклического обслуживания (WRR) использует тот же метод, что и простое циклическое обслуживание, но он обрабатывает очереди на основе их уровня приоритета и веса очереди (число, которое вводится в поле **Weight**), а не фиксированной доли пропускной способности. Алгоритм WRR запускается только тогда, когда на порт приходит больше трафика, чем он может обработать. Очереди с большим весом обрабатываются быстрее, чем очереди с малым весом. Этот механизм организации очереди эффективен потому, что он распределяет всю доступную пропускную способность между различными очередями трафика и возвращается к очередям, которые еще не закончились.

18.2 Настройка метода организации очередей

Выберите в навигационной панели **Advanced Application** > **Queuing Method**.

Рисунок 62 Экран Advanced Application > Queuing Method



Поля экрана описаны в следующей таблице.

Таблица 39 Экран Advanced Application > Queuing Method

ПОЛЕ	ОПИСАНИЕ
Method	Выберите **Strictly Priority** (строгая очередь приоритетов) или **Weighted Round Robin Scheduling** (взвешенное циклическое обслуживание). Алгоритм строгой очереди приоритетов SPQ обрабатывает очереди на основании только уровня приоритета. Когда опустошается очередь с наивысшим приоритетом, начинается обработка трафика в очереди со следующим уровнем приоритета. Самый высокий уровень приоритета – Q3, самый низкий – Q0. По умолчанию выбирается метод строгой очереди приоритетов **Strictly Priority**. Алгоритм взвешенного циклического обслуживания WRR обрабатывает очереди циклически в зависимости от их веса (число, которое вводится в поле веса **Weight** очереди). Очереди с большим весом обрабатываются быстрее, чем очереди с малым весом. При выборе **Strict Priority** данный метод применяется только к очереди Q3 (с приоритетом перед всеми другими очередями). Для очередей Q0 ~ Q2 используется **Weighted Round Robin Scheduling**.
Weight	При выборе алгоритма **Weighted Round Robin Scheduling** необходимо выбрать веса очередей в ниспадающем списке (1-15). Пропускная способность распределяется между очередями в зависимости от их веса.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

19

Мультивещание

В данной главе описана настройка различных функций мультивещания.

19.1 Обзор мультивещания

Обычно передача IP-пакетов происходит одним из двух способов: в режиме одноадресной передачи (от 1 отправителя к 1 получателю) или в режиме широковещания (от 1 отправителя всем получателям в сети). Мультивещание (или групповая передача) обеспечивает доставку IP-пакетов определенной группе хостов в сети.

Межсетевой протокол управления группами (Internet Group Management Protocol, IGMP) представляет собой протокол сетевого уровня, используемый для определения принадлежности к группе мультивещания. Для передачи пользовательских данных он не используется. Информацию о протоколе IGMP версий 1 2 и 3 можно найти соответственно в стандартах RFC 1112, RFC 2236 и RFC 3376.

19.1.1 IP-адреса мультивещания

В IPv4 адрес мультивещания позволяет устройству отправлять пакеты определенной группе хостов (группе мультивещания) в отличной подсети. IP-адрес мультивещания определяет группу получателей трафика, а не конкретное получающее устройство. В качестве IP-адресов мультивещания используются IP-адреса класса D (от 224.0.0.0 до 239.255.255.255). Некоторые IP-адреса мультивещания зарезервированы IANA для особых целей (более подробную информацию можно найти на сайте IANA).

19.1.2 Фильтрация IGMP

Функция фильтрации IGMP позволяет определять, к каким группам IGMP сможет присоединяться абонент на порту. Таким образом можно контролировать предоставление функций мультивещания (например, рассылку контента) в зависимости от тарифных планов и типов подписки.

В коммутаторе можно настроить отбрасывание запросов присоединения к группам мультивещания на уровне отдельного порта, для чего необходимо настроить профиль фильтрации IGMP и привязать этот профиль к конкретному порту.

19.1.3 Отслеживание многоадресного трафика IGMP

Данный коммутатор может пассивно отслеживать IGMP-пакеты, передаваемые между маршрутизаторами/коммутаторами IP-мультивещания и хостами IP-мультивещания, чтобы получать информацию об участии в группах IP-мультивещания. Он проверяет IGMP-пакеты, проходящие через него, считывает информацию о регистрации в группах, а затем соответствующим образом настраивает мультивещание. Функция отслеживания многоадресного трафика (IGMP snooping) позволяет коммутатору автоматически считывать информацию о группах мультивещания, избавляя от необходимости настраивать их вручную.

Данный коммутатор направляет мультивещательный трафик, предназначенный для групп мультивещания (которые были выявлены функцией отслеживания многоадресного трафика IGMP или введены вручную), на порты, являющиеся членами соответствующей группы. Функция отслеживания многоадресного трафика IGMP не создает дополнительного сетевого трафика, что позволяет значительно снизить объем мультивещательного трафика, проходящего через коммутатор.

19.1.4 Отслеживание многоадресного трафика IGMP и сети VLAN

Данный коммутатор может отслеживать многоадресный трафик IGMP максимум в 16 виртуальных локальных сетях VLAN. На коммутаторе можно настроить режим автоматического получения информации об участии в группе мультивещания для любых сетей VLAN. При этом коммутатор будет выполнять отслеживание многоадресного трафика IGMP в первых 16 виртуальных локальных сетях VLAN, от которых были получены пакеты IGMP. Такой режим называется автоматическим (auto). Кроме того, можно указать конкретные виртуальные локальные сети VLAN, для которых необходимо выполнять отслеживание многоадресного трафика IGMP. Такой режим называется фиксированным (fixed). В фиксированном режиме коммутатор получает информацию об участии в группах мультивещания только в таких виртуальных локальных сетях VLAN, которые были явным образом добавлены как VLAN отслеживания многоадресного трафика IGMP.

19.2 Состояние мультивещания

Чтобы отобразить следующий экран, нажмите **Advanced Applications > Multicast**. На этом экране отображается информация о группах мультивещания. Более подробную информацию о мультивещании можно найти в разд. 19.1 на стр. 147.

Рисунок 63 Экран Advanced Application > Multicast

Поля экрана описаны в следующей таблице.

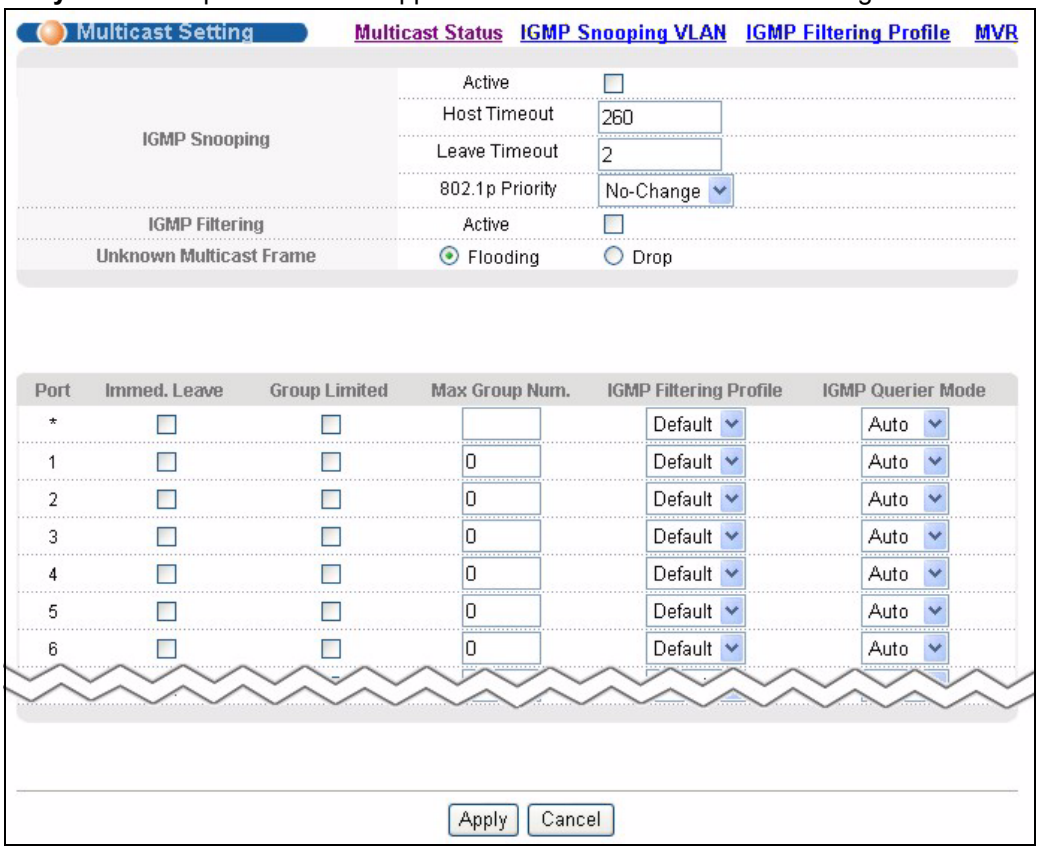
Таблица 40 Экран Multicast Status

ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер записи.
VID	В этом поле отображается идентификатор VLAN-сети мультивещания.
Port	В этом поле отображается номер порта, принадлежащего группе мультивещания.
Multicast Group	В этом поле отображаются IP-адреса группы мультивещания.

19.3 Настройка мультивещания

Чтобы отобразить показанный ниже экран, нажмите **Advanced Applications > Multicast > Multicast Setting**. Более подробную информацию о мультивещании можно найти в разд. 19.1 на стр. 147.

Рисунок 64 Экран Advanced Application > Multicast > Multicast Setting



Поля экрана описаны в следующей таблице.

Таблица 41 Экран Advanced Application > Multicast > Multicast Setting

ПОЛЕ	ОПИСАНИЕ
IGMP Snooping	Данные параметры позволяют настроить отслеживание многоадресного трафика IGMP.
Active	Выбор **Active** активирует отслеживание многоадресного трафика IGMP, при котором трафик группы мультивещания пересылается только на порты, входящие в соответствующую группу.
Host Timeout	Укажите время в секундах (от 1 до 16 711 450), по истечении которого коммутатор удаляет запись об участии в группе IGMP при отсутствии сообщений Report от порта.
Leave Timeout	Введите значение тайм-аута Leave для IGMP в секундах (от 1 до 16 711 450). Он определяет время, которое коммутатор выжидает после получения IGMP-сообщения Leave от хоста перед удалением записи об участии в группе IGMP.
802.1p Priority	Выберите приоритет (0-7), который устанавливается коммутатором для исходящих управляющих пакетов IGMP. Выбор **No-Change** оставляет приоритет без изменения.
IGMP Filtering	Выбор **Active** активирует функцию фильтрации IGMP, с помощью которой можно определять, к каким группам IGMP сможет присоединяться абонент на порту. Примечание: При включении фильтрации IGMP необходимо создать и назначить профили фильтрации IGMP тем портам, которым необходимо разрешить присоединение к группам мультивещания.
Unknown Multicast Frame	Выберите действие, выполняемое коммутатором при получении неизвестного кадра мультивещания. **Drop** – отбрасывание кадра. **Flooding** – пересылка кадра на все порты.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Immed. Leave	Выбор данной опции заставляет коммутатор удалять данный порт из дерева мультивещания сразу же при получении через данный порт Leave-сообщения протокола IGMP версии 2. Эту опцию следует выбирать лишь в том случае, когда к порту подключен только один хост.
Group Limited	Выбор данной опции позволяет ограничить число групп мультивещания, к которым разрешено присоединиться данному порту.
Max Group Num.	Введите число групп мультивещания (0-255), к которым разрешено присоединиться данному порту. После регистрации порта в указанном количестве групп мультивещания все последующие Join-сообщения IGMP от данного порта отбрасываются.

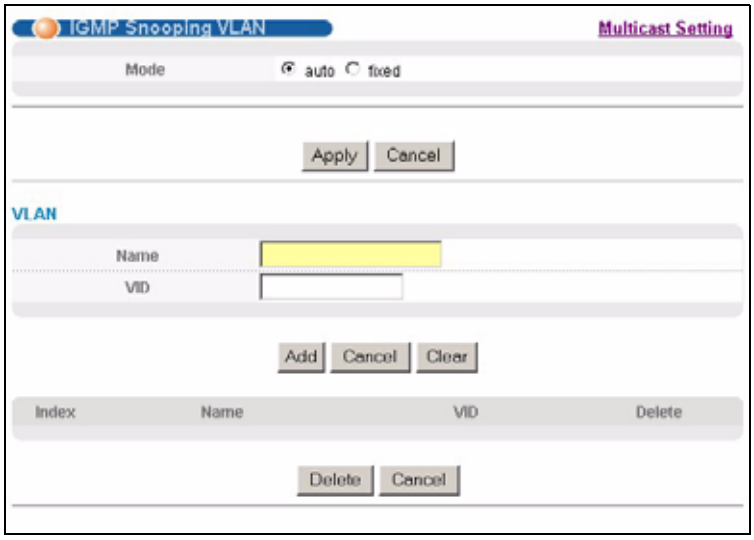
Таблица 41 Экран Advanced Application > Multicast > Multicast Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
IGMP Filtering Profile	Выберите имя профиля фильтрации IGMP, который будет использоваться для данного порта. Значение **Default** запрещает порту присоединение к любым группам мультивещания. Создание профилей фильтрации IGMP осуществляется на экране **Multicast** > **Multicast Setting** > **IGMP Filtering Profile**.
IGMP Querier Mode	Query-порт IGMP коммутатор рассматривает в качестве порта, к которому подключен маршрутизатор (или сервер) мультивещания IGMP. Join- и Leave-пакеты IGMP коммутатор направляет на Query-порт IGMP. Значение **Auto** заставляет коммутатор назначать порту статус Query-порта IGMP при получении Query-пакетов IGMP. Значение **Fixed** заставляет коммутатор постоянно использовать данный порт в качестве Query-порта IGMP. Данное значение следует выбрать в том случае, когда к порту подключается сервер мультивещания IGMP. Значение **Edge** заставляет коммутатор отменить для данного порта статус Query-порта IGMP. Данный коммутатор не сохраняет каких-либо записей о подключении маршрутизатора IGMP к данному порту. Join- и Leave-пакеты IGMP на этот порт коммутатором не пересылаются.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

19.4 VLAN отслеживания многоадресного трафика IGMP

Выберите в навигационной панели **Advanced Applications** > **Multicast**. Нажмите на ссылку **Multicast Setting** и затем на **IGMP Snooping VLAN**, чтобы отобразить показанный ниже экран. Дополнительную информацию о VLAN отслеживания многоадресного трафика IGMP можно найти в разд. 19.1.4 на стр. 148.

Рисунок 65 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN



Поля экрана описаны в следующей таблице.

Таблица 42 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

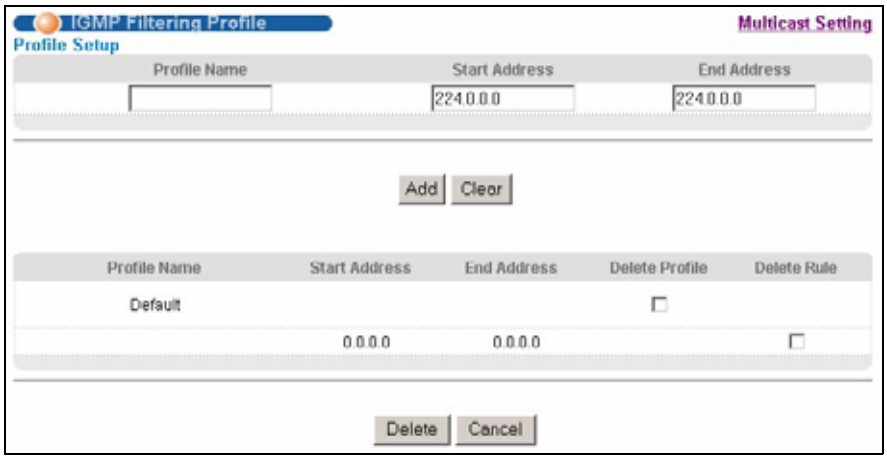
ПОЛЕ	ОПИСАНИЕ
Mode	Выберите **auto**, чтобы коммутатор автоматически получал информацию обо участии в группе мультивещания для любых сетей VLAN. Выберите **fixed**, чтобы коммутатор получал информацию об участии в группе мультивещания только для указанных ниже сетей VLAN. Как в автоматическом режиме **auto**, так и в фиксированном режиме **fixed** коммутатор способен получить информацию максимум о 16 виртуальных локальных сетях VLAN (включая максимум три сети VLAN, настроенные на экране **MVR**). Так, если на экране **MVR** была настроена одна VLAN-сеть мультивещания, на данном экране можно настроить не более 15 сетей VLAN. Данный коммутатор отбрасывает любые управляющие сообщения IGMP, которые не принадлежат одной из этих 16 сетей VLAN. Примечание: Предварительно необходимо включить отслеживание многоадресного трафика IGMP на экране **Multicast Setting**.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
VLAN	В данном разделе можно добавить сети VLAN, для которых коммутатор будет осуществлять отслеживание многоадресного трафика IGMP.
Name	Введите имя-описание VLAN, с помощью которого ее можно идентифицировать.
VID	Введите идентификатор статической VLAN; допустимое значение находится в диапазоне от 1 до 4094. Примечание: Не допускается использовать тот же идентификатор VLAN ID, что и на экране **MVR**.
Add	Нажмите **Add**, чтобы добавить запись в итоговую таблицу ниже и сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы сбросить поля к предыдущим значениям.
Clear	Нажатие на данную кнопку позволяет очистить поля.
Index	Номер записи VLAN отслеживания многоадресного трафика IGMP в таблице.
Name	В этом поле отображается имя-описание группы VLAN.
VID	В этом поле отображается идентификационный номер группы VLAN.
Delete	В столбце **Delete** установите переключатели правил, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

19.5 Профиль фильтрации IGMP

Профиль фильтрации IGMP определяет диапазон групп мультивещания, к которым могут присоединиться подключенные к коммутатору пользователи. Профиль содержит диапазон IP-адресов мультивещания, к которым необходимо разрешить подключение пользователей. Профили назначаются конкретным портам (на экране **Multicast Setting**). Подключающиеся через эти порты пользователи могут присоединяться к группам мультивещания, указанным в профиле Каждому порту может быть назначен только один профиль. Один и тот же профиль допускается назначать нескольким портам.

Чтобы отобразить показанный ниже экран, нажмите **Advanced Applications** > **Multicast** > **Multicast Setting** > **IGMP Filtering Profile**.

Рисунок 66 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile



Поля экрана описаны в следующей таблице.

Таблица 43 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

ПОЛЕ	ОПИСАНИЕ
Profile Name	Введите имя-описание профиля, с помощью которого его можно идентифицировать. Чтобы настроить дополнительные правила для уже добавленного профиля, необходимо ввести имя профиля и указать другие диапазоны IP-адресов мультивещания.
Start Address	Введите начальный адрес диапазона IP-адресов мультивещания, который необходимо включить в профиль фильтрации IGMP.
End Address	Введите конечный адрес диапазона IP-адресов мультивещания, который необходимо включить в профиль фильтрации IGMP. Чтобы добавить единственный IP-адрес мультивещания, укажите его и в поле **Start Address**, и в поле **End Address**.
Add	Нажмите **Add**, чтобы сохранить профиль в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Profile Name	В этом поле отображается имя-описание профиля.

Таблица 43 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
Start Address	В этом поле отображается начальный адрес диапазона IP-адресов мультивещания.
End Address	В этом поле отображается конечный адрес диапазона IP-адресов мультивещания.
Delete	Чтобы удалить профиль и все связанные с ним правила, выберите нужный профиль в столбце **Delete Profile** и нажмите на кнопку **Delete**. Чтобы удалить правило или правила из профиля, выберите нужные правила в столбце **Delete Rule** и нажмите на кнопку **Delete**.
Cancel	Нажатие на кнопку **Cancel** снимает выделения с переключателей в столбцах **Delete Profile**/**Delete Rule**.

19.6 Обзор MVR

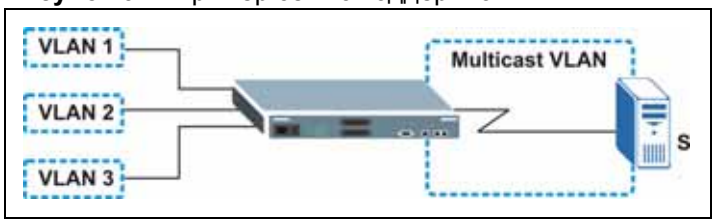
Механизм регистрации VLAN-сети мультивещания (Multicast VLAN Registration, MVR) предназначен для случаев, когда требуется передавать мультивещательный трафик через Ethernet-сеть провайдера услуг, имеющую конфигурацию кольца (например, для приложений «мультимедиа по требованию» – MoD).

MVR позволяет определить одну VLAN-сеть мультивещания, которая будет доступна различным абонентским сетям VLAN в сети. Даже изолированные по различным абонентским сетям VLAN устройства могут подписываться и отписываться от потока мультивещания во VLAN-сети мультивещания. Благодаря этому обеспечивается оптимальное использование пропускной способности за счет предотвращения дублирования мультивещательного трафика в абонентских сетях VLAN, а также упрощается управление группами мультивещания.

MVR реагирует только на управляющие Join- и Leave-запросы IGMP от групп мультивещания, которые были настроены в MVR. Join- и Leave-запросы от других групп мультивещания управляются отслеживанием IGMP.

Пример сети показан на следующем рисунке. Информация об абонентских сетях VLAN (**1**, **2** и **3**) скрыта от сервера потокового мультимедиа **S**. Кроме того, информация о VLAN-сети мультивещания видима только коммутатору и серверу **S**.

Рисунок 67 Пример сети с поддержкой MVR



19.6.1 Типы портов MVR

В MVR портом источника называется порт коммутатора, который отправляет и принимает трафик мультивещания из VLAN-сети мультивещания, тогда как порт приемника может только принимать трафик мультивещания. После настройки на коммутаторе создается таблица пересылки, которая соотносит поток мультивещания с соответствующей группой мультивещания.

19.6.2 Режимы MVR

Для коммутатора можно выбрать либо динамический режим, либо режим совместимости MVR.

В динамическом режиме коммутатор отправляет Leave- и Join-сообщения IGMP на другие устройства мультивещания (такие как маршрутизаторы или серверы мультивещания) во VLAN-сети мультивещания. Благодаря этому устройства мультивещания могут обновлять таблицу пересылки мультивещательного трафика и включать или отключать пересылку трафика мультивещания на порты приемников.

В режиме совместимости коммутатор не пересылает никаких запросов IGMP. В этом случае настройки пересылки на устройствах мультивещания во VLAN-сети мультивещания необходимо устанавливать вручную.

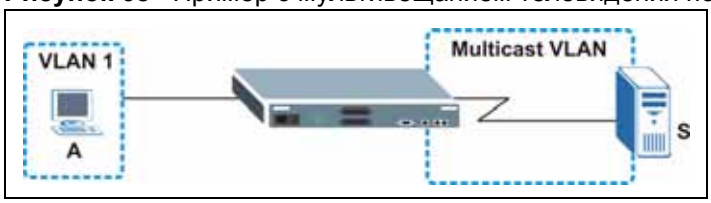
19.6.3 Как работает механизм MVR

Приведенный ниже рисунок иллюстрирует пример с мультивещанием телевизионного контента, когда абонентское устройство (такое как компьютер) в сети VLAN 1 принимает через коммутатор трафик мультивещания от сервера потокового мультимедиа **S**. Через порт, настроенный на коммутаторе в качестве порта приемника, возможно подключение нескольких абонентских устройств.

При выборе абонентом телевизионного канала компьютер **A** отправляет на коммутатор IGMP-запрос на присоединение к соответствующей группе мультивещания. Если IGMP-запрос соответствует одному из настроенных на коммутаторе адресов групп мультивещания MVR, в таблице пересылки коммутатора создается запись. В ней абонентская VLAN включается в список пунктов назначения для пересылки указанного трафика мультивещания.

Если абонент переключается на другой канал или выключает компьютер, на коммутатор направляется Leave-сообщение IGMP для выхода из группы мультивещания. Данный коммутатор направляет запрос в сеть VLAN 1 через порт приемника (в данном случае это порт каскадирования коммутатора). Если к данному порту в той же абонентской VLAN подключено еще хотя бы одно абонентское устройство, порт приемника по-прежнему останется в списке пунктов назначения для пересылки трафика мультивещания. В противном случае коммутатор удаляет порт приемника из таблицы пересылки.

Рисунок 68 Пример с мультивещанием телевидения посредством MVR



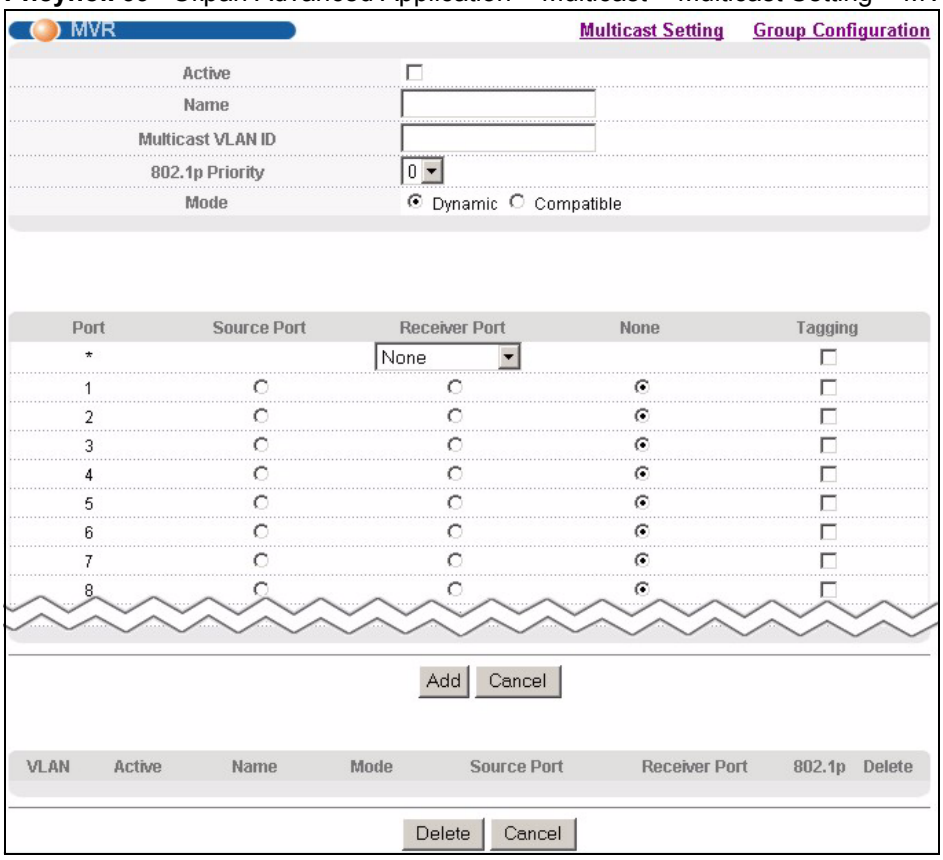
19.7 Общая настройка MVR

Создать VLAN-сети мультивещания и выбрать для каждой VLAN-сети мультивещания порты приемников и порт источника можно на экране **MVR**. Чтобы отобразить показанный ниже экран, нажмите **Advanced Applications > Multicast** > **Multicast Setting > MVR**.

Данный коммутатор позволяет определить максимум три VLAN-сети мультивещания и максимум 256 правил.

При создании на данном экране VLAN-сети мультивещания коммутатор автоматически создает статическую VLAN (с тем же идентификатором VID).

Рисунок 69 Экран Advanced Application > Multicast > Multicast Setting > MVR



Поля экрана описаны в следующей таблице.

Таблица 44 Экран Advanced Application > Multicast > Multicast Setting > MVR

ПОЛЕ	ОПИСАНИЕ
Active	Выберите данный переключатель для включения MVR, чтобы использовать одну единственную VLAN-сеть мультивещания для различных абонентских VLAN в сети.
Name	Введите имя-описание (до 32 символов в английской раскладке), по которому можно идентифицировать эту сеть.
Multicast VLAN ID	Введите идентификатор сети VLAN (от 1 до 4094) для VLAN-сети мультивещания.
802.1p Priority	Выберите приоритет (0-7), на который коммутатор заменяет приоритет в исходящих управляющих пакетах IGMP (принадлежащих к данной VLAN-сети мультивещания).
Mode	Укажите режим MVR для коммутатора. Можно выбрать значения **Dynamic** (динамический) и **Compatible** (режим совместимости). **Dynamic** – сообщения IGMP отправляются на все порты источников MVR во VLAN-сети мультивещания. **Compatible** – сообщения IGMP коммутатором не отправляются.
Port	В этом поле отображается номер порта коммутатора.

Таблица 44 Экран Advanced Application > Multicast > Multicast Setting > MVR

ПОЛЕ	ОПИСАНИЕ
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Source Port	Выберите данную опцию, чтобы назначить данный порт в качестве порта источника MVR, который осуществляет отправку и прием трафика мультивещания. Все порты источников должны принадлежать к одной VLAN-сети мультивещания.
Receiver Port	Выберите данную опцию, чтобы назначить данный порт в качестве порта приемника MVR, который только принимает трафик мультивещания.
None	Выберите данную опцию, если данный порт не участвует в механизме MVR. Через такой порт трафик мультивещания MVR не передается и не принимается.
Tagging	Выберите данный переключатель, если ко всем передаваемым через порт исходящим кадрам должен добавляться тег идентификатора VLAN.
Add	Нажмите **Add**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
VLAN	В этом поле отображается идентификатор VLAN-сети мультивещания.
Active	Данное поле показывает, включена ли поддержка группы мультивещания.
Name	В этом поле отображается имя-описание для данной настройки.
Mode	В этом поле отображается режим MVR.
Source Port	В этом поле отображаются номера портов источников.
Receiver Port	В этом поле отображаются номера портов приемников.
802.1p	В этом поле отображается уровень приоритета.
Delete	Чтобы удалить VLAN-сети мультивещания, выберите нужные сети в столбце **Delete** и нажмите на кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

19.8 Настройка группы MVR

Данные мультивещания, направляемые в группу мультивещания, могут принимать все порты источников и порты приемников, принадлежащие группе мультивещания.

IP-адреса группы мультивещания MVR настраиваются на экране **Group Configuration**. Нажмите на ссылку **Group Configuration** на экране **MVR**.

Порт может принадлежать нескольким VLAN-сетям мультивещания. Однако, IP-адреса различных групп мультивещания не должны перекрываться.

Рисунок 70 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

Поля экрана описаны в следующей таблице.

Таблица 45 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

ПОЛЕ	ОПИСАНИЕ
Multicast VLAN ID	Выберите из ниспадающего списка идентификатор VLAN-сети мультивещания (настроенный на экране **MVR**).
Name	Введите имя-описание для идентификации.
Start Address	Введите начальный IP-адрес группы мультивещания в виде десятичных чисел, разделенных точками. Более подробную информацию об IP-адресах мультивещания можно найти в разд. 19.1.1 на стр. 147.
End Address	Введите конечный IP-адрес группы мультивещания в виде десятичных чисел, разделенных точками. Если в группу мультивещания необходимо внести только один адрес, введите в это поле тот же IP-адрес, что и в поле **Start Address**. Более подробную информацию об IP-адресах мультивещания можно найти в разд. 19.1.1 на стр. 147.
Add	Нажмите **Add**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
MVLAN	В этом поле отображается идентификатор VLAN-сети мультивещания.
Name	В этом поле отображается имя-описание для данной настройки.
Start Address	В этом поле отображается начальный IP-адрес группы мультивещания.
End Address	В этом поле отображается конечный IP-адрес группы мультивещания.

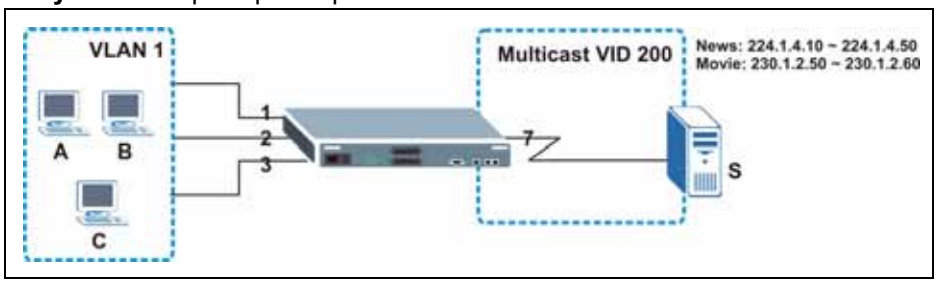
Таблица 45 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

ПОЛЕ	ОПИСАНИЕ
Delete	Для удаления из таблицы выбранных записей выберите **Delete Group** и нажмите **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей в таблице.

19.8.1 Пример настройки MVR

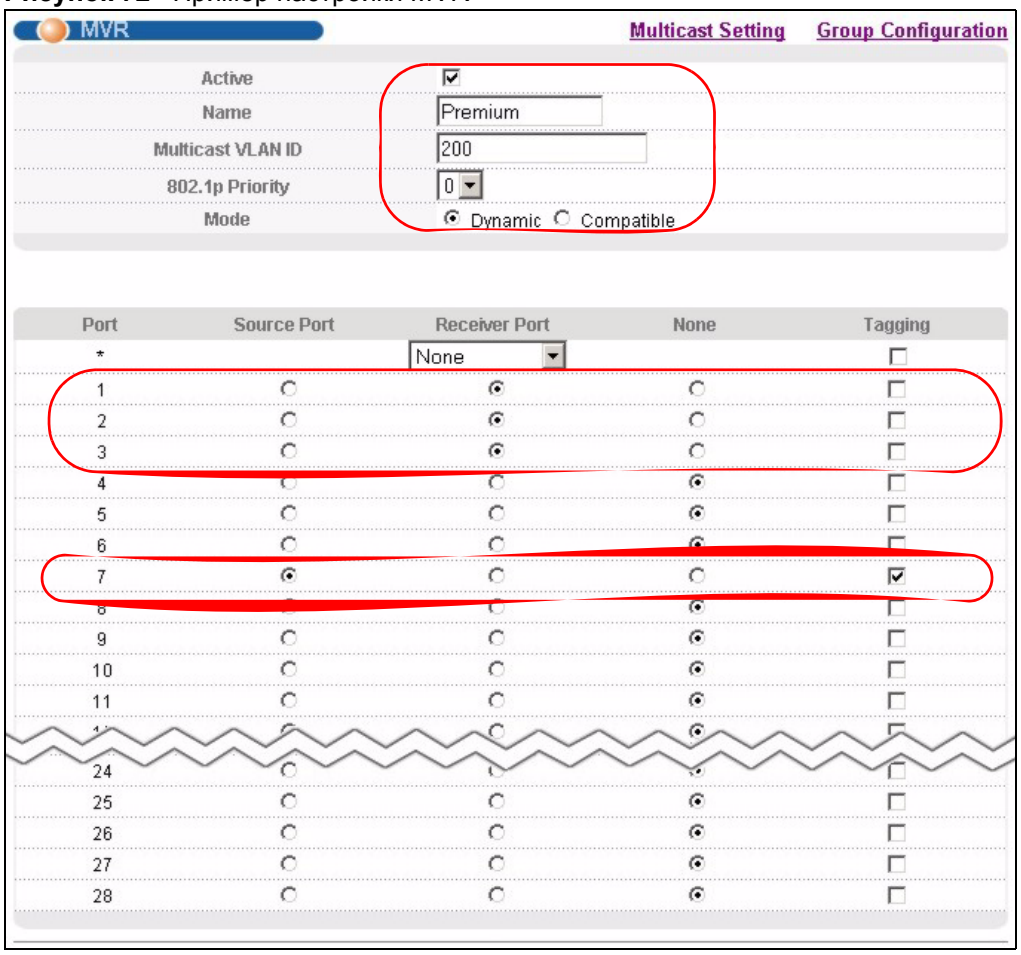
На приведенном ниже рисунке показан пример сети, в которой порты 1, 2 и 3 коммутатора принадлежат VLAN 1. Кроме того, порт 7 принадлежит к группе мультивещания с идентификатором VID 200 для получения трафика мультивещания (каналы **News** и **Movie**) от удаленного сервера потокового мультимедиа, **S**. Компьютеры A, B и C в сети VLAN 1 могут принимать трафик.

Рисунок 71 Пример настройки MVR



Для определения настроек MVR на коммутаторе необходимо создать группу мультивещания на экране **MVR** и назначить порты приемников и источников.

Рисунок 72 Пример настройки MVR



Чтобы коммутатор пересылал трафик группы мультивещания абонентам, необходимо определить настройки группы мультивещания на экране **Group Configuration**. На следующем рисунке показан пример настройки двух групп мультивещания (**News** и **Movie**) для VLAN-сети мультивещания 200.

Рисунок 73 Пример настройки групп MVR

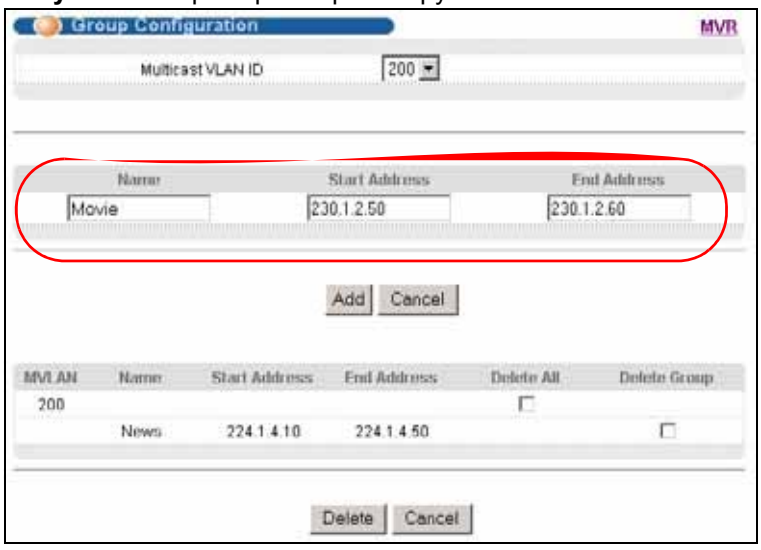
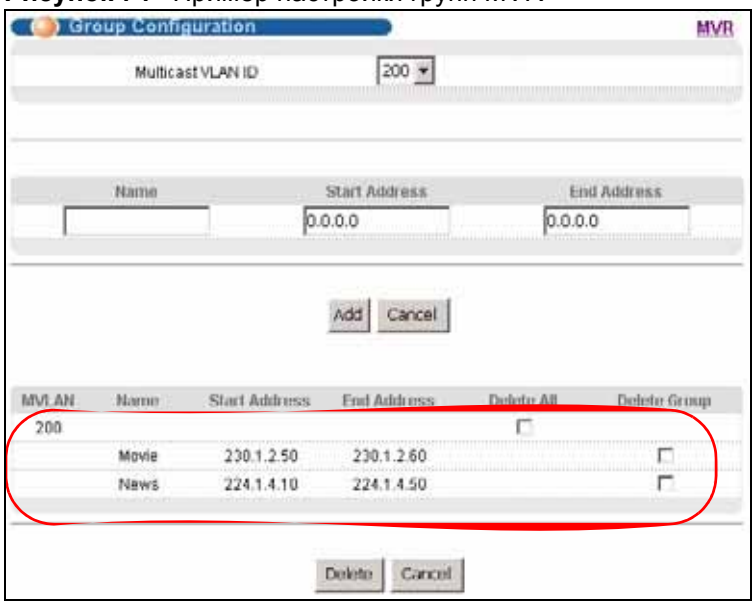


Рисунок 74 Пример настройки групп MVR



20

Аутентификация и учет

В данной главе описана настройка функций аутентификации и учета на коммутаторе.

20.1 Аутентификация, авторизация и учет

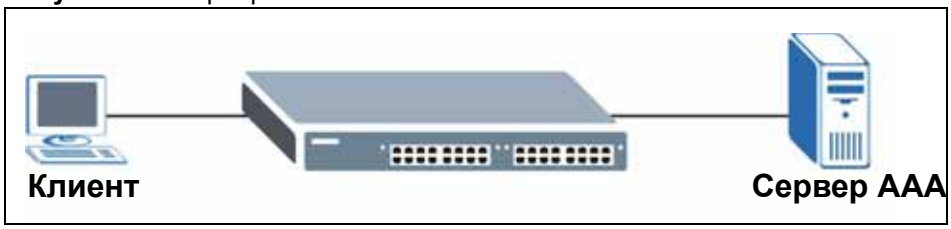
Аутентификацией называется процесс идентификации пользователя и проверки его прав доступа к коммутатору. Данный коммутатор позволяет проводить аутентификацию пользователей с использованием учетных записей, настроенных в самом коммутаторе. Кроме того, коммутатор позволяет использовать внешний сервер аутентификации в целях аутентификации большого количества пользователей.

Авторизацией называется процесс определения действий, которые допустимо выполнять пользователю. Различным пользовательским учетным записям могут быть назначены более высокие или более низкие уровни привилегий. Например, у пользователя A может быть право на создание новых учетных записей на коммутаторе, тогда как у пользователя B такого права не будет. Авторизация пользователей может осуществляться коммутатором с использованием учетных записей, настроенных на самом коммутаторе, или с использованием внешнего сервера в целях авторизации большого количества пользователей.

Учетом называется процесс регистрации действий пользователей. Данный коммутатор позволяет отслеживать вход пользователей, выход пользователей, выполняемые ими команды и другие действия с использованием внешнего сервера. В рамках учета могут также регистрироваться системные действия, такие как время загрузки и выключения коммутатора.

Внешние серверы, выполняющие функции аутентификации, авторизации и учета, сокращенно называются серверами AAA. В качестве внешних серверов аутентификации, авторизации и учета данный коммутатор поддерживает серверы RADIUS (Remote Authentication Dial-In User Service, см. разд. 20.1.2 на стр. 164) и TACACS+ (Terminal Access Controller Access-Control System Plus, см. разд. 20.1.2 на стр. 164).

Рисунок 75 Сервер AAA



20.1.1 Локальные учетные записи пользователей

Локальное хранение профилей пользователей на коммутаторе дает коммутатору возможность обходиться при аутентификации и авторизации пользователей без внешнего сервера AAA в сети. Однако, возможное количество пользователей при таком способе аутентификации ограничено (см. гл. 27 на стр. 221).

20.1.2 RADIUS и TACACS+

RADIUS и TACACS+ представляют собой протоколы безопасности, которые используются для аутентификации пользователей путем обращения к внешнему серверу вместо внутренней базы данных пользователей устройства, которая ограничена емкостью памяти этого устройства (внешний сервер может также использоваться в дополнение к внутренней базе данных). В целом аутентификация с использованием RADIUS и and TACACS+ позволяет идентифицировать неограниченное количество пользователей с помощью единой централизованной службы.

Некоторые основные различия между протоколами RADIUS и TACACS+ приводятся в следующей таблице.

Таблица 46 RADIUS и TACACS+

	RADIUS	TACACS+
Транспортный протокол	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Шифрование	Шифрование пароля, отправляемого для аутентификации.	Шифрование всей коммуникации между клиентом (коммутатором) и сервером TACACS.

20.2 Экраны настройки функций аутентификации и учета

Чтобы включить функции аутентификации и/или учета на коммутаторе, необходимо прежде всего указать настройки сервера аутентификации (RADIUS и/или TACACS+), а затем настроить приоритеты аутентификации и учета.

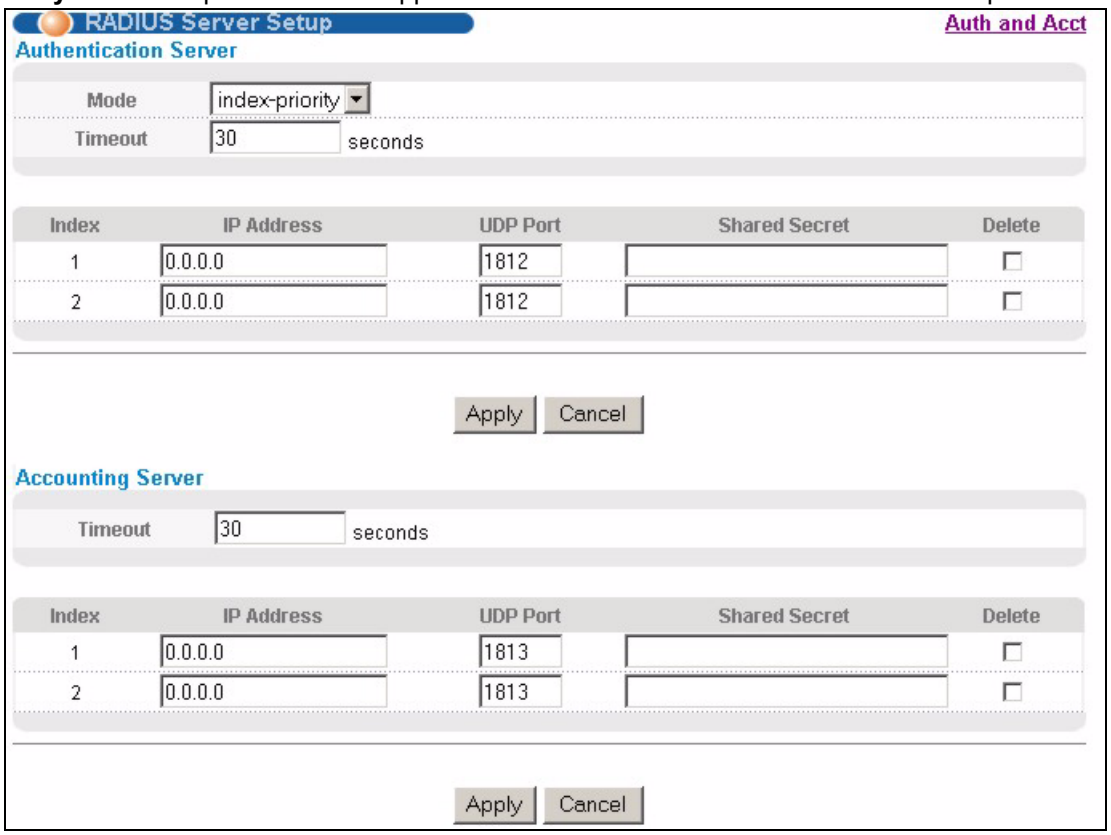
Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Auth and Acct**.

Рисунок 76 Экран Advanced Application > Auth and Acct

20.2.1 Настройка сервера RADIUS

Настройки сервера RADIUS вводятся на показанном ниже экране. Более подробную информацию о серверах RADIUS можно найти в разд. 20.1.2 на стр. 164. Чтобы отобразить показанный ниже экран, нажмите на ссылке **RADIUS Server Setup** на экране **Authentication and Accounting**.

Рисунок 77 Экран Advanced Application > Auth and Acct > RADIUS Server Setup



Поля экрана описаны в следующей таблице.

Таблица 47 Экран Advanced Application > Auth and Acct > RADIUS Server Setup

ПОЛЕ	ОПИСАНИЕ
Authentication Server	В данном разделе вводятся настройки аутентификации с использованием RADIUS.
Mode	Данное поле используется лишь при настройке нескольких серверов RADIUS. В случае выбора **index-priority** коммутатор будет пытаться осуществить аутентификацию с использованием первого настроенного сервера RADIUS; при отсутствии ответа коммутатор обратится ко второму серверу RADIUS. В случае выбора **round-robin** запросы на аутентификацию будут направляться серверам RADIUS поочередно.
Timeout	Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера RADIUS. В случае выбора режима **index-priority** и использования двух серверов RADIUS значение тайм-аута делится между двумя серверами RADIUS. Например, если установить период тайм-аута равным 30 секундам, коммутатор будет ожидать ответа от первого сервера RADIUS в течение 15 секунд, после чего направит запрос на второй сервер RADIUS.
Index	Порядковый номер записи о сервере RADIUS (только для чтения).

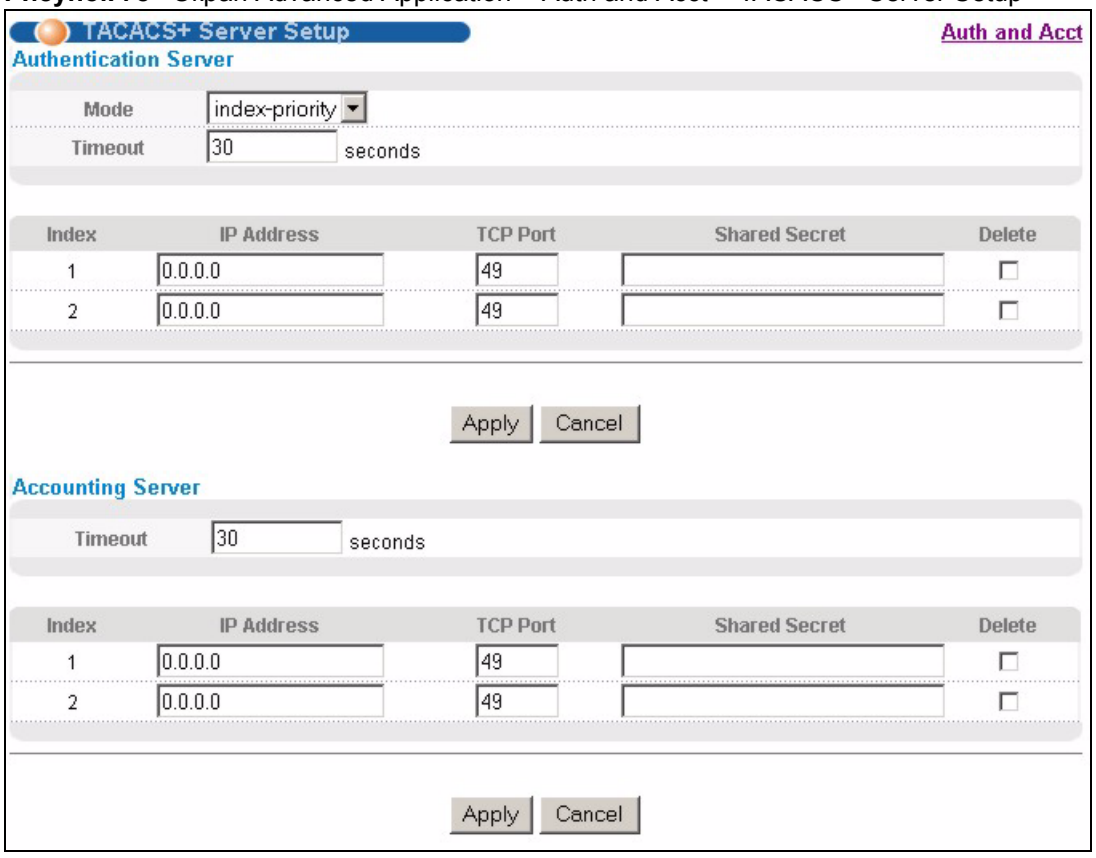
Таблица 47 Экран Advanced Application > Auth and Acct > RADIUS Server Setup

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес внешнего сервера RADIUS в виде десятичных чисел, разделенных точками.
UDP Port	По умолчанию аутентификация на сервере RADIUS производится через порт **1812**. Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера RADIUS и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере RADIUS и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере RADIUS установите данный переключатель. Удаление записи произойдет после нажатия на кнопку **Apply**.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Accounting Server	В данном разделе вводятся настройки учета с использованием RADIUS.
Timeout	Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера учета RADIUS.
Index	Порядковый номер записи о сервере учета RADIUS (только для чтения).
IP Address	Введите IP-адрес внешнего сервера учета RADIUS в виде десятичных чисел, разделенных точками.
UDP Port	По умолчанию учетная информация передается на сервер учета RADIUS через порт **1813**. Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера учета RADIUS и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере учета RADIUS и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере учета RADIUS установите данный переключатель. Удаление записи произойдет после нажатия на кнопку **Apply**.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

20.2.2 Настройка сервера TACACS+

Настройки сервера TACACS+ вводятся на показанном ниже экране. Более подробную информацию о серверах TACACS+ можно найти в разд. 20.1.2 на стр. 164. Чтобы отобразить показанный ниже экран, нажмите на ссылке **TACACS+ Server Setup** на экране **Authentication and Accounting**.

Рисунок 78 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup



Поля экрана описаны в следующей таблице.

Таблица 48 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup

ПОЛЕ	ОПИСАНИЕ
Authentication Server	В данном разделе вводятся настройки аутентификации с использованием TACACS+.
Mode	Данное поле используется лишь при настройке нескольких серверов TACACS+. В случае выбора **index-priority** коммутатор будет пытаться осуществить аутентификацию с использованием первого настроенного сервера TACACS+; при отсутствии ответа коммутатор обратится ко второму серверу TACACS+. В случае выбора **round-robin** запросы на аутентификацию будут направляться серверам TACACS+ поочередно.
Timeout	Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера TACACS+. В случае выбора режима **index-priority** и использования двух серверов TACACS+ значение тайм-аута делится между двумя серверами TACACS+. Например, если установить период тайм-аута равным 30 секундам, коммутатор будет ожидать ответа от первого сервера TACACS+ в течение 15 секунд, после чего направит запрос на второй сервер TACACS+.
Index	Порядковый номер записи о сервере TACACS+ (только для чтения).
IP Address	Введите IP-адрес внешнего сервера TACACS+ в виде десятичных чисел, разделенных точками.
TCP Port	По умолчанию аутентификация на сервере TACACS+ производится через порт **49**. Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.

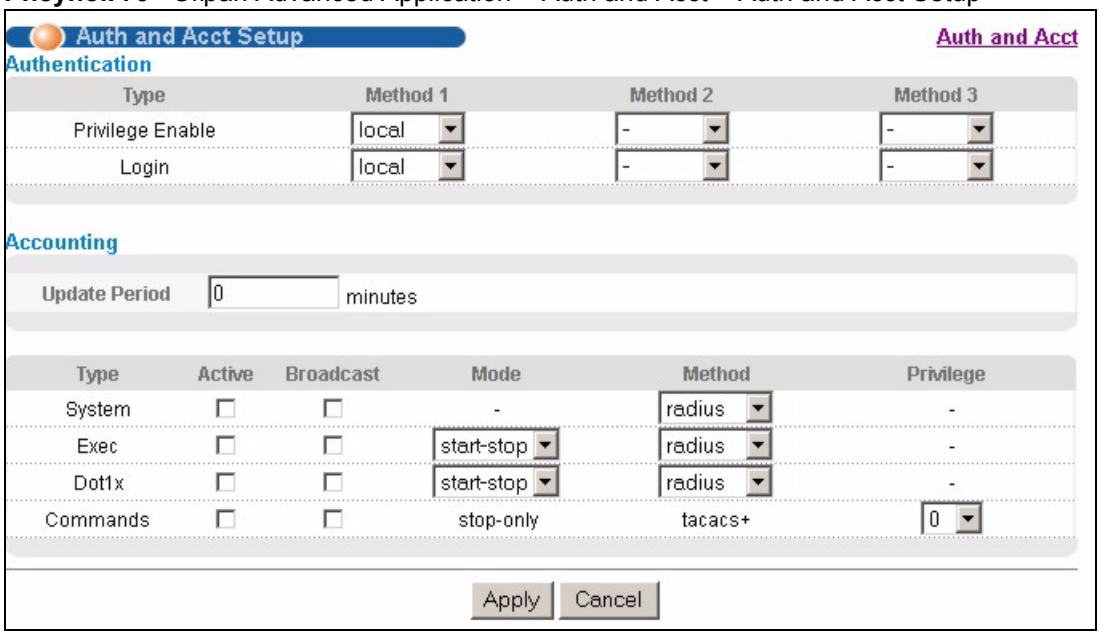
Таблица 48 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup

ПОЛЕ	ОПИСАНИЕ
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера TACACS+ и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере TACACS+ и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере TACACS+ установите данный переключатель. Удаление записи произойдет после нажатия на кнопку **Apply**.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Accounting Server	В данном разделе вводятся настройки учета с использованием TACACS+.
Timeout	Укажите период в секундах, в течение которого коммутатор будет ожидать ответа на запрос от сервера учета TACACS+.
Index	Порядковый номер записи о сервере учета TACACS+ (только для чтения).
IP Address	Введите IP-адрес внешнего сервера учета TACACS+ в виде десятичных чисел, разделенных точками.
TCP Port	По умолчанию информация передается на сервер учета TACACS+ через порт **49**. Изменять это значение не следует, за исключением тех случаев, когда об этом попросит администратор сети.
Shared Secret	Укажите пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера учета TACACS+ и коммутатора. Этот ключ не пересылается по сети. Ключ должен быть одинаковым на внешнем сервере учета TACACS+ и коммутаторе.
Delete	При необходимости удалить из коммутатора существующую запись о сервере учета TACACS+ установите данный переключатель. Удаление записи произойдет после нажатия на кнопку **Apply**.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

20.2.3 Настройка аутентификации и учета

Настройка функций аутентификации и учета коммутатора осуществляется на следующем экране. Чтобы отобразить показанный ниже экран, нажмите на ссылке **Auth and Acct Setup** на экране **Authentication and Accounting**.

Рисунок 79 Экран Advanced Application > Auth and Acct > Auth and Acct Setup



Поля экрана описаны в следующей таблице.

Таблица 49 Экран Advanced Application > Auth and Acct > Auth and Acct Setup

ПОЛЕ	ОПИСАНИЕ
Authentication	В данном разделе определяются способы аутентификации пользователей, пытающихся получить доступ к коммутатору.
Privilege Enable	В данных полях можно определить, к какой базе данных должен обращаться коммутатор (в первую, вторую и третью очередь) для аутентификации уровня привилегий учетных записей администраторов (пользователей, управляющих коммутатором). Привилегии доступа для учетных записей в случае использования локальной аутентификации (**local**) определяются при помощи команд (см. Справочное руководство по интерфейсу командной строки). **TACACS+** и **RADIUS** представляют собой внешние серверы. Прежде чем установить приоритет, убедитесь, что соответствующая база данных правильно настроена. Для аутентификации привилегий доступа администраторов на коммутаторе можно указать до трех методов. Данный коммутатор пытается использовать каждый из методов в том порядке, в котором они указаны (сначала **Method 1**, затем **Method 2** и наконец **Method 3**). В поле **Method 1** обязательно должен быть выбран один из методов. Если коммутатор должен обращаться и к другим источникам для проверки привилегий доступа, их необходимо указать в полях **Method 2** и **Method 3**. В случае выбора **local** для проверки уровня привилегий коммутатор будет обращаться к настроенным на нем записям. В случае выбора **radius** или **tacacs+** проверка уровня привилегий будет осуществляться коммутатором с помощью внешних серверов.

Таблица 49 Экран Advanced Application > Auth and Acct > Auth and Acct Setup

ПОЛЕ	ОПИСАНИЕ
Login	В данных полях можно определить, к какой базе данных должен обращаться коммутатор (в первую, вторую и третью очередь) для аутентификации учетных записей администраторов (пользователей, управляющих коммутатором). Локальные учетные записи пользователей настраиваются на экране **Access Control > Logins**. TACACS+ и RADIUS представляют собой внешние серверы. Прежде чем установить приоритет, убедитесь, что соответствующая база данных правильно настроена. Для аутентификации учетных записей администраторов на коммутаторе можно указать до трех методов. Данный коммутатор пытается использовать каждый из методов в том порядке, в котором они указаны (сначала **Method 1**, затем **Method 2** и наконец **Method 3**). В поле **Method 1** обязательно должен быть выбран один из методов. Если коммутатор должен обращаться и к другим источникам для проверки учетных записей администраторов, их необходимо указать в полях **Method 2** и **Method 3**. В случае выбора **local** для проверки учетных записей администраторов коммутатор будет обращаться к записям, настроенным на экране **Access Control > Logins**. В случае выбора **radius** для проверки учетных записей администраторов коммутатор будет обращаться к серверам RADIUS, настроенным на экране **RADIUS Server Setup**. В случае выбора **tacacs+** для проверки учетных записей администраторов коммутатор будет обращаться к серверам TACACS+, настроенным на экране **TACACS+ Server Setup**.
Accounting	В данном разделе вводятся настройки функции учета для коммутатора.
Update Period	Периодичность в минутах, с которой коммутатор отправляет на сервер учета обновленную информацию. Данное значение используется лишь в том случае, если для параметров **Exec** или **Dot1x** выбран вариант **start-stop**.
Type	Данный коммутатор поддерживает передачу на сервер(ы) учета следующих типов событий: • **System** – в случае выбора данного варианта коммутатор будет передавать информацию о следующих системных событиях: загрузка системы, отключение системы, включение учета на системе, отключение учета на системе. • **Exec** – в случае выбора данного варианта коммутатор будет передавать информацию о входе и выходе администратора и системы через консольный порт, Telnet или SSH. • **Dot1x** – в случае выбора данного варианта коммутатор будет передавать информацию о начале клиентами сеансов IEEE 802.1x (аутентификация на коммутаторе), завершении сеансов, а также промежуточных обновлениях о состоянии сеансов. • **Commands** – в случае выбора данного варианта коммутатор будет передавать информацию о выполнении на коммутаторе команд с уровнем привилегий, равным или выше указанного.
Active	Установите этот переключатель, чтобы активировать функцию учета для указанных типов событий.
Broadcast	Установите данный переключатель, чтобы учетная информация передавалась коммутатором сразу на все настроенные серверы учета. Если данный переключатель не установлен, но было настроено два сервера учета, коммутатор отправляет информацию на первый сервер учета; при отсутствии ответа информация отправляется на второй сервер учета.

Таблица 49 Экран Advanced Application > Auth and Acct > Auth and Acct Setup

ПОЛЕ	ОПИСАНИЕ
Mode	Данный коммутатор поддерживает два режима регистрации событий входа в систему. Выберите: • **start-stop** – чтобы коммутатор отправлял информацию на сервер учета при начале сеанса, в течение пользовательского сеанса (если он превышает период **Update Period**) и при завершении сеанса пользователем. • **stop-only** – чтобы коммутатор отправлял информацию на сервер учета только после завершения сеанса пользователем.
Method	Выберите метод (RADIUS или TACACS+) для учета событий определенного типа. Для регистрации событий типа **Commands** поддерживается только метод TACACS+.
Privilege	Данное поле настраивается только для событий типа **Commands**. Выберите пороговый уровень привилегий для команд, информация о которых будет направляться коммутатором на сервер учета. В этом случае коммутатор будет передавать учетную информацию в случае выполнения на коммутаторе команд, уровень привилегий которых равен или превышает указанный.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

20.2.4 Специальный атрибут производителя

Стандартом RFC 2865 определен метод обмена специфичной для производителя информацией между сервером RADIUS и сетевым устройством доступа (например, коммутатором). Для расширения функциональных возможностей сервера RADIUS компания может использовать специальные атрибуты производителя (VSA).

Данный коммутатор поддерживает атрибуты VSA, которые, в зависимости от результатов аутентификации пользователя, позволяют выполнять следующие действия:

- Ограничивать пропускную способность для входящего или исходящего трафика через порт, к которому подключен пользователь.
- Назначать уровни привилегий учетным записям (более подробную информацию об уровнях привилегий учетных записей можно найти в Справочном руководстве по интерфейсу командной строки) для пользователей, прошедших аутентификацию.

Атрибут VSA включает в себя следующие поля:

- **Vendor-ID**: Идентификационный номер, назначенный компании уполномоченной организацией по распределению нумерации в сети Интернет (IANA) . ZyXEL присвоен идентификатор 890.
- **Vendor-Type**: Определяемый производителем атрибут, идентифицирующий изменяемый параметр.
- **Vendor-data**: Значение, которое необходимо присвоить параметру.

Порядок настройки атрибутов VSA для пользователей, проходящий аутентификацию на сервере RADIUS, можно найти в документации к соответствующему серверу RADIUS.

Атрибуты VSA, поддерживаемые коммутатором, описаны в следующей таблице.

Таблица 50 Поддерживаемые атрибуты VSA

ФУНКЦИЯ	АТРИБУТ
Назначение пропускной способности для входящего трафика	Vendor-Id = **890** Vendor-Type = **1** Vendor-data = скорость входящего трафика (кбит/с в десятичном формате)
Назначение пропускной способности для исходящего трафика	Vendor-Id = **890** Vendor-Type = **2** Vendor-data = скорость исходящего трафика (кбит/с в десятичном формате)
Назначение привилегий	Vendor-ID = **890** Vendor-Type = **3** Vendor-Data = **"shell:priv-lvl=**N" или Vendor-ID = **9** (CISCO) Vendor-Type = **1** (CISCO-AVPAIR) Vendor-Data = **"shell:priv-lvl=**N" где N – уровень привилегий (от 0 до 14). Примечание: Если для учетной записи на сервере или серверах RADIUS и на коммутаторе установлены различные уровни привилегий, пользователю назначается уровень привилегий из той базы данных (RADIUS или локальной), которая первой была использована коммутатором для аутентификации пользователя.

20.2.4.1 Атрибут протокола туннелирования

С помощью атрибутов протокола туннелирования на сервере RADIUS (см. документацию к серверу RADIUS) можно назначить порт коммутатора виртуальной локальной сети VLAN с использованием аутентификации на основе IEEE 802.1x. Настройки VLAN порта – фиксированные, без тегов. При этом также назначается идентификатор VID порта. Значения, которые необходимо настроить, описаны в следующей таблице. Значения, выделенные в таблице полужирным шрифтом, являются фиксированными в соответствии с RFC 3580.

Таблица 51 Поддерживаемые атрибуты протокола туннелирования

ФУНКЦИЯ	АТРИБУТ

Назначение сети VLAN	`Tunnel-Type = **VLAN(13)**`
	`Tunnel-Medium-Type = **802(6)**`
	`Tunnel-Private-Group-ID =` VLAN ID
	
	Примечание: На коммутаторе необходимо создать сеть VLAN с указанным идентификатором VID.

20.3 Поддерживаемые атрибуты RADIUS

Атрибуты RADIUS представляют собой данные, используемые для определения специального порядка аутентификации, а также учетные элементы пользовательского профиля, сохраняемые на сервере RADIUS. В данном приложении перечислены атрибуты RADIUS, поддерживаемые коммутатором.

Более подробную информацию об атрибутах RADIUS, используемых для аутентификации, можно найти в RFC 2865. Описание атрибутов RADIUS, используемых для учета, можно найти в RFC 2866 и RFC 2869.

В данном приложении перечислены атрибуты, используемые коммутатором для функций аутентификации и учета. В тех случаях, когда с атрибутом связан особый формат, приводится описание формата.

20.3.1 Атрибуты, используемые для аутентификации

В приведенных ниже разделах перечислены атрибуты, передаваемые коммутатором на сервер RADIUS при осуществлении аутентификации.

20.3.1.1 Атрибуты, используемые при аутентификации привилегированного доступа

User-Name

– формат атрибута User-Name: **$enab#$**, где # представляет собой уровень привилегий (1-14)

User-Password

NAS-Identifier

NAS-IP-Address

20.3.1.2 Атрибуты, используемые для входа пользователей

User-Name

User-Password

NAS-Identifier
NAS-IP-Address

20.3.1.3 Атрибуты, используемые для аутентификации на основе IEEE 802.1x

User-Name
NAS-Identifier
NAS-IP-Address
NAS-Port
NAS-Port-Type
– Данное значение на коммутаторе устанавливается равным **Ethernet(15)**.
Calling-Station-Id
Frame-MTU
EAP-Message
State
Message-Authenticator

20.3.2 Атрибуты, используемые для учета

В приведенных ниже разделах перечислены атрибуты, передаваемые коммутатором на сервер RADIUS при использовании функций учета.

20.3.2.1 Атрибуты, используемые для учета системных событий

NAS-IP-Address
NAS-Identifier
Acct-Status-Type
Acct-Session-ID
– Формат идентификатора Acct-Session-Id: **дата+время+8-значный порядковый номер**, например, 200704191721030000000 1. (дата: 2007/04/19, время: 17:21:03, порядковый номер: 00000001)
Acct-Delay-Time

20.3.2.2 Атрибуты, используемые для учета событий выполнения команд (Exec)

Передаваемые атрибуты и момент времени, когда они передаются, перечислены в следующей таблице (различия между событиями Exec, связанными с выполнением команд с консоли или через Telnet/SSH заключается в том, для событий через Telnet/SSH используется атрибут Calling-Station-Id):

Таблица 52 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
User-Name	Д	Д	Д
NAS-Identifier	Д	Д	Д
NAS-IP-Address	Д	Д	Д
Service-Type	Д	Д	Д
Acct-Status-Type	Д	Д	Д
Acct-Delay-Time	Д	Д	Д

Таблица 52 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
Acct-Session-Id	Д	Д	Д
Acct-Authentic	Д	Д	Д
Acct-Session-Time		Д	Д
Acct-Terminate-Cause			Д

Таблица 53 Атрибуты RADIUS – события Exec при выполнении команд через Telnet/ SSH

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
User-Name	Д	Д	Д
NAS-Identifier	Д	Д	Д
NAS-IP-Address	Д	Д	Д
Service-Type	Д	Д	Д
Calling-Station-Id	Д	Д	Д
Acct-Status-Type	Д	Д	Д
Acct-Delay-Time	Д	Д	Д
Acct-Session-Id	Д	Д	Д
Acct-Authentic	Д	Д	Д
Acct-Session-Time		Д	Д
Acct-Terminate-Cause			Д

20.3.2.3 Атрибуты, используемые для учета событий IEEE 802.1x

Используемые атрибуты перечислены в следующей таблице с указанием момента времени, когда они передаются:

Таблица 54 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
User-Name	Д	Д	Д
NAS-IP-Address	Д	Д	Д
NAS-Port	Д	Д	Д
Class	Д	Д	Д
Called-Station-Id	Д	Д	Д
Calling-Station-Id	Д	Д	Д
NAS-Identifier	Д	Д	Д
NAS-Port-Type	Д	Д	Д
Acct-Status-Type	Д	Д	Д
Acct-Delay-Time	Д	Д	Д
Acct-Session-Id	Д	Д	Д
Acct-Authentic	Д	Д	Д
Acct-Input-Octets		Д	Д

Таблица 54 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
Acct-Output-Octets		Д	Д
Acct-Session-Time		Д	Д
Acct-Input-Packets		Д	Д
Acct-Output-Packets		Д	Д
Acct-Terminate-Cause			Д
Acct-Input-Gigawords		Д	Д
Acct-Output-Gigawords		Д	Д

21

Защита от подмены IP-адресов

Функция защиты от подмены IP-адресов позволяет отфильтровывать несанкционированные пакеты ARP в сети.

21.1 Обзор функции защиты от подмены IP-адресов

Для защиты от подмены IP-адресов применяется таблица привязок, позволяющая различать санкционированные и несанкционированные ARP-пакеты. При привязке используются следующие атрибуты:

- MAC-адрес
- VLAN ID
- IP-адрес
- Номер порта

При получении коммутатором пакета ARP производится поиск соответствующих MAC-адреса, идентификатора VLAN ID, IP-адреса и номера порта в таблице привязок. При наличии привязки коммутатор пересылает пакет. Если привязки не найдено, пакет коммутатором отбрасывается.

Таблица строится коммутатором на основе информации, вводимой администраторами вручную (статическая привязка).

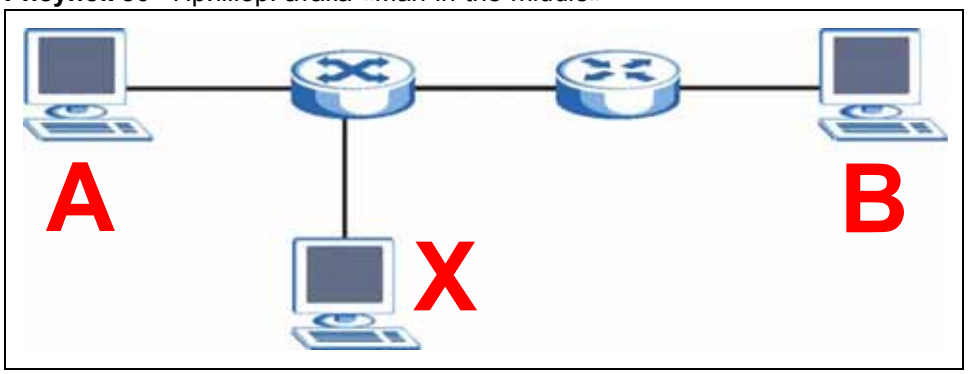
Функция защиты от подмены IP-адресов включает в себя следующие функции:

- Статическая привязка. Используется для создания статических связей в таблице привязок.
- Инспекция ARP-пакетов. Используется для отфильтровывания несанкционированных пакетов ARP.

21.1.1 Обзор функции инспекции ARP-пакетов

Инспекция ARP-пакетов используется для отфильтровывания несанкционированных пакетов ARP. Это позволяет предотвратить многие виды атак класса «man-in-the-middle», таких как описанная в следующем примере.

Рисунок 80 Пример: атака «Man-in-the-middle»



В данном примере компьютер **B** пытается установить соединение с компьютером **A**. Компьютер **X** находится в том же широковещательном домене, что и компьютер **A**, и перехватывает ARP-запрос для разрешения адреса компьютера **A**. После этого компьютер **X**:

- Выдает себя компьютером **A** и отвечает компьютеру **B**.
- Выдает себя компьютером **B** и отправляет сообщение компьютеру **A**.

В результате весь обмен данными между компьютером **A** и компьютером **B** происходит через компьютер **X**. Компьютер **X** получает возможность читать и изменять информацию, передаваемую между этими двумя компьютерами.

21.1.1.1 Инспекция ARP-пакетов и фильтры MAC-адресов

При обнаружении коммутатором несанкционированного ARP-пакета им автоматически создается фильтр MAC-адресов, блокирующий трафик от MAC-адреса и сети VLAN, от которых поступил несанкционированный ARP-пакет. Период активности фильтра MAC-адресов на коммутаторе можно настраивать.

Такие фильтры MAC-адресов отличаются от обычных фильтров MAC-адресов (см. гл. 10 на стр. 99).

- Они сохранятся только в энергозависимой памяти.
- В памяти они находятся в другой области, не вместе с обычными фильтрами MAC-адресов.
- Эти фильтры видны только на экранах и в командах функции инспекции ARP-пакетов **ARP Inspection**, и не видны на экранах и в командах фильтров MAC-адресов **MAC Address Filter**.

21.1.1.2 Доверенные и не заслуживающие доверия порты

Функция инспекции ARP-пакетов делит все порты на доверенные и не заслуживающие доверия. Пакеты ARP, приходящие через доверенные порты, коммутатором не отбрасываются ни по какой причине. Данный коммутатор отбрасывает ARP-пакеты, поступающие через не заслуживающие доверия порты, если информация об отправителе в ARP-пакете не совпадает с одной из существующих привязок.

21.1.1.3 Системный журнал Syslog

При пересылке или отбрасывании пакетов ARP коммутатор может отправлять сообщения системного журнала syslog на указанный сервер syslog (гл. 29 на стр. 243). В целях большей эффективности коммутатор может консолидировать сообщения контрольного журнала и отправлять их партиями.

21.1.1.4 Настройка инспекции ARP-пакетов

Чтобы настроить на коммутаторе функцию инспекции ARP-пакетов, выполните следующие действия.

1. Определите статические привязки, чтобы коммутатор мог различать санкционированные и несанкционированные ARP-пакеты.
2. Включите функцию инспекции ARP-пакетов на коммутаторе.
3. Включите функцию инспекции ARP-пакетов в каждой сети VLAN.
4. Настройте доверенные и не заслуживающие доверия порты, а также укажите максимальное количество пакетов ARP в секунду, принимаемое через каждый из портов.

21.2 Защита от подмены IP-адресов

На данном экране можно просмотреть существующие привязки для функции инспекции ARP-пакетов. На основе привязок функция инспекции ARP-пакетов различает санкционированные и несанкционированные ARP-пакеты. Данный коммутатор строит таблицу привязок с использованием информации, вводимой администраторами вручную (статическая привязка). Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard**.

Рисунок 81 Экран IP Source Guard

Поля экрана описаны в следующей таблице.

Таблица 55 Экран IP Source Guard

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер каждой привязки.
MAC Address	В этом поле отображается MAC-адрес источника для привязки.
IP Address	В этом поле отображается IP-адрес, назначенный для MAC-адреса в привязке.
Lease	В этом поле отображается количество дней, часов, минут и секунд, в течение которого действует привязка; например, **2d3h4m5s** означает, что привязка действует в течение 2 дней, 3 часов, 4 минут и 5 секунд. Для привязки, действительной в течение неограниченного времени (например, статической привязки), в этом поле отображается **infinity**.
Type	В этом поле отображается способ получения коммутатором информации о привязке. **static**: привязка создана с использованием информации, предоставленной администратором вручную.

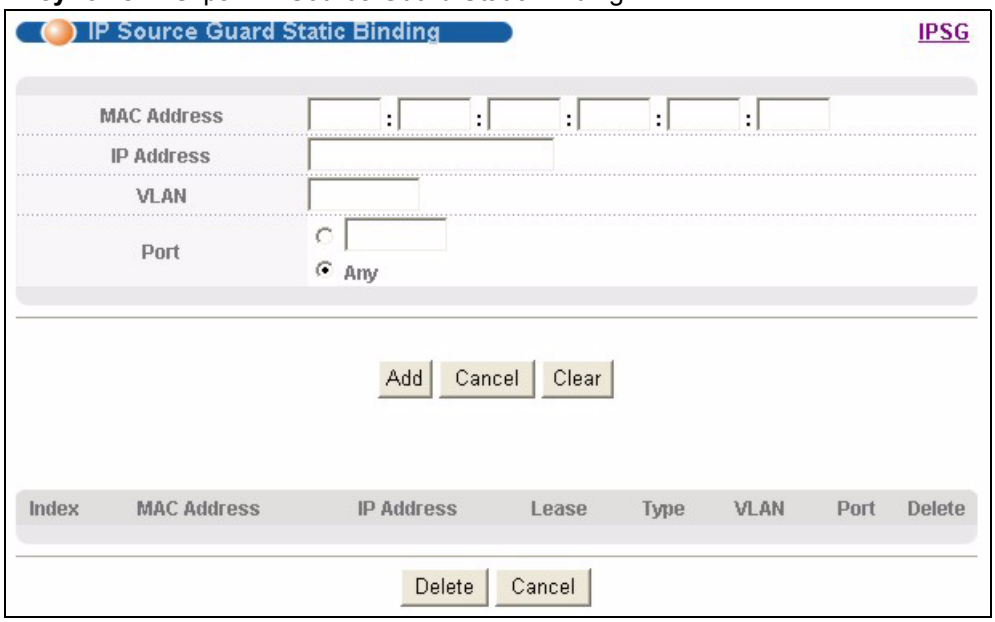
Таблица 55 Экран IP Source Guard (продолжение)

ПОЛЕ	ОПИСАНИЕ
VID	В этом поле отображается идентификатор VLAN для привязки.
Port	В этом поле отображается номер порта для привязки. Если данное поле пустое, привязка действует для всех портов.

21.3 Статическая привязка для защиты от подмены IP-адресов

На данном экране можно управлять статическими привязками для функции инспекции ARP-пакетов. Статические привязки идентифицируются по MAC-адресу и идентификатору VLAN ID. Для каждой комбинации MAC-адреса и идентификатора VLAN ID можно создать только одну статическую привязку. При попытке создать статическую привязку с теми же MAC-адресом и идентификатором VLAN ID, что и у существующей статической привязки, новая информация заменяет предыдущую. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > Static Binding**.

Рисунок 82 Экран IP Source Guard Static Binding



Поля экрана описаны в следующей таблице.

Таблица 56 Экран IP Source Guard Static Binding

ПОЛЕ	ОПИСАНИЕ
MAC Address	Введите MAC-адрес источника для привязки.
IP Address	Введите IP-адрес, назначенный для MAC-адреса в привязке.
VLAN	Введите идентификатор VLAN ID для привязки.
Port	Укажите порты для привязки. Если привязка относится к одному порту, выберите первый переключатель и введите номер порта в соответствующее поле справа. Если данная привязка относится ко всем портам, выберите переключатель **Any**.

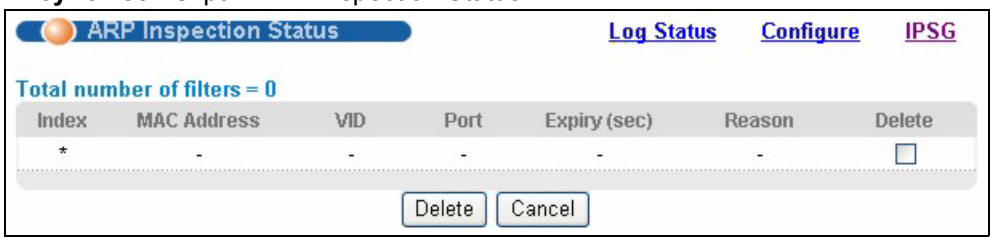
Таблица 56 Экран IP Source Guard Static Binding (продолжение)

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите на данную кнопку, чтобы добавить указанную статическую привязку или обновить существующую.
Cancel	Нажмите на данную кнопку, чтобы сбросить значения из последней выбранной статической привязке или, если ничего не было выбрано, очистить перечисленные выше поля.
Clear	Нажмите на данную кнопку, чтобы очистить перечисленные выше поля.
Index	В этом поле отображается порядковый номер каждой привязки.
MAC Address	В этом поле отображается MAC-адрес источника для привязки.
IP Address	В этом поле отображается IP-адрес, назначенный для MAC-адреса в привязке.
Lease	В этом поле отображается период действия привязки.
Type	В этом поле отображается способ получения коммутатором информации о привязке. **static**: привязка создана с использованием информации, предоставленной администратором вручную.
VLAN	В этом поле отображается идентификатор VLAN для привязки.
Port	В этом поле отображается номер порта для привязки. Если данное поле пустое, привязка действует для всех портов.
Delete	Установите переключатель и нажмите на **Delete**, чтобы удалить выбранную запись.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей **Delete**.

21.4 Состояние инспекции ARP-пакетов

На данном экране можно посмотреть текущий список фильтров MAC-адресов, созданных коммутатор в связи с обнаружением несанкционированных пакетов ARP. При обнаружении коммутатором несанкционированного ARP-пакета им автоматически создается фильтр MAC-адресов, блокирующий трафик от MAC-адреса и сети VLAN, от которых поступил несанкционированный ARP-пакет. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection**.

Рисунок 83 Экран ARP Inspection Status



Поля экрана описаны в следующей таблице.

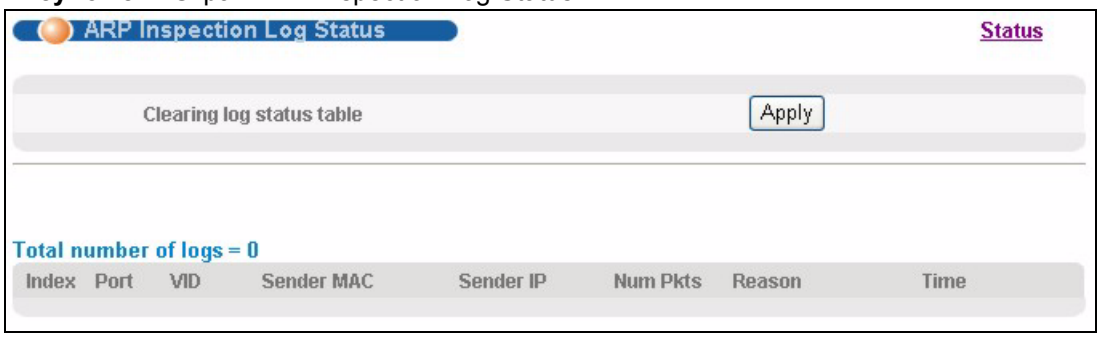
Таблица 57 Экран ARP Inspection Status

ПОЛЕ	ОПИСАНИЕ
Total number of filters	В данном поле отображается общее количество фильтров MAC-адресов, созданных коммутатором в связи с обнаружением несанкционированных пакетов ARP.
Index	В этом поле отображается порядковый номер фильтра MAC-адресов.
MAC Address	В этом поле отображается MAC-адрес источника для фильтра MAC-адресов.
VID	В этом поле отображается идентификатор VLAN для фильтра MAC-адресов.
Port	В этом поле отображается порт источника для отброшенного пакета ARP.
Expiry (sec)	В этом поле отображается период времени (в секундах), в течение которого фильтр MAC-адресов будет действовать на коммутаторе. Запись можно удалить вручную (**Delete**).
Reason	В этом поле отображается причина, по которой был отброшен пакет ARP. **MAC+VLAN**: MAC-адрес и идентификатор VLAN ID не найдены в таблице привязок. **IP**: MAC-адрес и идентификатор VLAN ID найдены в таблице привязок, но IP-адрес недействителен. **Port**: MAC-адрес, идентификатор VLAN ID и IP-адрес найдены в таблице привязок, но номер порта недействителен.
Delete	Установите переключатель и нажмите на **Delete**, чтобы удалить выбранную запись.
Delete	Нажмите на данную кнопку, чтобы удалить выбранные записи.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей **Delete**.

21.4.1 Состояние журнала инспекции ARP-пакетов

На данном экране можно просмотреть сообщения контрольного журнала, сгенерированные пакетами ARP, которые еще не были отправлены на сервер syslog. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Рисунок 84 Экран ARP Inspection Log Status



Поля экрана описаны в следующей таблице.

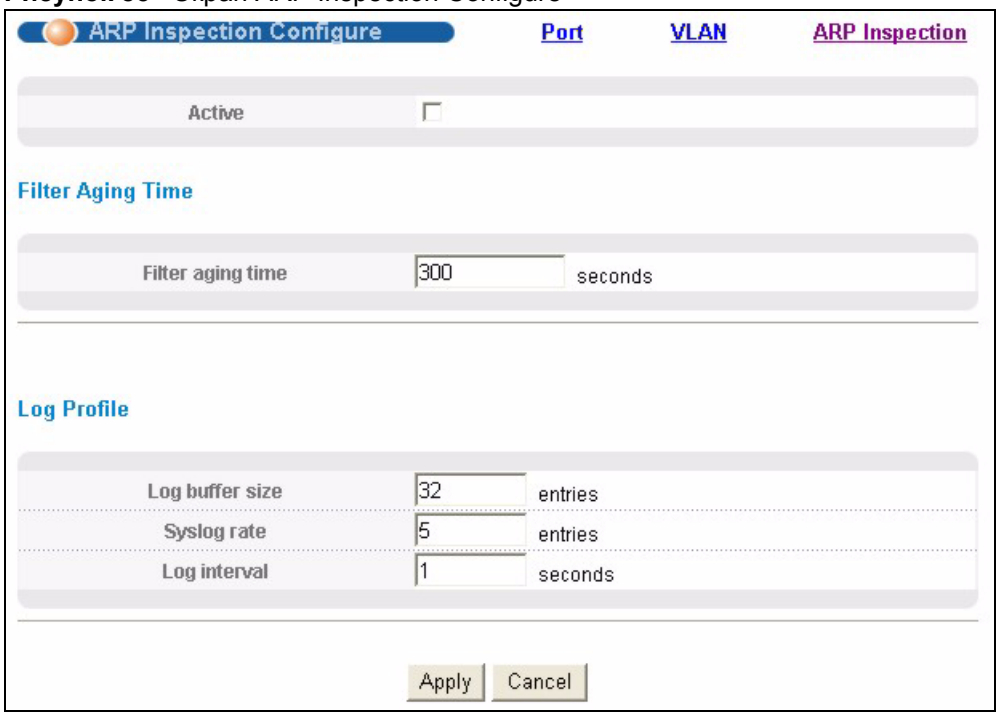
Таблица 58 Экран ARP Inspection Log Status

ПОЛЕ	ОПИСАНИЕ
Clearing log status table	Нажатие на **Apply** позволяет удалить все сообщения контрольного журнала, сгенерированные пакетами ARP, которые еще не были отправлены на сервер syslog.
Total number of logs	В данном поле отображается количество сообщений контрольного журнала, сгенерированных пакетами ARP, которые еще не были отправлены на сервер syslog. В случае отбрасывания одного или нескольких сообщений контрольного журнала из-за недоступности буфера соответствующие записи помечаются как **overflow**, с указанием текущего количества отброшенных сообщений.
Index	В этом поле отображается порядковый номер сообщения контрольного журнала.
Port	В этом поле отображается порт источника пакета ARP.
VID	В этом поле отображается идентификатор VLAN источника пакета ARP.
Sender MAC	В этом поле отображается MAC-адрес источника пакета ARP.
Sender IP	В этом поле отображается IP-адрес источника пакета ARP.
Num Pkts	В этом поле отображается количество пакетов ARP, консолидированных в данном сообщении контрольного журнала. Данный коммутатор консолидирует в одно сообщение идентичные сообщения контрольного журнала, сгенерированные пакетами ARP, за установленный период консолидации. Это период настраивается на экране **ARP Inspection Configure**.См. разд. 21.5 на стр. 183.
Reason	В этом поле отображается причина, по которой было сгенерировано сообщение контрольного журнала. **static deny**: ARP-пакет был отброшен из-за нарушения статической привязки MAC-адреса и идентификатора VLAN ID. **deny**: ARP-пакет был отброшен из-за отсутствия статической привязки MAC-адреса и идентификатора VLAN ID. **static permit**: Коммутатор переслал ARP-пакет, так как была найдена статическая привязка. На экране **ARP Inspection VLAN Configure** можно настроить коммутатор таким образом, чтобы он генерировал сообщения контрольного журнала при отбрасывании или пересылке пакетов ARP в зависимости от идентификатора VLAN ID пакета ARP.См. разд. 21.5.2 на стр. 186.
Time	В этом поле отображается время, в которое было сгенерировано сообщение контрольного журнала.

21.5 Настройка инспекции ARP-пакетов

На данном экране производится настройка функции инспекции ARP-пакетов на коммутаторе. Кроме того, можно настроить период времени, в течение которого коммутатор хранит записи об отброшенных пакетах ARP, а также определить глобальные параметры контрольного журнала функции инспекции ARP-пакетов. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Рисунок 85 Экран ARP Inspection Configure



Поля экрана описаны в следующей таблице.

Таблица 59 Экран ARP Inspection Configure

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на коммутаторе функцию инспекции ARP-пакетов. После этого необходимо включить функцию инспекции ARP-пакетов в конкретной сети VLAN и указать доверенные порты.
Filter Aging Time	
Filter aging time	Данная настройка не влияет на существующие фильтры MAC-адресов. Введите период времени (1-2147483647 секунд), в течение которого фильтр MAC-адресов будет действовать на коммутаторе с момента обнаружения коммутатором несанкционированного пакета ARP. По истечение этого времени фильтр MAC-адресов автоматически удаляется коммутатором. Чтобы фильтр MAC-адреса действовал постоянно, необходимо ввести в это поле значение 0.
Log Profile	
Log buffer size	Введите максимальное количество сообщений контрольного журнала (1-1024), которые могут быть сгенерированы пакетами ARP до отправки на сервер syslog. Данное значение должно соответствовать указанным значениям параметров **Syslog rate** и **Log interval**. Если количество сообщений контрольного журнала на коммутаторе превысит это значение, коммутатор остановит запись сообщений контрольного журнала и будет только подсчитывать количество записей, которые были отброшены из-за нехватки места в буфере. Для очистки контрольного журнала и сброса данного счетчика нажмите на **Clearing log status table** на экране **ARP Inspection Log Status**.См. разд. 21.4.1 на стр. 182.

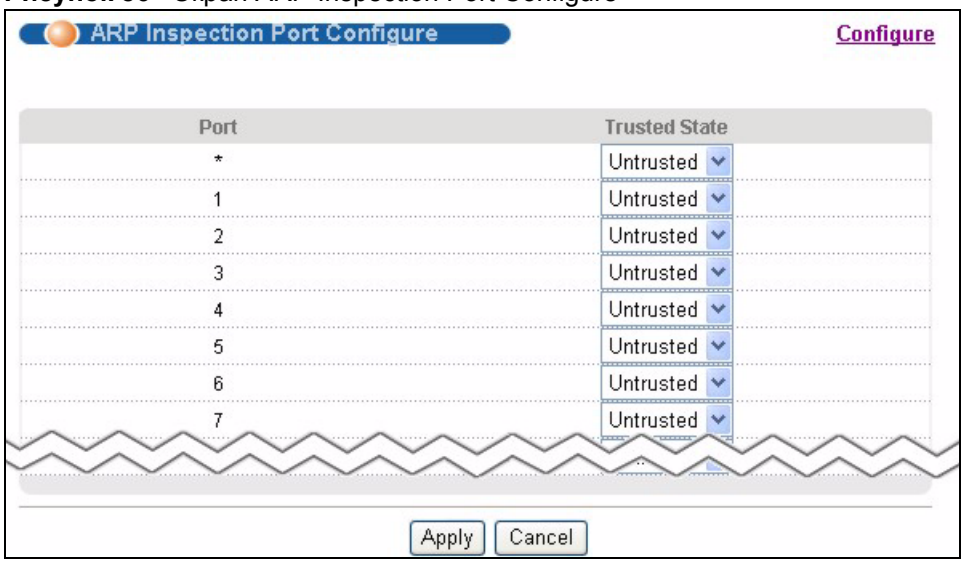
Таблица 59 Экран ARP Inspection Configure (продолжение)

ПОЛЕ	ОПИСАНИЕ
Syslog rate	Введите максимальное количество сообщений syslog, которые коммутатор может передать на сервер syslog в одной партии. Данное количество выражается в виде скорости, так как периодичность отправки партий устанавливается параметром **Log Interval**. Для использования этой функции необходимо настроить сервер syslog (гл. 29 на стр. 243). Чтобы коммутатор не отправлял сообщения контрольного журнала, генерируемые пакетами ARP, на сервер syslog, введите в данное поле значение 0. Взаимосвязь между параметрами **Syslog rate** и **Log interval** иллюстрируют следующие примеры: • 4 недействительных пакета ARP в секунду, **Syslog rate** равен 5, **Log interval** равен 1: коммутатор будет отправлять 4 сообщения syslog каждую секунду. • 6 недействительных пакетов ARP в секунду, **Syslog rate** равен 5, **Log interval** равен 2: коммутатор будет отправлять 10 сообщения syslog каждые 2 секунды.
Log interval	Введите периодичность (1-86400 секунд), с которой коммутатор будет отправлять партии сообщений syslog на сервер syslog. Чтобы сообщения отправлялись коммутатором на сервер syslog немедленно, введите в это поле значение 0. Пример взаимосвязи между параметрами **Syslog rate** и **Log interval** приводится в описании параметра **Syslog rate**.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

21.5.1 Настройка портов для инспекции ARP-пакетов

На данном экране можно определить порты как доверенные и не заслуживающие доверия для функции инспекции ARP-пакетов. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Рисунок 86 Экран ARP Inspection Port Configure



Поля экрана описаны в следующей таблице.

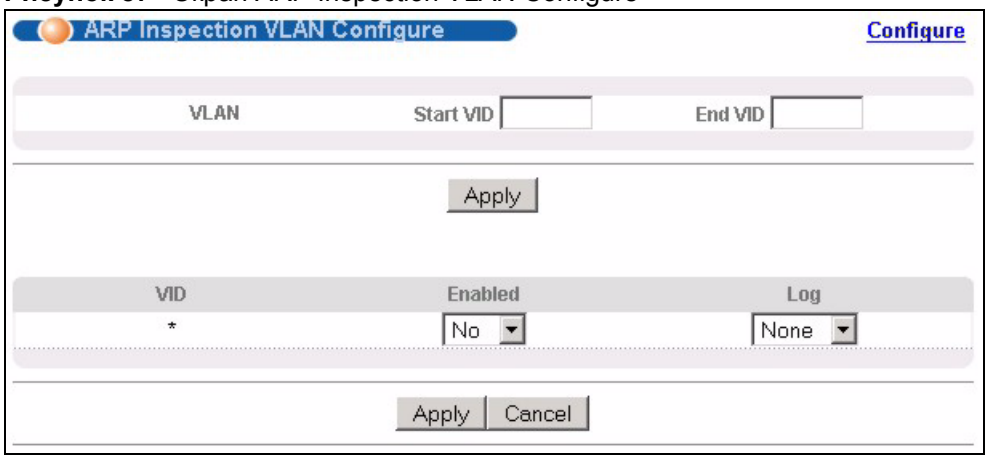
Таблица 60 Экран ARP Inspection Port Configure

ПОЛЕ	ОПИСАНИЕ
Port	В этом поле отображается номер порта. При настройке порта * эти настройки применяются ко всем портам.
Trusted State	Выберите, будет ли данный порт считаться доверенным (**Trusted**) или не заслуживающим доверия (**Untrusted**). Пакеты ARP, приходящие через доверенные порты, коммутатором не отбрасываются ни по какой причине. Данный коммутатор отбрасывает ARP-пакеты, поступающие через не заслуживающие доверия порты, если информация об отправителе в ARP-пакете не совпадает с одной из существующих привязок.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

21.5.2 Настройка сети VLAN для инспекции ARP-пакетов

На данном экране можно включить инспекцию ARP-пакетов для каждой виртуальной локальной сети и указать, должен ли коммутатор генерировать сообщения контрольного журнала при получении пакетов ARP от каждой из сетей VLAN. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Рисунок 87 Экран ARP Inspection VLAN Configure



Поля экрана описаны в следующей таблице.

Таблица 61 Экран ARP Inspection VLAN Configure

ПОЛЕ	ОПИСАНИЕ
VLAN	В данном разделе определяются виртуальные локальные сети VLAN, которые будут настраиваться в разделе ниже.
Start VID	Введите идентификатор начала диапазона для сетей VLAN, которые будут настраиваться в разделе ниже.
End VID	Введите идентификатор конца диапазона для сетей VLAN, которые будут настраиваться в разделе ниже.
Apply	Нажмите на данную кнопку, чтобы отобразить введенный диапазон сетей VLAN в разделе ниже.
VID	В данном поле отображаются идентификаторы VLAN ID каждой из сетей VLAN из выбранного выше диапазона. При настройке VLAN-сети * эти настройки применяются ко всем сетям VLAN.
Enabled	Выберите **Yes**, чтобы включить инспекцию ARP-пакетов в данной сети VLAN. Выберите **No**, чтобы отключить инспекцию ARP-пакетов в данной сети VLAN.
Log	Укажите, должен ли коммутатор генерировать сообщения контрольного журнала при получении пакетов ARP от данной VLAN. **None**: коммутатор не генерирует никаких сообщений контрольного журнала при получении пакетов ARP от данной VLAN. **Deny**: коммутатор генерирует сообщения контрольного журнала при отбрасывании пакета ARP от данной VLAN. **Permit**: коммутатор генерирует сообщения контрольного журнала при пересылке пакетов ARP от данной VLAN. **All**: коммутатор генерирует сообщения контрольного журнала при каждом получении пакетов ARP от данной VLAN.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

22

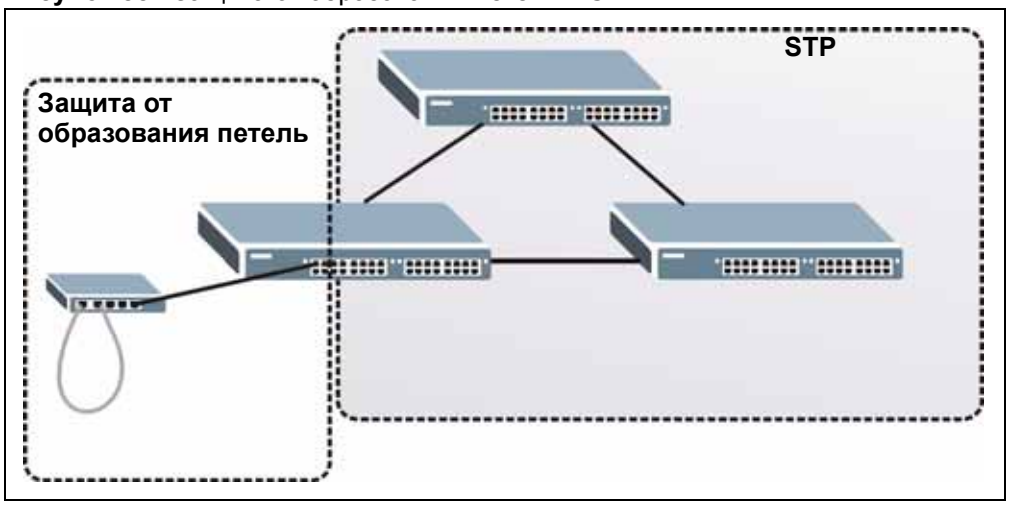
Защита от образования петель

В данной главе описана настройка на коммутаторе механизма защиты от образования петель на границе сети.

22.1 Обзор функции защиты от образования петель

Функция защиты от образования петель позволяет настроить на коммутаторе отключение определенного порта при обнаружении ситуации, когда отправляемые через этот порт пакеты возвращаются на коммутатор. Для защиты от образования петель в опорной сети можно использовать протокол покрывающего дерева (STP), однако STP не обеспечивает защиты от петель, которые могут возникнуть на границе сети.

Рисунок 88 Защита от образования петель и STP



Функция защиты от образования петель предназначена специально для устранения проблем на границе сети. Проблема может возникнуть при подключении порта к коммутатору, на котором образовалась петля. Петля образуется в результате человеческой ошибки. Она возникает, когда два порта коммутатора оказываются соединенными одним кабелем. При рассылке коммутатором с петлей широковещательных сообщений они возвращаются на коммутатор и повторно ретранслируются снова и снова, вызывая широковещательный шторм.

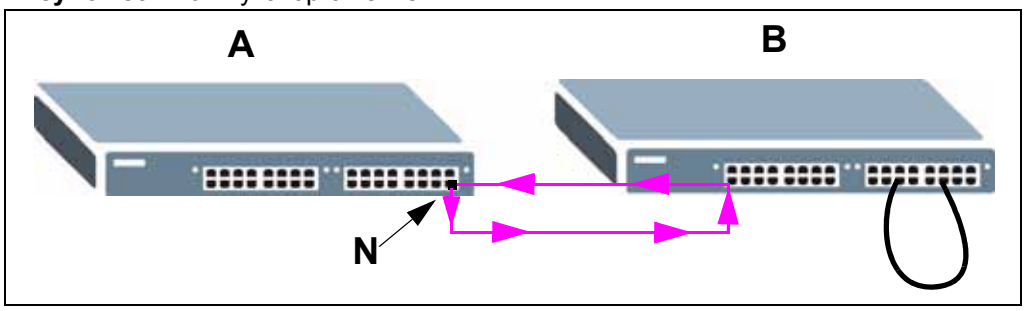
При подключении коммутатора (без петли) к коммутатору с петлей проблемы последнего отражаются на первом следующим образом:

- Он будет принимать широковещательные сообщения, рассылаемые коммутатором с петлей.

- Он будет получать собственные широковещательные сообщения, так как они будут возвращаться по петле к нему. После этого эти сообщения будут ретранслироваться коммутатором повторно.

На приведенном ниже рисунке показано подключение порта **N** на коммутаторе **A** к коммутатору **B**. На коммутаторе **B** образовалась петля. При выходе широковещательных или мультивещательных сообщений из порта **N** и их поступлении на коммутатор **B** эти сообщения вновь направляются на порт **N** коммутатора **A**, после их ретрансляции коммутатором B.

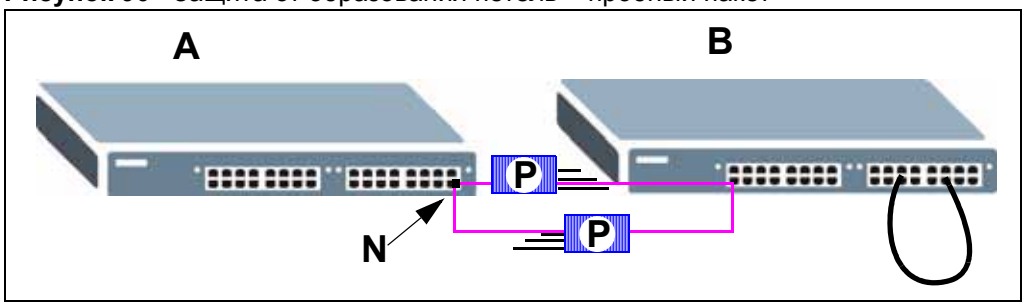
Рисунок 89 Коммутатор с петлей



Функция защиты от образования петель проверяет, не подключен ли порт с активированной функцией к коммутатору с петлей. Для этого она периодически рассылает пробные пакеты и проверяет, не возвращаются ли эти пакеты через тот же самый порт. При обнаружении такого события коммутатор отключает порт, который подключен к коммутатору с петлей.

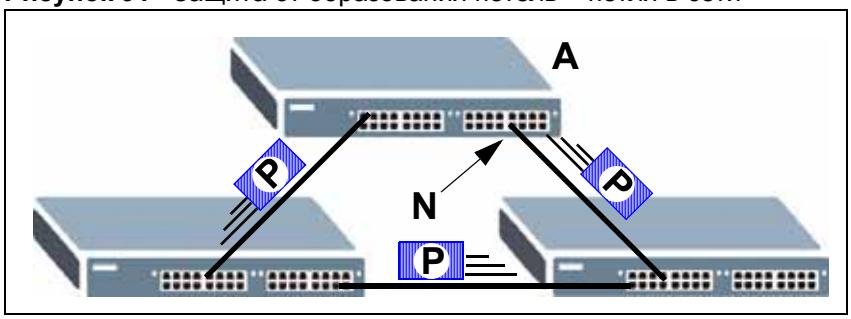
На приведенном ниже рисунке показан коммутатор **A** с активированной на порту **N** функцией защиты от образования петель, который отправляет пробный пакет **P** на коммутатор **B**. Так как на коммутаторе **B** имеется петля, пробный пакет **P** возвращается на порт **N** коммутатора **A**. Для защиты остальной части сети от коммутатора с петлей данный коммутатор отключает порт **N**.

Рисунок 90 Защита от образования петель – пробный пакет



Данный коммутатор также отключит порт **N**, если пробный пакет вернется на коммутатор **A** через любой другой порт. Другими словами, функция защиты от образования петель защищает также от обычных петель в сети. На приведенном ниже рисунке показан пример с тремя коммутаторами, образующими петлю. На рисунке также показан путь пробного пакета, отправляемого функцией защиты от образования петель. В данном примере пробный пакет отправляется из **N** и возвращается на другой порт. Если на порту **N** включена функция защиты от образования петель, коммутатор отключит порт **N** после обнаружения пробного пакета, вернувшегося на коммутатор.

Рисунок 91 Защита от образования петель – петля в сети



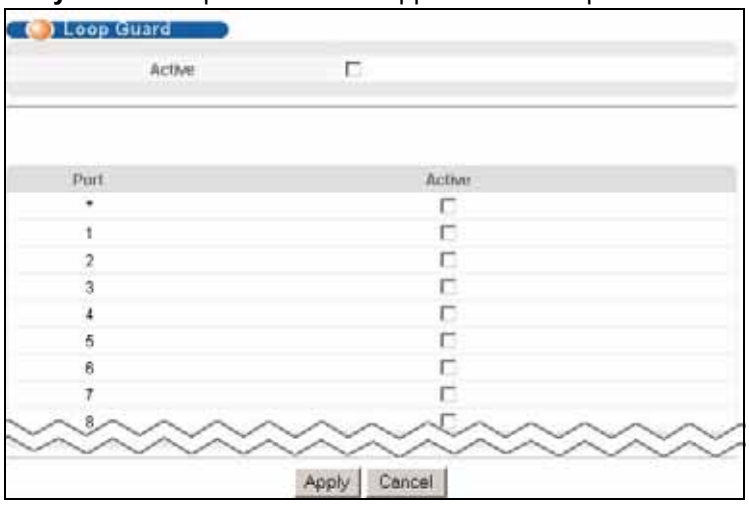
После устранения проблемы с петлей в сети отключенный порт можно снова активировать (см. разд. 7.7 на стр. 77).

22.2 Настройка защиты от образования петель

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Loop Guard**.

Функция защиты от образования петель не может быть включена на портах, для которых включен протокол покрывающего дерева (RSTP или MSTP).

Рисунок 92 Экран Advanced Application > Loop Guard



Поля экрана описаны в следующей таблице.

Таблица 62 Экран Advanced Application > Loop Guard

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить защиту от образования петель на коммутаторе. При отключении порта в результате действия функции защиты от образования петель коммутатор генерирует сообщения syslog, сообщения внутреннего контрольного журнала, а также «ловушки» SNMP.
Port	В этом поле отображается номер порта.
*	С помощью этой строки можно настроить одновременно все порты. С помощью этой строки можно назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить защиту от образования петель для данного порта. Данный коммутатор будет отправлять пробные пакеты через этот порт для проверки, не подключен ли он к коммутатору с петлей. В случае обнаружения подключения данного порта к коммутатору с петлей данный коммутатор отключит этот порт. Снимите выделение с переключателя, если необходимо отключить эту функцию защиты от образования петель.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

Часть IV
IP-приложения

23

Статические маршруты

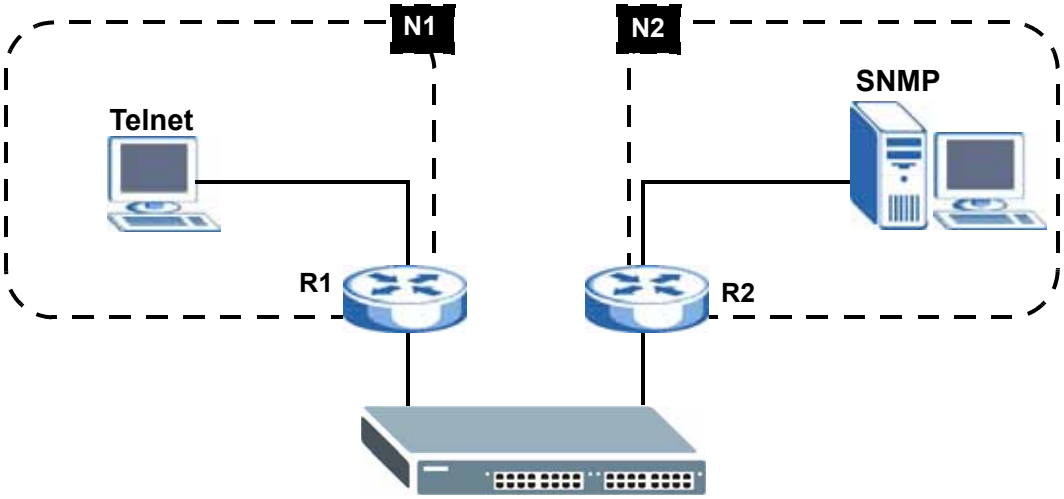
В данной главе описана настройка статических маршрутов.

23.1 Обзор статических маршрутов

Для взаимодействия с управляющими компьютерами, например, с использованием HTTP, telnet, SSH или SNMP данным коммутатором используется протокол IP. С помощью статических IP-маршрутов можно обеспечить управление данным коммутатором с удаленных станций, недоступных через шлюз по умолчанию. Кроме того, статические маршруты могут использоваться коммутатором для передачи данных на сервер или устройство, которое недоступно через шлюз по умолчанию, например, при отправке «ловушек» SNMP или использовании команд ping для проверки подключения по IP.

На данном рисунке показан сеанс **Telnet**, инициируемый из сети **N1**. Данный коммутатор отправляет ответный трафик на шлюз по умолчанию **R1**, который маршрутизирует его обратно на управляющий компьютер. Чтобы коммутатор передавал трафик на сервер регистрации «ловушек» SNMP в сети **N2**, на нем необходимо настроить статический маршрут, указывающий на маршрутизатор **R2**.

Рисунок 93 Обзор статических маршрутов



23.2 Настройка статических маршрутов

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application** > **Static Routing**.

Рисунок 94 Экран IP Application > Static Routing

Поля экрана, используемые для создания статического маршрута, описаны в следующей таблице.

Таблица 63 Экран IP Application > Static Routing

ПОЛЕ	ОПИСАНИЕ
Active	В этом поле можно активировать/деактивировать данный статический маршрут.
Name	Введите имя-описание (до 32 символов в английской раскладке), по которому можно идентифицировать данный маршрут.
Destination IP Address	Сетевой IP-адрес конечного пункта назначения. Маршрутизация всегда основывается на номере сети. Если нужно указать маршрут к конкретному хосту, в поле ввода маски подсети необходимо ввести маску 255.255.255.255, и тогда в качестве номера сети можно использовать идентификатор требуемого хоста.
IP Subnet Mask	Введите маску подсети для данного направления.
Gateway IP Address	Введите IP-адрес шлюза. Шлюз – это ближайший сосед коммутатора, который направляет пакет к пункту его назначения. Шлюз должен быть маршрутизатором в том же сегменте, что и коммутатор.
Metric	Метрика отражает «стоимость» передачи для целей маршрутизации. В IP-маршрутизации в качестве меры стоимости используется счетчик пройденных узлов, с минимальным значением 1 для сетей, соединенных напрямую. Введите число, примерно отражающее стоимость данного канала. Это число не обязательно должно быть точным, но оно должно находиться в диапазоне от 1 до 15. На практике обычно подходит 2 или 3.
Add	Нажмите **Add**, чтобы сохранить новый статический маршрут в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.

Таблица 63 Экран IP Application > Static Routing (продолжение)

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер маршрута. Нажмите на него, чтобы редактировать запись статического маршрута.
Active	В этом поле стоит **Yes**, если статический маршрут активирован, и **No**, если он отключен.
Name	В этом поле отображается имя-описание маршрута. Оно будет использоваться только для идентификации.
Destination Address	В этом поле отображается сетевой IP-адрес конечного пункта назначения.
Subnet Mask	В этом поле отображается маска подсети для данного направления.
Gateway Address	В этом поле отображается IP-адрес шлюза. Шлюз – это ближайший сосед коммутатора, который направляет пакет к пункту его назначения.
Metric	В этом поле отображается «стоимость» передачи для целей маршрутизации.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

24

Дифференцированное обслуживание

В данной главе описана настройка на коммутаторе механизмов дифференцированного обслуживания (DiffServ).

24.1 Обзор механизма DiffServ

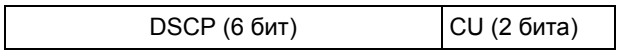
Механизмы управления качеством обслуживания (QoS) позволяют установить приоритеты для потоков трафика из источника в пункт назначения. Все пакеты в потоке получают одинаковый приоритет. Чтобы установить различные приоритеты для различных типов пакетов, можно использовать классы обслуживания (CoS).

DiffServ представляет собой модель на базе классов обслуживания (CoS), в которой пакеты маркируются таким образом, чтобы на пути следования маршрута на сетевых устройствах с поддержкой DiffServ они подвергались особой обработке на каждом конкретном переходе в зависимости от типа приложения и плотности трафика. Пакеты маркируются кодовыми маркерами DiffServ (DiffServ Code Points, DSCP), которые указывают на желаемый уровень обслуживания. Это позволяет промежуточным сетевым устройствам с поддержкой DiffServ обрабатывать пакеты различным образом в зависимости от маркера, без необходимости согласования путей или запоминания информации о состоянии для каждого потока. Кроме того, приложениям не требуется запрашивать конкретное обслуживание или выдавать предварительное уведомление о том, куда направляется трафик.

24.1.1 Маркер DSCP и обработка на каждом конкретном переходе

При использовании DiffServ в заголовок IP-пакетов добавляется новое поле DS (Differentiated Services), которое заменяет поле типа обслуживания ToS (Type of Service). Поле DS содержит 6-битное поле маркера DSCP, которое позволяет определить до 64 уровней обслуживания, а оставшиеся 2 бита на данный момент не используются (currently unused, CU). Поле DS изображено на следующем рисунке.

Рисунок 95 DiffServ: поле Differentiated Service



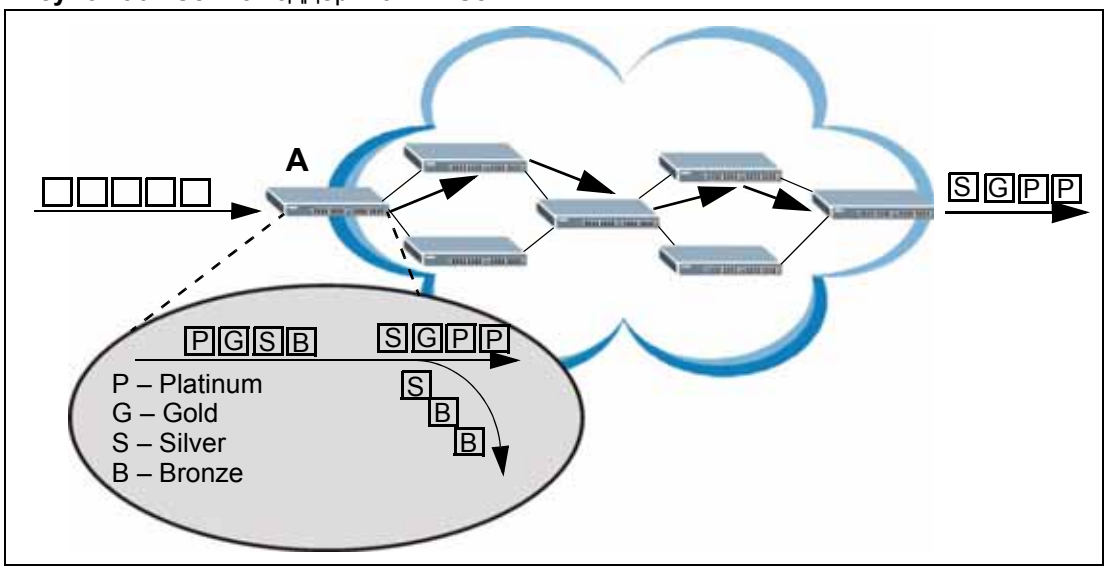
Маркер DSCP обратно совместим с тремя битами приоритета в октете ToS, благодаря чему сетевое устройство с поддержкой ToS, но без поддержки DiffServ не будет конфликтовать с отображением маркера DSCP.

Значение DSCP определяет так называемую обработку на каждом конкретном переходе (PHB, Per-Hop Behavior), которая осуществляется над каждым пакетом при пересылке по сети с поддержкой DiffServ. В зависимости от правила маркирования различные типы трафика могут получать различные приоритеты пересылки. Ресурсы могут быть распределены соответственно значениям DSCP и настроенным политикам.

24.1.2 Пример сети с поддержкой DiffServ

Пример простой сети с поддержкой DiffServ, состоящей из нескольких подключенных напрямую сетевых устройств с поддержкой DiffServ, показан на следующем рисунке. Граничный узел (**A** на рис. 96) в сети DiffServ классифицирует (помечает маркером DSCP) входящие пакеты, разделяя их на различные потоки трафика (**Platinum**, **Gold**, **Silver**, **Bronze**) на основе настроенных правил маркирования. После этого сетевой администратор может применять к потокам трафика различные политики. Один из примеров такой политики – назначение более высокого приоритета отбрасывания одному из потоков трафика по сравнению с другими. В нашем примере у пакетов потока трафика **Bronze** вероятность отбрасывания при перегрузках в процессе движения по сети DiffServ больше, чем у пакетов потока трафика **Platinum**.

Рисунок 96 Сеть с поддержкой DiffServ

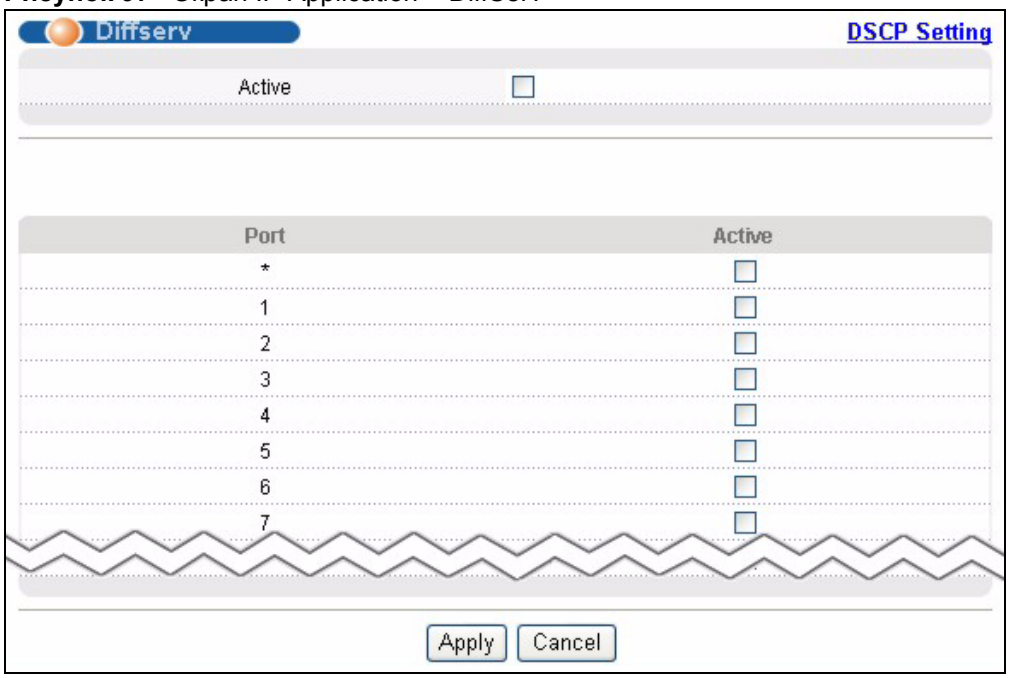


24.2 Активация механизма DiffServ

Включение DiffServ позволяет применять правила маркирования или отображение приоритетов IEEE 802.1p на выбранных портах.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application** > **DiffServ**.

Рисунок 97 Экран IP Application > DiffServ



Поля экрана описаны в следующей таблице.

Таблица 64 Экран IP Application > DiffServ

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить поддержку DiffServ на коммутаторе.
Port	В этом поле отображается порядковый номер порта коммутатора.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите переключатель **Active**, чтобы включить DiffServ для соответствующего порта.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

24.3 Настройка отображения маркеров DSCP на приоритеты IEEE 802.1p

Настройка отображения маркеров DSCP на приоритеты IEEE 802.1p позволяет коммутатору определять приоритеты всего трафика по значению входящих маркеров DSCP, согласно таблице отображения маркеров DiffServ на приоритеты IEEE 802.1p.

Отображение маркеров DSCP на приоритеты IEEE802.1P по умолчанию показано в следующей таблице.

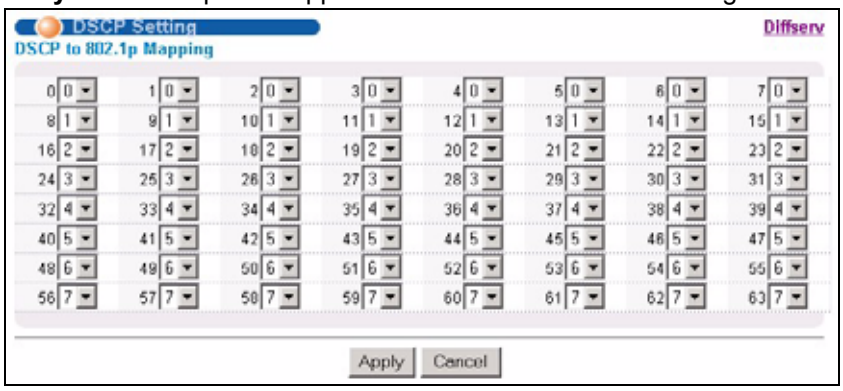
Таблица 65 Отображение маркеров DSCP на приоритеты IEEE 802.1p по умолчанию

ЗНАЧЕНИЕ DSCP	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

24.3.1 Настройка DSCP

Чтобы изменить отображение маркеров DSCP на приоритеты IEEE 802.1p, выберите **DSCP Setting** на экране **DiffServ**. Появится экран, показанный ниже.

Рисунок 98 Экран IP Application > DiffServ > DSCP Setting



Поля экрана описаны в следующей таблице.

Таблица 66 Экран IP Application > DiffServ > DSCP Setting

ПОЛЕ	ОПИСАНИЕ
0 … 63	Идентификационные номера классификации DSCP. Чтобы определить отображение на приоритет IEEE 802.1p, выберите уровень приоритета в ниспадающем списке.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

25

DHCP

В данной главе описана настройка функции DHCP.

25.1 Обзор DHCP

Протокол динамической конфигурации хоста DHCP (Dynamic Host Configuration Protocol, документы RFC 2131 и RFC 2132) позволяет отдельным компьютерам получать настройки TCP/IP с сервера при загрузке. Данный коммутатор можно настроить в качестве агента ретрансляции DHCP. При настройке коммутатора в качестве агента ретрансляции коммутатор пересылает запросы DHCP на сетевой сервер DHCP. Если не настраивать коммутатор в качестве агента ретрансляции DHCP, сервер DHCP должен находиться широковещательном домене клиентских компьютеров или клиентские компьютеры должны настраиваться вручную.

25.1.1 Режимы DHCP

Если в сети уже имеется сервер DHCP, данный коммутатор можно настроить в качестве агента ретрансляции DHCP. При получении коммутатором запроса от клиентского компьютера он обращается к серверу DHCP для получения нужной информации о протоколе IP, а затем передает полученные настройки обратно на компьютер.

25.1.2 Варианты настройки DHCP

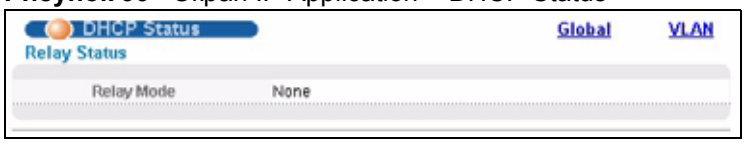
Настройки DHCP на коммутатор осуществляются на экранах **Global** и **VLAN**. Выбор экрана для настройки зависит от тех служб DHCP, которые должны быть предоставлены клиентам DHCP в сети. При выборе руководствуйтесь следующими критериями:

- **Global** – коммутатор пересылает все запросы DHCP на один и тот же сервер DHCP.
- **VLAN** – коммутатор настраивается на уровне отдельной VLAN. На коммутаторе можно настроить ретрансляцию запросов DHCP на различные серверы DHCP в зависимости от того, к какой сети VLAN относятся клиенты.

25.2 Состояние DHCP

Выберите в навигационной панели **IP Application** > **DHCP**. Появится экран **DHCP Status**.

Рисунок 99 Экран IP Application > DHCP Status



Поля экрана описаны в следующей таблице.

Таблица 67 Экран IP Application > DHCP Status

ПОЛЕ	ОПИСАНИЕ
Relay Status	В данном разделе отображаются настройки, относящиеся к режиму ретрансляции DHCP коммутатором.
Relay Mode	В этом поле отображается одно из следующих состояний: • **None** – если коммутатор не настроен в качестве агента ретрансляции DHCP. • **Global** – если коммутатор настроен только как агент ретрансляции DHCP. • **VLAN**, за которым следуют идентификаторы VLAN ID – если он настроен в качестве агента ретрансляции для конкретных VLAN.

25.3 Ретрансляция DHCP

Если клиенты DHCP и сервер DHCP находятся в различных широковещательных доменах, на коммутаторе необходимо настроить ретрансляцию DHCP. При первоначальном выделении IP-адреса коммутатор помогает передавать информацию о сети (такую как IP-адрес и маску подсети) от клиента DHCP к серверу DHCP. После получения клиентом DHCP IP-адреса и его подключения к сети обновление информации между клиентом DHCP и сервером DHCP производится без участия коммутатора.

Данный коммутатор можно настроить в качестве глобального агента ретрансляции DHCP. В этом случае коммутатор будет передавать все запросы DHCP от всех доменов на один и тот же сервер DHCP. Кроме того, на коммутаторе можно настроить ретрансляцию информации DHCP в зависимости от сети VLAN, к которой относится клиент.

25.3.1 Информация агента ретрансляции DHCP

Данный коммутатор позволяет добавлять информацию об источнике клиентского DHCP-запроса, который ретранслируется им на сервер DHCP, посредством добавления **информации агента ретрансляции**. Это помогает аутентифицировать источник запроса. После этого сервер DHCP может выделить IP-адрес с использованием этой информации. Дополнительную информацию можно найти в RFC 3046.

Функция **информации агента ретрансляции** DHCP добавляет поле информации агента к полю **Option 82**. Поле **Option 82** располагается в заголовке клиентских DHCP-запросов, ретранслируемых коммутатором на сервер DHCP.

Информация агента ретрансляции может включать в себя **имя системы**, если выбрать для коммутатора данный режим. Имя системы **System Name** можно изменить на экране **Basic Settings** > **General Setup**.

Информация агента ретрансляции DHCP, передаваемая коммутатором на сервер DHCP, описана ниже:

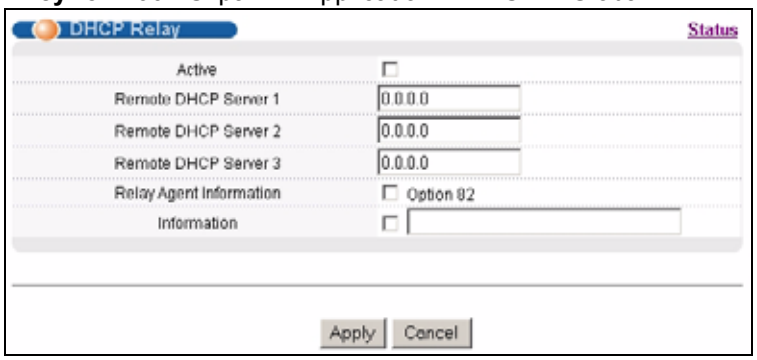
Таблица 68 Информация агента ретрансляции

ПОЛЕ	ОПИСАНИЕ
Slot ID	(1 байт) Данное значение всегда равно 0 для автономных коммутаторов.
Port ID	(1 байт) Номер порта, к которому подключен клиент DHCP.
VLAN ID	(2 байта) Идентификатор VLAN, к которой принадлежит порт.
Information	(до 32 байт) Опциональное поле только для чтения, которое устанавливается в соответствии с именем системы, настроенным на экране **Basic Settings > General Setup.**

25.3.2 Настройка глобальной ретрансляции DHCP

Настройка глобальной ретрансляции DHCP осуществляется на экране **DHCP Relay**. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application > DHCP** и нажмите на ссылке **Global**.

Рисунок 100 Экран IP Application > DHCP > Global



Поля экрана описаны в следующей таблице.

Таблица 69 Экран IP Application > DHCP > Global

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить ретрансляцию DHCP.
Remote DHCP Server 1 .. 3	Введите IP-адрес сервера DHCP в виде десятичных чисел, разделенных точками.
Relay Agent Information	Установите переключатель **Option 82**, чтобы коммутатор добавлял информацию (номер слота, номер порта и идентификатор VLAN ID) к клиентским запросам DHCP, ретранслируемым им на сервер DHCP.
Information	В этом доступном только для чтения поля отображается имя системы, настроенное на экране **General Setup**. Установите данный переключатель, чтобы коммутатор добавлял имя системы к клиентским DHCP-запросам, ретранслируемым на сервер DHCP.

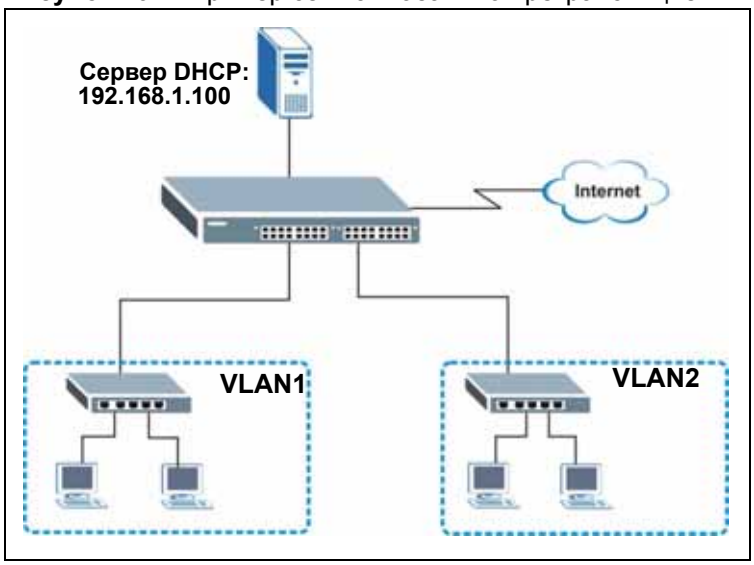
Таблица 69 Экран IP Application > DHCP > Global (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

25.3.3 Пример настройки глобальной ретрансляции DHCP

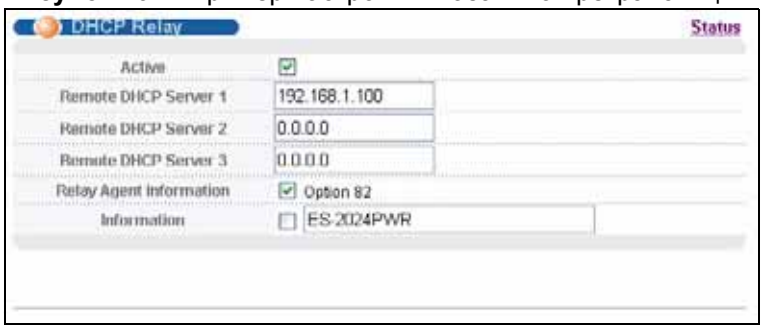
На приведенном ниже рисунке показан пример сети, в которой коммутатор используется для ретрансляции запросов DHCP в доменах **VLAN1** и **VLAN2**. В сети имеется только один сервер DHCP, который обслуживает клиентов DHCP в обоих доменах.

Рисунок 101 Пример сети с глобальной ретрансляцией DHCP



На экране **DHCP Relay** выполняются следующие настройки. Необходимо обязательно установить переключатель **Option 82**, чтобы коммутатор отправлял на сервер DHCP дополнительную информацию (в частности, идентификатор VLAN ID) вместе с запросами DHCP. В этом случае сервер DHCP сможет назначать нужные IP-адреса в зависимости от идентификатора VLAN ID.

Рисунок 102 Пример настройки глобальной ретрансляции DHCP

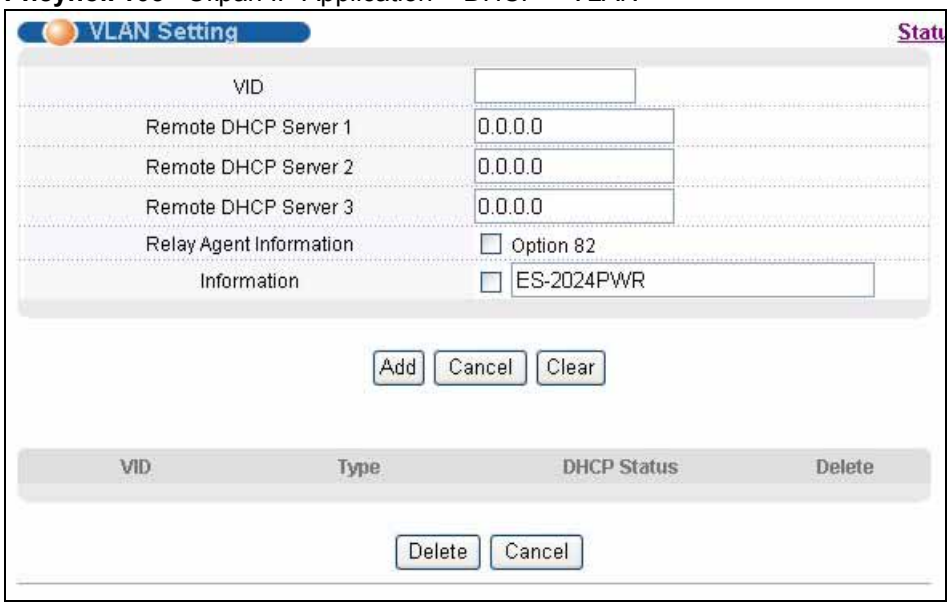


25.4 Настройка DHCP для конкретных VLAN

На данном экране можно настроить параметры DHCP для конкретных виртуальных локальных сетей VLAN, к которым относятся клиенты DHCP. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application** > **DHCP** и нажмите на ссылке **VLAN** на появившемся экране **DHCP Status**.

Для каждой сети VLAN, для которой требуется ввести настройки DHCP на коммутаторе, необходимо настроить собственный IP-адрес управления. О том, как это сделать, можно узнать в разд. 7.6 на стр. 74.

Рисунок 103 Экран IP Application > DHCP > VLAN



Поля экрана описаны в следующей таблице.

Таблица 70 Экран IP Application > DHCP > VLAN

ПОЛЕ	ОПИСАНИЕ
VID	Введите идентификатор VLAN, к которой относятся данные настройки DHCP.
Remote DHCP Server 1 .. 3	Введите IP-адрес сервера DHCP в виде десятичных чисел, разделенных точками.
Relay Agent Information	Установите переключатель **Option 82**, чтобы коммутатор добавлял информацию (номер слота, номер порта и идентификатор VLAN ID) к клиентским запросам DHCP, ретранслируемым им на сервер DHCP.
Information	В этом доступном только для чтения поля отображается имя системы, настроенное на экране **General Setup**. Установите данный переключатель, чтобы коммутатор добавлял имя системы к клиентским DHCP-запросам, ретранслируемым на сервер DHCP.

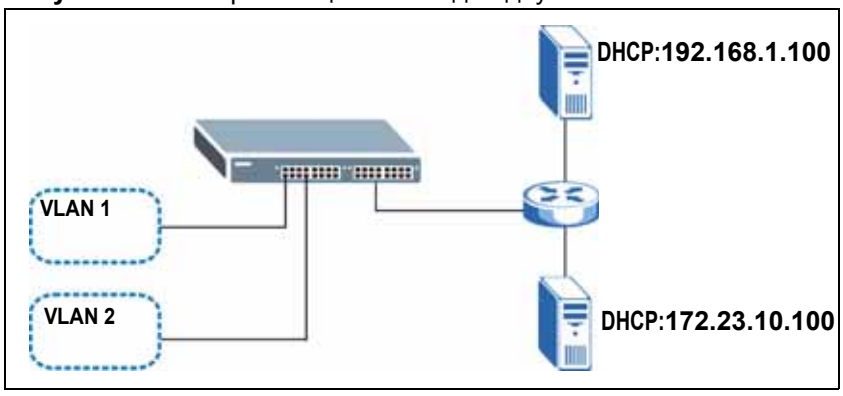
Таблица 70 Экран IP Application > DHCP > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите **Add**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Clear	Нажмите на данную кнопку, чтобы очистить перечисленные выше поля.
VID	В данном поле отображается идентификатор VLAN, к которой относятся настройки DHCP.
Type	В данном поле отображается **Relay** в качестве режима DHCP.
DHCP Status	В данном поле отображается IP-адрес первого удаленного сервера DHCP.
Delete	Выберите записи настройки, которые необходимо удалить, и нажмите на кнопку **Delete** для удаления.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

25.4.1 Пример: Ретрансляция DHCP для двух VLAN

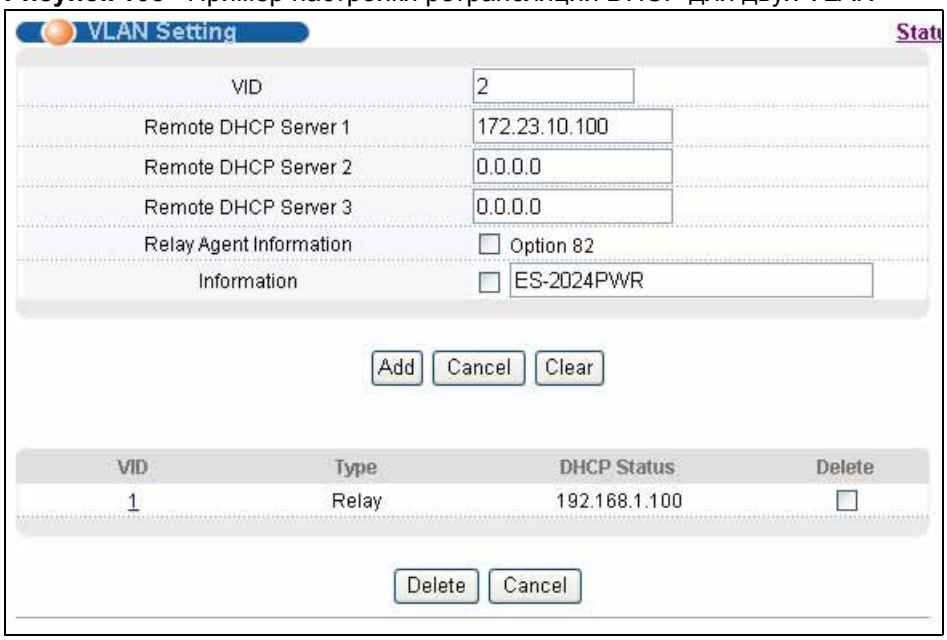
В следующем примере показана сеть группы зданий с двумя виртуальными локальными сетями VLAN (VID 1 и 2). Для обслуживания каждой из сетей VLAN установлено два сервера DHCP. В системе настроена ретрансляция запросов DHCP из комнат общежития (VLAN 1) на сервер DHCP с IP-адресом 192.168.1.100. Запросы из академических зданий (VLAN 2) направляются на другой сервер DHCP с IP-адресом 172.23.10.100.

Рисунок 104 Ретрансляция DHCP для двух VLAN



Для показанного примера настройки на экране **VLAN Setting** должны быть следующими.

Рисунок 105 Пример настройки ретрансляции DHCP для двух VLAN



Часть V
Управление

26

Обслуживание

В данной главе описаны настройки на экранах обслуживания, позволяющие работать с файлами встроенного программного обеспечения и конфигурации.

26.1 Экран Maintenance

На этом экране осуществляется управление встроенным программным обеспечением и файлами конфигурации. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **Maintenance**.

Рисунок 106 Экран Management > Maintenance

Поля экрана описаны в следующей таблице.

Таблица 71 Экран Management > Maintenance

ПОЛЕ	ОПИСАНИЕ
Current	В этом поле отображается, какая конфигурация используется коммутатором в данный момент (**Configuration 1**).
Firmware Upgrade	Нажмите **Click Here** для перехода к экрану обновления встроенного аппаратного обеспечения **Firmware Upgrade**.
Restore Configuration	Нажмите **Click Here** для перехода к экрану восстановления конфигурации **Restore Configuration**.
Backup Configuration	Нажмите **Click Here** для перехода к экрану резервного копирования конфигурации **Backup Configuration**.
Load Factory Default	Нажмите **Click Here** для сброса конфигурации к заводским настройкам по умолчанию.

Таблица 71 Экран Management > Maintenance (продолжение)

ПОЛЕ	ОПИСАНИЕ
Save Configuration	Нажмите **Config 1** для сохранения текущей конфигурации в качестве **Configuration 1** коммутатора.
Reboot System	Нажмите **Config 1** для перезагрузки системы с использованием на коммутаторе конфигурации **Configuration 1**. Примечание: Не забывайте нажимать на кнопку **Save** на экранах настройки при изменении текущей конфигурации коммутатора.

26.2 Загрузка заводских настроек по умолчанию

Чтобы вернуться на коммутаторе к заводским настройкам по умолчанию, выполните следующее.

1. Чтобы сбросить всю введенную информацию о настройках коммутатора и вернуться к заводским настройкам по умолчанию, нажмите кнопку **Click Here** рядом с надписью **Load Factory Defaults** на экране **Maintenance**.
2. Чтобы вернуть все настройки коммутатора к заводским настройкам по умолчанию, нажмите **OK**

Рисунок 107 Загрузка заводских настроек: запуск

3. Изменения вступают в силу после нажатия на кнопку **Save** в Web-конфигураторе. Для повторного входа в Web-конфигуратор коммутатора, возможно, придется изменить IP-адрес компьютера, чтобы он находился в той же подсети, что и IP-адрес коммутатора по умолчанию (192.168.1.1).

26.3 Сохранение конфигурации

Нажмите **Config 1** для сохранения текущей конфигурации в качестве **Configuration 1** коммутатора.

Кроме того, для сохранения изменений в текущей конфигурации можно воспользоваться кнопкой **Save** в правом верхнем углу на любом экране.

Нажатие на кнопки **Apply** и **Add** НЕ сохраняет изменения в постоянной памяти. Все несохраненные изменения будут утеряны после перезагрузки коммутатора.

26.4 Перезагрузка системы

Опция **Reboot System** позволяет перезагрузить коммутатор, не отключая питание физически. При перезагрузке коммутатор загружает первую конфигурацию (**Config 1**). Чтобы перезагрузить коммутатор, выполните следующее.

1 Чтобы перезагрузить коммутатор с использованием первой конфигурации, нажмите на кнопку **Config 1** в поле **Reboot System** экрана **Maintenance**. Появится следующий экран.

Рисунок 108 Перезагрузка системы: подтверждение

2 Нажмите **OK** еще раз и дождитесь, пока коммутатор перезагрузится. Этот процесс занимает до двух минут. Он не влияет на настройки коммутатора.

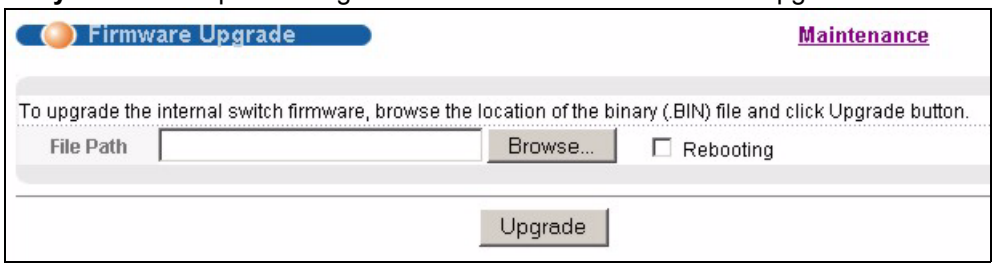
26.5 Обновление встроенного программного обеспечения

Прежде чем приступать к загрузке встроенного программного обеспечения в устройство, убедитесь, что на компьютер загружено (и распаковано) встроенное программное обеспечение нужной модели и версии.

Убедитесь, что загружаемое встроенное программное обеспечение подходит для соответствующей модели, так как программное обеспечение для другой модели может повредить устройство.

Находясь на экране **Maintenance**, выберите **Firmware Upgrade**, чтобы открыть показанный ниже экран.

Рисунок 109 Экран Management > Maintenance > Firmware Upgrade



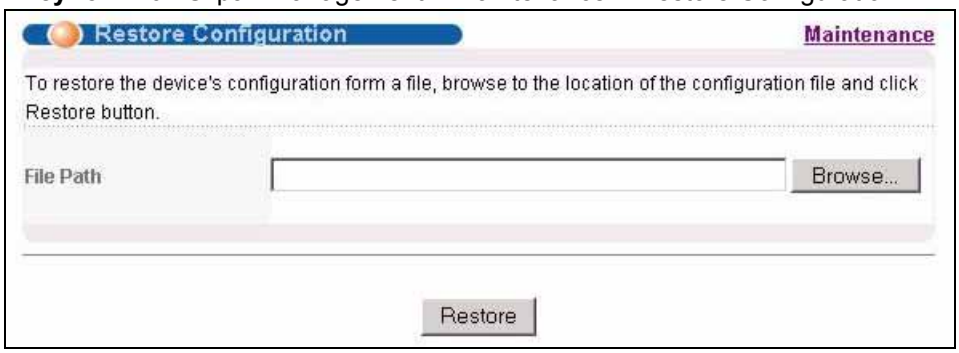
Введите путь и имя файла встроенного программного обеспечения, который необходимо загрузить в коммутатор, в текстовом поле **File Path**, или нажмите **Browse**, чтобы найти его вручную. Установите переключатель **Rebooting**, если необходимо перезагрузить коммутатор и применить новое встроенное программное обеспечение немедленно. (Обновления встроенного программного обеспечения применяются только после перезагрузки). Нажмите **Upgrade**, чтобы загрузить новое встроенное программное обеспечение.

После завершения процесса загрузки встроенного программного обеспечения откройте экран **System Info**, чтобы проверить текущий номер версии встроенного программного обеспечения.

26.6 Восстановление файла конфигурации

Экран **Restore Configuration** позволяет восстановить ранее сохраненные настройки с компьютера на коммутатор.

Рисунок 110 Экран Management > Maintenance > Restore Configuration



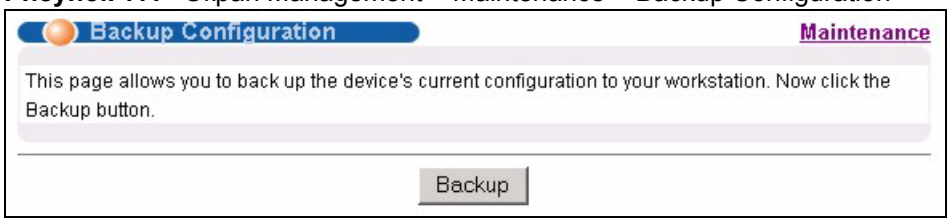
Введите путь и имя файла конфигурации, который необходимо восстановить, в текстовом поле **File Path**, или нажмите **Browse**, чтобы открыть экран **Choose File** и найти его вручную. После ввода пути к файлу нажмите **Restore**. Файл конфигурации в коммутаторе имеет имя «config», поэтому файл резервной копии конфигурации при восстановлении будет автоматически переименован.

26.7 Резервное копирование файла конфигурации

Функция резервного копирования конфигурации коммутатора позволяет создавать различные «снимки» конфигурации устройства, которые потом можно загрузить.

Резервное копирование конфигурации коммутатора на компьютер осуществляется с использованием экрана **Backup Configuration**.

Рисунок 111 Экран Management > Maintenance > Backup Configuration



Чтобы создать резервную копию текущей конфигурации коммутатора на компьютере, выполните на данном экране следующее.

1. Нажмите **Backup**.
2. Нажмите **Save**, чтобы открыть экран **Save As**.
3. Выберите расположение файла на компьютере в ниспадающем списке **Save in** и введите имя-описание для него в поле списка **File name**. Нажмите **Save**, чтобы сохранить конфигурацию на компьютере.

26.8 Командная строка FTP

В данном разделе описаны некоторые примеры загрузки или выгрузки с коммутатора файлов с помощью команд FTP. Прежде всего необходимо уяснить соглашения об именовании файлов.

26.8.1 Соглашения об именовании файлов

Файл конфигурации (также называемый файлом ROM) содержит заводские настройки по умолчанию для таких экранов, как коммутатор setup, IP Setup и т.д. После внесения изменений в настройки коммутатора их можно сохранить на компьютере под любым выбранным именем.

Операционная система ZyNOS (ZyXEL Network Operating System, часто называется «ras» -файлом) – это встроенное системное программное обеспечение, она имеет расширение файла «bin».

Таблица 72 Соглашения об именовании файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	config		Файл настроек коммутатора. При загрузке файла config данный файл конфигурации заменяется, в том числе заменяются настройки коммутатора, системная информация (в том числе пароль по умолчанию), журналы ошибок и отслеживания.
Встроенное программное обеспечение	ras	*.bin	Общее имя для встроенного программного обеспечения ZyNOS на коммутаторе.

26.8.1.1 Примеры команд FTP

```
ftp> put firmware.bin ras
```

Пример FTP-сессии, в которой происходит передача файла «firmware.bin» с компьютера на коммутатор.

```
ftp> get config config.cfg
```

Пример FTP-сессии, в которой происходит сохранение текущего файла конфигурации в файл с именем «config.cfg»на компьютере.

Если используемый (T)FTP-клиент не позволяет указывать имя конечного файла, отличное от исходного, файлы придется переименовать, так как коммутаторраспознает только имена «config»и «ras». Обязательно сохраните неизмененные копии обоих файлов для дальнейшего использования.

Убедитесь, что загружаемое встроенное программное обеспечение подходит для соответствующей модели, так как программное обеспечение для другой модели может повредить устройство.

26.8.2 Работа с командной строкой FTP

1. Запустите на компьютере FTP-клиент.
2. Введите команду `open`, потом пробел и IP-адрес коммутатора.
3. Нажмите [ENTER], получив запрос имени пользователя.
4. После получения приглашения введите пароль (по умолчанию «1234»).
5. Введите `bin`, чтобы установить двоичный режим передачи.
6. Для загрузки файлов с компьютера на коммутатор используйте команду `put`, например: команда `put firmware.bin ras` переносит файл встроенного программного обеспечения с компьютера (firmware.bin) в коммутатори переименовывает его в «ras». Точно так же команда `put config.cfg config` переносит файл конфигурации с компьютера (config.cfg) в коммутатори переименовывает его в «config». С помощью команды `get config config.cfg` можно перенести файл конфигурации с коммутатора на компьютер и переименовать его в «config.cfg». Дополнительную информацию о соглашениях в отношении именования файлов можно найти в табл. 72 на стр. 217.
7. Чтобы покинуть строку ftp-команд, введите `quit`.

26.8.3 FTP-клиенты с графическим пользовательским интерфейсом

Описания некоторых команд, которые встречаются в FTP-клиентах с графическим пользовательским интерфейсом, можно найти в следующей таблице.

Таблица 73 Общие команды для FTP-клиентов с графическим пользовательским интерфейсом

КОМАНДА	ОПИСАНИЕ
Host Address (Адрес хоста)	Введите адрес хост-сервера.
Login Type (Тип входа в систему)	Анонимный (Anonymous). Для тех случаев, когда идентификатор пользователя и пароль вводятся на сервере автоматически для анонимного доступа. Анонимные подключения работают только в том случае, если Интернет-провайдер или администратор службы включил эту опцию. Normal (Обычный). Для подключения к серверу требуются уникальные имя пользователя и пароль.
Transfer Type (Тип передачи)	Файлы передаются либо в формате ASCII (простой текстовый формат), либо в двоичном формате. Файлы настроек и встроенного программного обеспечения должны передаваться в двоичном формате.
Initial Remote Directory (Начальный удаленный каталог)	Укажите удаленный каталог по умолчанию (путь).
Initial Local Directory (Начальный локальный каталог)	Укажите локальный каталог по умолчанию (путь).

26.8.4 Ограничения FTP

Протокол FTP не будет работать, если:

- Служба FTP отключена на экране **Service Access Control**.
- IP-адрес (IP-адреса), введенные на экране **Remote Management**, не соответствуют IP-адресу клиента. Если адрес не совпадает, коммутатор немедленно разрывает Telnet-сессию.

27

Контроль доступа

В данной главе описан контроль доступа к коммутатору.

27.1 Обзор контроля доступа

Для доступа с консольного порта или через FTP допускается по одной сессии, для доступа через Telnet и SSH допускается в общей сложности девять сессий, для управления через Web поддерживается до пяти сессий (с пятью различными именами пользователей и паролями), количество сеансов контроля доступа через SNMP не ограничено.

Таблица 74 Обзор контроля доступа

Консольный порт	SSH	Telnet	FTP	Web	SNMP
Одна сессия	В общей сложности до девяти сессий		Одна сессия	До пяти учетных записей	Без ограничений

Сессии контроля доступа с консольного порта и через Telnet не могут быть осуществлены одновременно, если функция доступа нескольким пользователям (multi-login) отключена. Дополнительную информацию о запрещении доступа нескольким пользователям можно найти в Справочном руководстве по интерфейсу командной строки.

27.2 Главный экран контроля доступа

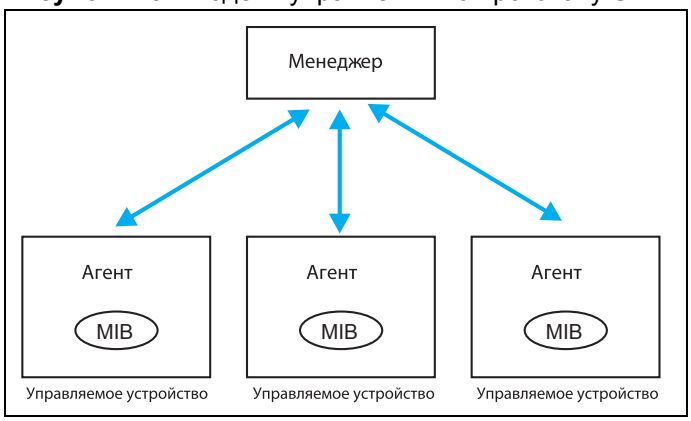
Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Access Control**.

Рисунок 112 Экран Management > Access Control

27.3 Знакомство с протоколом SNMP

Простой протокол сетевого управления (SNMP) – это протокол прикладного уровня, который используется для управления и мониторинга устройств на основе TCP/IP. Протокол SNMP используется для обмена управляющей информацией между системой сетевого управления (NMS) и сетевым элементом (NE). Станция управления может управлять и осуществлять мониторинг коммутатора по сети с помощью протокола SNMP версии 1 (SNMPv1), SNMP версии 2c или SNMP версии 3. Пример управления с помощью протокола SNMP показан на следующем рисунке. Протокол SNMP будет работать только в том случае, если настроен протокол TCP/IP.

Рисунок 113 Модель управления по протоколу SNMP



Сеть под управлением протокола SNMP состоит из двух основных компонентов: агентов и менеджера.

Агент – это программный модуль управления, находящийся на управляемом коммутаторе (коммутаторе). Агент переводит локальную информацию управления от управляемого коммутатора в форму, совместимую с протоколом SNMP. Менеджер – это консоль, посредством которой администраторы сети осуществляют функции сетевого управления. На ней запускаются приложения, осуществляющие контроль и мониторинг управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют, какую информацию о коммутаторе необходимо получить. Примерами таких переменных являются количество полученных пакетов, состояние порта и т.д. База управляющей информации (MIB) представляет собой совокупность управляемых объектов. Протокол SNMP позволяет менеджеру и агентам общаться между собой для получения доступа к этим объектам.

Сам по себе SNMP – это простой протокол типа «запрос/ответ» на основе модели «менеджер/агент». Менеджер отправляет запрос, а агент отвечает на него посредством следующих операций протокола:

Таблица 75 Команды протокола SNMP

КОМАНДА	ОПИСАНИЕ
Get	Позволяет менеджеру получать объектные переменные от агента.
GetNext	Позволяет менеджеру получить следующую объектную переменную из таблицы или списка, хранящегося у агента. В протоколе SNMPv1, когда менеджер хочет получить от агента все элементы таблицы, он инициирует операцию Get и сразу за ней серию операций GetNext.

Таблица 75 Команды протокола SNMP

КОМАНДА	ОПИСАНИЕ
Set	Позволяет менеджеру устанавливать значения объектных переменных, хранящихся у агента.
Trap	Используется агентом для оповещения менеджера о каких-либо событиях.

27.3.1 SNMP v3 и безопасность

В SNMP v3 улучшены средства безопасности для управления через SNMP. Перед началом сессий управления от менеджеров SNMP может быть затребована аутентификация на агентах.

Дополнительно безопасность может быть повышена с использованием шифрования сообщений SNMP, отправляемых менеджерами. Шифрование защищает содержимое сообщение SNMP. В случае шифрования сообщений SNMP они могут быть прочитаны только целевыми получателями.

27.3.2 Поддерживаемые базы MIB

Базы управляющей информации позволяют администраторам собирать статистику и осуществлять мониторинг за состоянием и производительностью.

Данный коммутатор поддерживает следующие базы управляющей информации:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIB
- RFC 1643 Ethernet MIB
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c или более поздней версии, совместимый со стандартом RFC 2011 SNMPv2 MIB для IP, RFC 2012 SNMPv2 MIB для TCP, RFC 2013 SNMPv2 MIB для UDP

27.3.3 Команды Trap протокола SNMP

Данный коммутатор отправляет SNMP-менеджеру «ловушку» (команду Trap), когда происходит какое-нибудь событие. Команды Trap протокола SNMP для различных категорий описаны в следующих таблицах.

Идентификаторы объектов OID (Object ID), начинающиеся с «**1.3.6.1.4.1.890.1.5.8.16**» (ES-2024A) или «**1.3.6.1.4.1.890.1.5.8.27**» (ES-2024PWR), определены в частных MIB. Все прочие OID определены в стандартных MIB.

Таблица 76 Системные команды Trap протокола SNMP (System)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	Эта команда Trap отправляется при включении коммутатора.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	Эта команда Trap отправляется при перезагрузке коммутатора.
fanspeed	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1	Эта команда Trap отправляется при понижении или повышении скорости вентилятора так, что она выходит из нормального рабочего диапазона.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при возвращении скорости вентилятора в нормальный рабочий диапазон.
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1	Эта команда Trap отправляется при понижении или повышении температуры так, что она выходит из нормального рабочего диапазона.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при возвращении температуры в нормальный рабочий диапазон.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при понижении или повышении напряжения так, что оно выходит из нормального рабочего диапазона.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при возвращении напряжения в нормальный рабочий диапазон.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при автоматическом сбросе коммутатора.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при сбросе коммутатора администратором через интерфейс управления.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	Эта команда Trap отправляется при перезагрузке коммутатора администратором через интерфейс управления.
timesync	RTCNotUpdatedEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при неполучении коммутатором времени и даты от сервера времени.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при получении коммутатором времени и даты от сервера времени.

Таблица 76 Системные команды Trap протокола SNMP (System) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при блокировке порта для защиты от вторжения.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при блокировке порта функцией защиты от образования петель.

Таблица 77 Интерфейсные команды Trap протокола SNMP (Interface)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	Эта команда Trap отправляется при установлении Ethernet-соединения.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при установлении Ethernet-соединения.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	Эта команда Trap отправляется при разрыве Ethernet-соединения.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при разрыве Ethernet-соединения.
autonegotiation	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется в случае, когда интерфейсу Ethernet не удается автоматически согласовать параметры соединения с другим интерфейсом Ethernet.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется в случае, когда интерфейсу Ethernet удается автоматически согласовать параметры соединения с другим интерфейсом Ethernet.

Таблица 78 Команды Trap протокола SNMP для аутентификации, авторизации и учета (AAA)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
аутентификация	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Эта команда Trap отправляется при невозможности аутентификации из-за неправильного имени пользователя и/или пароля.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при невозможности аутентификации из-за неправильного имени пользователя и/или пароля.
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при отсутствии ответа от сервера RADIUS.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при недоступности сервера RADIUS.
accounting	RADIUSAcctNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при отсутствии ответа от сервера учета RADIUS.
	RADIUSAcctNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при недоступности сервера учета RADIUS.

Таблица 79 Команды Trap протокола SNMP для IP

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	Эта команда Trap отправляется при неудаче выполнения одиночной команды ping.
	pingTestFailed	1.3.6.1.2.1.80.0.2	Эта команда Trap отправляется при неудаче выполнения теста соединения (включающего в себя несколько команд ping).
	pingTestCompleted	1.3.6.1.2.1.80.0.3	Эта команда Trap отправляется при завершении одиночной команды ping.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	Эта команда Trap отправляется при неудаче выполнения теста traceroute.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	Эта команда Trap отправляется при завершении теста traceroute.

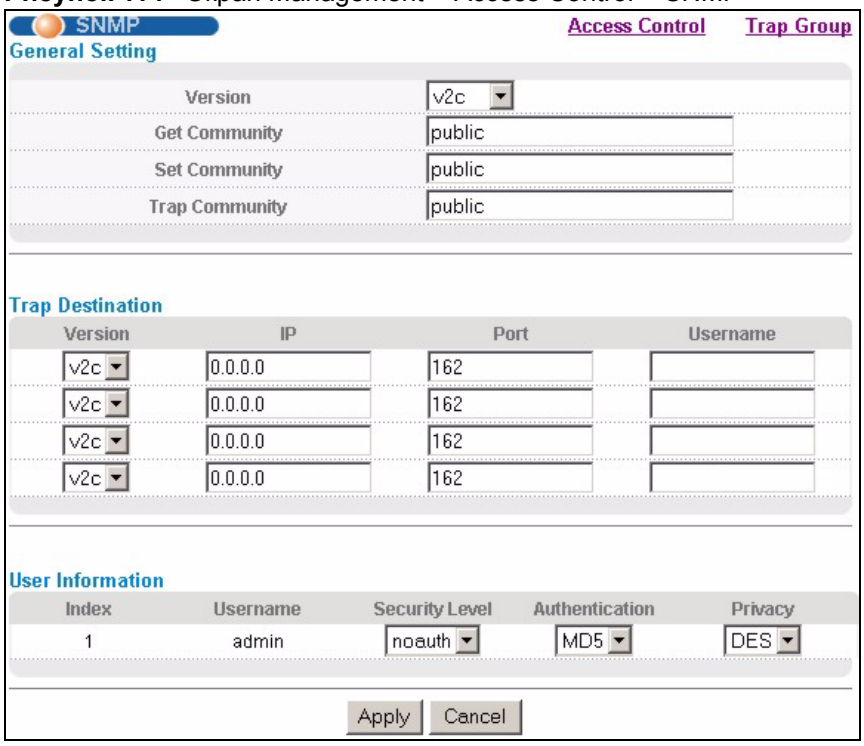
Таблица 80 Команды Trap протокола SNMP для коммутатора (Switch)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	Эта команда Trap отправляется при изменении корневого коммутатора STP.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.8.16.107.70.1 1.3.6.1.4.1.890.1.5.8.27.107.70.1	Эта команда Trap отправляется при изменении корневого коммутатора MSTP.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	Эта команда Trap отправляется при изменении топологии STP.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.16.107.70.2 1.3.6.1.4.1.890.1.5.8.27.107.70.2	Эта команда Trap отправляется при изменении топологии MSTP.
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	Эта команда Trap отправляется при использовании более 99% таблицы MAC-адресов.
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	Эта команда Trap отправляется при использовании менее 95% таблицы MAC-адресов.
rmon	RmonRisingAlarm	1.3.6.1.4.1.890.1.5.1.1.15	Эта команда Trap отправляется при выходе переменной за пределы верхнего порогового значения RMON.
	RmonFallingAlarm	1.3.6.1.4.1.890.1.5.1.1.16	Эта команда Trap отправляется при выходе переменной за пределы нижнего порогового значения RMON.

27.3.4 Настройка SNMP

Доступ к экрану **SNMP** осуществляется с экрана **Access Control**. Чтобы вернуться к экрану **Access Control**, выберите пункт **Access Control**.

Рисунок 114 Экран Management > Access Control > SNMP



Поля экрана описаны в следующей таблице.

Таблица 81 Экран Management > Access Control > SNMP

ПОЛЕ	ОПИСАНИЕ
General Setting	В данном разделе определяются версия SNMP и параметр community (пароль).
Version	Выберите версию SNMP для коммутатора. Версия SNMP, установленная на коммутаторе, должна совпадать с версией на менеджере SNMP. Выберите вариант SNMP версии 2c (**v2c**), SNMP версии 3 (**v3**) или оба этих варианта (**v3v2c**). Примечание: SNMP версии 2c обратно совместим с SNMP версии 1.
Get Community	Введите значение **Get Community** – это пароль для входящих запросов Get и GetNext от станции управления. Строка **Get Community** используется менеджерами SNMP только при выборе SNMP версии 2c и ниже.
Set Community	Введите значение **Set Community** – это пароль для входящих запросов Set от станции управления. Строка **Set Community** используется менеджерами SNMP только при выборе SNMP версии 2c и ниже.
Trap Community	Введите значение **Trap Community** – это пароль, отправляемый SNMP-менеджеру с каждой командой Trap. Строка **Trap Community** используется менеджерами SNMP только при выборе SNMP версии 2c и ниже.
Trap Destination	В данном разделе настраивается, куда должны отправляться команда Trap SNMP коммутатором.
Version	Укажите версию SNMP для отправки сообщений Trap.

Таблица 81 Экран Management > Access Control > SNMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP	Введите IP-адреса менеджеров (до 4-х), которым будут отправляться команды Trap.
Port	Введите номер порта, который прослушивается менеджером в ожидании сообщений Trap SNMP.
Username	Введите имя пользователя, отправляемое на менеджер SNMP в случае команды Trap через SNMP v3. Примечание: Данное имя пользователя должно соответствовать существующей учетной записи на коммутаторе (настраивается на экране **Management > Access Control > Logins**).
User Information	В данном разделе настраиваются пользователи для аутентификации на менеджерах при использовании SNMP v3. Примечание: Для создания учетных записей на менеджере SNMP v3 используйте имена пользователей и пароли, введенные в данном разделе.
Index	Порядковый номер (только для чтения) учетной записи на коммутаторе.
Username	В этом поле отображается имя пользователя для учетной записи на коммутаторе.
Security Level	Выберите, необходимо ли использовать аутентификацию и/или шифрование в сеансах SNMP с данным пользователем. Варианты: • **noauth** – имя пользователя используется в качестве пароля при отправке на менеджер SNMP. Это эквивалентно параметрам Get, Set и Trap Community в SNMP v2c. Наименее защищенный режим. • **auth** – для сообщений SNMP, отправляемых данным пользователем, используется механизм аутентификации. • **priv** – для сообщений SNMP, отправляемых данным пользователем, используются механизмы аутентификации и шифрования. Самый защищенный режим. Примечание: На менеджере SNMP должен быть настроен аналогичный или более высокий уровень безопасности, чем на коммутаторе.
Authentication	Выберите алгоритм аутентификации. При аутентификации данных SNMP применяются алгоритмы хэширования **MD5** (Message Digest 5) и **SHA** (Secure Hash Algorithm). Аутентификация SHA считается более стойкой по сравнению с MD5, но более медленной.
Privacy	Укажите алгоритм шифрования для обмена данными SNMP с этим пользователем. Можно выбрать один из следующих вариантов: • **DES** – стандарт Data Encryption Standard представляет собой широко распространенный (однако не очень стойкий) алгоритм шифрования данных. В этом алгоритме к каждому 64-битному блоку данных применяется 56-битный ключ. • **AES** – стандарт Advanced Encryption Standard представляет собой еще один метод шифрования с закрытым ключом. В AES к каждому 128-битному блоку данных применяется 128-битный ключ.

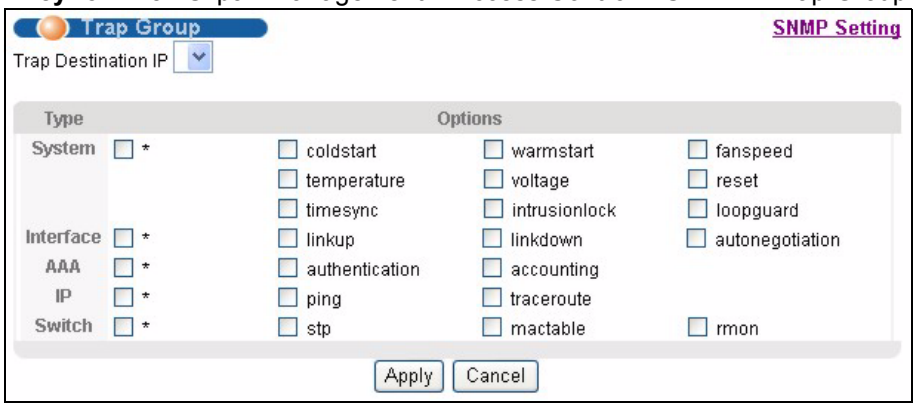
Таблица 81 Экран Management > Access Control > SNMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

27.3.5 Настройка группы «ловушек» SNMP

Чтобы отобразить показанный ниже экран, нажмите на экране **SNMP** на ссылку **Trap Group**. На экране **Trap Group** можно выбрать типы «ловушек» SNMP, которые должны отправляться на каждый из менеджеров SNMP.

Рисунок 115 Экран Management > Access Control > SNMP > Trap Group



Поля экрана описаны в следующей таблице.

Таблица 82 Экран Management > Access Control > SNMP > Trap Group

ПОЛЕ	ОПИСАНИЕ
Trap Destination IP	Выберите один из настроенных IP-адресов назначения для передачи команд Trap. Они представляют собой IP-адреса менеджеров SNMP. IP-адреса назначения должны быть предварительно настроены на экране **SNMP Setting**. Далее на этом экране настраиваются команды Trap, направляемые коммутатором на данный менеджер SNMP.
Type	Выберите категории сообщений Trap SNMP, которые будут отправляться коммутатором на данный менеджер SNMP.
Options	Выберите отдельные команды Trap SNMP, которые будут направляться коммутатором на станцию SNMP. Описания отдельных команд Trap приводятся в разд. 27.3.3 на стр. 223. Команды Trap группируются по категориям. При выборе категории автоматически выбираются все команды Trap, относящиеся к данной категории. При снятии выделения с переключателей отдельных команд Trap эти команды не будут отправляться коммутатором на станцию SNMP. Если снять выделение с переключателя категории, автоматически снимается выделение со всех переключателей отдельных команд, относящихся к данной категории (коммутатор отправляет команды Trap лишь для выбранных категорий).

Таблица 82 Экран Management > Access Control > SNMP > Trap Group (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

27.3.6 Настройка учетных записей пользователей

Доступ к коммутатору через Web-конфигуратор одновременно могут получить до пяти пользователей (один администратор и четыре обычных пользователя).

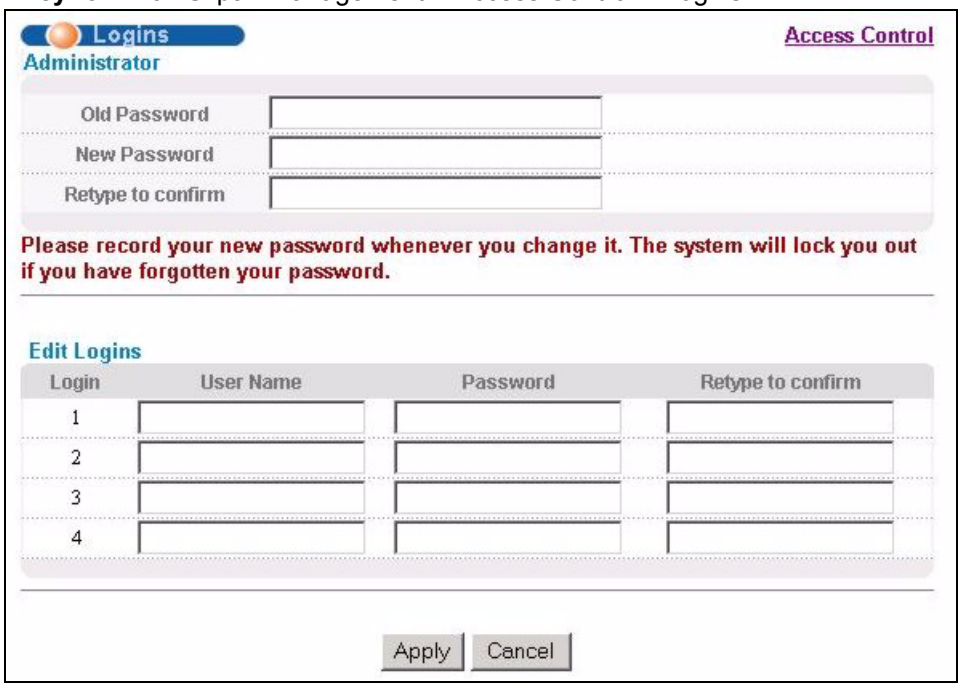
- Администратор – это пользователь, который может как просматривать, так и вносить изменения в настройки коммутатора. Имя пользователя для администратора не может быть изменено – это всегда **admin**. Пароль по умолчанию – **1234**.

Настоятельно рекомендуется изменить пароль администратора по умолчанию (**1234**).

- Обычный пользователь (не администратор, с именем, отличным от **admin**) может только просматривать, но не изменять настройки коммутатора.

Чтобы отобразить показанный ниже экран, выберите **Management > Access Control > Logins**.

Рисунок 116 Экран Management > Access Control > Logins



Поля экрана описаны в следующей таблице.

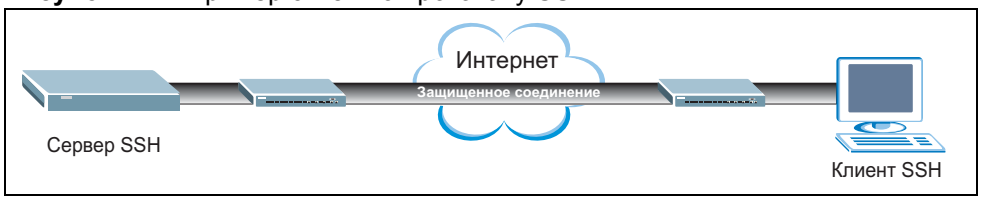
Таблица 83 Экран Management > Access Control > Logins

ПОЛЕ	ОПИСАНИЕ
Administrator Учетная запись администратора по умолчанию, с именем пользователя «admin». Имя пользователя администратора по умолчанию изменить нельзя. Только администратор имеет права чтения/записи.	
Old Password	Введите существующий системный пароль (пароль по умолчанию при поставке – **1234**).
New Password	Введите новый системный пароль.
Retype to confirm	Введите новый системный пароль еще раз для подтверждения.
Edit Logins Имеется возможность настроить до четырех пользовательских записей с паролями. Для этих пользователей устанавливается уровень привилегий 0 (базовый доступ только для чтения). Более высокие привилегии могут назначаться пользователям через интерфейс командной строки. Дополнительную информацию о назначении уровней привилегий можно найти в Справочном руководстве по интерфейсу командной строки.	
User Name	Введите имя пользователя (до 32 символов в английской раскладке).
Password	Введите новый системный пароль.
Retype to confirm	Введите новый системный пароль еще раз для подтверждения.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

27.4 Обзор протокола SSH

В отличие от протоколов Telnet или FTP, которые передают данные в обычном текстовом формате, протокол SSH (Secure Shell) является защищенным протоколом, который совмещает возможности аутентификации и шифрования для обеспечения безопасной передачи данных между двумя хостами с использованием небезопасной сети.

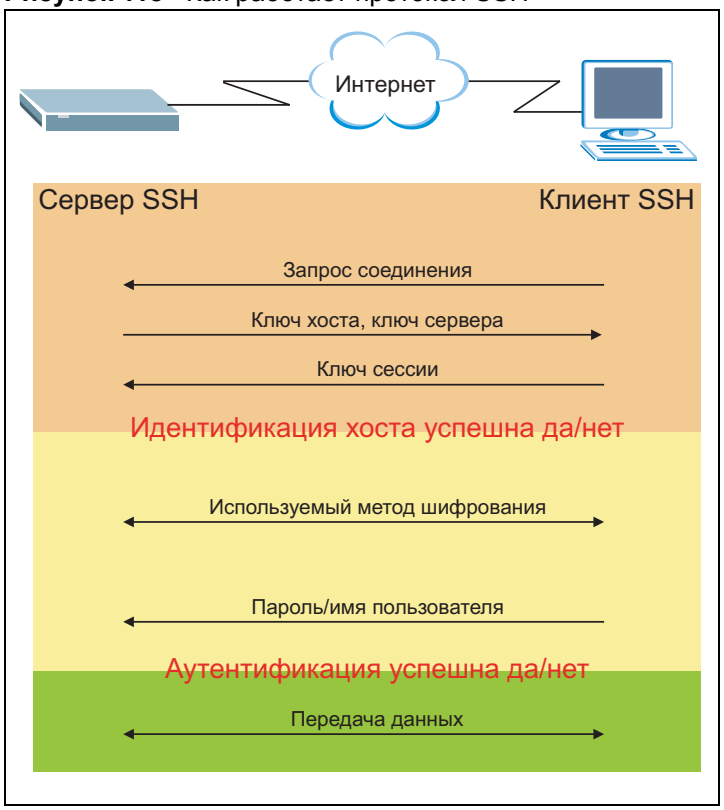
Рисунок 117 Пример связи по протоколу SSH



27.5 Как работает протокол SSH

Процесс установки защищенного соединения между двумя удаленными хостами описан в следующей таблице.

Рисунок 118 Как работает протокол SSH



1 Идентификация хоста

SSH-клиент отправляет запрос на соединение SSH-серверу. Сервер идентифицирует себя с помощью ключа хоста. Клиент шифрует случайно сгенерированный ключ сессии с помощью ключа хоста и ключа сервера, затем отправляет результат обратно на сервер.

Клиент автоматически сохраняет все новые открытые ключи сервера. При последующих подключениях открытый ключ сервера сверяется с сохраненной версией на клиентском компьютере.

2 Метод шифрования

После проверки идентификационной информации клиент и сервер должны согласовать используемый метод шифрования.

3 Аутентификация и передача данных

После проверки идентификационных данных и активации шифрования образуется защищенный туннель между клиентом и сервером. Для подключения к серверу клиент отправляет ему аутентификационную информацию (имя пользователя и пароль).

27.6 Реализация протокола SSH на коммутаторе

Данный коммутатор поддерживает протокол SSH версии 2 с использованием аутентификации по методу RSA и трех методов шифрования (DES, 3DES и Blowfish). Для удаленного управления и передачи файлов на коммутаторе реализован SSH-сервер (порт 22). Одновременно допускается только одно SSH-соединение.

27.6.1 Требования к использованию протокола SSH

Для подключения к коммутатору по протоколу SSH необходимо установить программу-клиент SSH на клиентском компьютере (с установленной операционной системой Windows или Linux).

27.7 Знакомство с протоколом HTTPS

Протокол HTTPS (протокол передачи гипертекста через протокол защищенных сокетов, или HTTP через SSL) – это Web-протокол, обеспечивающий шифрование и дешифрование Web-страниц. Протокол защищенных сокетов Secure Socket Layer (SSL) представляет собой протокол уровня приложений, реализующий безопасную передачу данных посредством обеспечения конфиденциальности (посторонние не смогут прочесть передаваемые данные), аутентификации (одна сторона может идентифицировать другую) и целостности данных (изменение данных будет заметно).

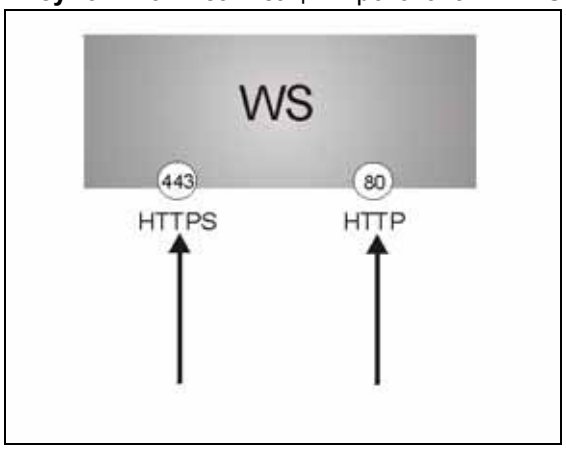
Этот протокол работает на основе сертификатов, открытых и секретных ключей.

Протокол HTTPS на коммутаторе используется для получения защищенного доступа к коммутатору через Web-конфигуратор. При запросе компьютером защищенного соединения HTTPS коммутатор отправляет на компьютер свой сертификат. Пользователь принимает решение, будет ли он доверять данному сертификату. Если пользователь решает доверять сертификату, этот сертификат используется для создания защищенного соединения HTTPS.

См. следующий рисунок.

1. Запросы на HTTPS-соединение от Web-браузера с поддержкой SSL поступают (по умолчанию) на порт 443 Web-сервера (WS) коммутатора.
2. Запросы на HTTP-соединение от Web-браузера поступают (по умолчанию) на порт 80 Web-сервера (WS) коммутатора.

Рисунок 119 Реализация протокола HTTPS



При отключении **HTTP** на экране **Service Access Control** коммутатор блокирует все попытки соединения по HTTP.

27.8 Пример подключения по протоколу HTTPS

Если порт HTTPS по умолчанию для коммутатора не менялся, введите в адресной строке браузера «https://IP-адрес коммутатора», где «IP-адрес коммутатора» – это IP-адрес или доменное имя коммутатора, к которому необходимо получить доступ.

27.8.1 Предупреждения от Internet Explorer

При попытке получить доступ к коммутатору через HTTPS-сервер появится диалоговое окно Windows с вопросом, доверяете ли вы сертификату сервера. Нажмите кнопку **View Certificate**, чтобы проверить, принадлежит ли сертификат коммутатору.

В Internet Explorer появляется следующее сообщение **Security Alert**. Нажмите **Yes**, чтобы проследовать на экран ввода имени пользователя и пароля Web-конфигуратора; Если нажать **No**, то доступ к Web-конфигуратору будет заблокирован.

Рисунок 120 Диалоговое окно Security Alert (Internet Explorer)

27.8.2 Предупреждения от Netscape Navigator

При попытке получить доступ к коммутатору через HTTPS-сервер появится сообщение **Website Certified by an Unknown Authority** с вопросом, доверяете ли вы сертификату сервера. Чтобы проверить, действительно ли сертификат принадлежит коммутатору, нажмите кнопку **Examine Certificate**.

В случае выбора варианта **Accept this certificate temporarily for this session** нажмите **OK**, чтобы продолжить работу в Netscape.

Чтобы импортировать сертификат коммутатора в SSL-клиент для постоянной работы, выберите **Accept this certificate permanently**.

Рисунок 121 Сертификат безопасности 1 (Netscape)

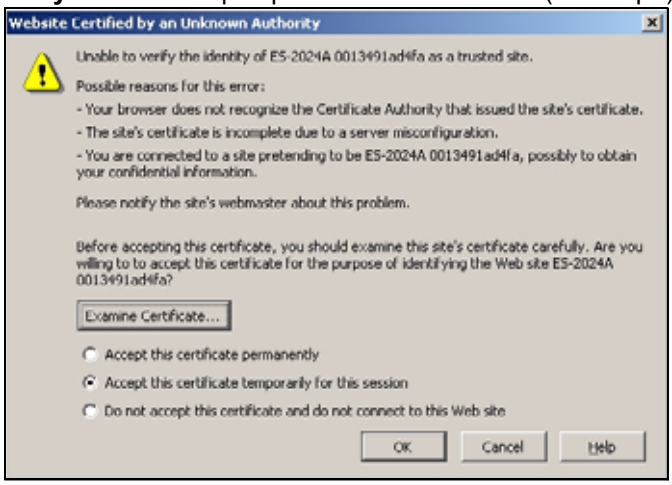
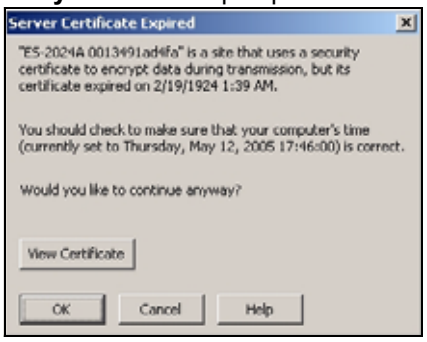


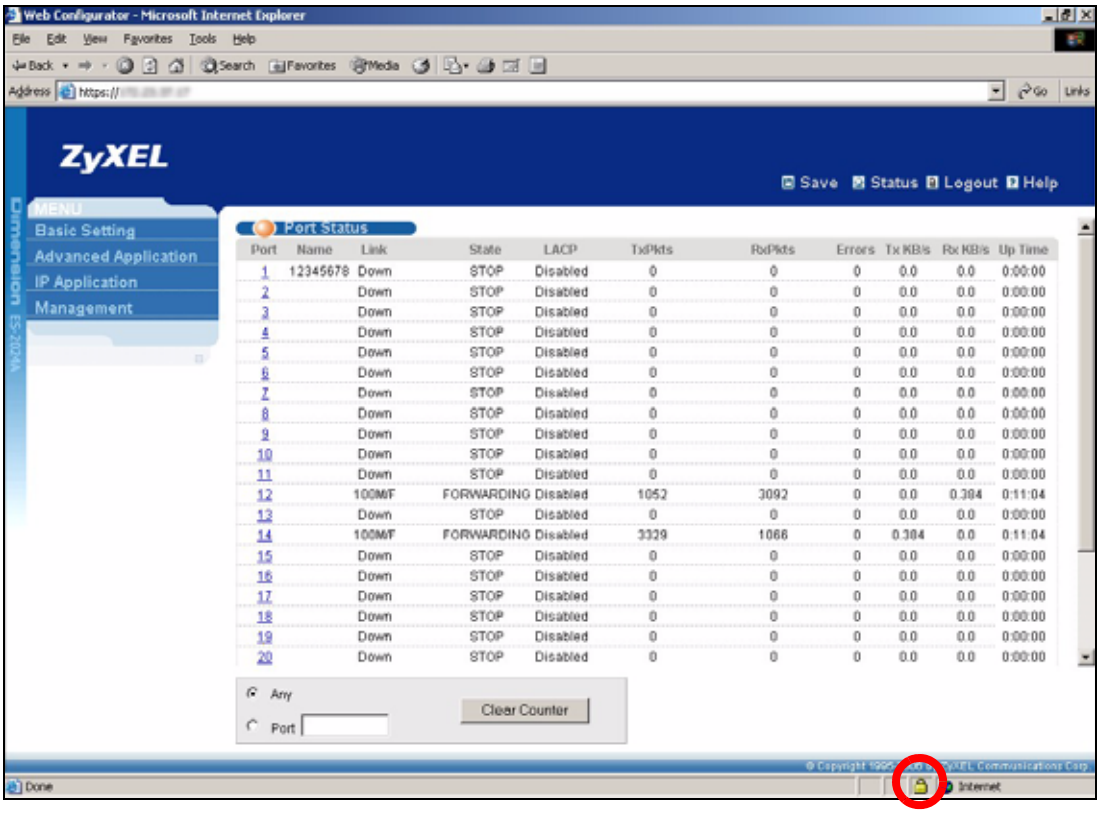
Рисунок 122 Сертификат безопасности 2 (Netscape)



27.8.3 Основной экран

После того, как был принят сертификат и введены имя пользователя и пароль, появится основной экран коммутатора. В нижней части экрана браузера появится значок замка, что свидетельствует об установлении защищенного соединения.

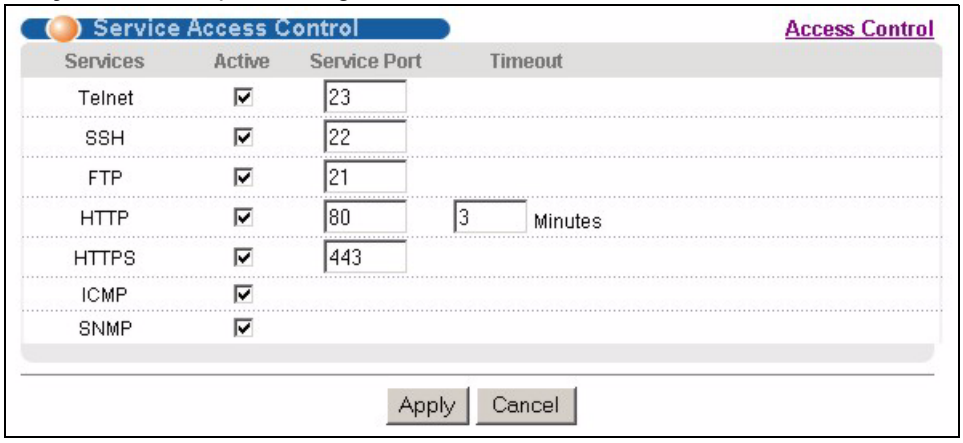
Рисунок 123 Пример: значок замка для защищенного соединения



27.9 Контроль доступа к портам служб

Контроль доступа к службам позволяет определить, каким службам разрешен доступ к коммутатору. Также имеется возможность изменить номер порта службы по умолчанию и настроить «доверенные компьютеры» для каждой службы на экране **Remote Management** (будет рассмотрен ниже). Для возврата к основному экрану **Access Control** нажмите **Access Control**.

Рисунок 124 Экран Management > Access Control > Service Access Control



Поля экрана описаны в следующей таблице.

Таблица 84 Экран Management > Access Control > Service Access Control

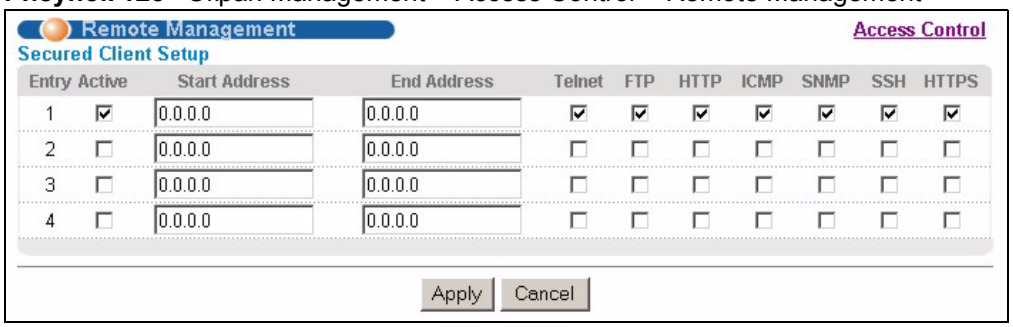
ПОЛЕ	ОПИСАНИЕ
Services	В этом столбце перечислены службы, с помощью которых можно получить доступ к коммутатору.
Active	Установите этот переключатель, чтобы разрешить соответствующей службе получать доступ к коммутатору.
Service Port	Номер порта службы по умолчанию для Telnet, SSH, FTP, HTTP или HTTPS; можно изменить посредством ввода нового номера порта в поле **Server Port**. В случае изменения номера порта по умолчанию не забудьте сообщить новый номер пользователям, которым может понадобиться эта служба.
Timeout	Укажите время простоя (1-255) сессии управления (через Web-конфигуратор), по истечении которого сессия будет прекращена по тайм-ауту. После тайм-аута необходимо будет заново ввести имя пользователя и пароль. Слишком большое значение Timeout создает угрозу безопасности.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

27.10 Удаленное управление

Находясь на экране **Access Control**, перейдите на экран **Remote Management**, показанный ниже.

Имеется возможность определить группу из одного или нескольких «доверенных компьютеров», с которых администратор может использовать службы управления коммутатором. Для возврата к экрану **Access Control** нажмите **Access Control**.

Рисунок 125 Экран Management > Access Control > Remote Management



Поля экрана описаны в следующей таблице.

Таблица 85 Экран Management > Access Control > Remote Management

ПОЛЕ	ОПИСАНИЕ
Entry	Порядковый номер клиентского набора. Клиентский набор – это группа из одного или нескольких компьютеров, с которых администратор может использовать службы управления коммутатором.
Active	Установите этот переключатель, чтобы активировать данный клиентский набор. Снимите выделение с переключателя, если необходимо временно отключить набор, не удаляя его.
Start Address End Address	Введите диапазон IP-адресов доверенных компьютеров, с которых можно управлять коммутатором. Данный коммутатор проверяет соответствие IP-адреса компьютера, запрашивающего службу или протокол, введенному здесь диапазону. Если адрес не совпадает, коммутатор немедленно разрывает сессию.
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Выберите службы, которые могут быть использованы для управления коммутатором с указанных доверенных компьютеров.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

28

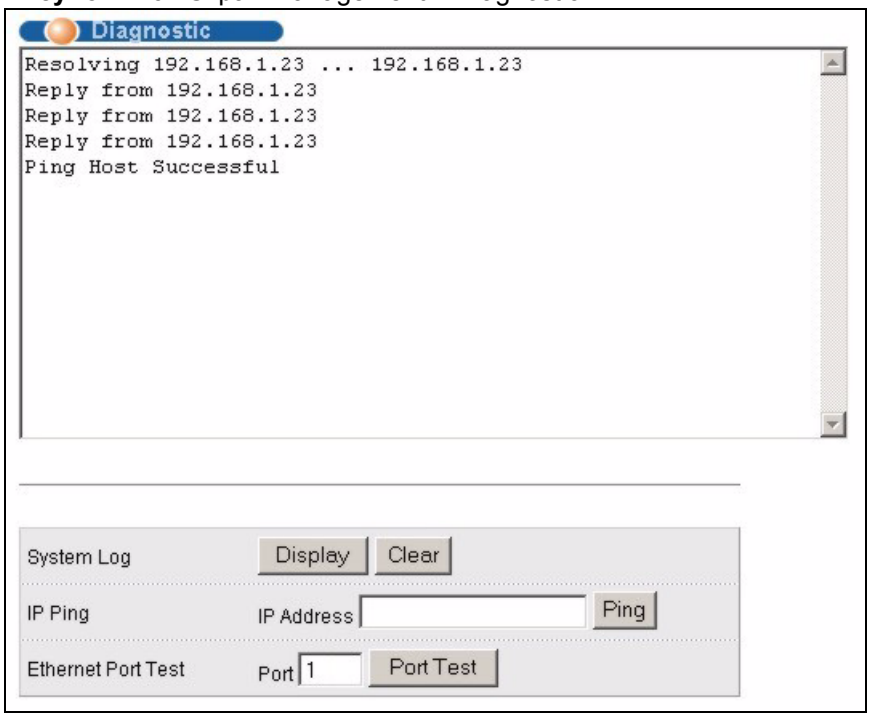
Диагностика

В данной главе описан экран диагностики **Diagnostic**.

28.1 Экран Diagnostic

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **Diagnostic**. На этом экране можно проверять системные журналы, пинговать IP-адреса и тестировать порты.

Рисунок 126 Экран Management > Diagnostic



Поля экрана описаны в следующей таблице.

Таблица 86 Экран Management > Diagnostic

ПОЛЕ	ОПИСАНИЕ
System Log	Нажмите **Display**, чтобы отобразить журнал событий в многострочном текстовом окне. Нажмите **Clear**, чтобы очистить текстовое окно и сбросить запись системного журнала.
IP Ping	Введите IP-адрес устройства, которое необходимо пропинговать для проверки соединения. Нажмите **Ping**, чтобы коммутаторпропинговал IP-адрес (введенный в поле слева).
Ethernet Port Test	Введите номер порта и нажмите **Port Test** для выполнения теста внутренней обратной петли.

29

Системный журнал Syslog

В данной главе описаны экраны системного журнала Syslog.

29.1 Обзор Syslog

С помощью протокола syslog устройства могут пересылать по IP-сети извещения о событиях серверам syslog, собирающим информацию о событиях. Устройства с поддержкой syslog позволяют генерировать сообщения syslog и отправлять их на сервер syslog.

Протокол Syslog определен в стандарте RFC 3164. RFC определяет формат пакета, содержание и относящуюся к системному журналу информацию в сообщениях syslog. Каждое сообщение syslog содержит определение категории (facility) и уровня серьезности (level). Категория syslog идентифицирует файл на сервере syslog. Более подробную информацию можно найти в документации на сервер syslog. Уровни серьезности протокола syslog описаны в следующей таблице.

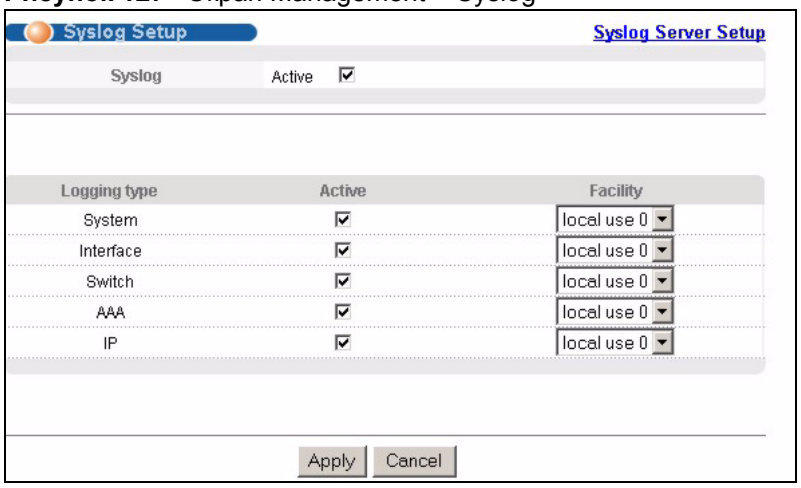
Таблица 87 Уровни серьезности Syslog

КОД	УРОВЕНЬ СЕРЬЕЗНОСТИ
0	Авария: система неработоспособна.
1	Тревога: требуются немедленные действия.
2	Критическое состояние: система находится в критическом состоянии.
3	Ошибка: обнаружена ошибка в системе.
4	Предупреждение: системой сгенерировано предупреждение.
5	Уведомление: нормальное, но важное состояние в системе.
6	Информация: информационное сообщение в журнале syslog.
7	Отладка: сообщение предназначено для отладки.

29.2 Настройка Syslog

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **Syslog**. Функция syslog позволяет передавать записи системных журналов на внешний сервер syslog. На этом экране можно настроить параметры ведения системного журнала устройства.

Рисунок 127 Экран Management > Syslog



Поля экрана описаны в следующей таблице.

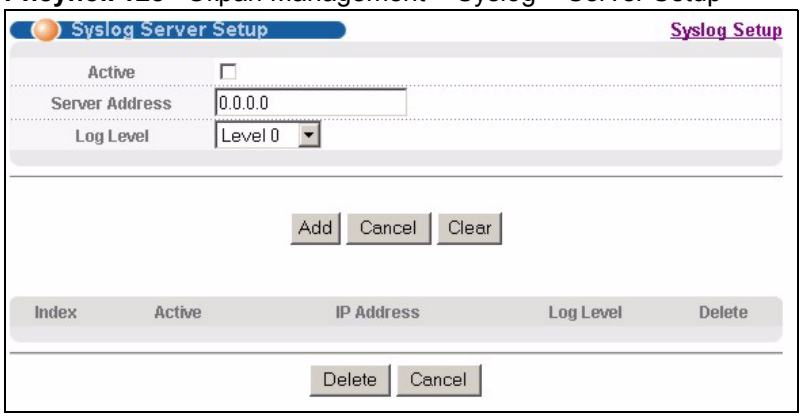
Таблица 88 Экран Management > Syslog

ПОЛЕ	ОПИСАНИЕ
Syslog	Выберите **Active**, чтобы включить syslog (ведение системного журнала) и настроить параметры syslog.
Logging Type	В данном столбце отображаются имена категорий журналов, которые могут генерироваться устройством.
Active	Установите данный переключатель, чтобы активировать на устройстве генерирование журнала соответствующей категории.
Facility	В этом поле можно выбрать категорию журнала, чтобы записывать журналы в различные файлы на сервере syslog. Более подробную информацию можно найти в документации на сервер syslog.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

29.3 Настройка сервера Syslog

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **Syslog** > **Syslog Server Setup**. На открывшемся экране можно настроить список внешних серверов syslog.

Рисунок 128 Экран Management > Syslog > Server Setup



Поля экрана описаны в следующей таблице.

Таблица 89 Экран Management > Syslog > Server Setup

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на устройстве отправку журналов на сервер syslog. Снимите выделение с переключателя, если необходимо внести запись о сервере syslog, но не отправлять на него журналы с устройства (запись можно изменить позднее).
Server Address	Введите IP-адрес сервера syslog.
Log Level	Выберите уровень серьезности для сообщений, которые будут отправляться устройством на данный сервер syslog. Меньшие номера соответствуют более важным сообщениям системного журнала.
Add	Нажмите **Add**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Порядковый номер записи сервера syslog. Нажатие на данный номер позволяет внести изменения в запись.
Active	В данном поле отображается **Yes**, если устройство отправляет журналы на сервер syslog. Значение **No** означает, что журналы на сервер syslog устройством не отправляются.
IP Address	В этом поле отображается IP-адрес сервера syslog.
Log Level	В этом поле отображается уровень серьезности для сообщений, которые отправляются устройством на данный сервер syslog.
Delete	Для удаления записи установите переключатель в столбце **Delete** этой записи и нажмите на **Delete**.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

30

Управление кластерами

В данной главе описано управление кластерами.

30.1 Обзор управления кластерами

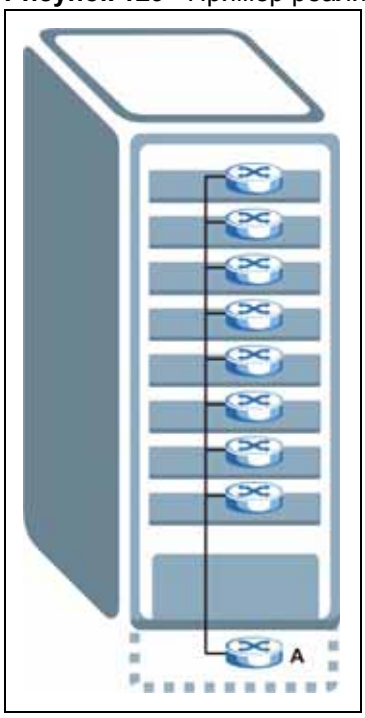
Управление кластерами позволяет управлять несколькими коммутаторами через один коммутатор, называемый менеджером кластера. Чтобы коммутаторы могли взаимодействовать друг с другом, они должны быть подключены напрямую и принадлежать к одной группе VLAN.

Таблица 90 Спецификации управления кластерами ZyXEL

Максимальное количество членов кластера	24
Модели членов кластера	Должны быть совместимы с реализацией управления кластерами ZyXEL.
Менеджер кластера	Коммутатор, с помощью которого осуществляется управление другими коммутаторами.
Члены кластера	Коммутаторы, управление которыми осуществляется через коммутатор-менеджер кластера.

В данном примере коммутатор **A**, стоящий в подвале, является менеджером кластера, а остальные коммутаторы на верхних этажах здания – членами кластера.

Рисунок 129 Пример реализации кластера

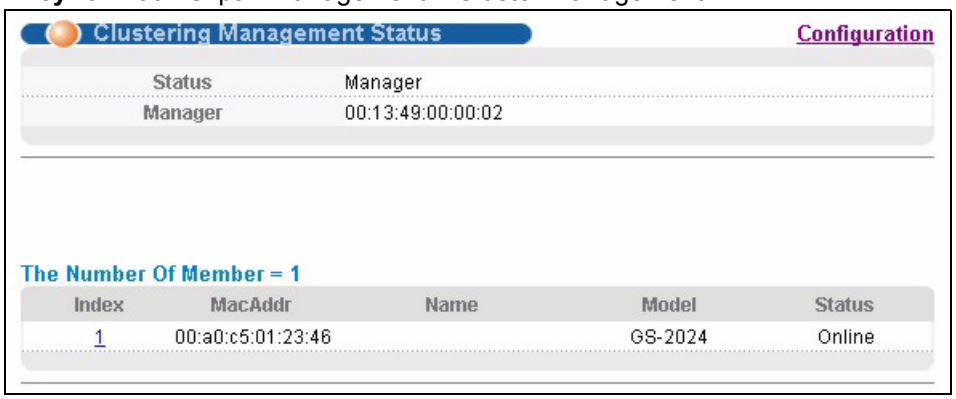


30.2 Состояние управления кластером

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **Cluster Management**.

У кластера может быть только один менеджер.

Рисунок 130 Экран Management > Cluster Management



Поля экрана описаны в следующей таблице.

Таблица 91 Экран Management > Cluster Management

ПОЛЕ	ОПИСАНИЕ
Status	В этом поле отражается роль данного коммутатора внутри кластера. **Manager** – менеджер **Member** – член (отображается, если доступ на этот экран осуществляется непосредственно через члена кластера, а не его менеджера) **None** – коммутатор не является ни менеджером, ни членом кластера
Manager	В этом поле отображается аппаратный MAC-адрес коммутатора-менеджера кластера.
The Number of Member	В этом поле отображается количество коммутаторов в данном кластере. В следующих полях описаны коммутаторы-члены кластера.
Index	Коммутаторами-членами кластера можно управлять через коммутатор-менеджер. Каждый номер в столбце **Index** – это гиперссылка на Web-конфигуратор коммутатора-члена кластера (см. рис. 131 на стр. 249).
MacAddr	В этом поле отображается аппаратный MAC-адрес коммутатора-члена кластера.
Name	Системное имя (**System Name**) члена кластера.
Model	В этом поле отображается название модели.
Status	В этом поле отображается одно из следующих состояний: **Online** (член кластера доступен) **Error** (ошибка; например, пароль доступа к коммутатору-члену кластера изменился или коммутатор стал менеджером и покинул список членов, и т.д). **Offline** (коммутатор отключен – состояние **Offline** возникает примерно через полторы минуты после того, как канал между членом кластера и менеджером разрывается)

30.2.1 Управление коммутаторами-членами кластера

Откройте экран **Clustering Management Status** на коммутаторе-менеджере кластера, затем нажмите на гиперссылку **Index** в списке членов, чтобы открыть домашнюю страницу Web-конфигуратора этого члена кластера. Домашняя страница Web-конфигуратора члена кластера отличается от домашней страницы коммутатора, доступ к которому осуществляется напрямую.

Рисунок 131 Управление кластером: экран Web-конфигуратора члена кластера

30.2.1.1 Загрузка встроенного программного обеспечения на коммутатор-член кластера

Загрузить встроенное программное обеспечение на коммутатор-член кластера через менеджер кластера можно посредством FTP, как показано на следующем примере.

Рисунок 132 Пример: загрузка встроенного программного обеспечения на коммутатор-член кластера

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 коммутатор FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.1.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 370lt0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

Некоторые параметры FTP описаны в следующей таблице.

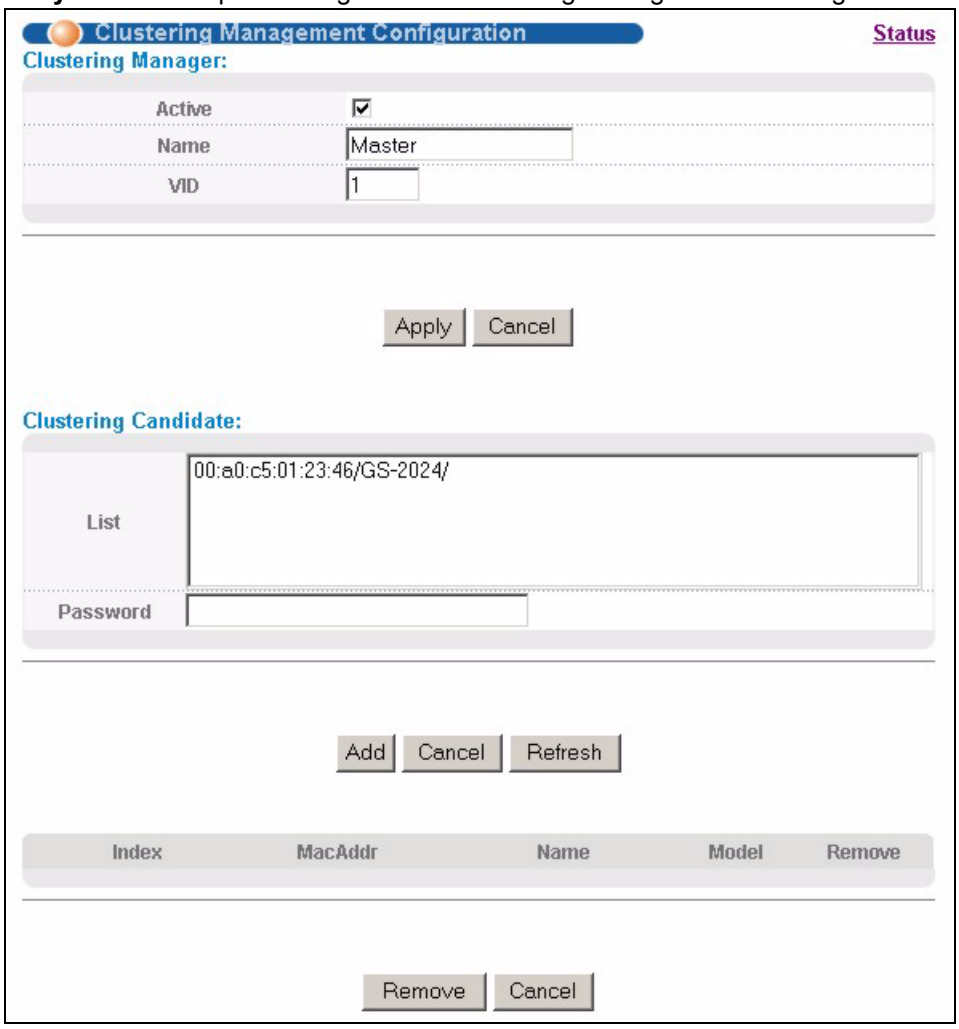
Таблица 92 Пример загрузки встроенного программного обеспечения на член кластера посредством FTP

ПАРАМЕТР FTP	ОПИСАНИЕ
`User`	Введите «admin».
`Password`	Пароль Web-конфигуратора по умолчанию – «1234».
`ls`	Введите эту команду, чтобы вывести на экран имена файлов встроенного программного обеспечения и конфигурации коммутатора-члена кластера.
`360lt0.bin`	Имя файла встроенного программного обеспечения, который загружается на коммутатор-член кластера.
`fw-00-a0-c5-01-23-46`	Имя файла встроенного программного обеспечения члена кластера в том виде, в котором его воспринимает менеджер кластера.
`config-00-a0-c5-01-23-46`	Имя файла конфигурации члена кластера в том виде, в котором его воспринимает менеджер кластера.

30.3 Настройка управления кластерами

Данный экран используется для настройки управления кластерами. Чтобы отобразить показанный ниже экран, выберите **Configuration** на экране **Cluster Management**.

Рисунок 133 Экран Management > Clustering Management > Configuration



Поля экрана описаны в следующей таблице.

Таблица 93 Экран Management > Clustering Management > Configuration

ПОЛЕ	ОПИСАНИЕ
Clustering Manager	
Active	Установите переключатель **Active**, чтобы этот коммутатор стал менеджером кластера. У кластера может быть только один менеджер. Остальные (подключенные напрямую) коммутаторы, назначенные менеджерами кластера, не будут отображаться в списке **Clustering Candidates**. Если коммутатор ранее был членом кластера, а затем был назначен менеджером кластера, то его состояние **Status** на экране **Cluster Management Status** может отображаться как **Error** («Ошибка»), а в соответствующей строке в итоговом списке членов кластера появится значок предупреждения (⚠).

Таблица 93 Экран Management > Clustering Management > Configuration (продолжение)

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя, по которому можно будет идентифицировать менеджер кластера (**Clustering Manager**). Можно использовать до 32 отображаемых символов (пробелы допускаются).
VID	Идентификатор VLAN, и он доступен только в том случае, если коммутатором используются виртуальные локальные сети типа **802.1Q**. Коммутаторы, принадлежащие к одному кластеру, должны быть подключены напрямую и принадлежать к одной группе VLAN. Коммутаторы, которые не принадлежат к одной группе VLAN, не будут отображаться в списке **Clustering Candidates**. Если на коммутаторе-менеджере кластера (**Clustering Manager**) используются виртуальные локальные сети на основе портов (**Port-based**), данное поле будет не активно.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Clustering Candidate	Следующие поля относятся к коммутаторам, являющимся потенциальными членами кластера.
List	Здесь отображается список подходящих кандидатов в члены кластера, обнаруженных автоматически. Коммутаторы должны быть соединены напрямую. Напрямую подключенные коммутаторы, назначенные менеджерами кластера, в списке **Clustering Candidate** отображаться не будут. Коммутаторы, которые не принадлежат к одной группе управления VLAN, в списке **Clustering Candidates** также отображаться не будут.
Password	Пароль каждого члена кластера – это пароль его Web-конфигуратора. Выберите член кластера в списке **Clustering Candidate** и введите пароль его Web-конфигуратора. Если после этого администратор того коммутатора изменит пароль Web-конфигуратора, то управлять коммутатором с менеджера кластера станет невозможно. В этом случае его состояние **Status** на экране **Cluster Management Status** будет отображаться как **Error** («Ошибка»), а в соответствующей строке в итоговом списке членов кластера появится значок предупреждения (⚠). Если у нескольких устройств одинаковый пароль, то их можно выбрать, удерживая нажатой клавишу [SHIFT]. Затем введите их общий пароль Web-конфигуратора.
Add	Нажмите **Add**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Refresh	Нажмите кнопку **Refresh**, чтобы провести поиск потенциальных кандидатов в члены кластера еще раз.
В следующей итоговой таблице отображается информация о настроенных членах кластера.	
Index	Порядковый номер коммутатора-члена кластера.
MacAddr	В этом поле отображается аппаратный MAC-адрес коммутатора-члена кластера.
Name	Системное имя (**System Name**) члена кластера.
Model	Название модели коммутатора-члена кластера.

Таблица 93 Экран Management > Clustering Management > Configuration (продолжение)

ПОЛЕ	ОПИСАНИЕ
Remove	Установите этот переключатель и нажмите кнопку **Remove**, чтобы удалить коммутатор-член из кластера.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

31

Таблица MAC-адресов

В данной главе описан экран настройки таблицы MAC-адресов **MAC Table**.

31.1 Обзор таблицы MAC-адресов

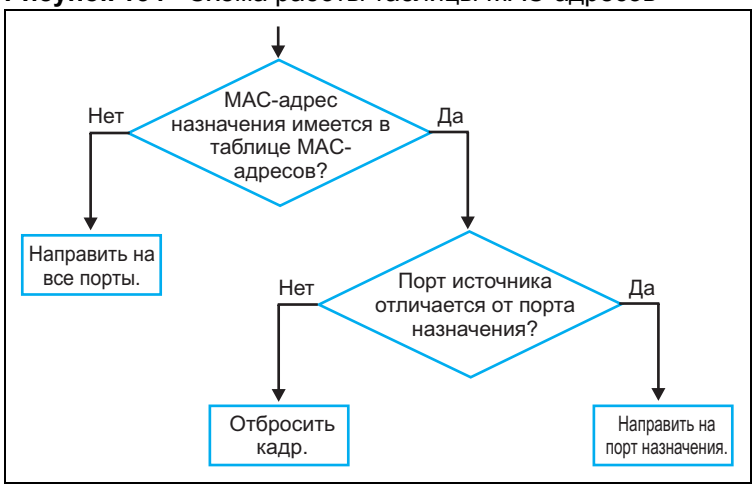
На экране настройки таблицы MAC-адресов **MAC Table** (которую еще называют базой данных фильтрации) можно увидеть, каким образом кадры пересылаются или фильтруются на портах коммутатора. На этом экране отображается, на какой порт(ы) передается MAC-адрес какого устройства, принадлежащего к какой из групп VLAN (если они определены), и является ли MAC-адрес динамическим (полученным коммутатором) или статическим (введенным вручную на экране настроек **Static MAC Forwarding**).

Чтобы определить, куда направлять кадры, коммутатор пользуется таблицей MAC-адресов. См. следующий рисунок.

1. Данный коммутатор изучает полученный кадр и запоминает порт, на который пришел этот MAC-адрес источника.
2. Затем коммутатор проверяет, соответствует ли MAC-адрес назначения этого кадра MAC-адресу источника, уже имеющемуся в таблице MAC-адресов.

- Если коммутатору уже известен порт для этого MAC-адреса, то он направляет кадр на этот порт.
- Если коммутатору еще не известен порт для этого MAC-адреса, то кадр направляется на все порты сразу. Если таким образом направляется слишком много кадров, то происходит перегрузка сети.
- Если коммутатору уже известен порт для MAC-адреса, и порт назначения совпадает с портом источника, то этот кадр отбрасывается.

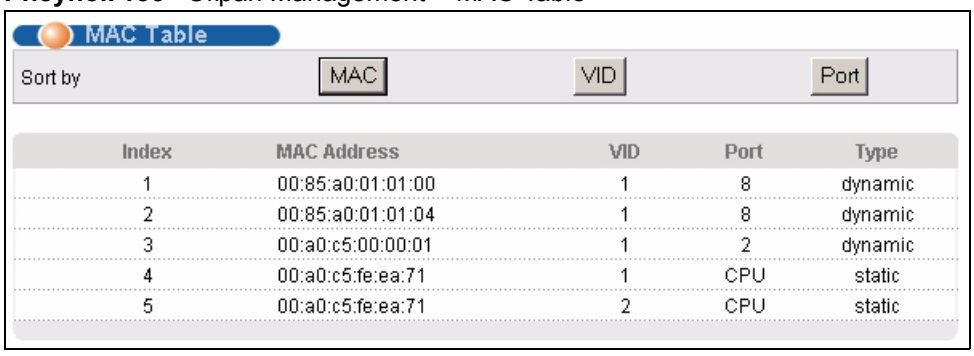
Рисунок 134 Схема работы таблицы MAC-адресов



31.2 Просмотр таблицы MAC-адресов

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **MAC Table**.

Рисунок 135 Экран Management > MAC Table



Поля экрана описаны в следующей таблице.

Таблица 94 Экран Management > MAC Table

ПОЛЕ	ОПИСАНИЕ
Sort by	Нажмите на одну из кнопок, чтобы отобразить и отсортировать данные по одному из параметров. После этого информация отображается в итоговой таблице ниже.
MAC	Нажмите эту кнопку, чтобы отсортировать данные по MAC-адресу.
VID	Нажмите эту кнопку, чтобы отсортировать данные по группе VLAN.
Port	Нажмите эту кнопку, чтобы отсортировать данные по номеру порта.
Index	Порядковый номер входящего кадра.
MAC Address	MAC-адрес устройства, с которого прибыл входящий кадр.
VID	Группа VLAN, к которой принадлежит данный кадр.

Таблица 94 Экран Management > MAC Table (продолжение)

ПОЛЕ	ОПИСАНИЕ
Port	Номер порта, с которого был получен указанный выше MAC-адрес.
Type	В этом поле отображается тип MAC-адреса – **dynamic** (динамический, то есть полученный коммутатором) или **static** (статический, то есть внесенный вручную на экране **Static MAC Forwarding**).

32

Таблица ARP

В данной главе описана таблица протокола разрешения адресов (ARP).

32.1 Обзор таблицы ARP

Протокол разрешения адресов (ARP) – это протокол, предназначенный для определения соответствия между IP-адресом и физическим адресом машины, также известным как адрес управления доступом к среде, или MAC-адрес, в локальной сети.

Длина IP-адреса (версии 4) составляет 32 бита. В локальной сети Ethernet длина MAC-адреса составляет 48 бит. Таблица протокола ARP определяет соответствие между каждым MAC-адресом и соответствующим ему IP-адресом.

32.1.1 Как работает протокол ARP

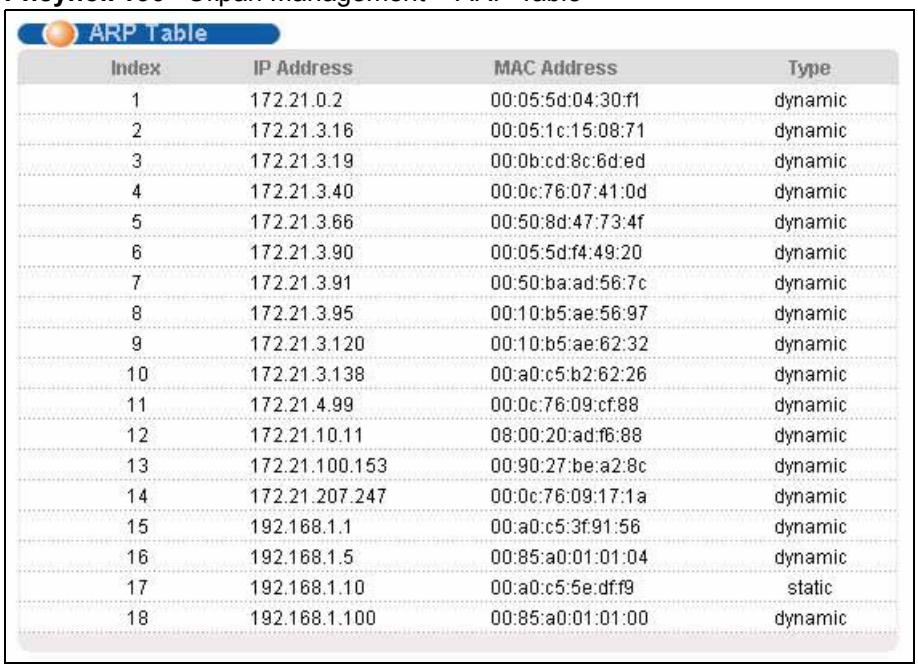
Когда входящий пакет, предназначенный для хост-устройства в локальной сети, прибывает на коммутатор, программа протокола ARP на коммутаторе ищет его в таблице ARP и, если адрес обнаружен, отправляет пакет на устройство.

Если для IP-адреса не найдено записи, протокол ARP направляет широковещательный запрос всем устройствам в локальной сети. Данный коммутатор заполняет поля его собственных MAC-адреса и IP-адреса в адресе отправителя, а затем вносит известный IP-адрес получателя в соответствующем поле. Кроме того, коммутатор заполняет единицами поле MAC-адреса пункта назначения (FF.FF.FF.FF.FF.FF – адрес для широковещательных сообщений в сети Ethernet). Отвечающее устройство (устройство с искомым IP-адресом или маршрутизатор, которому известен путь к нему) заменяет широковещательный адрес на свой MAC-адрес, меняет местами пары отправитель-получатель и отправляет одноадресный ответ непосредственно машине, приславшей запрос. Протокол ARP обновляет таблицу ARP для дальнейших обращений и затем отправляет пакет на ответивший MAC-адрес.

32.2 Просмотр таблицы ARP

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **ARP Table**. Таблица ARP используется для просмотра соответствия между IP-адресами и MAC-адресами.

Рисунок 136 Экран Management > ARP Table



ARP Table

Index	IP Address	MAC Address	Type
1	172.21.0.2	00:05:5d:04:30:f1	dynamic
2	172.21.3.16	00:05:1c:15:08:71	dynamic
3	172.21.3.19	00:0b:cd:8c:6d:ed	dynamic
4	172.21.3.40	00:0c:76:07:41:0d	dynamic
5	172.21.3.66	00:50:8d:47:73:4f	dynamic
6	172.21.3.90	00:05:5d:f4:49:20	dynamic
7	172.21.3.91	00:50:ba:ad:56:7c	dynamic
8	172.21.3.95	00:10:b5:ae:56:97	dynamic
9	172.21.3.120	00:10:b5:ae:62:32	dynamic
10	172.21.3.138	00:a0:c5:b2:62:26	dynamic
11	172.21.4.99	00:0c:76:09:cf:88	dynamic
12	172.21.10.11	08:00:20:ad:f6:88	dynamic
13	172.21.100.153	00:90:27:be:a2:8c	dynamic
14	172.21.207.247	00:0c:76:09:17:1a	dynamic
15	192.168.1.1	00:a0:c5:3f:91:56	dynamic
16	192.168.1.5	00:85:a0:01:01:04	dynamic
17	192.168.1.10	00:a0:c5:5e:df:f9	static
18	192.168.1.100	00:85:a0:01:01:00	dynamic

Поля экрана описаны в следующей таблице.

Таблица 95 Экран Management > ARP Table

ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер записи в таблице ARP.
IP Address	IP-адрес, полученный от устройства, подключенного к порту коммутатора, с соответствующим ему MAC-адресом.
MAC Address	MAC-адрес устройства с соответствующим ему IP-адресом.
Type	В этом поле отображается тип MAC-адреса – **dynamic** (динамический, то есть полученный коммутатором) или **static** (статический, то есть внесенный вручную на экране **Static MAC Forwarding**).

33

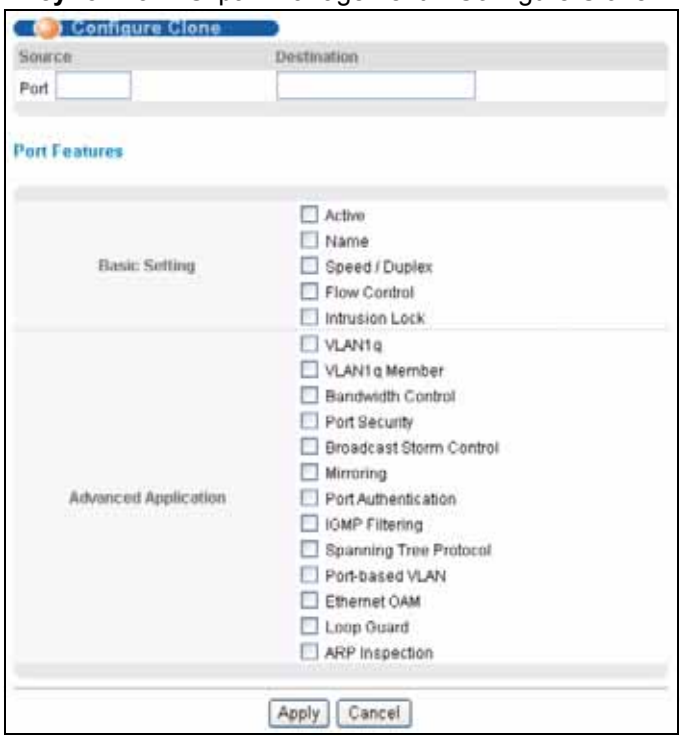
Настройка клонирования

В данной главе описывается возможность копирования настроек одного порта на другие порты.

33.1 Настройка клонирования

С помощью клонирования можно скопировать основные и расширенные настройки порта-источника на один или несколько портов назначения. Чтобы отобразить показанный ниже экран, нажмите **Management** > **Configure Clone**.

Рисунок 137 Экран Management > Configure Clone



Поля экрана описаны в следующей таблице.

Таблица 96 Экран Management > Configure Clone

ПОЛЕ	ОПИСАНИЕ
Source/ Destination Port	Введите номер порта-источника в поле **Source**. Параметры этого порта будут копироваться. Введите порты или порты назначения в поле **Destination**. На эти порты будут скопированы параметры порта-источника. Можно ввести несколько номеров портов через запятую, либо диапазон портов через дефис. Пример: • **2, 4, 6** – в качестве портов назначения используются порты 2, 4 и 6. • **2-6** – в качестве портов назначения используются порты со 2 по 6.
Basic Setting	Выберите настройки порта (установленные на экранах основных настроек **Basic Setting**), которые должны быть скопированы на порты назначения.
Advanced Application	Выберите настройки порта (установленные на экранах расширенных приложений **Advanced Application**), которые должны быть скопированы на порты назначения.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

Часть VI Приложения и индекс

A

Характеристики продукта

Характеристики аппаратного обеспечения и встроенного программного обеспечения коммутатора описаны в приведенных ниже таблицах.

Таблица 97 Характеристики аппаратного обеспечения

СПЕЦИФИКАЦИЯ	ОПИСАНИЕ
Габариты	Возможность установки в стандартную 19-дюймовую стойку ES-2024A: 438 мм (ширина) x 173 мм (глубина) x 44,5 mm (высота) ES-2024PWR: 438 мм (ширина) x 270 мм (глубина) x 44,5 mm (высота)
Вес	ES-2024A: 2,2 кг ES-2024PWR: 4,0 кг
Источник питания	100-240 В перем. тока, 50/60 Гц ES-2024A: 0,4 A ES-2024PWR: 2 A
Потребляемая мощность	ES-2024A: 24 Вт ES-2024PWR: 200 Вт
Условия эксплуатации	Температура: 0є C ~ 45є C (32є F ~ 113є F) Влажность: 10 ~ 90% (без конденсации)
Условия хранения	Температура: -25є C ~ 70є C (13є F ~ 158є F) Влажность: 10 ~ 90% (без конденсации)
Порты Fast Ethernet	24 порта 100Base-Tx Разъем RJ-45 для кабеля Ethernet Автосогласование Автоматический выбор режима MDI/MDI-X Совместимость со стандартом 802.3/802.3u Управление потоком методом обратного давления для полудуплексного режима Управление потоком согласно 802.3x для дуплексного режима (только в ES-2024PWR) Питание по витой паре 24 портов PoE (макс. 15,4 Вт/порт, 185 Вт/систему) Управление бюджетом мощности
Порты Gigabit Ethernet	2 совмещенных интерфейса (1000Base-T и SFP) Поддержка только дуплексного режима 100/1000 Мбит/с Соответствие стандартам 802.3z/802.3ab Автоматический выбор интерфейса витой пары/оптоволокна при обнаружении сигнала (приоритет у оптоволоконного порта)

Таблица 97 Характеристики аппаратного обеспечения (продолжение)

СПЕЦИФИКАЦИЯ	ОПИСАНИЕ
Консольный порт	9-пиновый разъем D-Sub типа «мама» (DCE)
Мониторинг системы	Напряжение: 1,25 В: +/- 6% 1,8 В: +/- 6% 3,3 В: +/- 6% 2,5 В: +/- 6% Температура: CPU: 60 градусов C MAC: 60 градусов C Скорость вентилятора: 3500~8000 об/мин

Таблица 98 Описание функций

ХАРАКТЕРИСТИКИ	ОПИСАНИЕ
Виртуальные локальные сети (VLAN)	Виртуальные локальные сети (VLAN) позволяют разделить одну физическую сеть на несколько логических. Устройства в логической сети принадлежат к одной группе. Устройство может принадлежать к нескольким группам. При использовании сетей VLAN устройство не может отправлять или принимать данные от устройств, не принадлежащих к той же группе (группам); такой трафик должен проходить через маршрутизатор.
Фильтр MAC-адресов	Фильтрация трафика на основе MAC-адреса источника и/или назначения и группы VLAN (идентификатора).
DHCP (Протокол динамической конфигурации хоста)	С помощью данной функции можно ретранслировать запросы DHCP к серверам DHCP в сети.
Отслеживание многоадресного трафика IGMP	Данный коммутатор поддерживает функцию отслеживания многоадресного трафика IGMP, благодаря которой мультивещательный трафик направляется только на порты, принадлежащие к определенной группе; это позволяет значительно снизить объем многоадресного трафика, проходящего через коммутатор.
Дифференцированное обслуживание (DiffServ)	При использовании механизма DiffServ коммутатор помечает пакеты, чтобы на сетевых устройствах с поддержкой DiffServ по пути следования они подвергались особой обработке в зависимости от типов приложений и плотности трафика.
Организация очередей	Организация очередей помогает решить проблему снижения производительности в случаях перегрузки сети. Поддерживаются три алгоритма организации очередей: строгая очередь приоритетов (Strict Priority Queuing, SPQ) и взвешенное циклическое обслуживание (Weighted Round Robin, WRR). Это позволяет коммутатору поддерживать раздельные очереди для пакетов от каждого отдельного источника или потока, а также предотвращать захват всей пропускной способности одним источником.
Зеркальное копирование портов	Зеркальное копирование портов позволяет копировать трафик, поступающий из одного порта или со всех портов на другой порт или на все порты, чтобы можно было анализировать трафик на зеркальном порту (том, на который копируется трафик), не вмешиваясь в поток.
Статические маршруты	Статические маршруты указывают коммутатору, куда следует направлять IP-трафик при ручной настройке параметров протокола TCP/IP.

Таблица 98 Описание функций (продолжение)

ХАРАКТЕРИСТИКИ	ОПИСАНИЕ
Регистрация VLAN-сети мультивещания (MVR)	Механизм регистрации VLAN-сети мультивещания (Multicast VLAN Registration, MVR) предназначен для случаев, когда требуется передавать мультивещательный трафик в масштабе всей сети (например, для приложений «мультимедиа по требованию» – MoD). MVR позволяет определить одну VLAN-сеть мультивещания, которая будет доступна различным абонентским сетям VLAN в сети. Благодаря этому обеспечивается оптимальное использование пропускной способности за счет предотвращения дублирования мультивещательного трафика в абонентских сетях VLAN, а также упрощается управление группами мультивещания.
Протокол покрывающего дерева (STP) / быстрый протокол покрывающего дерева (RSTP) / протокол нескольких экземпляров покрывающего дерева (MSTP)	Протокол (R)STP обнаруживает и разрывает сетевые петли и обеспечивает наличие запасных каналов между коммутаторами, мостами или маршрутизаторами. Он позволяет коммутатору взаимодействовать с другими устройствами, поддерживающими протокол (R)STP, благодаря чему достигается наличие только одного пути между любыми двумя станциями в сети. Данный коммутатор также позволяет настроить несколько конфигураций STP (несколько деревьев). После этого порты могут быть отнесены к различным деревьям.
Защита от образования петель	Функция защиты от образования петель позволяет предотвратить образование петель на границе сети.
Защита от подмены IP-адресов	Функция защиты от подмены IP-адресов позволяет отфильтровывать несанкционированные пакеты ARP в сети.
Агрегация каналов	Агрегация (группирование) каналов – это объединение нескольких физических портов в один логический канал большей пропускной способности. Объединить несколько портов в один канал можно в том случае, если, например, дешевле использовать несколько каналов меньшей скорости, чем не на полную мощность загружать высокоскоростной, но более дорогой канал с одним портом.
Аутентификация и средства безопасности портов	Для обеспечения безопасности в коммутаторе предусмотрена аутентификация по стандарту IEEE 802.1x с использованием внешнего RADIUS-сервера и средства безопасности портов, которые пропускают через порты коммутатора только пакеты с динамически полученными MAC-адресами и/или настроенными статическими MAC-адресами.
Аутентификация и учет	Данный коммутатор поддерживает службы аутентификации и учета на серверах RADIUS и TACACS+.
Управление устройством	С помощью Web-конфигуратора и команд можно легко настроить широкий спектр поддерживаемых коммутатором функций.
Клонирование порта	Функция клонирования порта позволяет скопировать настройки одного порта на один или несколько других портов.
Системный журнал Syslog	Данный коммутатор может генерировать сообщения syslog и отправлять их на сервер syslog.
Обновление встроенного программного обеспечения	Новые версии встроенного программного обеспечения можно получать (по мере выпуска) с сайта ZyXEL и загружать в коммутатор с использованием Web-конфигуратора, интерфейса командной строки или инструмента FTP/TFTP. Примечание: Загружайте только то встроенное программное обеспечение, которое предназначено конкретно для вашей модели!

Таблица 98 Описание функций (продолжение)

ХАРАКТЕРИСТИКИ	ОПИСАНИЕ
Резервное копирование и восстановление конфигурации	Данный коммутатор поддерживает создание резервных копий конфигурации, которые могут быть загружены в коммутатор при необходимости возврата к более ранней версии.
Управление кластерами	Управление кластерами (известная также как технология iStacking) позволяет управлять несколькими коммутаторами через один коммутатор, который называется менеджером кластера. Чтобы коммутаторы могли взаимодействовать друг с другом, они должны быть подключены напрямую и принадлежать к одной группе VLAN.

Таблица 99 Характеристики встроенного программного обеспечения

ХАРАКТЕРИСТИКИ	СПЕЦИФИКАЦИИ
IP-адрес по умолчанию	192.168.1.1
Количество настраиваемых IP-адресов	64
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Имя пользователя для администратора	admin
Пароль по умолчанию	1234
Количество учетных записей, настраиваемых на коммутаторе	На коммутаторе настраивается 4 учетных записи для управления. Также поддерживается аутентификация через RADIUS и TACACS+.
Мостовая конфигурация	8 тыс. MAC-адресов (2-канальная ассоциативность) Пересылка на основе статических MAC-адресов (256 записей) Контроль широковещательных штормов на уровне порта Автоматическое получение и устаревание адресов Время устаревания от 10 до 3000 секунд, по умолчанию 300 секунд
Коммутация	8,8 Гбит/с, без блокирования Максимальный размер кадра: 1522 байт включая тег/CRC-код С промежуточной буферизацией (Store and forward)
Управление качеством обслуживания (QoS)	802.1p Четыре очереди приоритетов с поддержкой механизмов строгой очереди/взвешенного циклического обслуживания Управление скоростью на уровне отдельного порта с шагом 64 кбит/с как для входящего, так и для исходящего трафика Отслеживание многоадресного трафика IGMP Отображение маркеров DSCP на приоритеты 802.1p
Мультивещание	Отслеживание многоадресного трафика IGMP на уровне VLAN (IGMPv1/v2/v3, до 16 VLAN, настраивается пользователем), до 256 групп Фильтрация IGMP MVR Настраиваемые таймеры и приоритеты отслеживания многоадресного трафика IGMP
IP-службы	Ретрансляция DHCP
Покрывающее дерево	Быстрый протокол покрывающего дерева 802.1w 802.1s MSTP

Таблица 99 Характеристики встроенного программного обеспечения (продолжение)

ХАРАКТЕРИСТИКИ	СПЕЦИФИКАЦИИ
Виртуальные локальные сети (VLAN)	VLAN на основе портов VLAN на базе 802.1Q Максимальное число VLAN: 4 тыс., 256 статических VLAN GVRP для динамической регистрации групп Фильтрация входящих кадров VLAN Возможность приема только кадров с тегами или всех кадров
Безопасность	Пересылка на основе статических MAC-адресов Фильтрация на основе статических MAC-адресов Блокирование пересылки неразрешенных адресов/средства безопасности портов Ограничение количества динамических адресов на порт Аутентификация порта согласно 802.1x через RADIUS Вход в систему для управления с аутентификацией через RADIUS. SSHv1/v2 SSL Преобразование динамической таблицы MAC-адресов в статическую (MAC freeze) Защита от вторжений Несколько серверов RADIUS Несколько серверов TACACS+ Назначение VLAN и пропускной способности через 802.1X Вход в систему с аутентификацией через RADIUS Вход в систему с аутентификацией через TACACS+ Защита от подмены IP-адресов Статическая привязка IP-/MAC-адреса Инспекция ARP-пакетов
Учет	Учет с использованием RADIUS Учет с использованием TACACS+
Агрегация портов	2 группы для Fast Ethernet, 1 группа для Gigabit Ethernet 4 порта на группу, выбираемых произвольным образом (100BaseTX) Поддержка статического и динамического (LACP) группирования портов на основе 802.3ad
Зеркальное копирование портов	Зеркальное копирование трафика отдельного порта на порт мониторинга
Управление пропускной способностью	Ограничение скорости входящего трафика с шагом 64 кбит/с Ограничение скорости исходящего трафика с шагом 64 кбит/с

Таблица 99 Характеристики встроенного программного обеспечения (продолжение)

ХАРАКТЕРИСТИКИ	СПЕЦИФИКАЦИИ
Кластеризация	Поддержка роли главного или подчиненного коммутатора кластера Управление максимум 24 подчиненными коммутаторами в кластере
Системное управление	Настройка с консоли/через telnet/web Обновление встроенного программного обеспечения через FTP/web/консольный порт Резервное копирование и восстановление конфигурации через FTP/web/консольный порт Контроль доступа к функциям системного управления Системные часты с настройкой вручную или через NTP SNMP v2c / v3 Telnet (до 9 одновременных сессий) Группы RMON 1, 2, 3, 9 Эхо-запросы/ответы ICMP Аналогичные Cisco команды интерфейса командной строки Текстовые файлы конфигурации Управление пользователями администраторами Системный журнал Syslog Поддержка летнего времени 802.3ah OAM Защита от образования петель

Поддерживаемые коммутатором стандарты приводятся в следующем списке (который не является исчерпывающим).

Таблица 100 Поддерживаемые стандарты

СТАНДАРТ	ОПИСАНИЕ
RFC 826	Протокол разрешения адресов (ARP)
RFC 867	Протокол времени суток
RFC 868	Протокол службы времени
RFC 894	Инкапсуляция Ethernet II
RFC 1112	Межсетевой протокол управления группами IGMP v1
RFC 1155	SMI
RFC 1157	SNMPv1: простой протокол сетевого управления версии 1
RFC 1213	SNMP MIB II
RFC 1305	Протокол сетевого времени (NTP версии 3)
RFC 1441	SNMPv2: простой протокол сетевого управления версии 2
RFC 1493	Bridge MIB
RFC 1643	Ethernet MIB
RFC 1757	RMON
RFC 1901	SNMPv2c: простой протокол сетевого управления версии 2c
RFC 2131, RFC 2132	Протокол динамической конфигурации хоста (DHCP)
RFC 2138	Служба RADIUS (Remote Authentication Dial In User Service)
RFC 2139	Учет с использованием RADIUS
RFC 2236	Межсетевой протокол управления группами IGMP версия 2

Таблица 100 Поддерживаемые стандарты (продолжение)

СТАНДАРТ	ОПИСАНИЕ
RFC 2475	Отображение маркеров DSCP на приоритеты IEEE 802.1p
RFC 2674	SNMP v2, v2c P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 2865	RADIUS – специальный атрибут производителя
RFC 3046	Ретрансляция DHCP
RFC 3164	Системный журнал Syslog
RFC 3376	Межсетевой протокол управления группами IGMP версия 3
RFC 3414	Модель безопасности на базе пользователей (USM) для версии 3 простого протокола сетевого управления (SNMP v3)
RFC 3580	RADIUS – атрибут протокола туннелирования
IEEE 802.1x	Контроль доступа к сети на основе портов
IEEE 802.1d	Мосты MAC
IEEE 802.1p	Типы трафика – приоритеты пакетов
IEEE 802.1q	VLAN на основе тегов
IEEE 802.1w	Быстрый протокол покрывающего дерева (RSTP)
IEEE 802.1s	Протокол нескольких экземпляров покрывающего дерева (MSTP)
IEEE 802.3	Формат пакетов
IEEE 802.3ad	Агрегация каналов
IEEE 802.3af	Питание устройств по витой паре
IEEE 802.3ah	Ethernet OAM (эксплуатация, администрирование и обслуживание)
IEEE 802.3u	Fast Ethernet
IEEE 802.3x	Управление потоком
Безопасность	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
Электромагнитная совместимость (EMC)	FCC Часть 15 (Класс A) CE EMC (Класс A)

B

IP-адреса и подсети

В данном приложении описываются IP-адреса и маски подсетей.

IP-адреса используются для идентификации устройств в сети. Для взаимодействия по сети IP-адрес должен быть назначен каждому сетевому устройству (в том числе компьютерам, серверам, маршрутизаторам, принтерам и т.д.). Такие устройства в сети называют хостами.

С помощью маски подсети определяется максимально возможное число хостов в конкретной сети. Маски подсети позволяют разделить одну сеть на несколько подсетей.

Знакомство с IP-адресами

Одна часть IP-адреса представляет собой номер сети, другая – идентификатор хоста. Точно так же, как у разных домов на одной улице в адресе присутствует одно и то же название улицы, у хостов в сети в адресе имеется общий номер сети. И точно так же, как у различных домов имеется собственный номер дома, у каждого хоста в сети имеется собственный уникальный идентификационный номер – идентификатор хоста. Номер сети используется маршрутизаторами для передачи пакетов в нужные сети, тогда как идентификатор хоста определяет конкретное устройство в этой сети, которому должны быть доставлены пакеты.

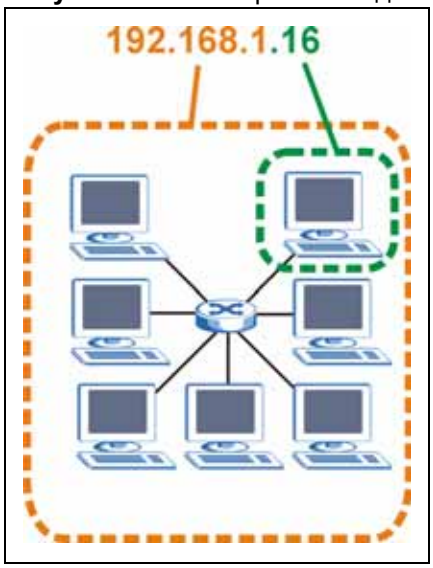
Структура

IP-адрес состоит из четырех частей, записанных в виде десятичных чисел с точками (например, 192.168.1.1). Каждую из этих четырех частей называют октетом. Октет представляет собой восемь двоичных цифр (например, 11000000, или 192 в десятичном виде).

Таким образом, каждый октет может принимать в двоичном виде значения от 00000000 до 11111111, или от 0 до 255 в десятичном виде.

На следующем рисунке показан пример IP-адреса, в котором первые три октета (192.168.1) представляют собой номер сети, а четвертый октет (16) – идентификатор хоста.

Рисунок 138 Номер сети и идентификатор хоста



Количество двоичных цифр в IP-адресе, которые приходятся на номер сети, и количество цифр в адресе, приходящееся на идентификатор хоста, может быть различным в зависимости от маски подсети.

Маски подсети

Маска подсети используется для определения того, какие биты являются частью номера сети, а какие – частью идентификатора хоста (для этого применяется логическая операция конъюнкции – «И»).

Маска подсети включает в себя 32 бита. Если бит в маске подсети равен «1», то соответствующий бит IP-адреса является частью номера сети. Если бит в маске подсети равен «0», то соответствующий бит IP-адреса является частью идентификатора хоста.

На следующем рисунке показана маска подсети, выделяющая номер сети (полужирным шрифтом) и идентификатор хоста в IP-адресе (который в десятичном виде записывается как 192.168.1.2).

Таблица 101 Пример выделения номера сети и идентификатора хоста в IP-адресе

	1-ЫЙ ОКТЕТ: (192)	2-ОЙ ОКТЕТ: (168)	3-ИЙ ОКТЕТ: (1)	4-ЫЙ ОКТЕТ: (2)
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Маска подсети (двоичная)	**11111111**	**11111111**	**11111111**	00000000
Номер сети	**11000000**	**10101000**	**00000001**	
Идентификатор хоста				00000010

Маски подсети всегда состоят из серии последовательных единиц начиная с самого левого бита маски, за которой следует серия последовательных нулей, составляющих в общей сложности 32 бита.

Маску подсети можно определить как количество бит в адресе, представляющих номер сети (количество бит со значением «1»). Например, «8-битной маской» называют маску, в которой 8 бит – единичные, а остальные 24 бита – нулевые.

Маски подсети записываются в формате десятичных чисел с точками, как и IP-адреса. В следующих примерах показаны двоичная и десятичная запись 8-битной, 16-битной, 24-битной и 29-битной масок подсети.

Таблица 102 Маски подсети

	ДВОИЧНАЯ				ДЕСЯТИЧНАЯ
	1-ЫЙ ОКТЕТ:	2-ОЙ ОКТЕТ:	3-ИЙ ОКТЕТ:	4-ЫЙ ОКТЕТ:	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Количество разрядов в номере сети определяет максимальное количество хостов, которые могут находиться в такой сети. Чем больше бит в номере сети, тем меньше бит остается на идентификатор хоста в адресе.

IP-адрес с идентификатором хоста из всех нулей представляет собой IP-адрес сети (192.168.1.0 с 24-битной маской подсети, например). IP-адрес с идентификатором хоста из всех единиц представляет собой широковещательный адрес данной сети (192.168.1.255 с 24-битной маской подсети, например).

Так как такие два IP-адреса не могут использоваться в качестве идентификаторов отдельных хостов, максимально возможное количество хостов в сети вычисляется следующим образом:

Таблица 103 Максимально возможное число хостов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИФИКАТОРА ХОСТА		МАКСИМАЛЬНОЕ КОЛИЧЕСТВО ХОСТОВ
8 бит	255.0.0.0	24 бит	$2^{24} – 2$	16777214
16 бит	255.255.0.0	16 бит	$2^{16} – 2$	65534
24 бит	255.255.255.0	8 бит	$2^{8} – 2$	254
29 бит	255.255.255.248	3 бит	$2^{3} – 2$	6

Формат записи

Поскольку маска всегда является последовательностью единиц слева, дополняемой серией нулей до 32 бит, можно просто указывать количество единиц, а не записывать значение каждого октета. Обычно это записывается как «/» после адреса и количество единичных бит в маске.

Например, адрес 192.1.1.0 /25 представляет собой адрес 192.1.1.0 с маской 255.255.255.128.

Некоторые возможные маски подсети в обоих форматах показаны в следующей таблице.

Таблица 104 Альтернативный формат записи маски подсети

МАСКА ПОДСЕТИ	АЛЬТЕРНАТИВНЫЙ ФОРМАТ ЗАПИСИ	ПОСЛЕДНИЙ ОКТЕТ (В ДВОИЧНОМ ВИДЕ)	ПОСЛЕДНИЙ ОКТЕТ (В ДЕСЯТИЧНОМ ВИДЕ)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

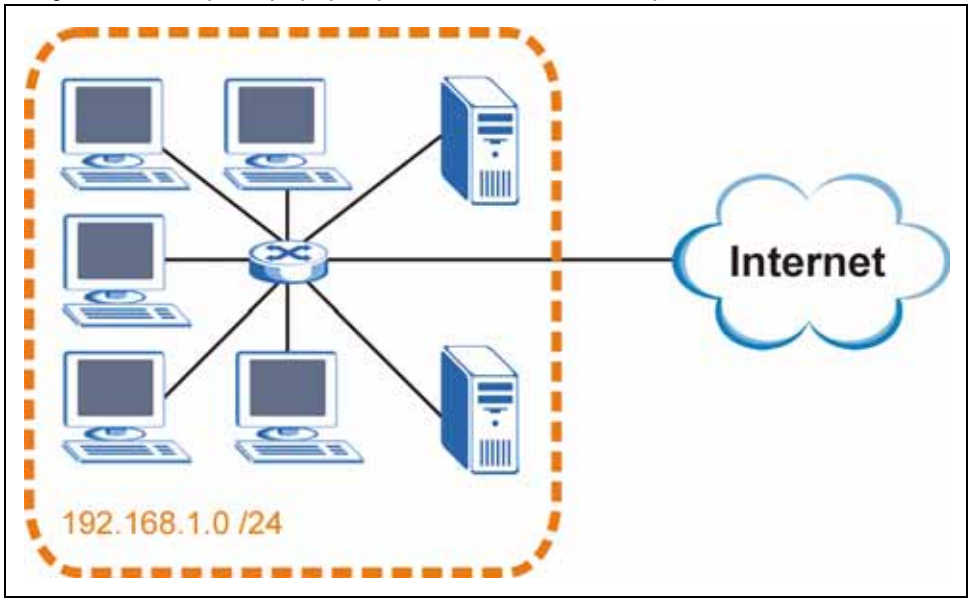
Формирование подсетей

С помощью подсетей одну сеть можно разделить на несколько. В приведенном ниже примере администратор сети создает две подсети, чтобы изолировать группу серверов от остальных устройств в целях безопасности.

В этом примере сеть компании имеет адрес 192.168.1.0. Первые три октета адреса (192.168.1) представляют собой номер сети, а оставшийся октет – идентификатор хоста, что позволяет использовать в сети максимум $2^8 – 2 = 254$ хостов.

Сеть компании до ее деления на подсети показана на следующем рисунке.

Рисунок 139 Пример формирования подсетей: до разделения на подсети

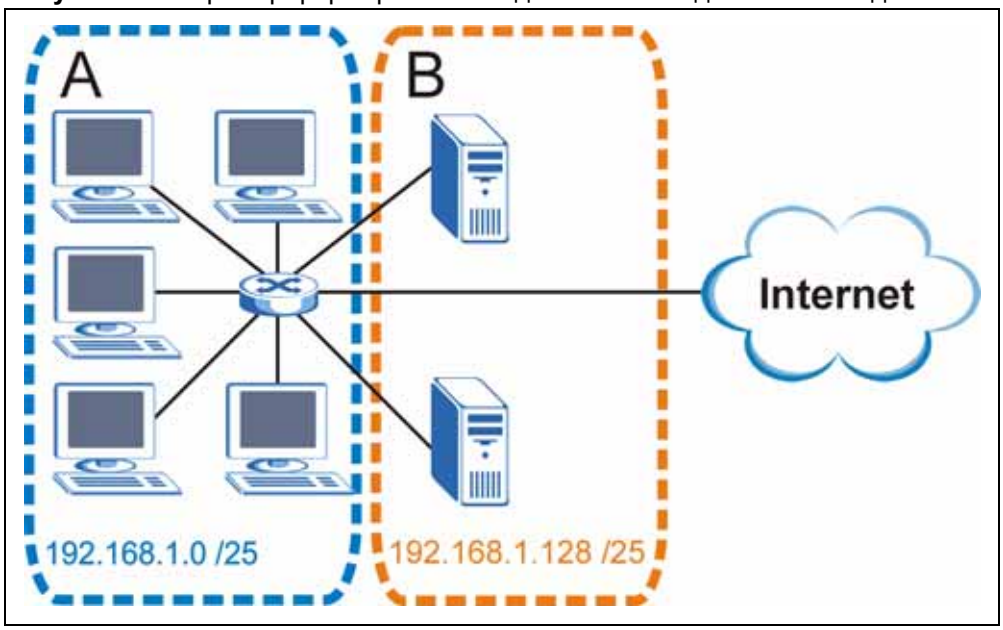


Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, можно «позаимствовать» один бит из идентификатора хоста. В этом случае маска подсети станет 25-битной (255.255.255.128 или /25).

«Одолженный» бит идентификатора хоста может быть либо нулем, либо единицей, что дает нам две подсети; 192.168.1.0 /25 и 192.168.1.128 /25.

Сеть компании после ее деления на подсети показана на следующем рисунке. Теперь она включает в себя две подсети, **A** и **B**.

Рисунок 140 Пример формирования подсетей: после деления на подсети



В 25-битной подсети на идентификатор хоста выделяется 7 бит, поэтому в каждой подсети может быть максимум $2^7 – 2 = 126$ хостов (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети).

Адрес 192.168.1.0 с маской 255.255.255.128 является адресом подсети **A**, а 192.168.1.127 с маской 255.255.255.128 является ее широковещательным адресом. Таким образом, наименьший IP-адрес, который может быть закреплен за действительным хостом в подсети **A** – это 192.168.1.1, а наибольший – 192.168.1.126.

Аналогичным образом, диапазон идентификаторов хоста для подсети **B** составляет от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В предыдущем примере было показано использование 25-битной маски подсети для разделения 24-битного адреса на две подсети. Аналогичным образом, для разделения 24-битного адреса на четыре подсети потребуется «одолжить» два бита идентификатора хоста, чтобы получить четыре возможных комбинации (00, 01, 10 и 11). Маска подсети состоит из 26 бит (11111111.11111111.11111111.**11**000000), то есть 255.255.255.192.

Каждая подсеть содержит 6 битов идентификатора хоста, что в сумме дает $2^6 – 2 = 62$ хоста для каждой подсети (идентификатор хоста из всех нулей – это сама подсеть, а из всех единиц – широковещательный адрес для подсети).

Таблица 105 Подсеть 1

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес (десятичный)	192.168.1.	0
IP-адрес (двоичный)	11000000.10101000.00000001.	**00**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000
Адрес подсети 192.168.1.0	Наименьший идентификатор хоста: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Наибольший идентификатор хоста: 192.168.1.62	

Таблица 106 Подсеть 2

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	64
IP-адрес (двоичный)	11000000.10101000.00000001.	**01**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000
Адрес подсети 192.168.1.64	Наименьший идентификатор хоста: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Наибольший идентификатор хоста: 192.168.1.126	

Таблица 107 Подсеть 3

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	128
IP-адрес (двоичный)	11000000.10101000.00000001.	**10**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000
Адрес подсети 192.168.1.128	Наименьший идентификатор хоста: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Наибольший идентификатор хоста: 192.168.1.190	

Таблица 108 Подсеть 4

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес	192.168.1.	192
IP-адрес (двоичный)	11000000.10101000.00000001.	**11**000000
Маска подсети (двоичная)	11111111.11111111.11111111.	**11**000000

Таблица 108 Подсеть 4 (продолжение)

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
Адрес подсети 192.168.1.192	Наименьший идентификатор хоста: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Наибольший идентификатор хоста: 192.168.1.254	

Пример: Восемь подсетей

Аналогичным образом для создания восьми подсетей используется 27-битная маска (000, 001, 010, 011, 100, 101, 110 и 111).

Значения последнего октета IP-адреса для каждой подсети показаны в следующей таблице.

Таблица 109 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩА-ТЕЛЬНЫЙ АДРЕС
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Планирование подсетей

Сводная информация по планированию подсетей для сети с 24-битным номером сети приводится в следующей таблице.

Таблица 110 Планирование подсетей для сети с 24-битным номером

КОЛИЧЕСТВО «ОДОЛЖЕННЫХ» БИТОВ ИДЕНТИФИКАТОРА ХОСТА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Сводная информация по планированию подсетей для сети с 16-битным номером сети приводится в следующей таблице.

Таблица 111 Планирование подсетей для сети с 16-битным номером

КОЛИЧЕСТВО «ОДОЛЖЕННЫХ» БИТОВ ИДЕНТИФИКАТОРА ХОСТА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Настройка IP-адресов

Где именно можно получить номер сети – зависит от конкретной ситуации. Если провайдером услуг Интернета или администратором сети был выделен блок зарегистрированных IP-адресов, при выборе IP-адресов и маски подсети необходимо выполнять полученные от них инструкции.

Если провайдер не указал явным образом номер IP-сети, скорее всего у вас однопользовательская учетная запись, и IP-адрес назначается провайдером динамически при установлении соединения. В этом случае в качестве номера сети рекомендуется использовать значения от 192.168.0.0 до 192.168.255.0. Уполномоченной организацией по распределению нумерации в сети Интернет (IANA) этот блок адресов специально зарезервирован для частного использования; адреса вне этого диапазона следует использовать, лишь получив явные на то указания. Кроме того, необходимо включить на коммутаторе коммутатор механизм трансляции сетевых адресов (NAT).

Определившись с номером сети, выберите легкий для запоминания адрес для своего коммутатора коммутатор (например, 192.168.1.1), и позаботьтесь о том, чтобы этот адрес не использовался никаким другим устройством в сети.

Маска подсети определяет, какую часть в IP-адресе занимает номер сети. коммутатор вычислит маску подсети автоматически на основе введенного IP-адреса. Изменять автоматически вычисленную коммутатором коммутатор маску подсети можно, лишь получив соответствующие инструкции.

Частные IP-адреса

У каждой машины в сети Интернет должен быть уникальный адрес. Если ваши сети изолированы от Интернета (например, связывают два филиала), для хостов без проблем можно использовать любые IP-адреса. Однако, Уполномоченной организацией по распределению нумерации в сети Интернет (IANA) специально для частных сетей зарезервированы следующие три блока IP-адресов:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

IP-адреса можно получить через IANA, у своего провайдера услуг Интернет, или назначить из диапазона адресов для частных сетей. Если ваша организация является небольшой и осуществляет доступ к Интернету через провайдера услуг Интернет, именно провайдер выделит Интернет-адреса для ваших локальных сетей. С другой стороны, если вы являетесь отделом более крупной организации, соответствующие IP-адреса можно получить у администратора корпоративной сети.

В любом случае, не следует назначать IP-адреса произвольным образом; обязательно придерживайтесь приведенных выше рекомендаций. Дополнительную информацию о назначении адресов можно найти в стандартах RFC 1597, *Выделение адресов для частных IP-сетей*, и RFC 1466, *Рекомендации по управлению адресным пространством IP-сетей.*

C

Правовая информация

Уведомление об авторских правах

Уведомление

ZyXEL снимает с себя любую ответственность за последствия использования любых продуктов или программного обеспечения, описанных в настоящем документе. Кроме того, ZyXEL не передает никаких лицензий в отношении принадлежащих ZyXEL патентов или патентов третьих лиц. ZyXEL оставляет за собой право вносить изменения в описанные ниже продукты без какого-либо предварительного уведомления. Данная публикация может быть изменена без уведомления.

Товарные знаки

ZyNOS (ZyXEL Network Operating System) является зарегистрированным товарным знаком ZyXEL Communications, Inc. Прочие товарные знаки, упоминающиеся в настоящей публикации, используются исключительно для идентификации и могут представлять собой собственность соответствующих компаний.

Важная информация

Регистрация прав собственника

После завершения установки мы рекомендуем зарегистрировать ваше изделие ZyXEL через Интернет по адресу http://zyxel.ru.

Регистрация через Интернет дает дополнительный год бесплатной гарантии, персональную техническую поддержку, уведомление по электронной почте об обновлениях, ряд других преимуществ и льгот.

Информация о сертификации

Коммутаторы ZyXEL серии ES-2024 одобрены для применения государственными органами по сертификации средств связи.

Система сертификации ГОСТ Р, Госстандарт России

Сертификат соответствия № РОСС TW.АЯ46.В11222. Срок действия с 29.12.2006 по 28.12.2009. Сертификат соответствия № РОСС TW.АЯ46.В08943. Срок действия с 13.09.2006 по 13.09.2008. Соответствует требованиям: ГОСТ Р МЭК 60950-2002, ГОСТ Р 51318.22-99 (класс Б), ГОСТ Р 51318.24-99 (группа 1), ГОСТ Р 51317.3.2-99, ГОСТ Р 51317.3.3-99.

Система сертификации в области связи

Сертификат соответствия № ОС-1-СПД-0247. Срок действия с 25.09.2006 по 25.09.2009. Соответствует требованиям: РД45.176-2001.

Государственная Санитарно-эпидемиологическая служба РФ

Санитарно-эпидемиологическое заключение № 77.01.09.401.П.087979.12.06. Срок действия с 26.12.2006 по 18.12.2011. Соответствует требованиям: СанПиН 2.2.2./ 2.4.1340-03.

Юридический адрес изготовителя

ZyXEL Communications Corporation, N 6, Innovation Road II, Science-Based Industrial Park, Hsin-Chu, Taiwan, R.O.C.

Установленный производителем в порядке п.2 ст.5 Федерального закона РФ «О защите прав потребителей» срок службы изделия равен 5 годам с даты производства при условии, что изделие используется в строгом соответствии с настоящим руководством и применимыми техническими стандартами.

© ZyXEL, 2007. Все права защищены.

Предупреждения по безопасности

В целях вашей безопасности внимательно прочитайте и следуйте всем предупреждениям и указаниям.

- Чтобы снизить риск возникновения пожара, используйте телекоммуникационные кабели с сечением жил №26 согласно Американскому сортаменту проводов AWG или большего сечения.
- НЕ открывайте устройство. В результате вскрытия или снятия защитных кожухов вы подвергаете себя опасности прикосновения к оголенным токоведущим участкам с опасным высоким напряжением и иным рискам. Обслуживать данное устройство разрешается ТОЛЬКО квалифицированному сервисному персоналу. Для получения дополнительной информации свяжитесь с поставщиком.
- Используйте ОТДЕЛЬНЫЙ источник питания для устройства. Подключите шнур питания или адаптер к источнику питания с требуемым номиналом напряжения (110 В перем. тока в Северной Америке или 230 В перем. тока в Европе).
- НЕ используйте устройство, если источник питания поврежден, так как в этом случае существует опасность поражения электрическим током.
- Если источник питания поврежден, выньте его из розетки.
- НЕ пытайтесь починить источник питания. Чтобы заказать новый источник питания, свяжитесь с местным поставщиком.
- Аккуратно расположите соединительные кабели так, чтобы никто не мог наступить или споткнуться о них. НЕ кладите ничего на шнур питания и НЕ располагайте продукт в таком месте, где кто-нибудь может наступить на шнур.
- При креплении устройства на стене убедитесь, что при этом не пострадают электропроводка, трубы газоснабжения или водоснабжения.
- Не занимайтесь установкой и не эксплуатируйте устройство во время грозы. Существует опасность поражения электрическим током в результате удара молнии.
- НЕ подвергайте устройство воздействию сырости, пыли или агрессивных жидкостей.
- НЕ используйте данный продукт вблизи воды, например, в сыром подвале или неподалеку от плавательного бассейна.
- Убедитесь, что кабели подключены к нужным портам.
- НЕ заслоняйте вентиляционные отверстия устройства, так как ограниченный приток воздуха может послужить причиной повреждения устройства.
- НЕ кладите ничего поверх устройства.
- К устройству разрешается подключать ТОЛЬКО подходящие дополнительные модули.

Гарантийное обслуживание ZyXEL

Мы гордимся надежностью и качеством нашей продукции и верим, что это изделие прослужит вам безотказно долгие годы. Тем не менее, если вы столкнетесь с вопросами при использовании этого изделия, пожалуйста, обратитесь за помощью в региональный офис ZyXEL Communications Corporation.

Гарантийные обязательства

1. Настоящая гарантия действует в течение трех лет с даты приобретения изделия ZyXEL и подразумевает гарантийное обслуживание в случае обнаружения дефектов, связанных с материалами и сборкой. В этом случае потребитель имеет право на бесплатный ремонт изделия.
2. При регистрации приобретенного изделия через Интернет на сайте, указанном в таблице, потребитель получает дополнительный год гарантийного обслуживания.
3. Максимальный срок гарантии, предоставляемой компанией ZyXEL, исчисляется с даты производства изделия и составляет четыре с половиной года. Дата производства определяется по серийному номеру на корпусе изделия: SYxW-Wxxxxx, где Y – последняя цифра года, а WW – номер недели с начала года.
4. Настоящая гарантия распространяется только на изделия ZyXEL, проданные через официальные каналы дистрибуции ZyXEL.
5. Настоящая гарантия предоставляется компанией ZyXEL в дополнение к правам потребителя, установленным действующим законодательством в стране приобретения.

Условия гарантии

1. Гарантийное обслуживание изделия ZyXEL осуществляется в авторизованных сервисных центрах (АСЦ) ZyXEL на приведенных ниже условиях.
2. Настоящая гарантия действительна только при предъявлении вместе с неисправным изделием правильно заполненного фирменного гарантийного талона с проставленной датой продажи. Компания ZyXEL оставляет за собой право отказать в бесплатном гарантийном обслуживании, если гарантийный талон не будет предоставлен или если содержащаяся в нем информация будет неполной или неразборчивой.
3. Настоящая гарантия недействительна в случаях, если:

   - серийный номер на изделии изменен, стерт, удален или неразборчив;

   - изделие переделывалось без предварительного письменного согласия ZyXEL;

   - изделие неправильно эксплуатировалось, в том числе: а) использовалось не по назначению или не в соответствии с руководством ZyXEL; б) устанавливалось или эксплуатировалось в условиях, не соответствующих стандартам и нормам безопасности, действующим в стране использования;

   - изделие ремонтировалось не уполномоченными на то сервисными центрами или дилерами;

- изделие вышло из строя по причине несчастного случая, удара молнии, затопления, пожара, неправильной вентиляции и иных причин, находящихся вне контроля ZyXEL;

- изделие пострадало при транспортировке, за исключением случаев, когда она производится АСЦ;

- изделие использовалось в дефектной системе.

Контактная информация

СТРАНА	РОССИЯ	УКРАИНА	КАЗАХСТАН
Поддержка через Интернет	http://zyxel.ru/support	support@ua.zyxel.com	http://zyxel.kz/support
Телефон службы поддержки	(800) 200-8929 (495) 542-8929	(800) 504-0040 (044) 247-6978	(800) 080-0055 (3272) 590-689
Сервер в Интернете	http://zyxel.ru	http://www.ua.zyxel.com	http://zyxel.kz
Почтовый адрес	ZyXEL Россия 117279, Москва ул. Островитянова 37а	ZyXEL Украина 04050, Киев ул. Пимоненко 13	ZyXEL Казахстан 050010, Алматы пр. Достык 43, офис 414

D

Поддержка пользователей

При обращении в службу поддержки пользователей убедитесь, что у вас имеется следующая информация.

Требуемая информация

- Модель продукта и серийный номер.
- Информация о гарантии.
- Дата получения устройства.
- Краткое описание проблемы и шагов, которые были предприняты для ее решения.

«+» обозначает префикс, необходимый для выхода на международную линию.

Штаб-квартира компании (всемирная)

- E-mail поддержки: support@zyxel.com.tw
- E-mail отдела продаж: sales@zyxel.com.tw
- Телефон: +886-3-578-3942
- Факс: +886-3-578-2439
- Интернет: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Обычная почта: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Тайвань

Казахстан

- Поддержка: http://zyxel.kz/support
- E-mail отдела продаж: sales@zyxel.kz
- Телефон: (800) 080-0055, (3272) 590-689
- Факс: (3272) 590-689
- Интернет: www.zyxel.kz
- Обычная почта: ZyXEL Казахстан, 050010, Алматы, пр. Достык 43, офис 414

Россия

- Поддержка: http://zyxel.ru/support
- E-mail отдела продаж: sales@zyxel.ru
- Телефон: (800) 200-8929, (495) 542-8929
- Факс: (495) 542-8925
- Интернет: www.zyxel.ru
- Обычная почта: ZyXEL Россия, 117279 Москва, ул. Островитянова 37а

Украина

- E-mail поддержки: support@ua.zyxel.com
- E-mail отдела продаж: sales@ua.zyxel.com
- Телефон: (800) 504-0040, (044) 247-6978
- Факс: (044) 494-4932
- Интернет: www.ua.zyxel.com
- Обычная почта: ZyXEL Украина, 04050 Киев, ул. Пимоненко 13

Индекс

Символы

A

Б

B (C)

Г (D)

Д

Е (F)

Ж (G)

З (H)

И (I)

K

Л (L)

M

Н (N)

О

П (P)

P (R)

C (S)

Т

У

Ф (V)

X (W)

Ч

Э