ES-4124

Интеллектуальный коммутатор уровня 3+

Руководство пользователя

Версия 3.8
4/2007
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-4124 с использованием Web-конфигуратора или интерфейса командной строки. 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.

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!

ZyXEL Россия,
117279, Москва,
ул. Островитянова 37а

E-mail: info@zyxel.ru

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.

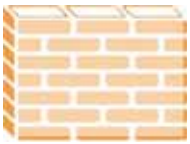
В примечаниях приводится важная информация (например, дополнительные требования по настройке или полезные советы) или рекомендации.

Обозначения

- Устройство ES-4124 может называться в данном руководстве пользователя как «коммутатор», «устройство», «система» или «продукт».
- 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.
- 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**.
- 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.

Данный 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.
- В целях защиты от пожара замену предохранителей следует осуществлять исключительно на предохранители того же типа и номинала.
- 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.
- НЕ заслоняйте вентиляционные отверстия устройства, так как ограниченный приток воздуха может послужить причиной повреждения устройства.

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

Модель ES-4124 представляет собой автономный Ethernet-коммутатор уровня 3 с 24 портами на 10/100 Мбит/с, двумя портами Gigabit Ethernet с разъемами RJ-45 и 2 совмещенными интерфейсами GbE для каскадирования, а также с консольным портом и портом управления для локального администрирования. Совмещенные интерфейсы включают в себя один порт Gigabit Ethernet и один слот для трансивера mini-GBIC (модуля SFP), из которых только один может быть активен в каждый момент времени.

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

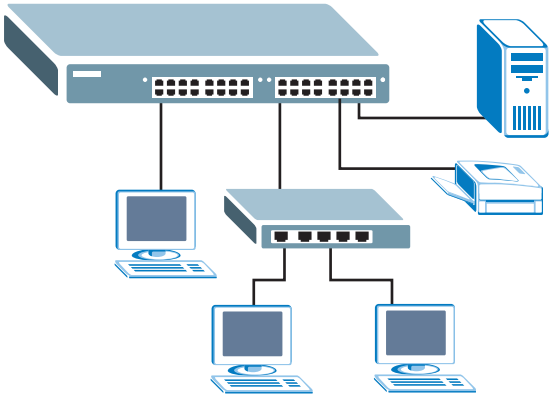
Полный перечень функций программного обеспечения, доступных на коммутаторе, можно найти в прил. A на стр. 499.

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

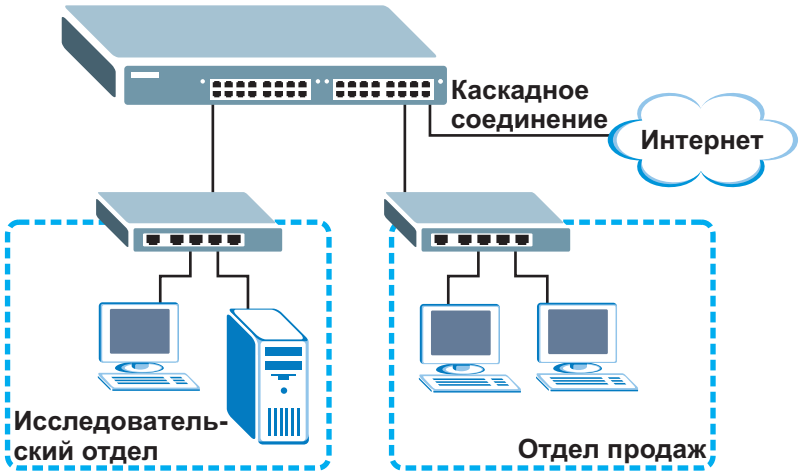


1.1.2 Пример мостовой конфигурации

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

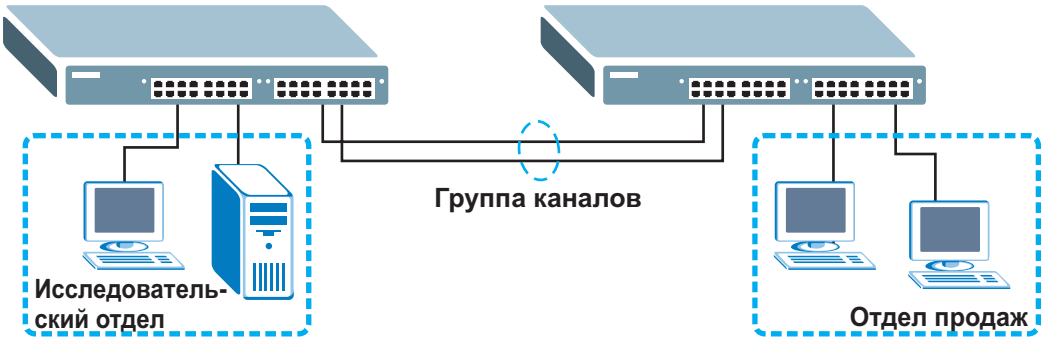


1.1.3 Пример высокоскоростной коммутации

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) 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.

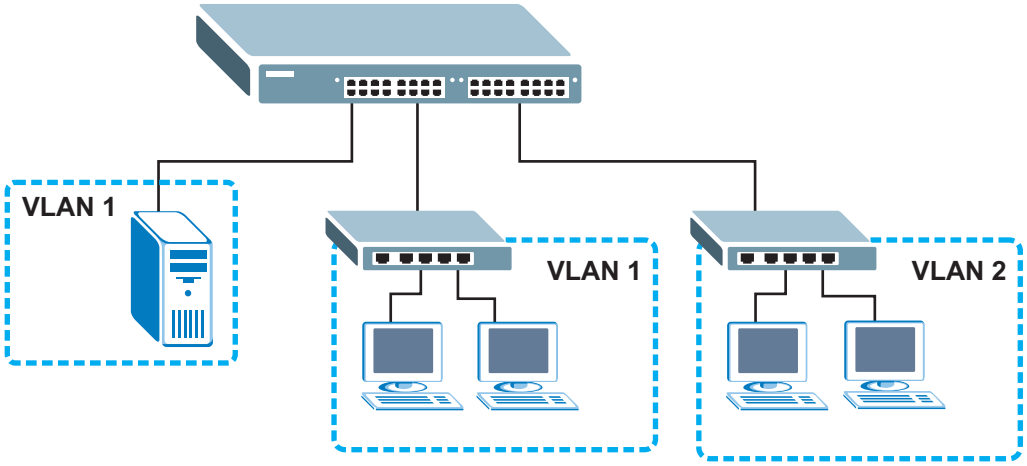
Дополнительную информацию о виртуальных локальных сетях можно найти в гл. 8 на стр. 95.

1.1.4.1 Пример виртуальной локальной сети на базе тегов

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. 55.
- Интерфейс командной строки. Интерфейс командной строки является альтернативой Web-конфигуратору и может потребоваться для настройки расширенных функций. См. гл. 45 на стр. 369.
- FTP. Протокол передачи файлов File Transfer Protocol можно использовать для обновления встроенного программного обеспечения и резервного копирования/восстановления конфигурации. См. разд. 35.8 на стр. 317.
- SNMP. Мониторинг и/или управление устройством возможно с использованием менеджера SNMP. См. разд. 36.3 на стр. 322.

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

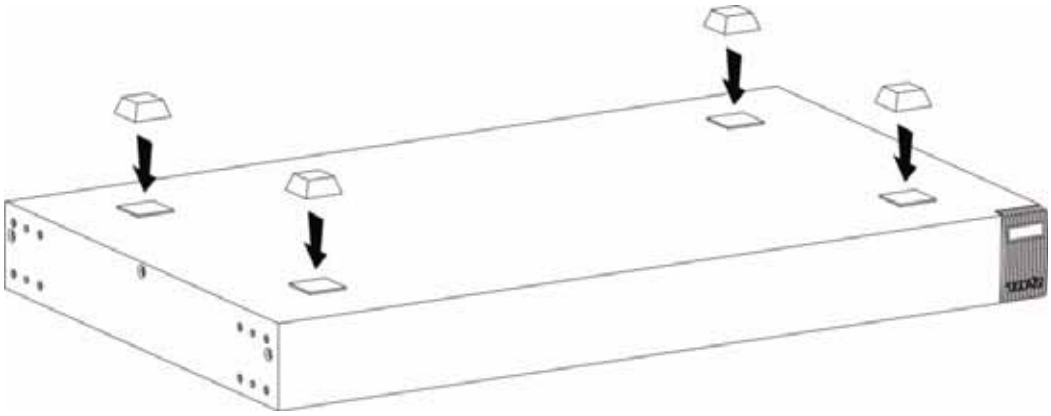
Установка и подключение аппаратного обеспечения

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.

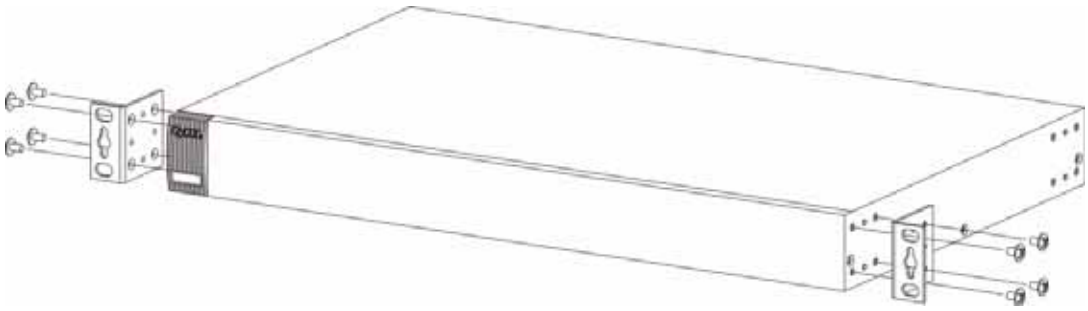
2.2.1.1 Меры предосторожности

- 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.

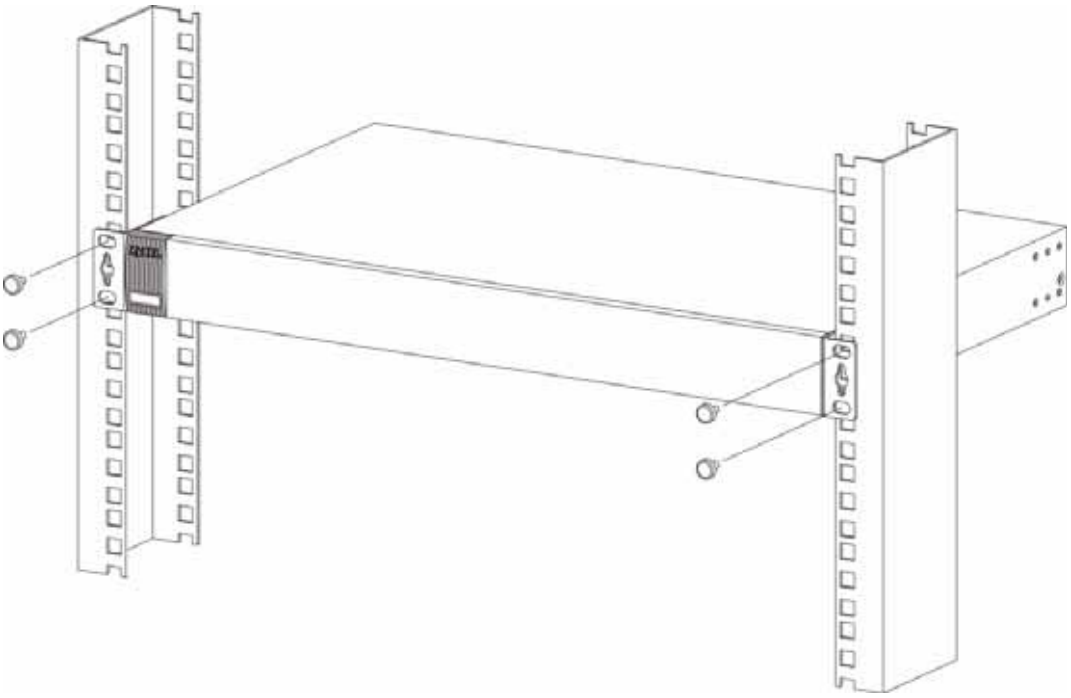
3 Повторите шаги 1 и 2, чтобы закрепить кронштейн на другой стороне коммутатора.

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

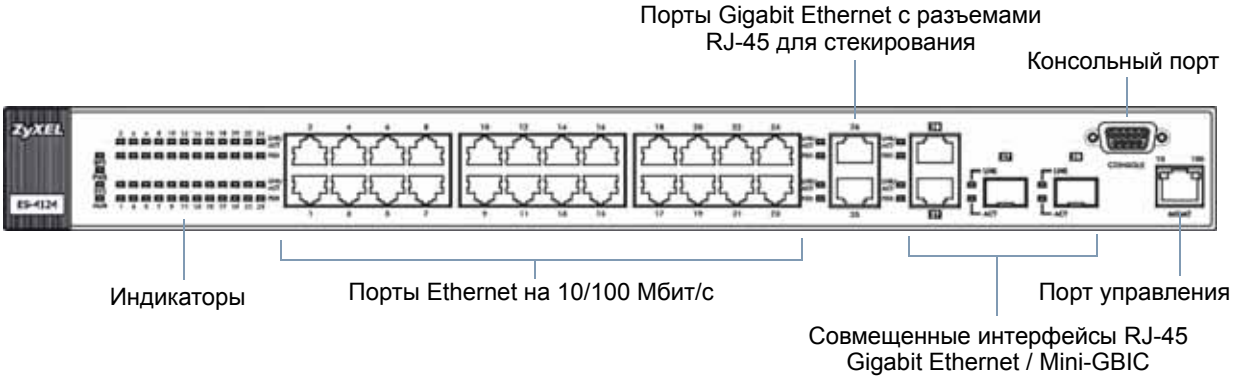
Обзор аппаратного обеспечения

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



Расположенные на передней панели порты описаны в следующей таблице.

Таблица 1 Подключения на передней панели

РАЗЪЕМ	ОПИСАНИЕ
24 порта Ethernet на 10/100 Мбит/с с разъемами RJ-45	К этим портам можно подключать компьютеры, концентраторы, Ethernet-коммутаторы или маршрутизаторы.
Два порта Gigabit Ethernet на 100/1000 Мбит/с с разъемами RJ-45	Порты Gigabit Ethernet подключаются к высокоскоростным магистральным Ethernet-коммутаторам или используются для последовательного соединения нескольких коммутаторов.

Таблица 1 Подключения на передней панели (продолжение)

РАЗЪЕМ	ОПИСАНИЕ
Два совмещенных интерфейса	Каждый интерфейс включает в себя порт для витой пары 1000 Base-T с разъемом RJ-45 и порт для оптоволоконного модуля SFP, из которых только один может быть активен в каждый момент времени.
	• 2 порта Gigabit Ethernet на 100/1000 Мбит/с с разъемами RJ-45: Данные порты Gigabit Ethernet используются для подключения к высокоскоростным магистральным коммутаторам Ethernet.
	• 2 порта mini-GBIC: В эти слоты можно вставить трансиверы mini-GBIC для подключения к магистральным Ethernet-коммутаторам посредством оптоволокна.
Консольный порт	К этому порту следует подключаться только тогда, когда требуется настроить коммутатор с помощью интерфейса командной строки через консольный порт.
Порт управления	Подключается к компьютеру с использованием Ethernet-кабеля с разъемом RJ-45 для локальной настройки коммутатора.

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.

Кроме того, в устройстве предусмотрены два совмещенных интерфейса (порты 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 (100/1000 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: Не горит

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)

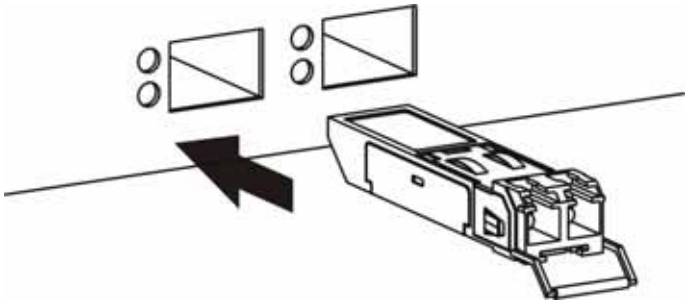
Во избежание возможной травмы глаз НЕ смотрите в разъемы работающего оптоволоконного модуля.

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.

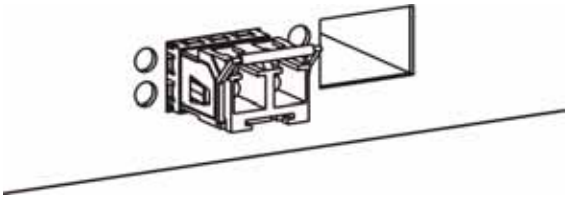
Рисунок 9 Пример установки трансивера



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 10 Установленный трансивер

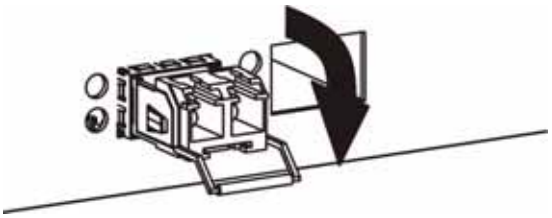


3.1.3.2 Удаление трансивера

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

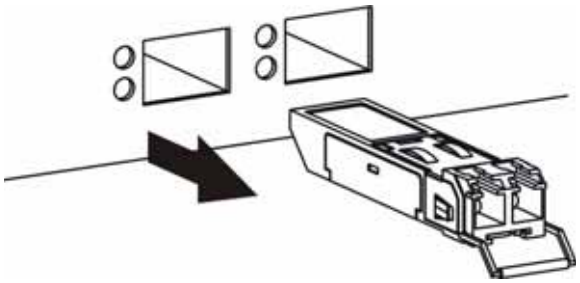
1 Откройте защелку трансивера (их вид может различаться).

Рисунок 11 Пример открытия защелки трансивера



2 Выньте трансивер из слота.

Рисунок 12 Пример удаления трансивера



3.2 Задняя панель

На приведенных ниже рисунках показаны задние панели моделей с питанием от переменного и от постоянного тока. На задней панели располагается разъем для подключения резервного источника питания (BPS) и розетка питания. На модели с питанием от постоянного тока на задней панели имеется также выключатель питания.

Рисунок 13 Задняя панель – модель с питанием от переменного тока

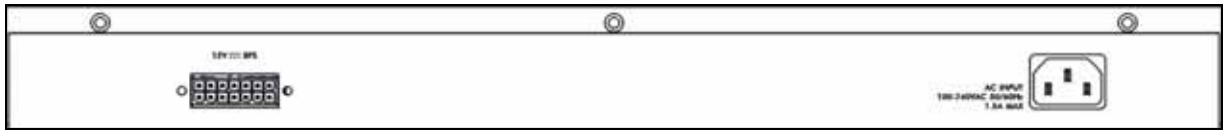
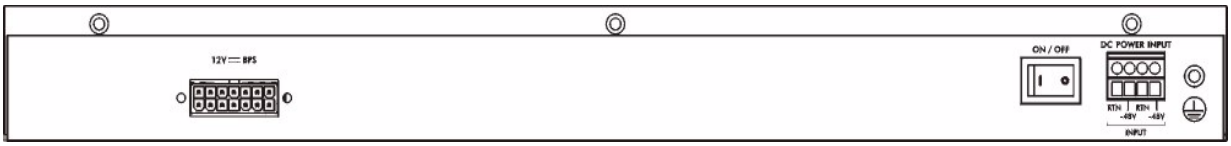


Рисунок 14 Задняя панель – модель с питанием от постоянного тока



3.2.1 Разъем питания

Убедитесь, что параметры питающей сети соответствуют указанным на панели.

Чтобы подключить питание к устройству ES-4124 с питанием от переменного тока, вставьте разъем типа «мама» шнура питания в розетку на задней панели. Другой конец шнура питания из комплекта поставки подключите к розетке питающей сети, обеспечивающей 100~240 В перем. тока, 1,5 А. Убедитесь, что притоку воздуха ничто не мешает.

Модель ES-4124 с питанием от постоянного тока требует на входе от -48 В до -60 В пост. тока, 1,5 А без допуска. Чтобы подключить питание к устройству, вставьте один из разъемов поставляемого в комплекте шнура питания в розетку на задней панели, а другой разъем подключите к питающей сети. Убедитесь, что притоку воздуха ничто не мешает.

3.2.2 Разъем для внешнего резервного источника питания

Данный коммутатор поддерживает внешний резервный источник питания (BPS).

Резервный источник питания непрерывно отслеживает состояние встроенного источника питания. В случае пропадания питания коммутатор автоматически переключается на питание от резервного источника. После переключения коммутатора на питание от резервного источника, даже в случае возобновления подачи питания, обратно на питание от встроенного источника питания он автоматически не переключается.

3.3 Индикаторы

Описание индикаторов приводится в следующей таблице.

Таблица 2 Индикаторы

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
BPS	Зеленый	Мигает	Система получает питание от резервного источника питания.
		Горит	Резервный источник питания подключен и активен.
		Не горит	Резервный источник питания не подключен или не активен.
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	Зеленый	Мигает	Осуществляется передача/прием данных на скорости 10 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 10 Мбит/с.
	Желтый	Мигает	Осуществляется передача/прием данных на скорости 100 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 100 Мбит/с.
		Не горит	Соединение с сетью Ethernet не установлено.
FDX	Желтый	Горит	Порт Ethernet работает в дуплексном режиме.
		Не горит	Порт Ethernet работает в полудуплексном режиме.
Порты Gigabit Ethernet			
LNK/ACT	Зеленый	Мигает	Осуществляется передача/прием данных на скорости 10/1000 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 10/1000 Мбит/с.
	Желтый	Мигает	Осуществляется передача/прием данных на скорости 100 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 100 Мбит/с.
		Не горит	Соединение с сетью Ethernet не установлено.
FDX	Желтый	Горит	Порт Ethernet работает в дуплексном режиме.
		Не горит	Порт Ethernet работает в полудуплексном режиме.

Таблица 2 Индикаторы (продолжение)

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
Слоты Mini-GBIC			
LNK	Зеленый	Горит	Соединение установлено успешно.
		Не горит	Соединение не установлено.
ACT	Зеленый	Мигает	Осуществляется прием или передача данных через порт.
Порт MGMT			
10	Зеленый	Мигает	Осуществляется обмен данными (прием/передача) с устройством Ethernet.
		Горит	Установлено соединение на скорости 10 Мбит/с.
		Не горит	Нет соединения на скорости 10 Мбит/с или соединения с устройством Ethernet.
100	Желтый	Мигает	Осуществляется обмен данными (прием/передача) с устройством Ethernet.
		Горит	Установлено соединение на скорости 100 Мбит/с.
		Не горит	Нет соединения на скорости 100 Мбит/с или соединения с устройством Ethernet.

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

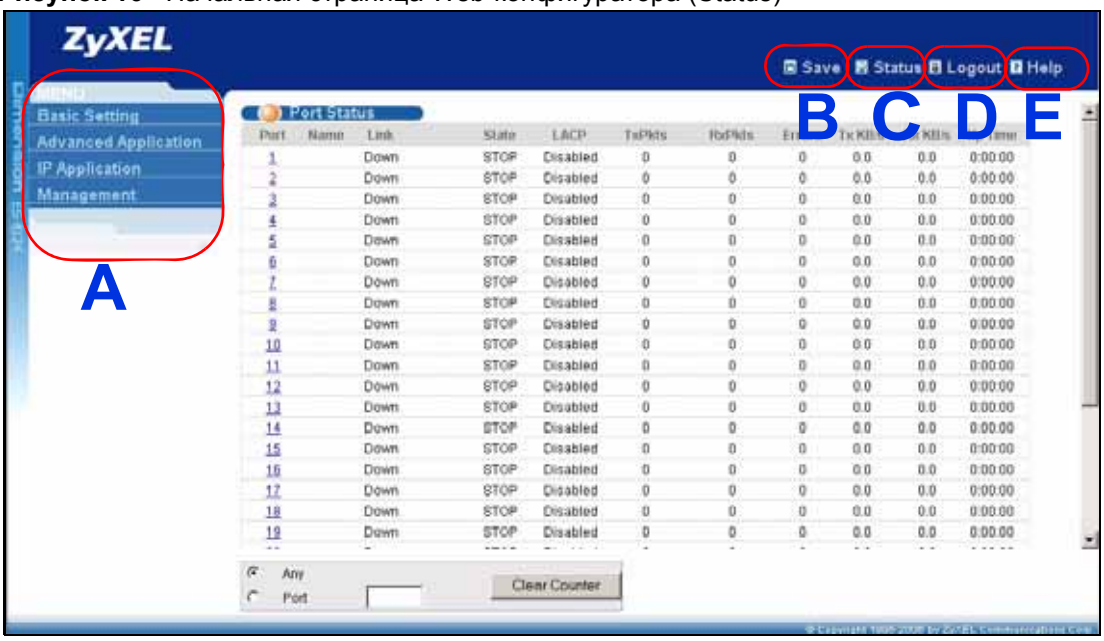
4 Нажмите **OK**, чтобы попасть на начальный экран Web-конфигуратора.

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. 35.3 на стр. 314.

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 (Виртуальные локальные сети) VLAN Port Setting (Настройки портов VLAN) Subnet Based VLAN (VLAN на основе подсетей) Protocol Based VLAN (VLAN на основе протоколов) Static VLAN (Статические VLAN) Static MAC Forwarding (Пересылка на основе статических MAC-адресов) Filtering (Фильтрация) Spanning Tree Protocol (Протокол покрывающего дерева) Configuration (Настройка) RSTP (Быстрый протокол покрывающего дерева) MRSTP (Быстрый протокол нескольких экземпляров покрывающего дерева) MSTP (Протокол нескольких экземпляров покрывающего дерева) Bandwidth Control (Управление пропускной способностью) Broadcast Storm Control (Контроль широковещательных штормов) Mirroring (Зеркальное копирование) Link Aggregation (Агрегация каналов) Link Aggregation Setting (Настройка агрегации каналов) Ling Aggregation Control Protocol (Протокол LACP) Port Authentication (Аутентификация портов) 802.1x MAC Authentication (Аутентификация по MAC-адресам)	Static Routing (Статические маршруты) RIP (Протокол маршрутной информации) OSPF Status (Состояние OSPF) OSPF Configuration (Настройка OSPF) OSPF Interface (Интерфейс OSPF) OSPF Virtual Link (Виртуальный канал OSPF) IGMP (Протокол IGMP) DVMRP (Протокол маршрутизации мультивещания «вектор-длина» IP Multicast (IP-мультивещание) DiffServ (Дифференцированное обслуживание) 2-Rate 3 Color Marker (Маркировка TRTCM) DSCP Setting (Настройки DSCP) DHCP Status (Состояние DHCP) DHCP Relay (Ретрансляция DHCP) VLAN Setting (Настройки VLAN) VRRP (Протокол резервирования виртуального маршрутизатора) VRRP Configuration (Настройка VRRP)	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) Logins (Пользователи и пароли) Service Access Control (Контроль доступа к службам) Remote Management (Удаленное управление) Diagnostic (Диагностика) Syslog (Системный журнал) Syslog Setup (Настройки системного журнала) Server Setup (Настройка сервера) Cluster Management (Управление кластерами) Status (Состояние) Configuration (Настройка) MAC Table (Таблица MAC-адресов)

Таблица 4 Содержание экранов подменю Web-конфигуратора (продолжение)

BASIC SETTING (ОСНОВНЫЕ НАСТРОЙКИ)	ADVANCED APPLICATION (РАСШИРЕННЫЕ ПРИЛОЖЕНИЯ)	IP APPLICATION (IP-ПРИЛОЖЕНИЯ)	MANAGEMENT (УПРАВЛЕНИЕ)
	Port Security (Средства безопасности портов) Classifier (Классификация) Policy Rule (Правила политики) Queuing Method (Метод организации очередей) VLAN Stacking (Стекирование VLAN) Multicast (Мультивещание) 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) DHCP Snooping (Отслеживание DHCP) ARP Inspection Status (Состояние инспекции ARP-пакетов) Loop Guard (Защита от образования петель)		IP Table (Таблица IP-адресов) ARP Table (Таблица ARP) Routing Table (Таблица маршрутизации) 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, отслеживание многоадресного трафика IGMP, 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 до 64 доменов 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). На этих экранах имеется также возможность настроить VLAN на основе протоколов и VLAN на основе подсетей.
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/MRSTP/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, а также аутентификацию по MAC-адресам для клиентов, подключающихся к коммутатору.

Таблица 5 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
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.
Classifier (Классификация)	Этот пункт открывает экран, позволяющий настроить на коммутаторе группировку пакетов по определенным критериям.
Policy Rule (Правила политики)	Этот пункт открывает экран, позволяющий настроить на коммутаторе особую обработку сгруппированных пакетов.
Queuing Method (Метод организации очередей)	Этот пункт открывает экран, позволяющий настроить методы постановки в очередь, а также установить значения весов для каждого из портов.
VLAN Stacking (Стекирование VLAN)	Этот пункт открывает экран, позволяющий настроить стекирование сетей VLAN.
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 DHCP и 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)	
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.
RIP (Протокол маршрутной информации)	Этот пункт открывает экран, позволяющий настроить направления работы и версии протокола RIP (протокола маршрутной информации).
OSPF (Протокол OSPF)	Этот пункт открывает экраны, позволяющие просмотреть состояние протокола OSPF и настроить параметры OSPF.
IGMP (Протокол IGMP)	Этот пункт открывает экран, позволяющий настроить протокол IGMP.
DVMRP (Протокол маршрутизации мультивещания «вектор-длина»	Этот пункт открывает экран, позволяющий настроить параметры протокола DVMRP (протокола маршрутизации мультивещания «вектор-длина»).
IP Multicast (IP-мультивещание)	Этот пункт открывает экран, позволяющий настроить на коммутаторе удаление тегов VLAN из мультивещательных IP-пакетов на исходящих портах.
DiffServ (Дифференцированное обслуживание)	Этот пункт открывает экраны, позволяющие включить DiffServ, настроить правила маркировки и определить отображения между битами DSCP и IEEE802.1p.
DHCP (Протокол DHCP)	Этот пункт открывает экран, позволяющий настроить протокол DHCP.
VRRP (Протокол резервирования виртуального маршрутизатора)	Этот пункт открывает экраны, позволяющие настроить в сети резервированные виртуальные маршрутизаторы.

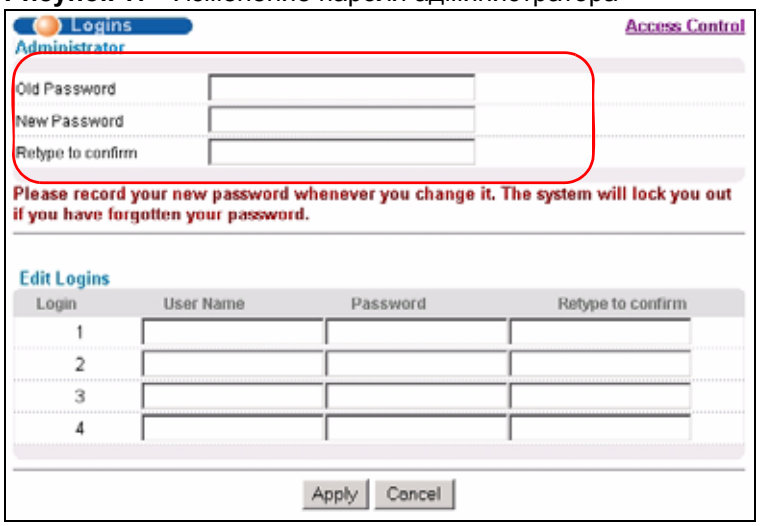
Таблица 5 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
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.
IP Table (Таблица IP-адресов)	Этот пункт открывает экран, позволяющий просматривать IP-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.
Routing Table (Таблица маршрутизации)	Этот пункт открывает экран, позволяющий просматривать таблицу маршрутизации.
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** и затем **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. В случае блокирования доступа попробуйте воспользоваться для настройки коммутатора внеполосным каналом управления (через порт управления).

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. 46.
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.

Рисунок 18 Сброс коммутатора: через консольный порт

```
Bootbase Version: V0.7 | 02/17/2006 11:56:33
RAM:Size = 64 Mbytes
DRAM POST: Testing: 65536K   OK
DRAM Test SUCCESS !
FLASH: Intel 32M

ZyNOS Version: V3.80(AIC.0)b0 | 01/19/2007 19:06:37

Press any key to enter debug mode within 3 seconds.....................
Enter Debug Mode
ES-4124> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total  393216 bytes received.
Erasing..
.............................................................
OK
ES-4124> 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 данного примера сети включает в себя следующие шаги:

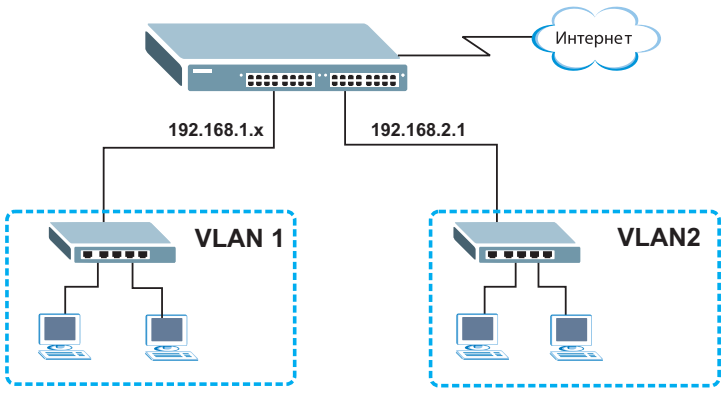
- Настройка IP-интерфейса
- Настройка параметров сервера DHCP
- Создание виртуальной локальной сети VLAN
- Определение идентификаторов VLAN для портов
- Включение протокола RIP

5.1.1 Настройка IP-интерфейса

На коммутаторе уровня 3 IP-интерфейс (также называемый доменом IP-маршрутизации) не привязан к физическому порту. По умолчанию на коммутаторе используется IP-адрес 192.168.1.1 с маской подсети 255.255.255.0.

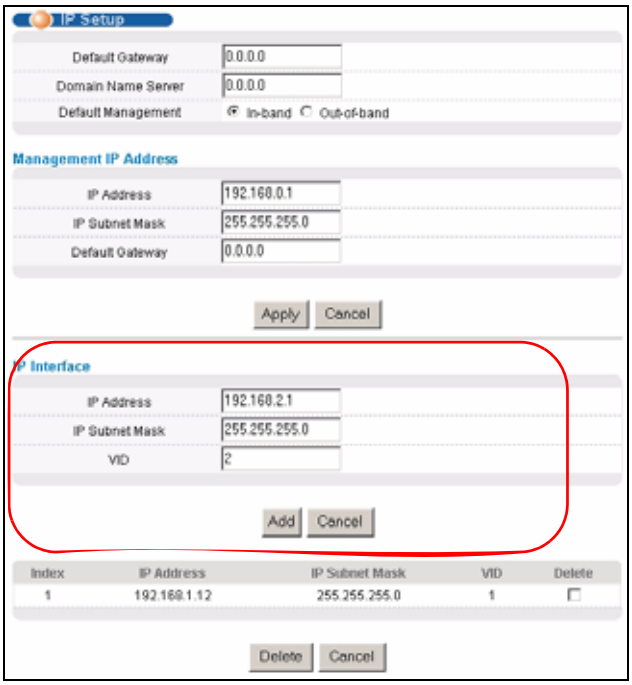
В показанном примере сети ввиду того, что сеть **Исследовательского отдела** уже находится на том же IP-интерфейсе, что и коммутатор, создавать IP-интерфейс для этой сети не требуется. Однако, если сеть **Отдела продаж** необходимо вынести в другой домен маршрутизации, для нее необходимо будет создать новый IP-интерфейс. Это позволит коммутатору маршрутизировать трафик между сетями **Исследовательского отдела** и **Отдела продаж**.

Рисунок 20 Пример первичной настройки сети: IP-интерфейс



1. Подключите свой компьютер к порту **MGMT**, который используется только для управления. Убедитесь, что компьютер находится в той же подсети, что и порт **MGMT**.
2. Откройте Web-браузер и введите в строке адреса 192.168.0.1 (IP-адрес порта **MGMT** по умолчанию), чтобы получить доступ к Web-конфигуратору. Дополнительную информацию можно найти в разд. 4.2 на стр. 55.
3. Выберите в навигационной панели **Basic Setting** и **IP Setup**.
4. Введите нужную информацию на экране **IP Setup**.

   Для сети **Отдела продаж** введите IP-адрес 192.168.2.1 и маску подсети 255.255.255.0.
5. В поле **VID** введите идентификатор группы VLAN, к которой должен принадлежать этот IP-интерфейс. Это должно быть то же значение, которое было введено в поле VLAN ID на экране меню **Static VLAN**.
6. Нажмите **Add**, чтобы сохранить настройки в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

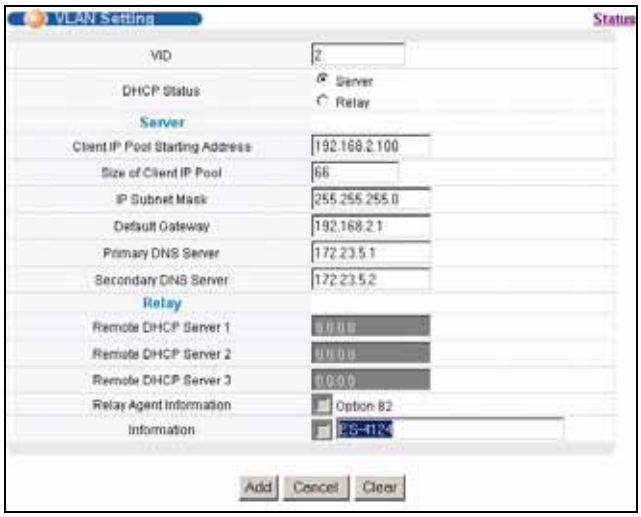


5.1.2 Настройка параметров сервера DHCP

Данный коммутатор можно настроить в качестве сервера, назначающего клиентам DHCP нужные параметры (такие как IP-адрес, адрес сервера DNS и т.д.).

В данном примере сети на коммутаторе настроены два пула клиентских параметров DHCP для клиентов DHCP в сети **Исследовательского отдела** и **Отдела продаж**.

1. Выберите в навигационной панели Web-конфигуратора **IP Application** и **DHCP**, затем нажмите на ссылке **VLAN**.
2. На экране **VLAN Setting** укажите идентификатор сети VLAN, к которой принадлежат клиенты DHCP, и введите начальный адрес пула IP-адресов, маску подсети, адрес шлюза по умолчанию и адрес или адреса серверов DNS.
3. Нажмите **Add**, чтобы сохранить настройки в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

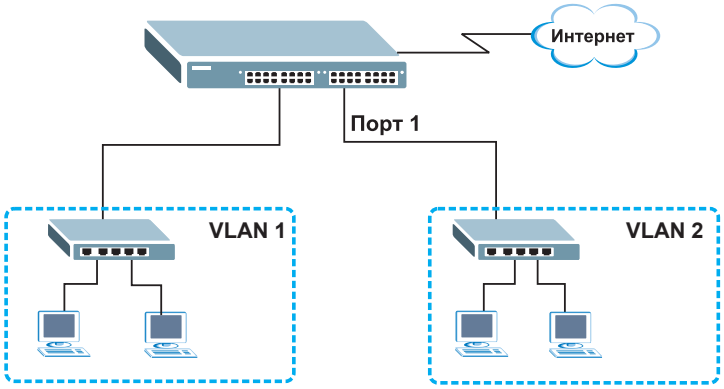


5.1.3 Создание виртуальной локальной сети VLAN

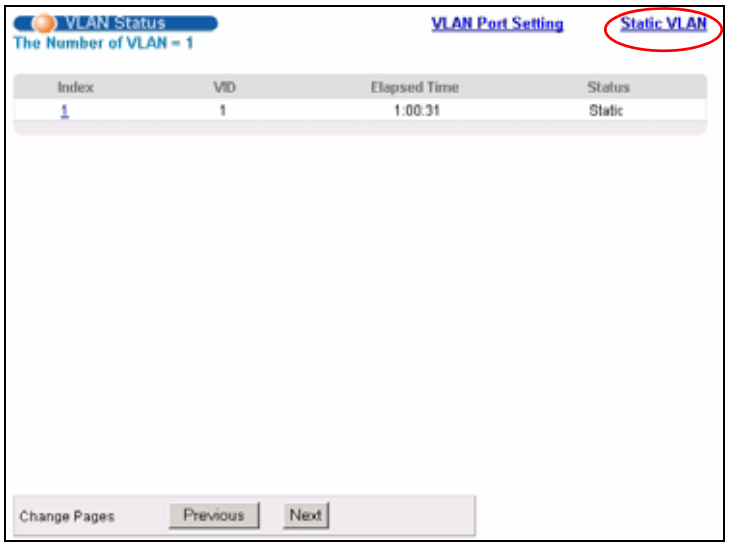
Виртуальные локальные сети ограничивают широковещательные кадры той группой VLAN, к которой принадлежит порт (порты). Для этого можно использовать виртуальные локальные сети на основе портов или статические виртуальные локальные сети на основе тегов с фиксированными портами-членами.

В данном примере порт 1 конфигурируется в качестве члена виртуальной локальной сети VLAN 2.

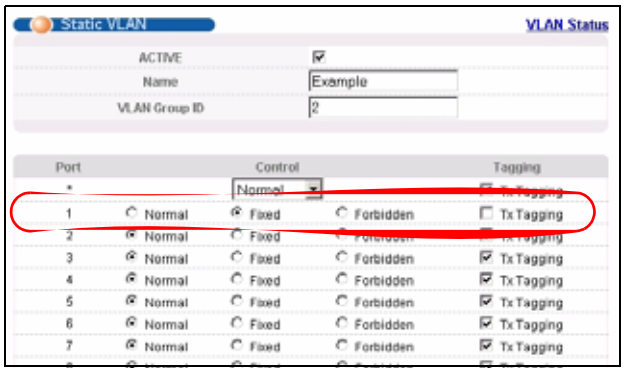
Рисунок 21 Пример первичной настройки сети: виртуальная локальная сеть



1 Выберите в навигационной панели **Advanced Application** > **VLAN** и нажмите на ссылке **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 1 коммутатора, выберите пункт **Fixed**, чтобы назначить порт 1 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.

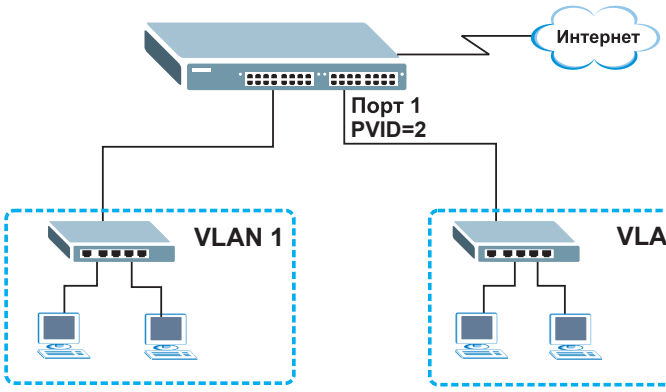
5 Нажмите **Add**, чтобы сохранить настройки в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

5.1.4 Назначение идентификатора виртуальной локальной сети VID для порта

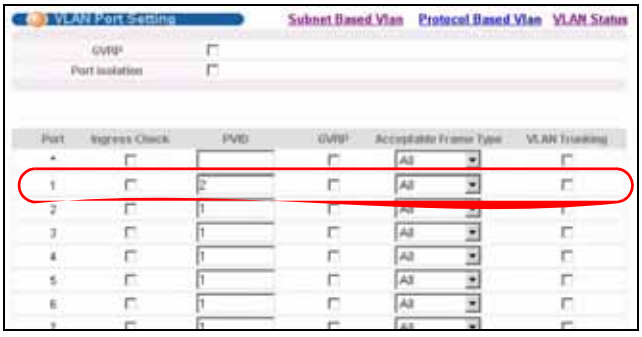
Идентификатор виртуальной локальной сети для порта (PVID) используется для добавления тегов к кадрам без тегов, поступающим на этот порт, чтобы такие кадры направлялись в ту группу VLAN, которую определяет тег.

В данном примере необходимо установить 2 в качестве идентификатора VID для порта 1, чтобы все непомеченные тегами кадры, принятые через этот порт, отправлялись в виртуальную локальную сеть VLAN 2.

Рисунок 22 Пример первичной настройки сети: идентификатор виртуальной локальной сети для порта



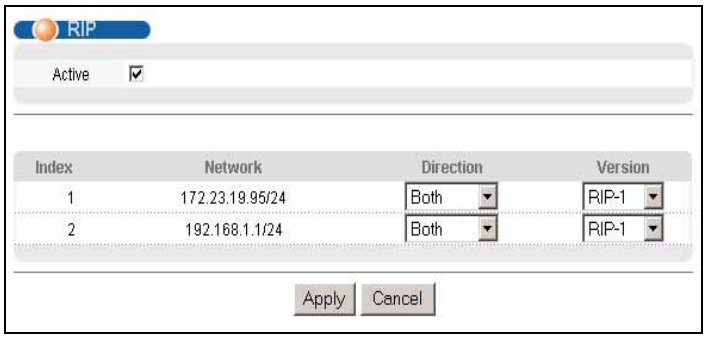
1. Выберите в навигационной панели **Advanced Applications** и **VLAN**. Затем выберите пункт **VLAN Port Setting**.
2. Введите 2 в поле **PVID** для порта 1 и нажмите **Apply**, чтобы сохранить изменения в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.



5.1.5 Включение протокола RIP

Чтобы обмениваться маршрутной информацией с другими маршрутизаторами в различных доменах маршрутизации, необходимо включить на экране **RIP** протокол RIP (протокол маршрутной информации).

1. Выберите в навигационной панели **IP Application** и затем **RIP**.



2. В поле **Direction** выберите **Both**, чтобы коммутатор передавал в широковещательном режиме и принимал маршрутную информацию.
3. В поле **Version** выберите **RIP-1**, чтобы использовать универсальный, поддерживаемый повсеместно формат пакетов RIP.
4. Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

6

Состояние системы и статистика портов

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

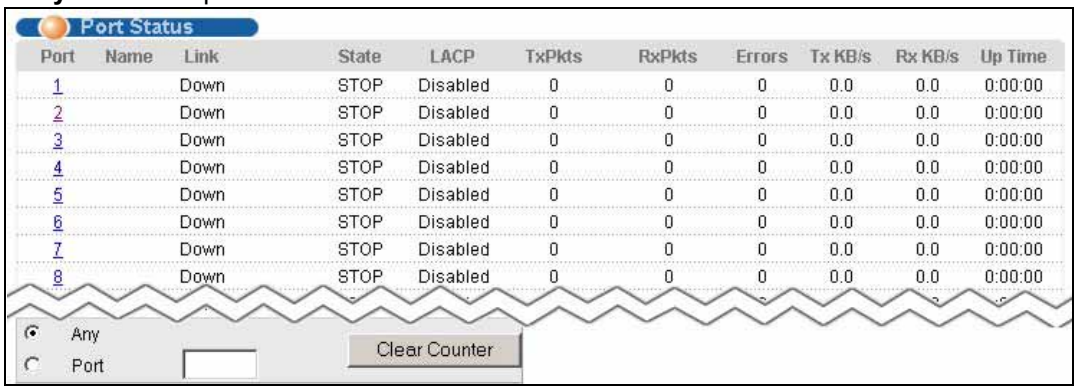
6.1 Обзор

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 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. 75).
Name	Имя, назначенное данному порту на экране **Basic Setting**, **Port Setup**.

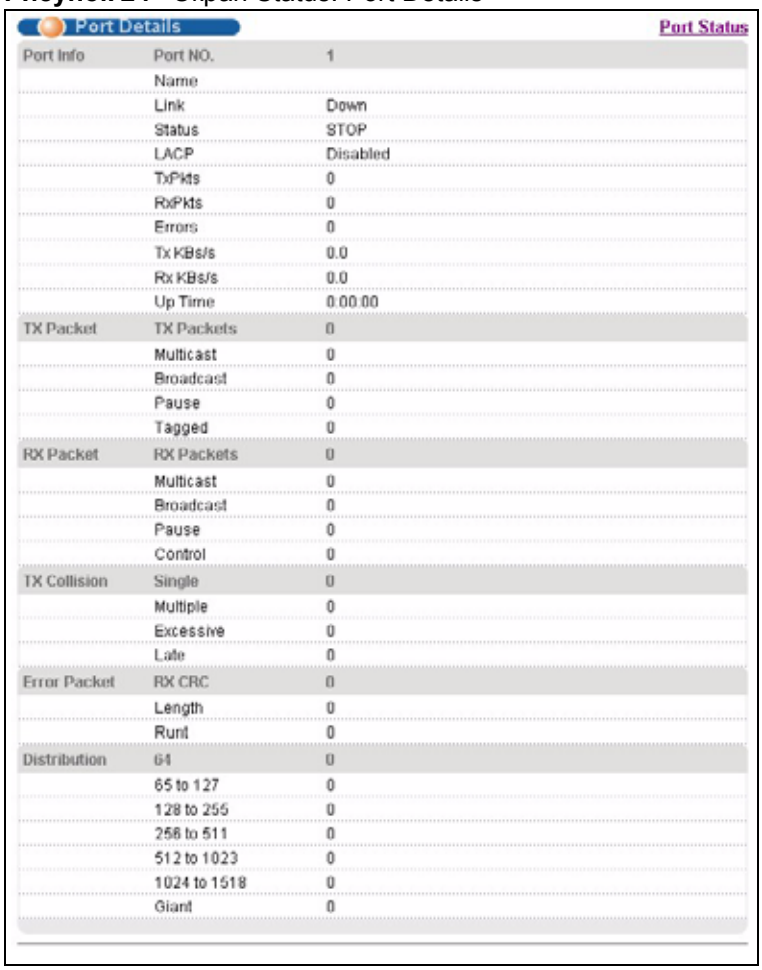
Таблица 6 Экран Status (продолжение)

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. 121). Если протокол STP отключен, в этом поле отображается **FORWARDING** в случае установленного соединения и **STOP** в противном случае.
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 (Состояние)	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. 121). Если протокол STP отключен, в этом поле отображается FORWARDING в случае установленного соединения и STOP в противном случае.
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.

Таблица 7 Экран Status > Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
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 Packet	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.
Tagged	В этом поле отображается количество переданных пакетов с тегами VLAN.
Rx Packet В следующих полях отображается подробная информация о принятых пакетах.	
RX Packet	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.
Control	В этом поле отображается количество принятых управляющих пакетов (в том числе с ошибками CRC), однако без учета пакетов Pause стандарта 802.3x.
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.
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.
Length	В этом поле отображается количество принятых пакетов, длина которых выходит за пределы диапазона.
Runt	В этом поле отображается количество принятых пакетов, оказавшихся слишком короткими (менее 64 октетов), включая пакеты с ошибками CRC.

Таблица 7 Экран Status > Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
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

System Info

System Name	ES-4124
ZyNOS F/W Version	V3.80(AIC.0)b0 | 01/19/2007
Ethernet Address	00:13:49:00:00:02

Hardware Monitor

Temperature Unit C

Temperature (C)	Current	MAX	MIN	Threshold	Status
MAC	33.5	34.0	26.0	85.0	Normal
CPU	33.0	33.0	25.0	85.0	Normal
PHY	30.5	30.5	25.0	85.0	Normal
FAN Speed (RPM)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
FAN1	6167	6392	6009	2750	Normal
FAN2	6222	6222	5958	2750	Normal
FAN3	6061	6167	5859	2750	Normal
Voltage (V)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
VCOREA	2.592	2.592	2.592	+/-10%	Normal
VINRO	1.264	1.264	1.264	+/-10%	Normal
3.3VIN	3.392	3.392	3.376	+/-8%	Normal
12VIN	12.099	12.160	12.099	+/-11%	Normal
1.3VIN	1.328	1.344	1.328	+/-10%	Normal
1.25VIN	1.264	1.264	1.264	+/-8%	Normal
1.8VIN	1.856	1.856	1.856	+/-10%	Normal
BPS_12VIN	--	--	--	--	Absent

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.
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).
Temperature:	**MAC**, **CPU** и **PHY** 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.

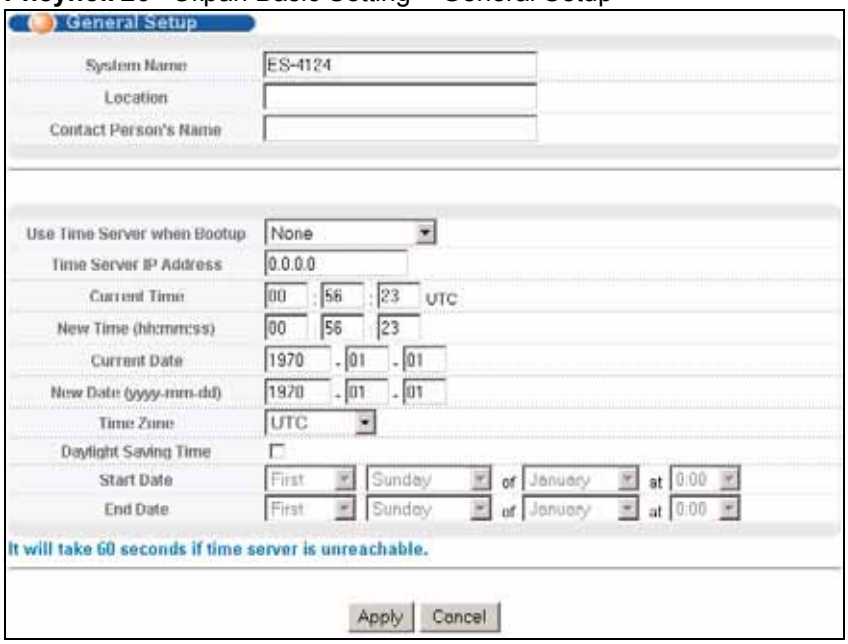
Таблица 8 Экран Basic Setting > System Info (продолжение)

ПОЛЕ	ОПИСАНИЕ
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 печатных символов ASCII; пробелы допускаются.
Contact Person's Name	Введите имя ответственного лица для данного коммутатора. В поле можно ввести до 32 печатных символов ASCII; 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 0:0 1970-1-1.
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.

Таблица 9 Экран Basic Setting > General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
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).
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.

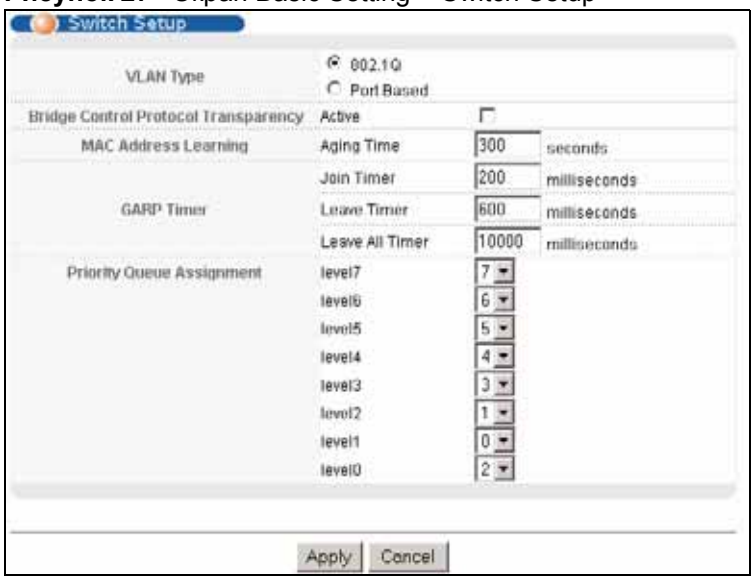
Механизм поддержки виртуальных локальных сетей VLAN работает только в одном направлении; им контролируется только исходящий трафик.

Информацию о виртуальных локальных сетях на основе портов и на основе тегов 802.1Q можно найти в гл. 8 на стр. 95.

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. 95.
Bridge Control Protocol Transparency	Выберите **Active**, чтобы разрешить на коммутаторе обработку протоколов управления мостами (например, STP). Кроме того, необходимо будет определить порядок обработки блоков данных мостового протокола BPDU на экране **Port Setup**.
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.
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.

Таблица 10 Экран Basic Setting > Switch Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
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 два поля используются для определения соответствия между уровнями приоритетов и физическими очередями. У коммутатора имеется восемь физических очередей, 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.

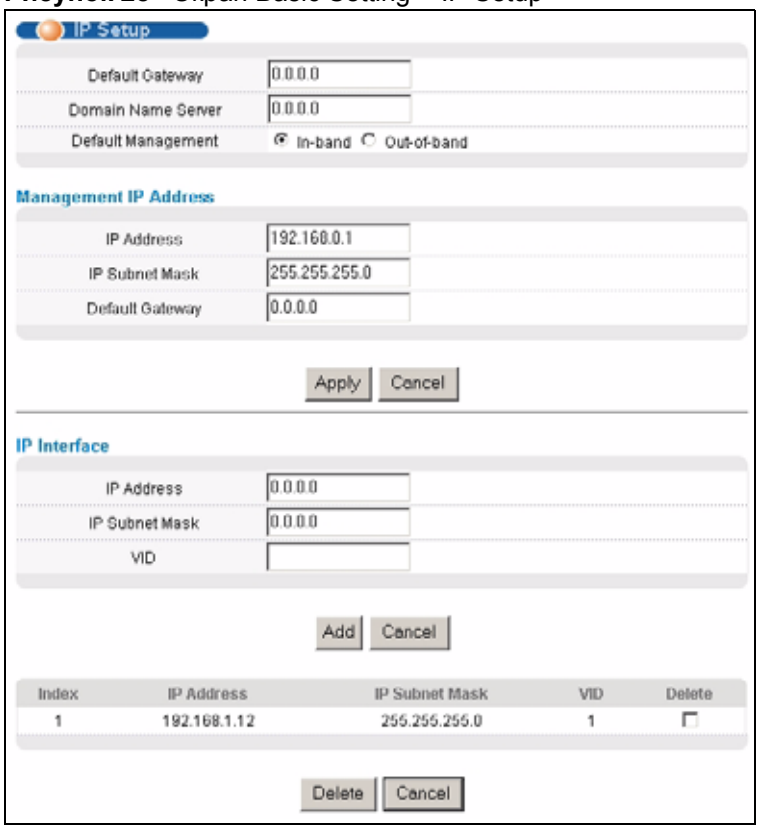
7.6.1 IP-интерфейсы

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.

На коммутаторе, как на устройстве уровня 3, IP-адрес не привязан к какому-либо физическому порту. Так как каждый IP-адрес коммутатора должен находиться в отдельной подсети, настроенные IP-адреса называют также IP-интерфейсами (или доменами маршрутизации). Более того, это позволяет осуществлять маршрутизацию между подсетями на основе IP-адресов, без использования дополнительных маршрутизаторов.

В одной и той же виртуальной локальной сети VLAN можно настроить несколько доменов маршрутизации, при условии, что диапазоны IP-адресов в них не перекрываются. Чтобы изменить IP-адрес коммутатора в конкретном домене маршрутизации, просто введите новую запись о домене маршрутизации с отличным IP-адресом в той же самой подсети.

Рисунок 28 Экран Basic Setting > IP Setup



Поля экрана описаны в следующей таблице.

Таблица 11 Экран Basic Setting > IP Setup

ПОЛЕ	ОПИСАНИЕ
Default Gateway	Введите IP-адрес исходящего шлюза по умолчанию в виде десятичных чисел, разделенных точками, например 192.168.1.254.
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	Укажите, по какому из путей (внутриполосному **In-Band** или внеполосному **Out-of-band**) данный коммутатор должен отправлять собственные пакеты (такие как «ловушки» SNMP), а также пакеты от неизвестных источников. В случае выбора **Out-of-band** данный коммутатор будет отправлять пакеты на порт управления, обозначенный как **MGMT**. При этом устройства, подключенные к другим портам, данных пакетов не получат. В случае выбора **In-Band** данный коммутатор будет отправлять пакеты на все порты, за исключением порта управления (обозначенного как **MGMT**); подключенные к последнему устройства данных пакетов не получат.
Management IP Address В данных полях указываются настройки внеполосного порта управления.	
IP Address	Введите IP-адрес внеполосного порта управления вашего коммутатора в виде десятичных чисел, разделенных точками. Например, 192.168.0.1.
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 192.168.0.254.
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.
IP Interface Данные поля используются для создания или изменения доменов IP-маршрутизации на коммутаторе.	
IP Address	Введите IP-адрес коммутатора в виде десятичных чисел, разделенных точками, например 192.168.1.1. Этот IP-адрес станет адресом коммутатора в домене IP-маршрутизации.
IP Subnet Mask	Введите IP-маску подсети домена IP-маршрутизации а в виде десятичных чисел, разделенных точками. Например, 255.255.255.0.
VID	Введите идентификационный номер сети VLAN, к которой принадлежит домен IP-маршрутизации.
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 сбросить поля к предыдущим значениям.
Index	В этом поле отображается порядковый номер записи.
IP Address	В этом поле отображается IP-адрес коммутатора в IP-домене.
Subnet Mask	В этом поле отображается маска подсети коммутатора в IP-домене.

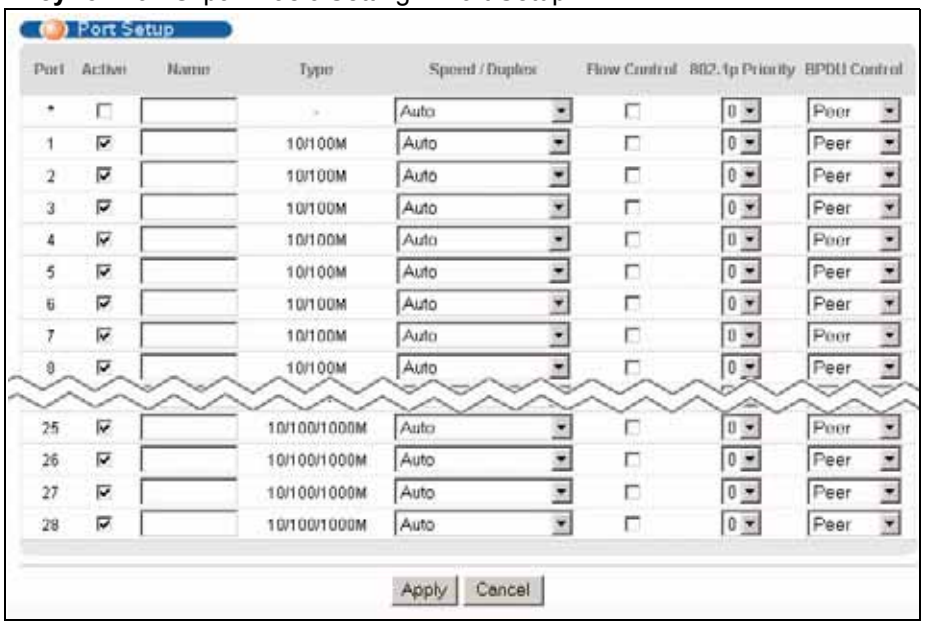
Таблица 11 Экран Basic Setting > IP Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
VID	В этом поле отображается идентификационный номер VLAN IP-домена коммутатора.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы. Примечание: При удалении всех IP-подсетей доступ к коммутатору будет заблокирован.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

7.7 Настройки портов

Данный экран используется для настройки портов коммутатора. Чтобы открыть экран настроек, 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.

Таблица 12 Экран Basic Setting > Port Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.
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. 85.

Таблица 12 Экран Basic Setting > Port Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
BPDU Control	Выберите способ обработки блоков данных мостового протокола BPDU, получаемых через данный порт. Предварительно необходимо включить режим прозрачности мостовых протоколов (Bridging Control Protocol Transparency) на экране **Switch Setup**. В случае выбора **Peer** все принимаемые через данный порт блоки данных мостового протокола BPDU будут обрабатываться. В случае выбора **Tunnel** все принимаемые через данный порт блоки BPDU будут ретранслироваться. В случае выбора **Discard** все принимаемые через данный порт блоки BPDU будут отбрасываться. В случае выбора **Network** блоки BPDU, не имеющие тега VLAN, будут обрабатываться, а блоки BPDU с тегами – ретранслироваться.
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

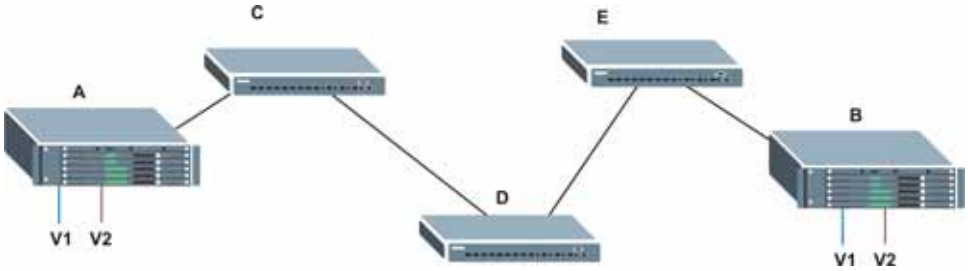
ПАРАМЕТРЫ VLAN	ТЕРМИН	ОПИСАНИЕ
Тип VLAN	Постоянная VLAN	Статическая виртуальная локальная сеть VLAN, созданная вручную.
	Динамическая VLAN	Сеть VLAN, настроенная в процессе регистрации/ дерегистрации протоколом GVRP.
Административный контроль над VLAN	Фиксированная регистрация	Порты с фиксированной регистрацией 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 VLAN порта	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.

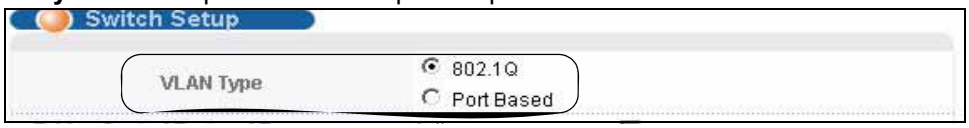
Рисунок 30 Магистральные порты VLAN



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

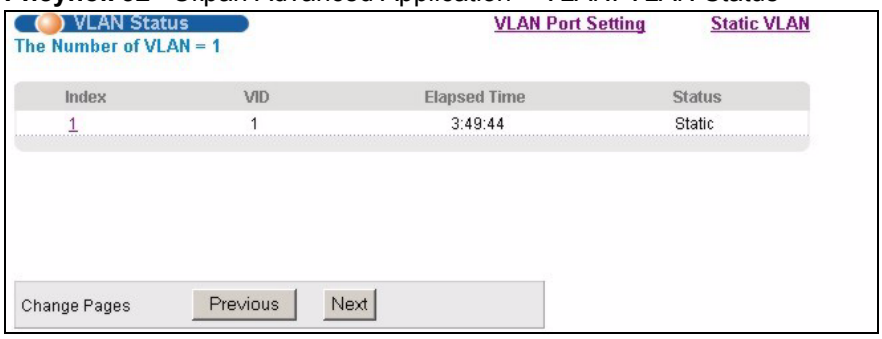
- отправлен в группу VLAN обычным образом, в зависимости от его тега VLAN.
- отправлен в группу независимо от того, имеется у него тег VLAN или нет.
- заблокирован от направления в группу VLAN независимо от его тега VLAN.

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. 95.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.

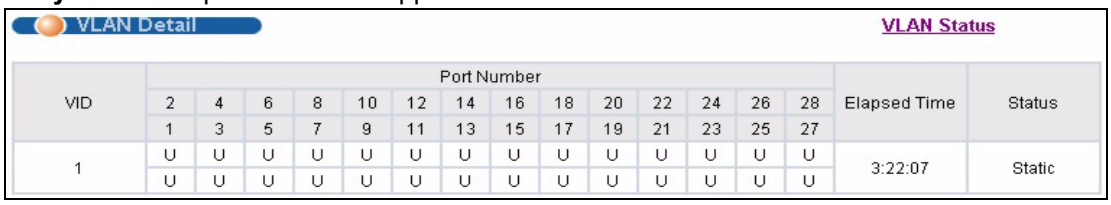
Таблица 14 Экран Advanced Application > VLAN: VLAN Status

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. 95. 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


VLAN Detail

VLAN Status

VID	Port Number														Elapsed Time	Status
	2	4	6	8	10	12	14	16	18	20	22	24	26	28		
	1	3	5	7	9	11	13	15	17	19	21	23	25	27		
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	3:22:07	Static
	U	U	U	U	U	U	U	U	U	U	U	U	U	U		

Поля экрана описаны в следующей таблице.

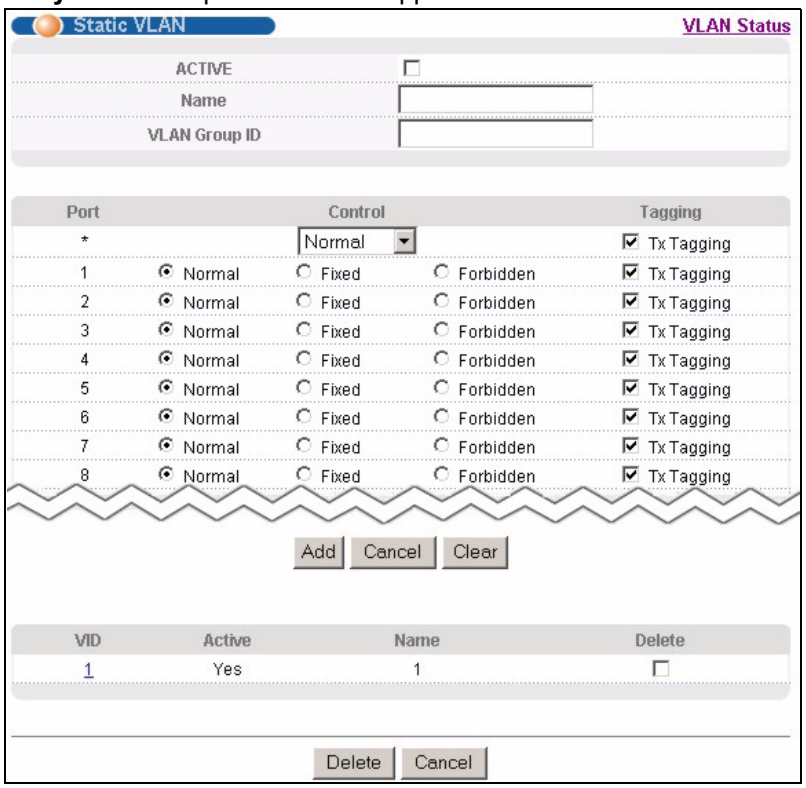
Таблица 15 Экран Advanced Application > VLAN > VLAN Detail

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. 95. 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.

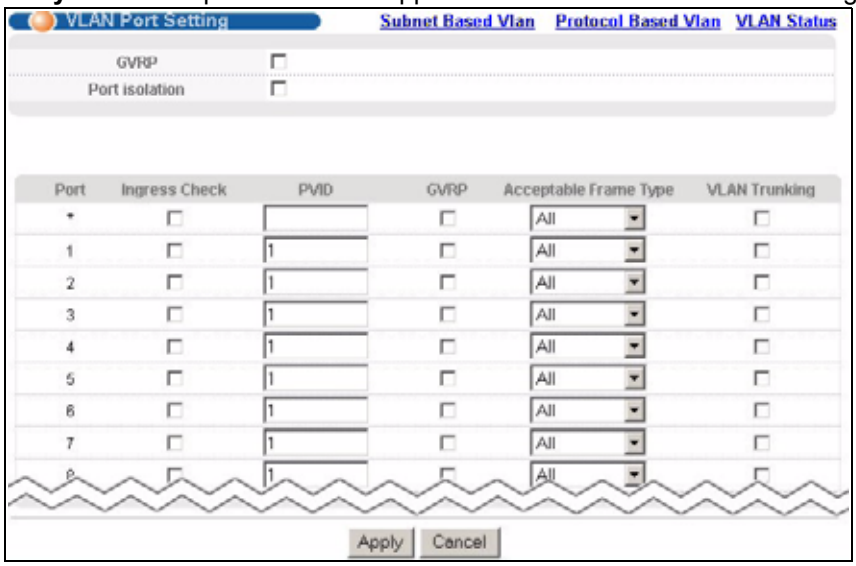
Таблица 16 Экран Advanced Application > VLAN > Static VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
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. 95.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.
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.
Ingress Check	Если данный переключатель для порта установлен, коммутатор отбрасывает входящие кадры для VLAN, членом которых не является данный порт. Снимите выделение с переключателя, если требуется отключить фильтрацию входящих кадров.
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.

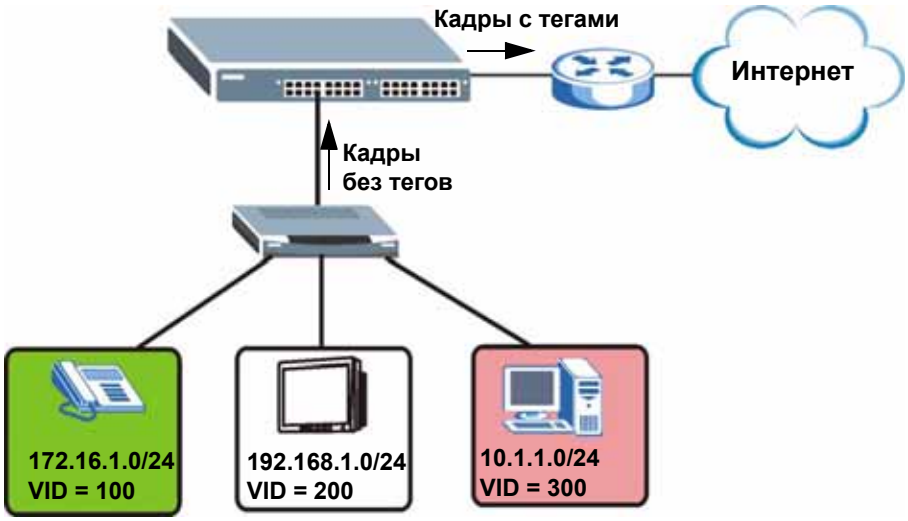
8.6 VLAN на основе подсетей

VLAN на основе подсетей позволяют сгруппировать трафик по логическим сетям VLAN на основе указанных IP-подсетей источников пакетов. При поступлении кадра через порт коммутатор проверяет, не был ли добавлен к нему тег и из какой IP-подсети он поступил. Пакеты без тегов от одной и той же IP-подсети помещаются в одну VLAN на основе подсетей. Одно из преимуществ VLAN на основе подсетей заключается в возможности назначения приоритетов для трафика из конкретных IP-подсетей.

Например, провайдер услуг Интернета (ISP) может распределить различные типы предоставляемых клиентам услуг по различным IP-подсетям. Трафик услуг голосовой связи будет назначен IP-подсети 172.16.1.0/24, видео – подсети 192.168.1.0/24, а передачи данных – подсети 10.1.1.0/24. После этого на коммутаторе можно настроить группировку входящего трафика в зависимости от IP-подсети, из которой поступают входящие кадры.

Например, для трафика из IP-подсети 172.16.1.0/24 (услуги голосовой связи) может быть настроена VLAN на основе подсетей с приоритетом 6 и идентификатором VID, равным 100. Для трафика из IP-подсети 192.168.1.0/24 (услуги передачи видео) может быть настроена VLAN на основе подсетей с приоритетом 5 и идентификатором VID, равным 200. Наконец, для трафика из IP-подсети 10.1.1.0/24 (услуги передачи данных) может быть настроена VLAN на основе подсетей с приоритетом 3 и идентификатором VID, равным 300. Все не имеющие тегов входящие кадры будут классифицироваться на основе IP-подсети источника, с назначением соответствующего приоритета. Таким образом, трафик видео получит наивысший приоритет, а трафик передачи данных – самый низкий.

Рисунок 36 Пример использования VLAN на основе подсетей

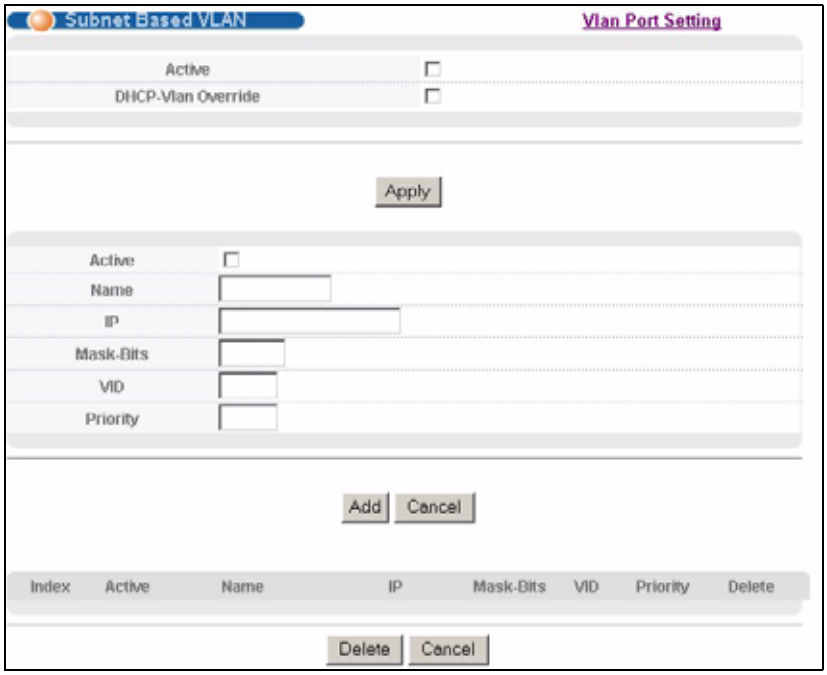


8.7 Настройка VLAN на основе подсетей

Чтобы отобразить показанный ниже экран настроек, выберите **Subnet Based VLAN** на экране **VLAN Port Setting**.

VLAN на основе подсетей применяются только к не имеющим тегов пакетам и работают лишь при использовании VLAN на основе тегов IEEE 802.1Q.

Рисунок 37 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN



Поля экрана описаны в следующей таблице.

Таблица 18 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на коммутаторе VLAN на основе подсетей.
DHCP-Vlan Override	При включении функции отслеживания DHCP клиенты DHCP могут обновлять свои IP-адреса через DHCP VLAN или через другой сервер DHCP во VLAN на основе подсетей. Установите данный переключатель, чтобы клиенты DHCP в данной IP-подсети принудительно получали IP-адреса через DHCP 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.
Active	Установите данный переключатель, чтобы включить создаваемую или изменяемую VLAN на основе подсети.
Name	Введите до 32 алфавитно-цифровых символов для обозначения данной VLAN на основе подсети.
IP	Введите IP-адрес подсети, для которой необходимо настроить VLAN.
Mask-Bits	Введите количество битов в маске подсети. Чтобы определить количество битов, переведите маску подсети в двоичную форму и подсчитайте число единичных битов. Возьмем, к примеру, маску «255.255.255.0». 255 в двоичной форме – это восемь единиц. Всего в маске 3 байта со значением «255», поэтому количество единичных битов будет три на восемь (24).
VID	Введите идентификатор сети VLAN, к которой привязываются при помощи тегов все не имеющие тегов кадры из IP-подсети для данной VLAN на основе подсети. Данная VLAN должна быть предварительно определена на экранах **Advanced Applications**, **VLAN**.

Таблица 18 Экран Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Priority	Выберите уровень приоритета, назначаемый коммутатором кадрам из данной 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.
Index	Порядковый номер данной VLAN на основе подсети. Нажатие на любом из этих номеров позволяет отредактировать параметры существующей VLAN на основе подсети.
Active	В данном поле указано, является ли данная VLAN на основе подсети активной.
Name	В этом поле отображается имя VLAN на основе подсети.
IP	В этом поле отображается IP-адрес подсети для данной VLAN на основе подсети.
Mask-Bits	В этом поле отображается маска подсети в виде количества единичных битов для данной VLAN на основе подсети.
VID	В данном поле отображается идентификатор VLAN ID для кадров, принадлежащих к данной VLAN на основе подсети.
Priority	В данном поле отображается приоритет, назначаемый кадрам из данной VLAN на основе подсети.
Delete	Нажмите на данную кнопку, чтобы удалить выделенные для удаления VLAN на основе подсетей.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

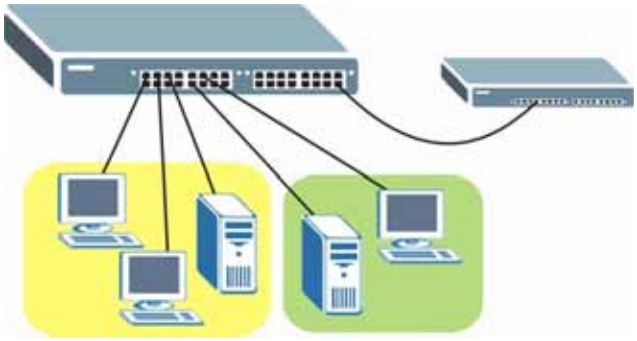
8.8 VLAN на основе протоколов

VLAN на основе протоколов позволяют сгруппировать трафик по логическим сетям VLAN на основе указанных протоколов. При поступлении от устройства более низкого уровня кадра через порт (для которого настроена VLAN на основе протокола) коммутатор проверяет, не был ли добавлен к нему тег, а также используемый кадром протокол. Пакеты без тегов с одним и тем же протоколом помещаются в одну VLAN на основе протокола. Одно из преимуществ VLAN на основе протоколов заключается в возможности назначения приоритетов для трафика с конкретным протоколом.

VLAN на основе протоколов применяются только к не имеющим тегов пакетам и работают лишь при использовании VLAN на основе тегов IEEE 802.1Q.

Например, пусть порты 1, 2, 3 и 4 принадлежат статической VLAN 100, а порты 4, 5, 6, 7 – статической VLAN 120. Пользователь настраивает VLAN на основе протоколов A с приоритетом 3 для трафика ARP, принимаемого через порты 1, 2 и 3. Также настраивается VLAN на основе протоколов B с приоритетом 2 для трафика Apple Talk, принимаемого через порты 6 и 7. В этом случае весь трафик ARP от устройств более низкого уровня, принимаемый через порты 1, 2 и 3, будет помещаться в одну группу, а весь трафик Apple Talk, поступающий через порты 6 и 7 – в другую, причем этот трафик будет иметь более высокий приоритет по сравнению с трафиком ARP при отправке на магистральный коммутатор C.

Рисунок 38 Пример использования VLAN на основе протоколов

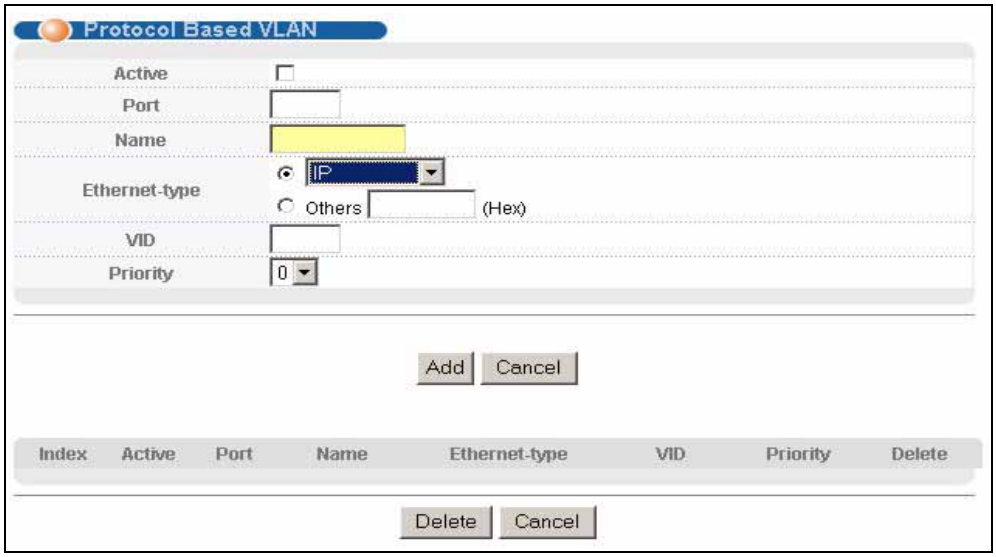


8.9 Настройка VLAN на основе протоколов

Чтобы отобразить показанный ниже экран настроек, выберите **Protocol Based VLAN** на экране **VLAN Port Setting**.

VLAN на основе протоколов применяются только к не имеющим тегов пакетам и работают лишь при использовании VLAN на основе тегов IEEE 802.1Q.

Рисунок 39 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN



Поля экрана описаны в следующей таблице.

Таблица 19 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить данную VLAN на основе протокола.
Port	Введите порт, который должен быть включен в данную VLAN на основе протокола. Данный порт должен принадлежать статической VLAN – только в этом случае он может использоваться во VLAN на основе протокола. Дополнительную информацию о настройке VLAN можно найти в гл. 8 на стр. 95.
Name	Введите до 32 алфавитно-цифровых символов для обозначения данной VLAN на основе протокола.
Ethernet-type	Выберите один из предустановленных протоколов из ниспадающего списка или выберите значение **Others** и введите номер протокола в шестнадцатеричном виде. Например, протокол IP имеет в шестнадцатеричном виде номер 0800, а протокол Novell IPX – номер 8137. Примечание: Протоколы с номерами в диапазоне от 0x0000 до 0x05ff (в шестнадцатеричном виде) использовать во VLAN на основе протоколов не допускается.
VID	Введите идентификатор VLAN, к которой принадлежит порт. Данная VLAN должна быть предварительно определена на экранах **Advanced Applications**, **VLAN**.
Priority	Выберите уровень приоритета, назначаемый коммутатором кадрам из данной 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.

Таблица 19 Экран Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup (продолжение)

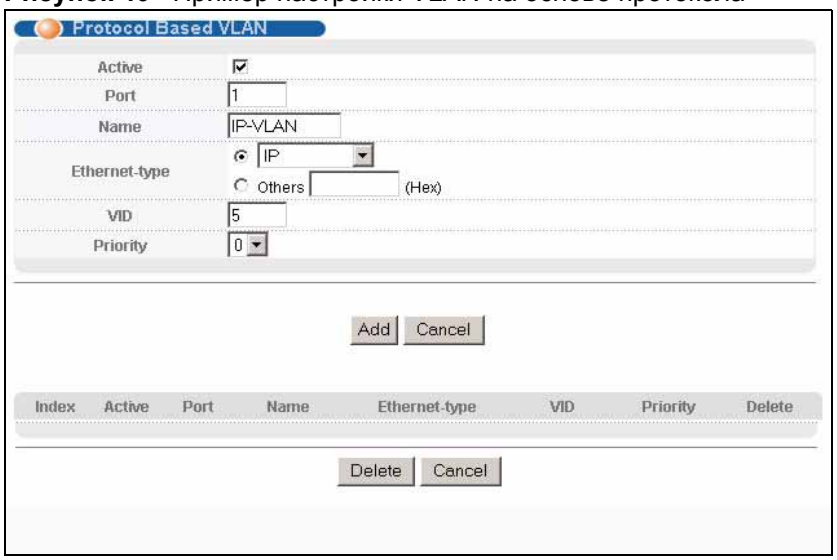
ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер данной VLAN на основе протокола. Нажатие на любом из этих номеров позволяет отредактировать параметры существующей VLAN на основе протокола.
Active	В данном поле указано, является ли данная VLAN на основе протокола активной.
Port	В этом поле указано, какой порт принадлежит к данной VLAN на основе протокола.
Name	В этом поле отображается имя VLAN на основе протокола.
Ethernet Type	В этом поле указано, какой из протоколов Ethernet принадлежит к данной VLAN на основе протокола.
VID	В этом поле отображается идентификатор VLAN порта.
Priority	В данном поле отображается приоритет, назначаемый кадрам из данной VLAN на основе протокола.
Delete	Нажмите на данную кнопку, чтобы удалить выделенные для удаления VLAN на основе протоколов.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

8.10 Пример создания VLAN на основе протокола IP

В данном примере показано создание VLAN на основе протокола IP, в которую включаются порты 1, 4 и 8. Для этого необходимо выполнить следующие действия:

1. Активировать данную VLAN на основе протокола.
2. Ввести номер порта, который должен быть включен в данную VLAN на основе протокола. Введите **1**.
3. Указать имя-описание данной VLAN на основе протокола. Введите **IP-VLAN**.
4. Выбрать протокол. Оставьте выбранное по умолчанию значение **IP**.
5. Ввести идентификатор существующей VLAN. В нашем примере используется уже созданная статическая VLAN с идентификатором 5. Введите **5**.
6. Оставить приоритет равным значению по умолчанию **0** и нажать **Add**.

Рисунок 40 Пример настройки VLAN на основе протокола



Чтобы добавить дополнительные порты в данную VLAN на основе протокола:

1. Нажмите на порядковый номер записи в таблице VLAN на основе протоколов. Нажмите на **1**
2. Измените значение в поле **Port** на номер следующего порта, который требуется добавить.
3. Нажмите **Add**.

8.11 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.

8.11.1 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 41 Экран Advanced Application > VLAN: Port Based VLAN Setup (All Connected)

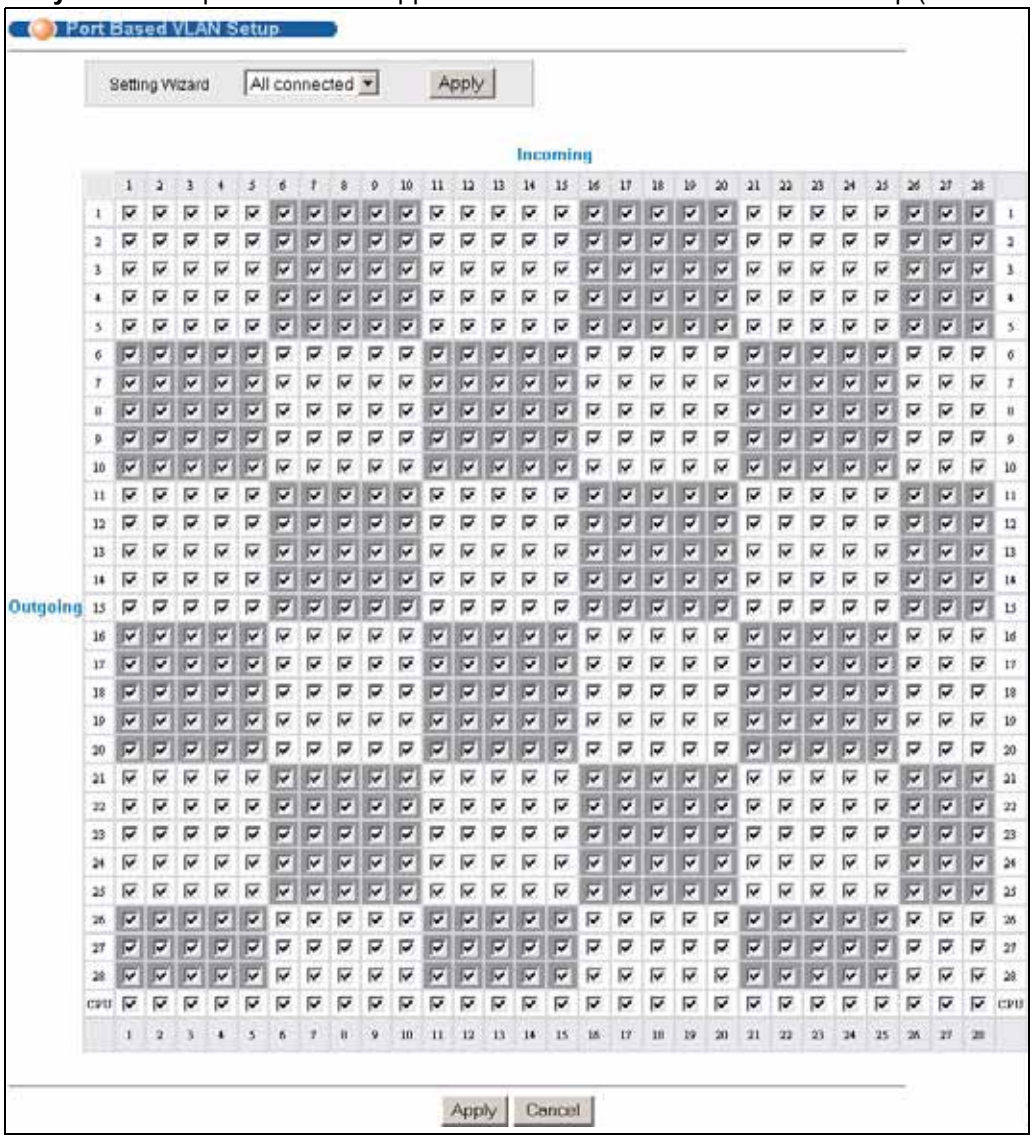
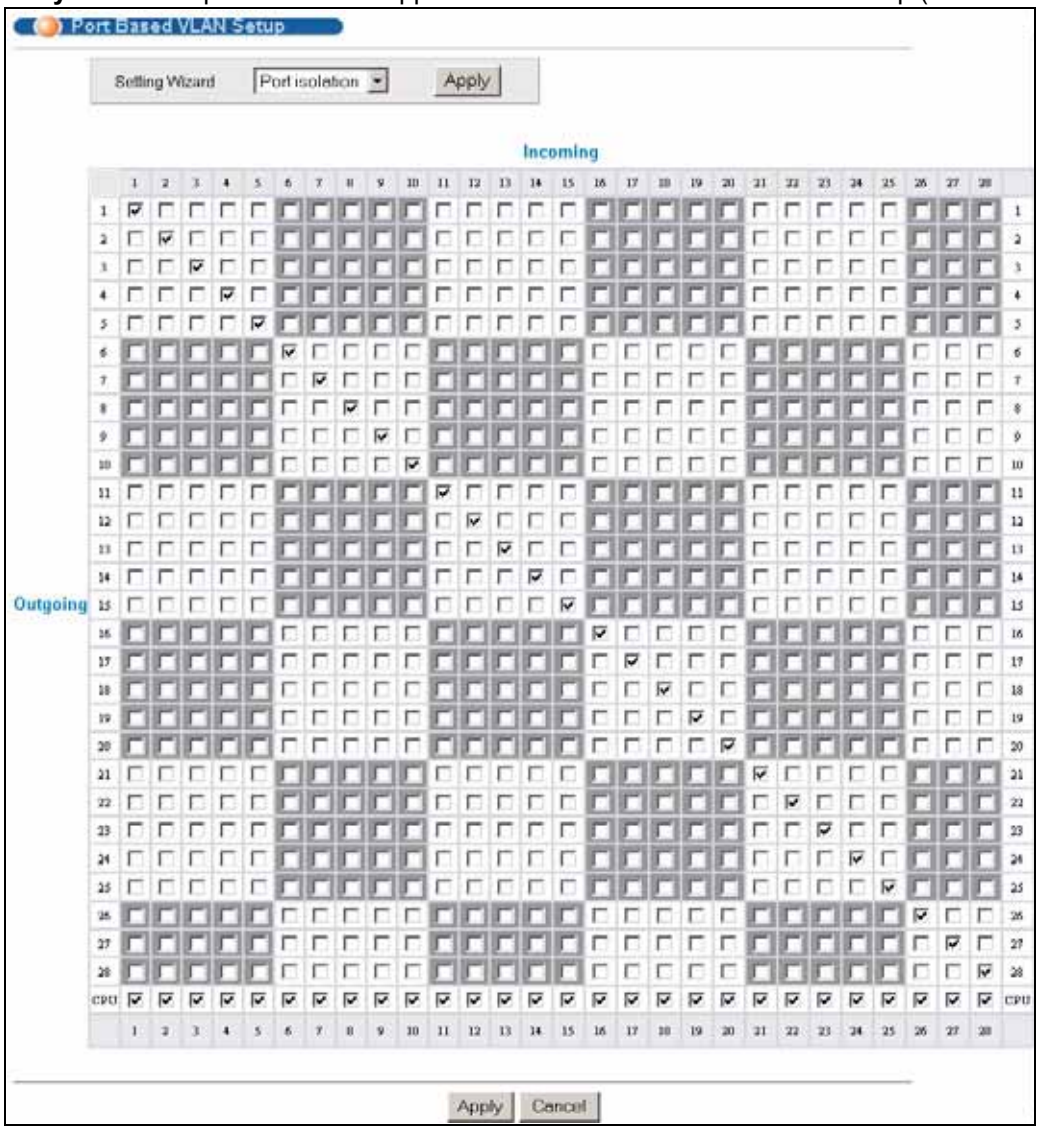


Рисунок 42 Экран Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



Поля экрана описаны в следующей таблице.

Таблица 20 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.

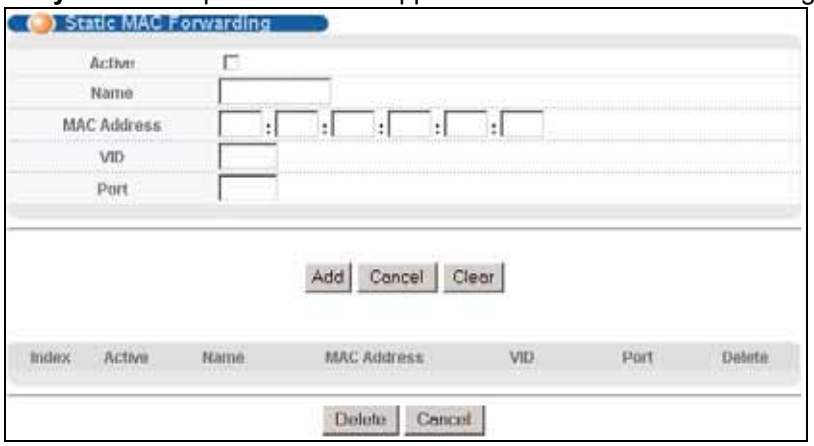
9.2 Настройка пересылки на основе статических MAC-адресов

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. 163.

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

Рисунок 43 Экран Advanced Application > Static MAC Forwarding



Поля экрана описаны в следующей таблице.

Таблица 21 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.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

10

Фильтрация

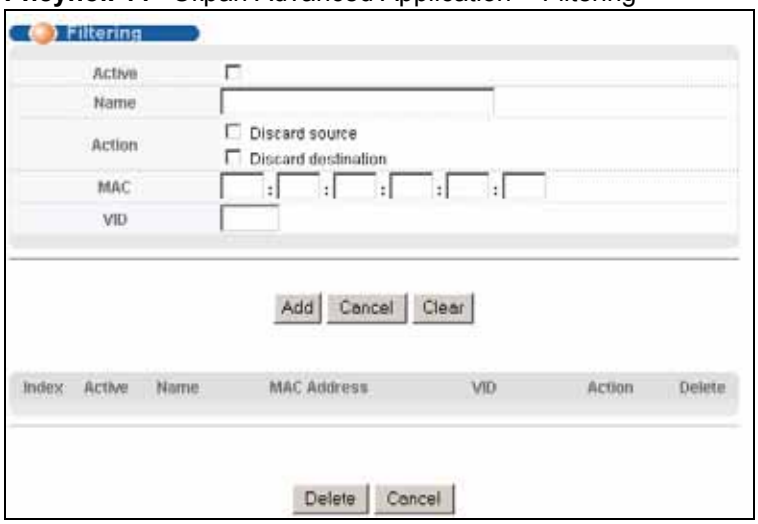
В этой главе описана фильтрация MAC-адресов на портах.

10.1 Настройка правила фильтрации

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

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

Рисунок 44 Экран Advanced Application > Filtering



Поля экрана описаны в следующей таблице.

Таблица 22 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 ASCII-символов) для этого правила. Оно будет использоваться только для идентификации.

Таблица 22 Экран Advanced Application > FIltering (продолжение)

ПОЛЕ	ОПИСАНИЕ
Action	Выберите **Discard source**, чтобы отбрасывать кадры от указанного MAC-адреса источника (указанного в поле **MAC**). При этом коммутатор будет по-прежнему отправлять кадры на указанный MAC-адрес. Выберите **Discard destination**, чтобы отбрасывать кадры на указанный MAC-адрес назначения (указанный в поле **MAC**). При этом коммутатор будет по-прежнему получать кадры от указанного MAC-адреса. Выберите **Discard source** и **Discard destination**, чтобы блокировать трафик от указанного в поле **MAC** адреса и на этот адрес.
MAC	Введите MAC-адрес в соответствующем формате, то есть шесть пар шестнадцатеричных чисел.
VID	Введите идентификационный номер 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 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 источника/пункта назначения, 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 23 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 24 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 Быстрый протокол нескольких экземпляров покрывающего дерева

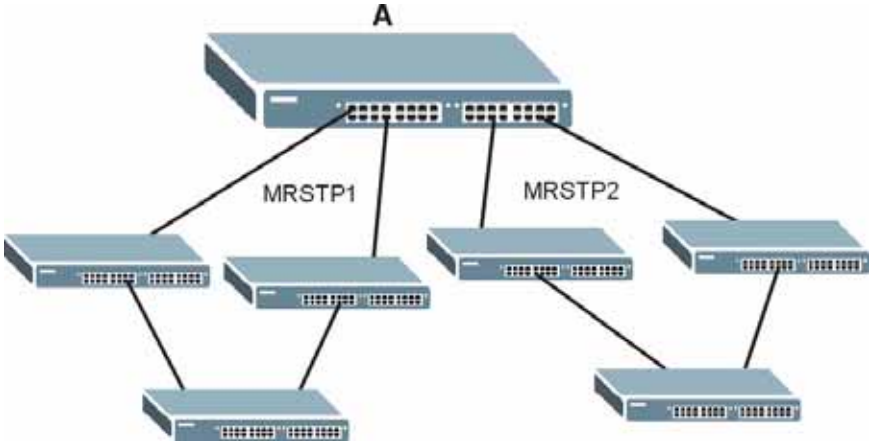
Протокол MRSTP (быстрый протокол нескольких экземпляров покрывающего дерева, Multiple RSTP) представляет собой фирменную функцию ZyXEL, совместимую с протоколами RSTP и STP. Поддержка MRSTP позволяет настроить на коммутаторе несколько экземпляров покрывающего дерева и назначать порты каждому дереву. Каждое из покрывающих деревьев работает независимо с использованием собственной информации о мостах.

В показанном ниже примере на коммутаторе **A** используются два экземпляра RSTP (**MRSTP 1** и **MRSTP2**).

Для настройки MRSTP необходимо включить MRSTP на коммутаторе и указать порты, принадлежащие к каждому из экземпляров покрывающего дерева.

Каждый порт может принадлежать только к одному дереву STP.

Рисунок 45 Пример сети с поддержкой MRSTP



11.1.5 Протокол MSTP

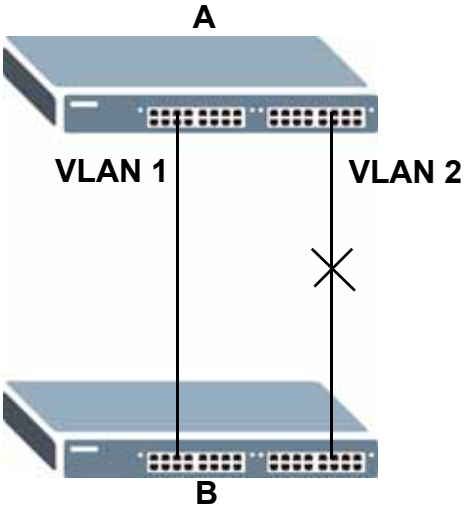
Протокол нескольких экземпляров покрывающего дерева MSTP (IEEE 802.1s) обратно совместим с протоколами STP/RSTP и устраняет ограничения, характерные для существующих протоколов STP и RSTP за счет реализации следующих функций:

- 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.

11.1.5.1 Пример сети с поддержкой MSTP

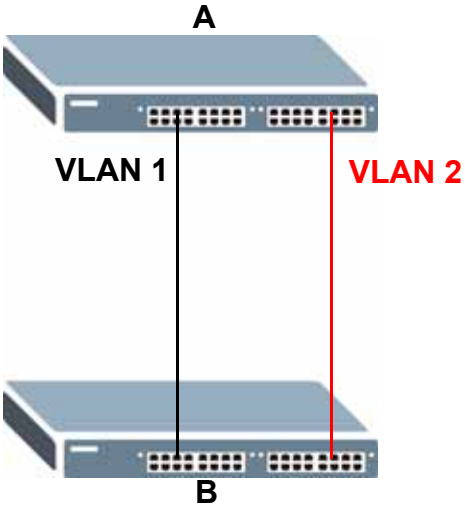
На приведенном ниже рисунке показан пример сети, в которой на двух коммутаторах настроены две сети VLAN. В случае использования на коммутаторах протокола STP или RSTP канал для VLAN 2 будет заблокирован, так как протоколы STP и RSTP допускают наличие только одного канала и блокируют избыточные каналы.

Рисунок 46 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 47 Пример сети с поддержкой MSTP



11.1.5.2 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:

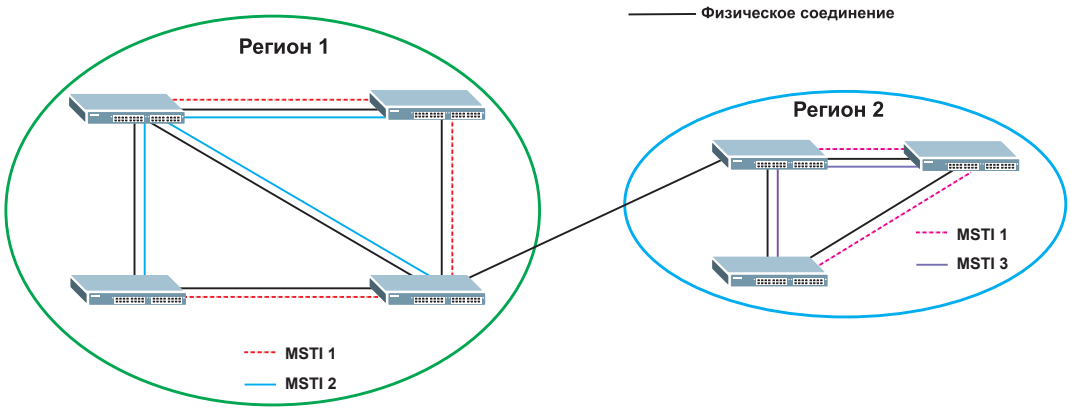
- Имя региона MST
- Номер версии в качестве уникального номера региона MST
- Связывание VLAN с конкретным экземпляром MST

11.1.5.3 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.

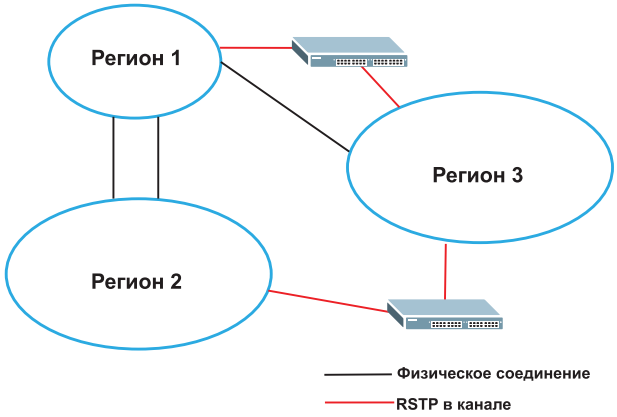
Рисунок 48 Экземпляры MSTI в различных регионах



11.1.5.4 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.

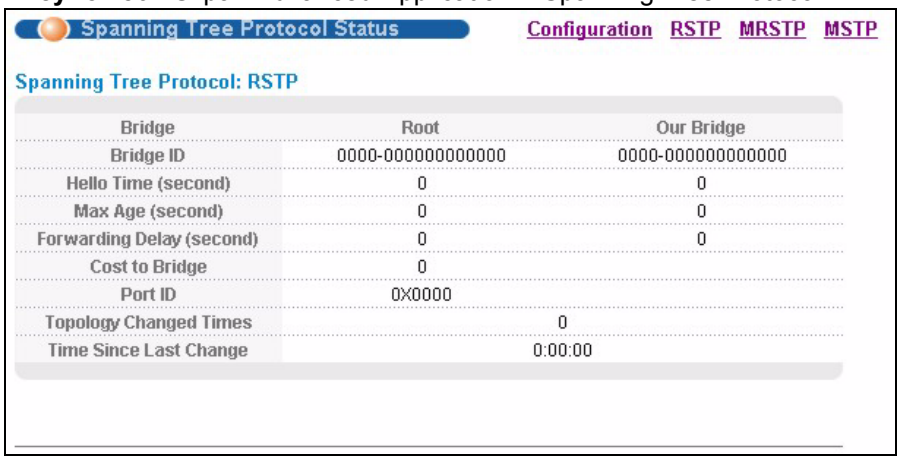
Рисунок 49 Пример сети с использованием MSTP и традиционного протокола RSTP



11.2 Экран состояния протокола STP

Вид экрана состояния протокола покрывающего дерева зависит от того, какой стандарт был выбран для сети. Чтобы открыть приведенный ниже экран, нажмите **Advanced Application** > **Spanning Tree Protocol**.

Рисунок 50 Экран Advanced Application > Spanning Tree Protocol



Вид данного экрана зависит от того, какой из режимов STP (RSTP, MRSTP или MSTP) был выбран на коммутаторе. Подробное описание данного экрана приводится в разделе, следующим за разделом с описанием настройки соответствующего режима STP. Чтобы выбрать один из режимов STP для коммутатора, нажмите на **Configuration**.

11.3 Настройка протокола покрывающего дерева

На экране **Spanning Tree Configuration** можно активировать на коммутаторе один из режимов STP. Нажмите на **Configuration** на экране **Advanced Application** > **Spanning Tree Protocol**.

Рисунок 51 Экран Advanced Application > Spanning Tree Protocol > Configuration

Поля экрана описаны в следующей таблице.

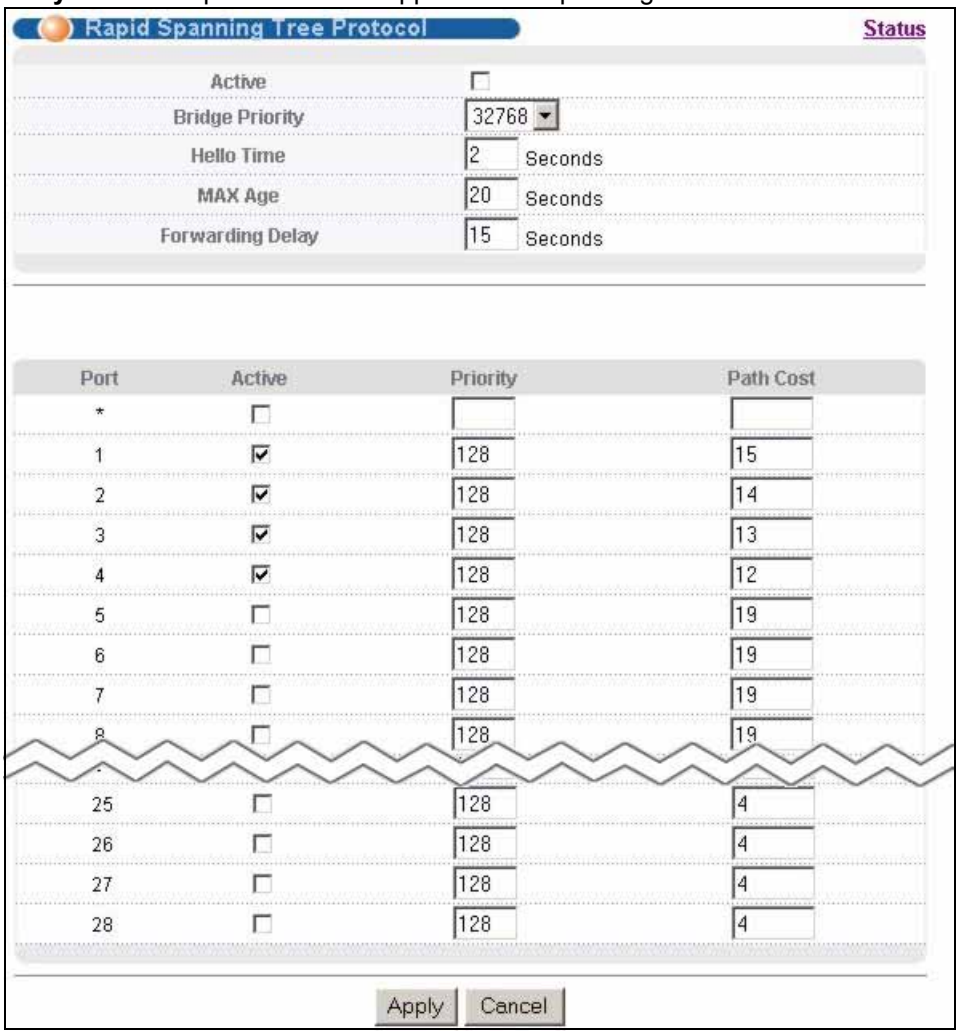
Таблица 25 Экран Advanced Application > Spanning Tree Protocol > Configuration

ПОЛЕ	ОПИСАНИЕ
Spanning Tree Mode	На коммутаторе можно активировать один из режимов STP: Выберите **Rapid Spanning Tree**, **Multiple Rapid Spanning Tree** или **Multiple Spanning Tree**. Общую информацию о STP можно найти в разд. 11.1 на стр. 119.
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 Настройка быстрого протокола покрывающего дерева

Данный экран используется для настройки RSTP; более подробную информацию о RSTP можно найти в разд. 11.1 на стр. 119. Нажмите на **RSTP** на экране **Advanced Application** > **Spanning Tree Protocol**.

Рисунок 52 Экран Advanced Application > Spanning Tree Protocol > RSTP



Поля экрана описаны в следующей таблице.

Таблица 26 Экран Advanced Application > Spanning Tree Protocol > RSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите **Status**, чтобы отобразить экран состояния **RSTP Status** (см. рис. 53 на стр. 129).
Active	Установите этот переключатель, чтобы включить протокол RSTP. Снимите выделение с переключателя, чтобы отключить RSTP. Примечание: Чтобы включить протокол RSTP на коммутаторе, необходимо также активировать режим **Rapid Spanning Tree** на экране **Advanced Application** > **Spanning Tree Protocol** > **Configuration**.

Таблица 26 Экран Advanced Application > Spanning Tree Protocol > RSTP

ПОЛЕ	ОПИСАНИЕ
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.
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.

Таблица 26 Экран Advanced Application > Spanning Tree Protocol > RSTP

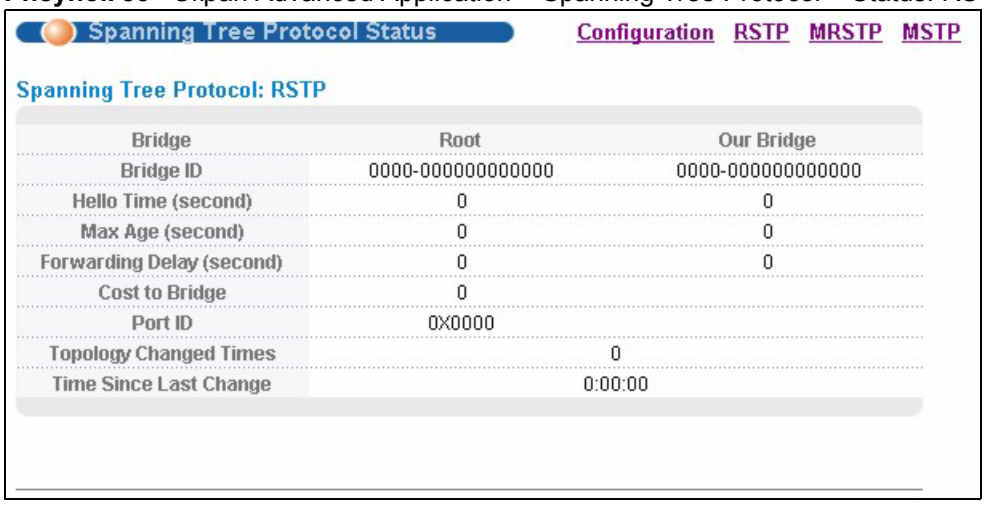
ПОЛЕ	ОПИСАНИЕ
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – дополнительную информацию можно найти в табл. 23 на стр. 120.
Apply	Нажмите **Apply**, чтобы 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.

11.5 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. 119.

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

Рисунок 53 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP



Поля экрана описаны в следующей таблице.

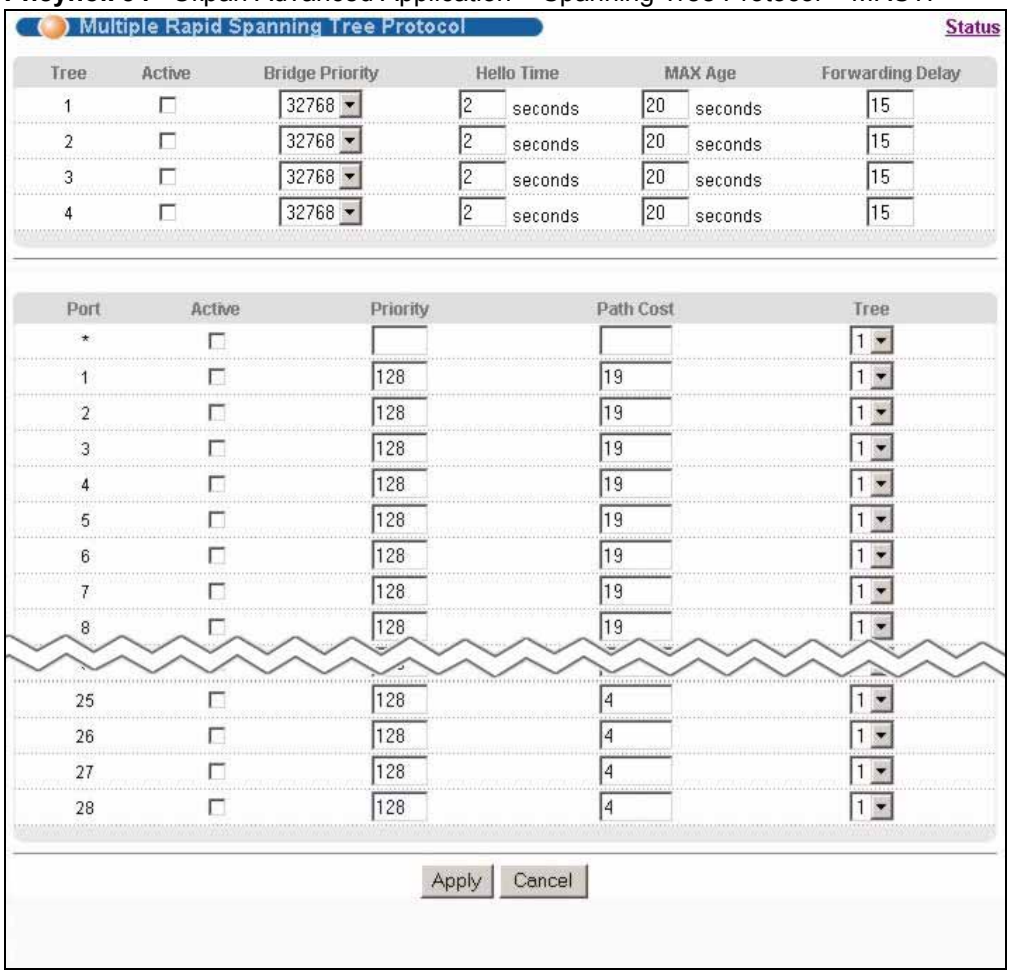
Таблица 27 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP

ПОЛЕ	ОПИСАНИЕ
Configuration	Нажмите **Configuration**, чтобы выбрать нужный режим STP. Чтобы изменить настройки RSTP коммутатора, нажмите **RSTP**.
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.
Topology Changed Times	Количество смен конфигурации покрывающего дерева.
Time Since Last Change	Время, прошедшее с последней смены конфигурации покрывающего дерева.

11.6 Настройка протокола MRSTP

Чтобы настроить протокол MRSTP, нажмите на **MRSTP** на экране **Advanced Application** > **Spanning Tree Protocol**. Более подробную информацию о MRSTP можно найти в разд. 11.1 на стр. 119.

Рисунок 54 Экран Advanced Application > Spanning Tree Protocol > MRSTP



Поля экрана описаны в следующей таблице.

Таблица 28 Экран Advanced Application > Spanning Tree Protocol > MRSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите **Status**, чтобы отобразить экран состояния **MRSTP Status** (см. рис. 53 на стр. 129).
Tree	Порядковый номер дерева STP (только для чтения).
Active	Установите этот переключатель, чтобы включить дерево протокола STP. Снимите выделение с переключателя, чтобы отключить дерево протокола STP. Примечание: Чтобы включить протокол MRSTP на коммутаторе, необходимо также активировать режим **Multiple Rapid Spanning Tree** на экране **Advanced Application** > **Spanning Tree Protocol** > **Configuration**.

Таблица 28 Экран Advanced Application > Spanning Tree Protocol > MRSTP

ПОЛЕ	ОПИСАНИЕ
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.
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 STP.
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. 23 на стр. 120.

Таблица 28 Экран Advanced Application > Spanning Tree Protocol > MRSTP

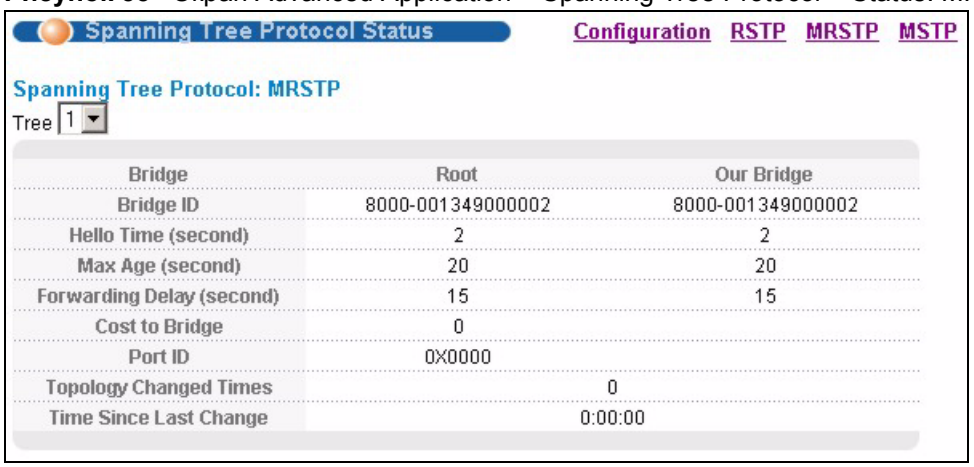
ПОЛЕ	ОПИСАНИЕ
Tree	Укажите, к какому дереву STP должен принадлежать данный порт.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать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

11.7 Состояние протокола MRSTP

Чтобы отобразить следующий экран состояния, нажмите в навигационной панели **Advanced Application** > **Spanning Tree Protocol**. Более подробную информацию о MRSTP можно найти в разд. 11.1 на стр. 119.

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

Рисунок 55 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP



Поля экрана описаны в следующей таблице.

Таблица 29 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP

ПОЛЕ	ОПИСАНИЕ
Configuration	Нажмите **Configuration**, чтобы выбрать нужный режим STP. Для изменения настроек MRSTP коммутатора нажмите на **MRSTP**.
Tree	Выберите дерево STP, настройки которого необходимо отобразить.
Bridge	**Root** относится к основанию покрывающего дерева (корневой мост). **Our Bridge** – данный коммутатор. Данный коммутатор также может быть корневым мостом.

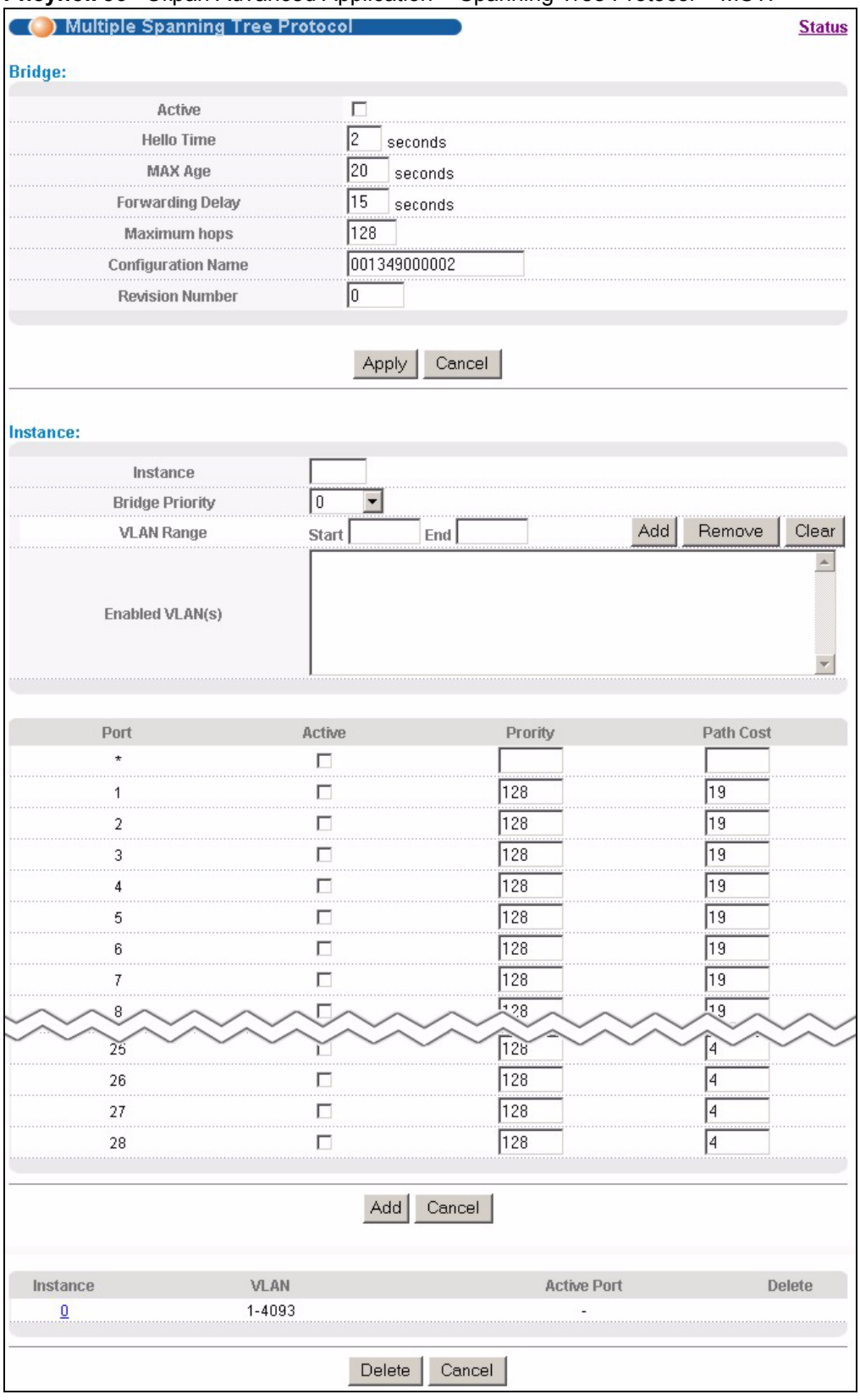
Таблица 29 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP

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

11.8 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. 11.1.5 на стр. 122.

Рисунок 56 Экран Advanced Application > Spanning Tree Protocol > MSTP



Поля экрана описаны в следующей таблице.

Таблица 30 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите **Status**, чтобы отобразить экран состояния **MSTP Status** (см. рис. 57 на стр. 139).
Active	Установите этот переключатель, если необходимо включить протокол MSTP на коммутаторе. Снимите выделение с переключателя, если требуется отключить протокол MSTP на коммутаторе. Примечание: Чтобы включить протокол MSTP на коммутаторе, необходимо также активировать режим **Multiple Spanning Tree** на экране **Advanced Application > Spanning Tree Protocol > Configuration**.
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.
MaxAge	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).

Таблица 30 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
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 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 и 61440).
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. 23 на стр. 120.
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.

Таблица 30 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
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.

11.9 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. 11.1.5 на стр. 122.

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

Рисунок 57 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

Поля экрана описаны в следующей таблице.

Таблица 31 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.
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.

Таблица 31 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

ПОЛЕ	ОПИСАНИЕ
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 Обзор управления пропускной способностью

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

12.1.1 CIR и PIR

Гарантированная скорость передачи информации (Committed Information Rate, CIR) представляет собой гарантированную пропускную способность для входящего трафика через порт. Пиковая скорость передачи информации (Peak Information Rate, PIR) представляет собой максимальную пропускную способность, которая может быть предоставлена для входящего трафика через порт при отсутствии перегрузок в сети.

Значения CIR и PIR должны быть установлены для всех портов, для которых используется общая пропускная способность канала каскадирования. При достижении значения CIR пакеты пересылаются со скоростью, которая может достигать PIR. В случае перегрузок в сети поступающие через входящий порт пакеты, занимающие пропускную способность сверх CIR, помечаются на отбрасывание.

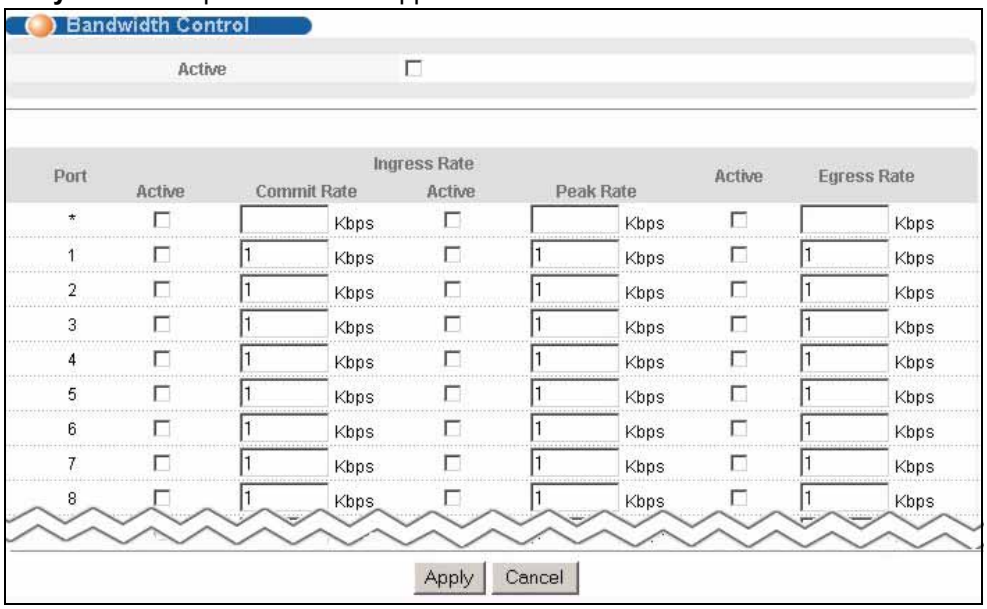
Значение CIR должно быть меньше PIR.

Сумма значений CIR должна быть меньше или равна пропускной способности канала каскадирования.

12.2 Настройка управления пропускной способностью

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

Рисунок 58 Экран Advanced Application > Bandwidth Control



Поля экрана описаны в следующей таблице.

Таблица 32 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.
Ingress Rate	
Active	Установите этот переключатель, чтобы включить на этом порту ограничения гарантированной скорости.
Commit Rate	Укажите гарантированную пропускную способность в килобитах в секунду (кбит/с) для входящего потока трафика через этот порт. Гарантированная скорость должна быть меньше пиковой скорости (Peak Rate). Сумма значений гарантированной скорости должна быть меньше или равна пропускной способности канала каскадирования.
Active	Установите этот переключатель, чтобы включить на этом порту ограничения пиковой скорости.
Peak Rate	Укажите максимальную разрешенную пропускную способность в килобитах в секунду (кбит/с) для входящего потока трафика через этот порт.

Таблица 32 Экран Advanced Application > Bandwidth Control (продолжение)

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на этом порту ограничения скорости для исходящего трафика.
Egress Rate	Укажите максимальную разрешенную пропускную способность в килобитах в секунду (кбит/с) для исходящего потока трафика через этот 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.

13

Контроль широковещательных штормов

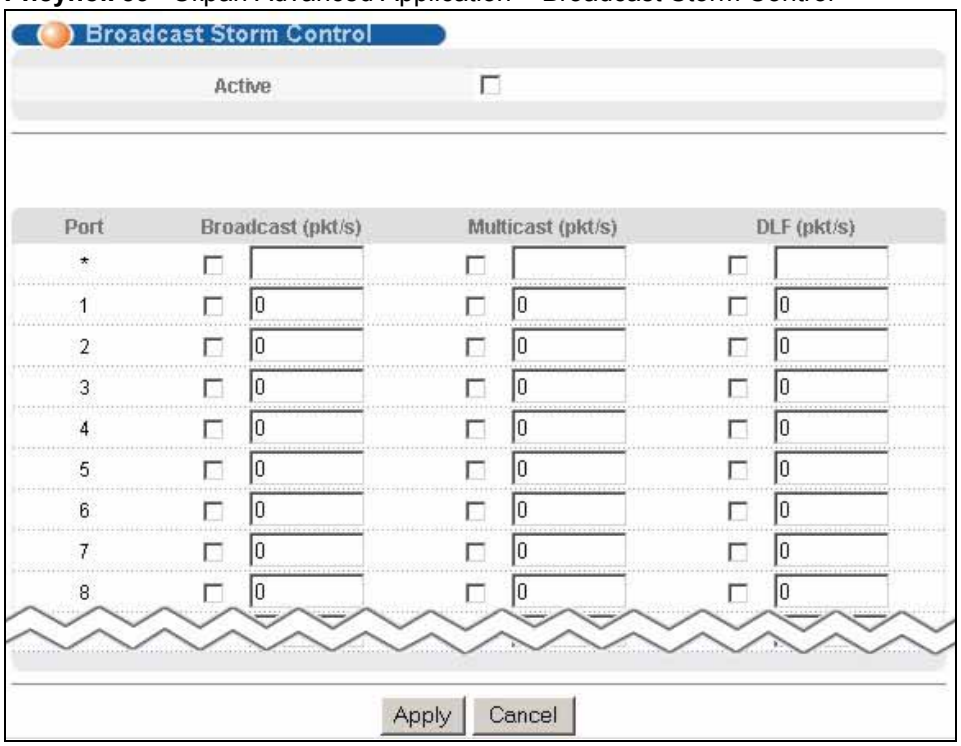
В этой главе описывается функция контроля широковещательных штормов и порядок ее настройки.

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 59 Экран Advanced Application > Broadcast Storm Control



Поля экрана описаны в следующей таблице.

Таблица 33 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.
Broadcast (pkt/s)	Выберите данную опцию и укажите количество широковещательных пакетов, которое может приниматься портом в секунду.
Multicast (pkt/s)	Выберите данную опцию и укажите количество мультивещательных пакетов, которое может приниматься портом в секунду.
DLF (pkt/s)	Выберите данную опцию и укажите количество DLF-пакетов (destination lookup failure), которое может приниматься портом в секунду.
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

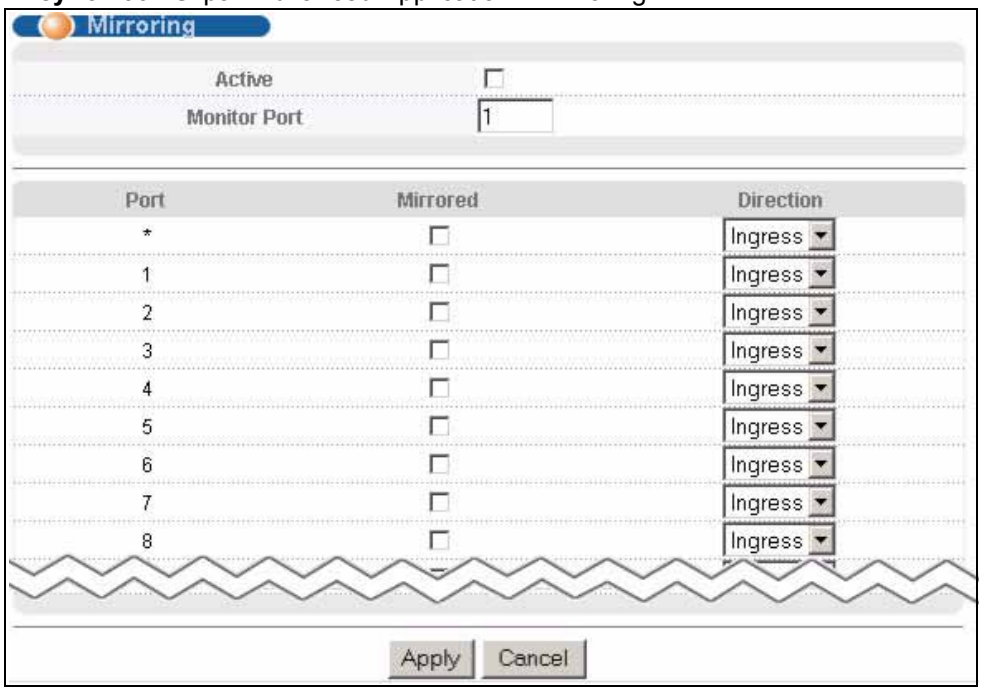
В данной главе описаны экраны настройки зеркального копирования портов.

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 60 Экран Advanced Application > Mirroring



Поля экрана описаны в следующей таблице.

Таблица 34 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.
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. 154.

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 35 Идентификатор агрегации каналов: локальный коммутатор

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

Таблица 36 Идентификатор агрегации каналов: коммутатор-партнер

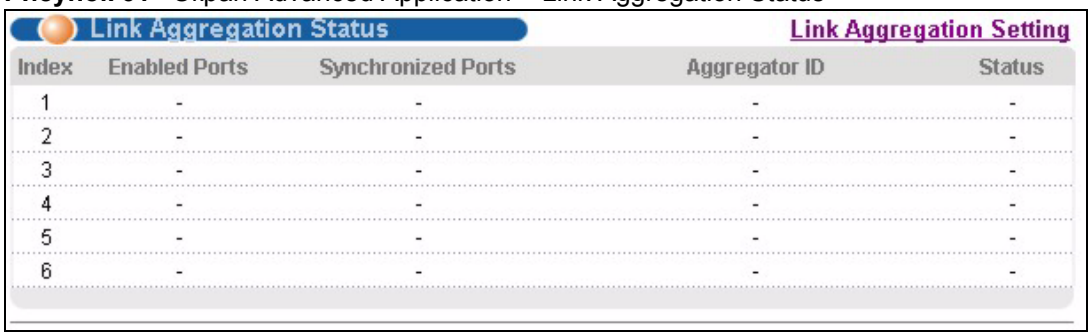
ПРИОРИТЕТ СИСТЕМЫ	MAC-АДРЕС	КЛЮЧ	ПРИОРИТЕТ ПОРТА	НОМЕР ПОРТА
0000	00-00-00-00-00	0000	00	0000

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. 149.

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

Рисунок 61 Экран Advanced Application > Link Aggregation Status



Поля экрана описаны в следующей таблице.

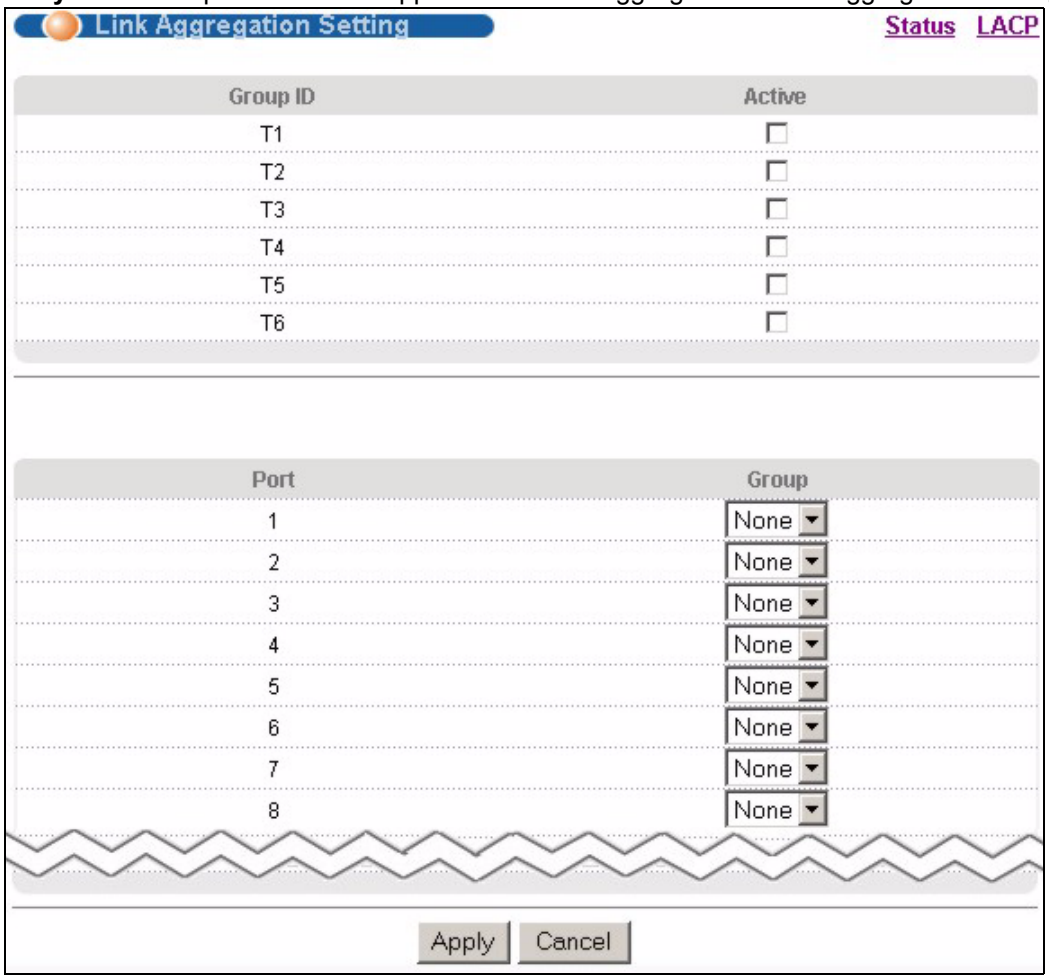
Таблица 37 Экран Advanced Application > Link Aggregation Status

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается идентификатор группы, который определяет группу портов, то есть логический канал, объединяющий несколько портов.
Enabled Port	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. 150.
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. 149.

Рисунок 62 Экран Advanced Application > Link Aggregation > Link Aggregation Setting



Поля экрана описаны в следующей таблице.

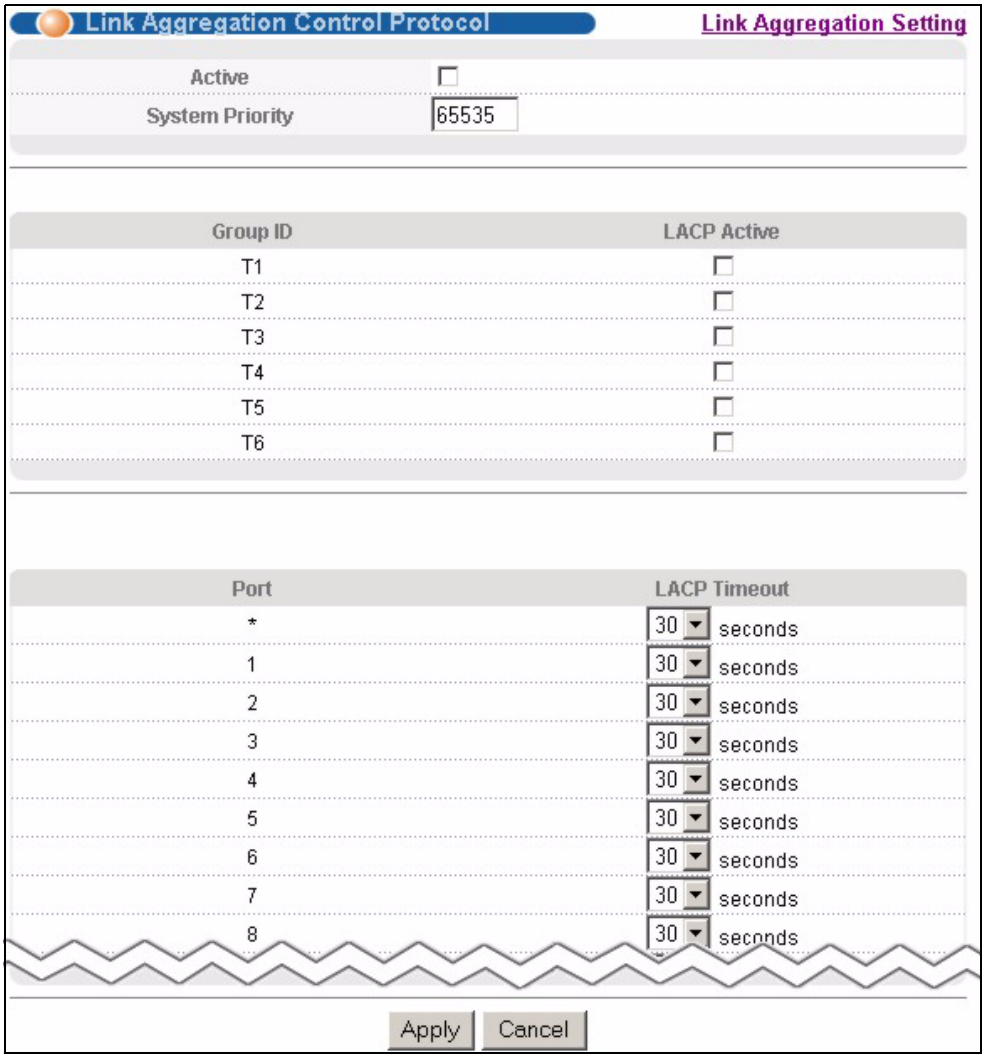
Таблица 38 Экран Advanced Application > Link Aggregation > Link Aggregation Setting

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. 149.

Рисунок 63 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



Поля экрана описаны в следующей таблице.

Таблица 39 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.

Таблица 39 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (продолжение)

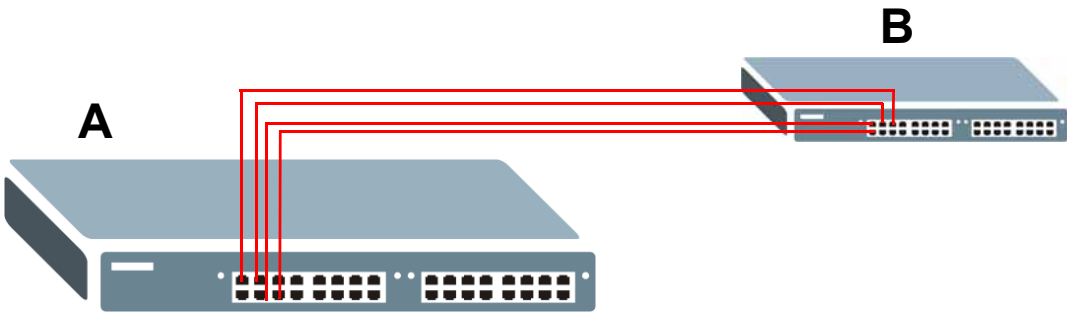
ПОЛЕ	ОПИСАНИЕ
System Priority	Приоритет системы протокола LACP – это число от 1 до 65 535. Коммутатор с наименьшим приоритетом системы (и наименьшим номером порта, если значения приоритета системы одинаковы) становится «сервером» протокола LACP. «Сервер» LACP управляет работой протокола LACP. Введите 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.
*	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.

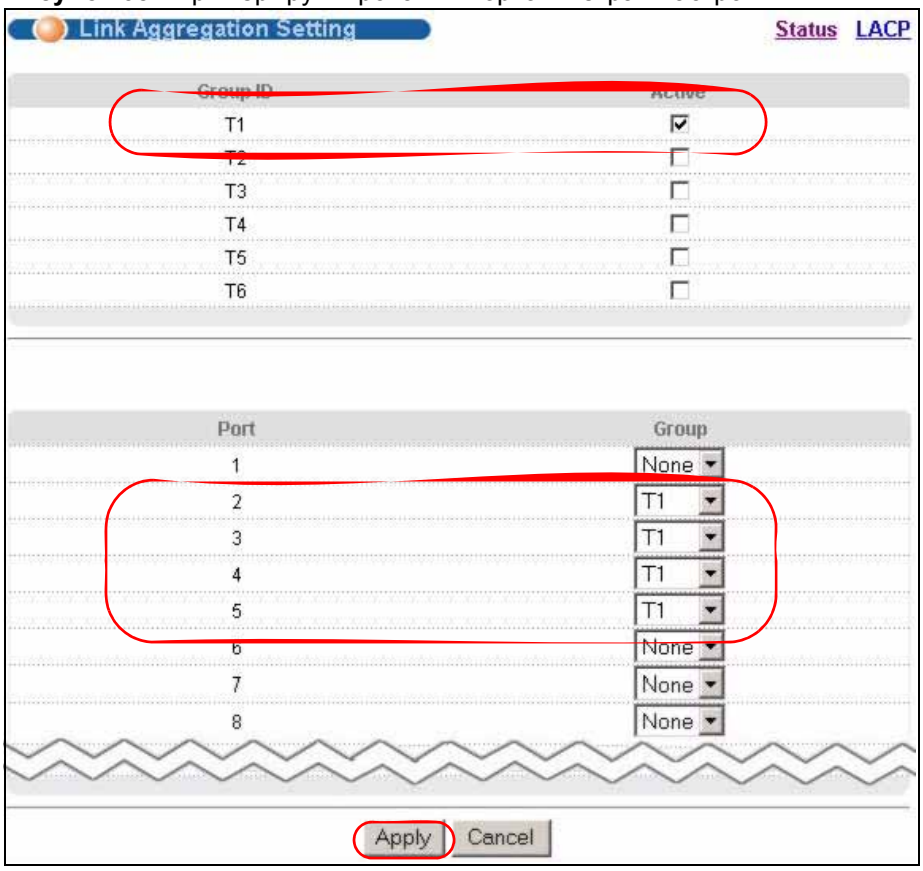
1 **Выполните физические подключения** – подключите все порты, которые должны войти в группу, к одному и тому же пункту назначения. На приведенном ниже рисунке показано подключение портов 2-5 коммутатора **A** к коммутатору **B**.

Рисунок 64 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 65 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 и по MAC-адресам.

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 следующие методы аутентификации портов:

- **IEEE 802.1x**[2] – предусматривает проверку прав доступа к портам на сервере аутентификации с использованием имени пользователя и пароля, предоставленных пользователем.
- **По MAC-адресам** – предусматривает проверку прав доступа к портам с использованием MAC-адреса и пароля пользователя.

Проверка прав пользователя в каждом из способов 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. 23.1.2 на стр. 208.

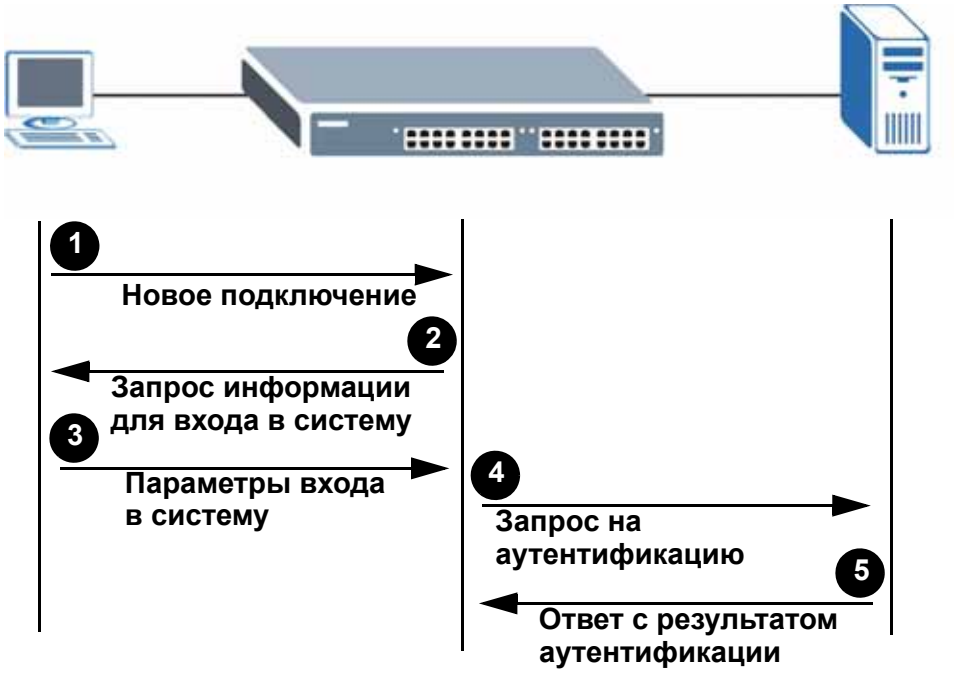
Если включить на одном и том же порту и аутентификацию по IEEE 802.1x, и аутентификацию по MAC-адресам, то коммутатор в первую очередь осуществляет аутентификацию по стандарту IEEE 802.1x. В случае невозможности осуществить аутентификацию пользователя по стандарту IEEE 802.1x доступ к порту будет запрещен.

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.

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.

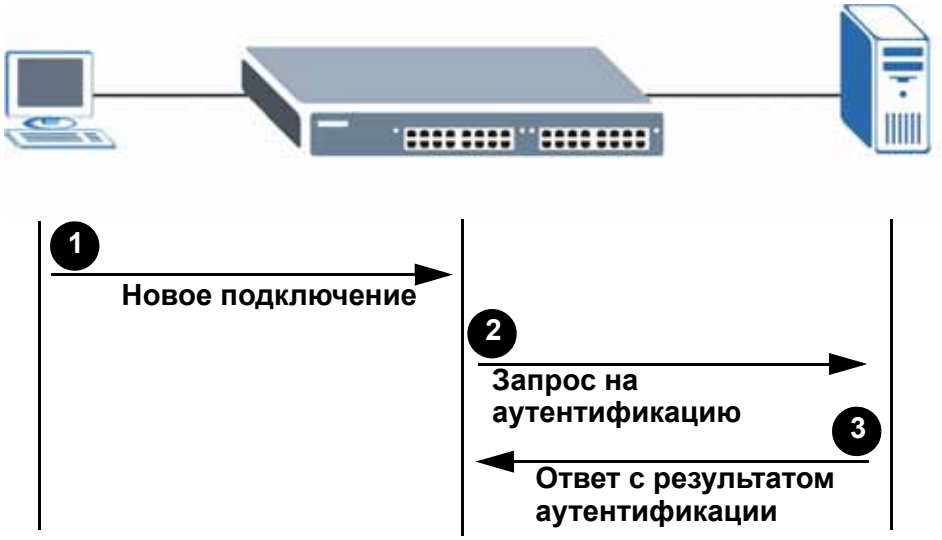
Рисунок 66 Процесс аутентификации на основе IEEE 802.1x



16.1.2 Аутентификация по MAC-адресам

Аутентификация по MAC-адресам работает практически так же, как и аутентификация по стандарту IEEE 802.1x. Основное различие заключается в том, что коммутатор не запрашивает у пользователя параметров входа. Параметрами входа являются MAC-адрес пользователя, подключающегося к порту коммутатора, а также пароль, настроенный на коммутаторе специально для аутентификации по MAC-адресам.

Рисунок 67 Процесс аутентификации по MAC-адресу



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**.

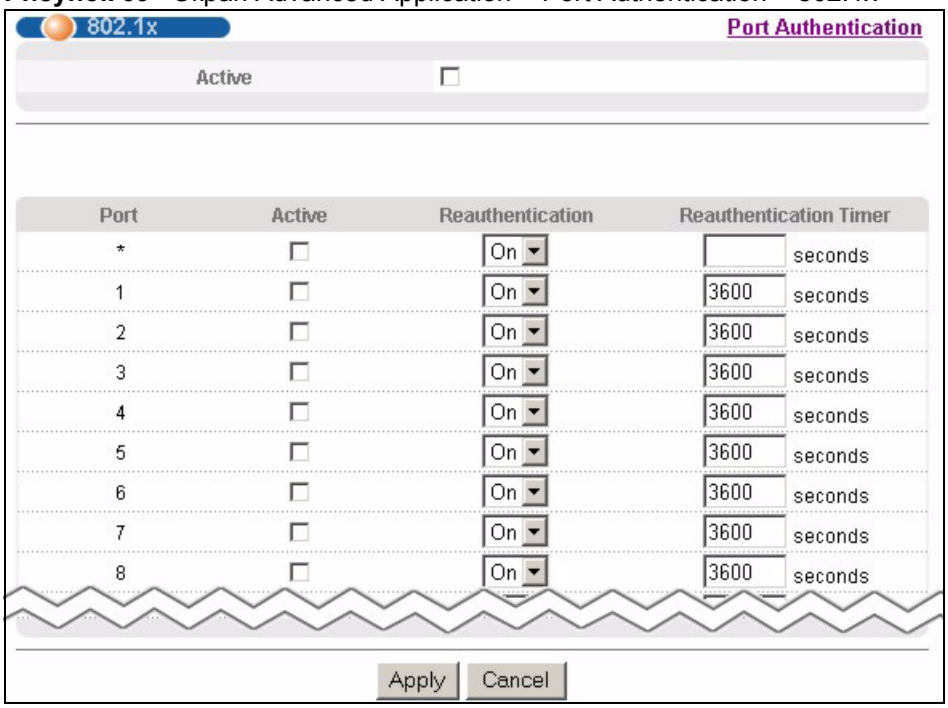
Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Port Authentication**.

Рисунок 68 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 69 Экран Advanced Application > Port Authentication > 802.1x



Поля экрана описаны в следующей таблице.

Таблица 40 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.

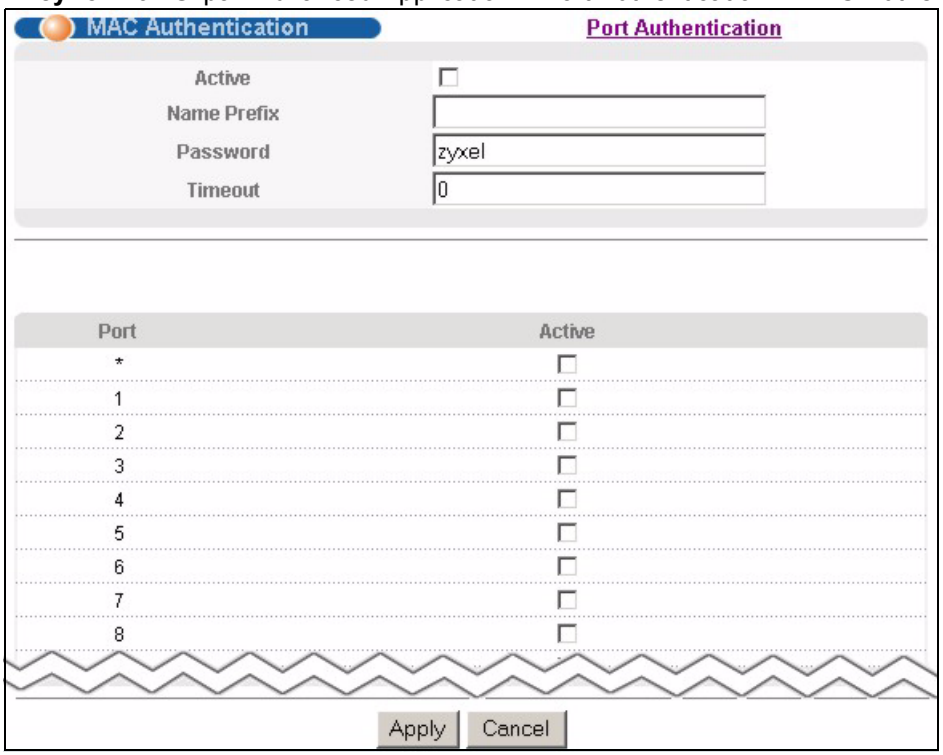
Таблица 40 Экран Advanced Application > Port Authentication > 802.1x (продолжение)

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.

16.2.2 Включение аутентификации по MAC-адресам

Данный экран используется для включения аутентификации по MAC-адресам. На экране **Port Authentication** нажмите на **MAC Authentication**, чтобы отобразить показанный ниже экран настройки.

Рисунок 70 Экран Advanced Application > Port Authentication > MAC Authentication



Поля экрана описаны в следующей таблице.

Таблица 41 Экран Advanced Application > Port Authentication > MAC Authentication

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы разрешить аутентификацию по MAC-адресам на коммутаторе. Примечание: Прежде чем приступать к настройке аутентификации по MAC-адресам на каждом порту, необходимо включить ее на коммутаторе.
Name Prefix	Введите префикс имени, который будет добавляться ко всем MAC-адресам, отправляемым на сервер RADIUS для аутентификации. В поле можно ввести до 32 печатных символов ASCII. Если оставить это поле пустым, то на сервер RADIUS будет отправляться только MAC-адрес пользователя.
Password	Введите пароль, который коммутатор будет отправлять вместе с MAC-адресом пользователя на сервер RADIUS для аутентификации. В поле можно ввести до 32 печатных символов ASCII.
Timeout	Укажите период времени, по прошествии которого коммутатор разрешит пользователю с MAC-адресом, отвергнутым при аутентификации, повторить попытку аутентификации. Максимальное значение равно 3000 секунд. Когда пользователь не проходит аутентификацию по MAC-адресу, его MAC-адрес запоминается в таблице MAC-адресов с указанием статуса запрета. Указанный в данном поле период тайм-аута представляет собой время, в течение которого такой MAC-адрес будет находиться в таблице MAC-адресов; по прошествии этого времени запись удаляется. Если указать в этом поле значение тайм-аута 0, то удаление записей из таблицы MAC-адресов не производится. Примечание: В случае указания в поле **Aging Time** на экране **Switch Setup** меньшего значения оно имеет приоритет перед данным параметром. См. разд. 7.5 на стр. 81.
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 разрешить аутентификацию по MAC-адресам на этом порту. Прежде чем приступать к настройке аутентификации по MAC-адресам на каждом порту, необходимо включить ее на коммутаторе.
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 О средствах безопасности портов

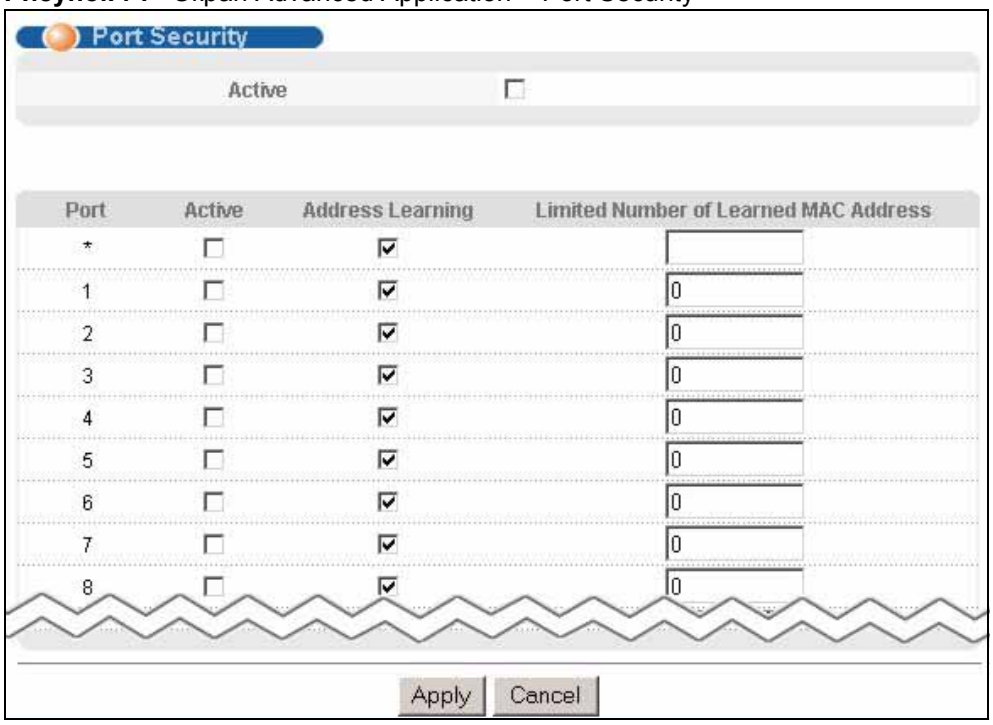
Средства безопасности портов позволяют разрешить прохождение через порт коммутатора только пакетов с динамически полученными MAC-адресами и/или настроенными статическими MAC-адресами. Данный коммутатор может запомнить в общей сложности до 16 тыс. MAC-адресов, без ограничений на количество запоминаемых адресов на один порт (при условии, что общее количество не превышает 16 тыс.).

Для обеспечения максимальной безопасности порта необходимо отключить получение MAC-адресов и настроить для порта статический MAC-адрес (или MAC-адреса). Не рекомендуется отключать средства безопасности портов одновременно запоминанием MAC-адресов, так как это приведет к большому числу широковещательных пакетов. По умолчанию функция получения MAC-адресов остается активированной, даже если средства безопасности портов не включены.

17.2 Настройка средств безопасности портов

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

Рисунок 71 Экран Advanced Application > Port Security



Поля экрана описаны в следующей таблице.

Таблица 42 Экран Advanced Application > Port Security

ПОЛЕ	ОПИСАНИЕ
Active	Установите данный 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. Чтобы получение MAC-адресов происходило для данного порта, порт должен быть активен и на нем должна быть включена функция получения адресов.

Таблица 42 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 16384. «0» означает отключение функции.
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.

18

Классификация

В этой главе описывается настройка на коммутаторе функции классификации пакетов.

18.1 О классификации и управлении качеством обслуживания

Под управлением качеством обслуживания (QoS) понимается как способность сети доставлять данные с минимальной задержкой, так и применяемые в сети методы управления пропускной способностью. Если QoS не используется, то весь трафик имеет равную вероятность отбрасывания при возникновении перегрузок в сети. Это может привести к снижению производительности работы сети и сделать ее непригодной для критичных ко времени приложений, таких как видео по запросу.

При классификации трафик группируется на потоки данных по определенным критериям, таким как адрес источника, адрес назначения, номер порта источника, номер порта назначения и номер входящего порта. Например, можно настроить классификацию таким образом, чтобы в отдельный поток отбирался трафик порта определенного протокола (например, Telnet).

Настройка управления качеством обслуживания на коммутаторе позволяет сгруппировать и приоритезировать трафик приложений для точной настройки производительности сети. Настройка QoS включает в себя два отдельных этапа:

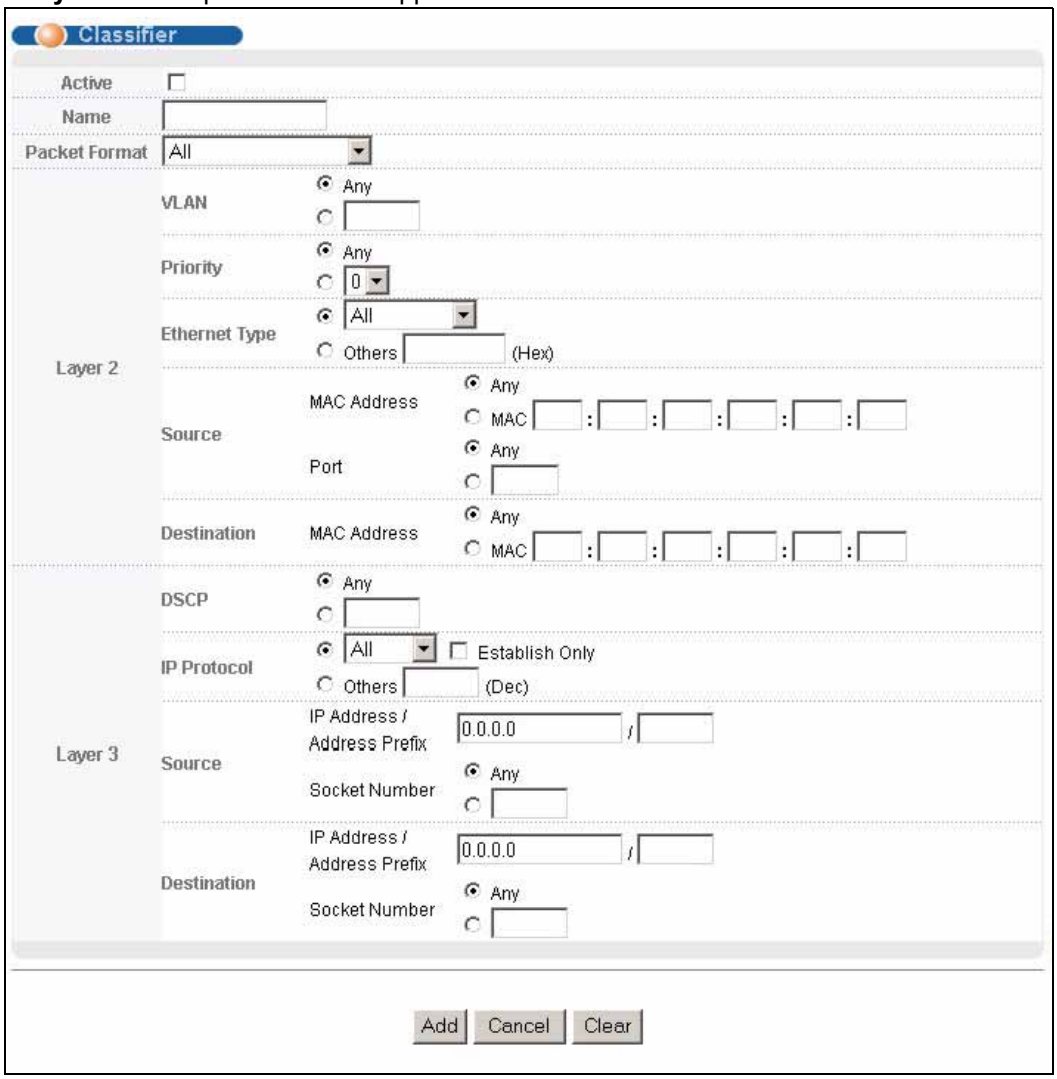
1. Настройка классификации для сортировки трафика между различными потоками.
2. Настройка правил политики, определяющих действия над классифицированными потоками трафика (настройка правил политики описана в гл. 19 на стр. 173).

18.2 Настройка классификации

Настройка классификации осуществляется на экране **Classifier**. После настройки классификации можно определить действия (политики), применяемые к отвечающим правилам трафику. Настройка правил политик описана в гл. 19 на стр. 173.

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

Рисунок 72 Экран Advanced Application > Classifier



Поля экрана описаны в следующей таблице.

Таблица 43 Экран Advanced Application > Classifier

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить данное правило.
Name	Введите имя-описание данного правила, с помощью которого его можно идентифицировать.
Packet Format	Укажите формат пакетов. Возможные значения: **All** (все), **802.3 tagged** (802.3 с тегами), **802.3 untagged** (802.3 без тегов), **Ethernet II tagged** (Ethernet II с тегами) и **Ethernet II untagged** (Ethernet II без тегов). Значение **802.3** означает, что пакеты форматируются согласно стандартам IEEE 802.3. Значение **Ethernet II** означает, что пакеты форматируются согласно RFC 894, инкапсуляция Ethernet II.
Layer 2 В этом разделе приводятся поля, позволяющие настроить классификацию на уровне 2.	
VLAN	Выберите **Any**, чтобы классифицировался трафик из любой сети VLAN, или выберите второй вариант и укажите идентификатор VLAN ID нужной сети в поле рядом.

Таблица 43 Экран Advanced Application > Classifier (продолжение)

ПОЛЕ	ОПИСАНИЕ
Priority	Выберите **Any**, чтобы классифицировался трафик с любым уровнем приоритета, или выберите второй вариант и укажите нужный уровень приоритета в поле рядом.
Ethernet Type	Выберите тип Ethernet, установив первый переключатель, или выберите вариант **Other** и введите номер типа Ethernet в шестнадцатеричном виде. Описание можно найти в табл. 45 на стр. 171.
Source	
MAC Address	Выберите **Any**, чтобы правило применялось ко всем MAC-адресам. Чтобы указать определенный источник, выберите второй вариант и введите MAC-адрес в правильном формате (шесть пар шестнадцатеричных цифр).
Port	Введите номер порта, для которого будет действовать данное правило. Можно выбрать один из портов или все порты (**Any**).
Destination	
MAC Address	Выберите **Any**, чтобы правило применялось ко всем MAC-адресам. Чтобы указать определенный пункт назначения, выберите второй вариант и введите MAC-адрес в правильном формате (шесть пар шестнадцатеричных цифр).
Layer 3 В этом разделе приводятся поля, позволяющие настроить классификацию на уровне 3.	
DSCP	Выберите **Any**, чтобы классифицировался трафик с любым кодовым маркером DSCP, или выберите второй вариант и укажите номер DSCP (кодового маркера DiffServ) в диапазоне от 0 до 63 в поле рядом.
IP Protocol	Выберите тип IP-протокола, установив первый переключатель, или выберите вариант **Other** и введите номер протокола в десятичном виде. Дополнительную информацию можно найти в табл. 46 на стр. 171. Для типа протокола **TCP** можно установить переключатель **Establish Only**. В этом случае коммутатор будет отбирать только пакеты, отправляемые для установления TCP-соединений.
Source	
IP Address/ Address Prefix	Введите IP-адрес источника в виде десятичных чисел, разделенных точками. Укажите префикс адреса, который представляет собой количество единиц в двоичной записи маски подсети.
Socket Number	Примечание: Чтобы настроить номера сокетов, предварительно необходимо выбрать в поле **IP Protocol** значение **UDP** или **TCP**. Выберите **Any**, чтобы правило применялось для всех номеров портов протоколов TCP/UDP, или выберите второй вариант и введите номер порта протокола TCP/UDP.
Destination	
IP Address/ Address Prefix	Введите IP-адрес назначения в виде десятичных чисел, разделенных точками. Укажите префикс адреса, который представляет собой количество единиц в двоичной записи маски подсети.

Таблица 43 Экран Advanced Application > Classifier (продолжение)

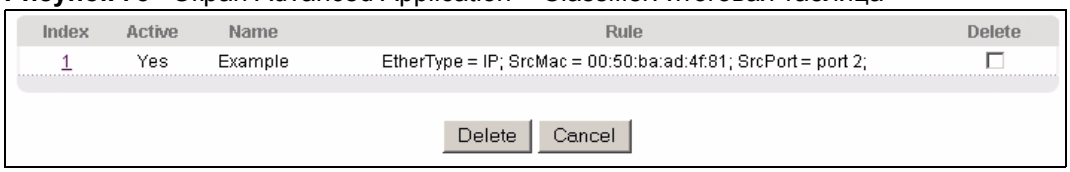
ПОЛЕ	ОПИСАНИЕ
Socket Number	Примечание: Чтобы настроить номера сокетов, предварительно необходимо выбрать в поле **IP Protocol** значение **UDP** или **TCP**. Выберите **Any**, чтобы правило применялось для всех номеров портов протоколов TCP/UDP, или выберите второй вариант и введите номер порта протокола TCP/UDP.
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 начать настройку на этом экране заново.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.

18.3 Просмотр и редактирование настройки классификации

Чтобы просмотреть сводную информацию о настройках классификации, перейдите к итоговой таблице в нижней части экрана **Classifier**. Чтобы изменить настройки правила, нажмите на номере в поле **Index**.

В случае противоречия между двумя правилами приоритет имеет правило более высокого уровня.

Рисунок 73 Экран Advanced Application > Classifier: итоговая таблица



Поля экрана описаны в следующей таблице.

Таблица 44 Экран Classifier: итоговая таблица

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер правила. Нажмите на этот номер, чтобы отредактировать правило.
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.
Rule	В этом поле отображаются сводные сведения по настройкам правила классификации.

Таблица 44 Экран Classifier: итоговая таблица

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

Некоторые наиболее распространенные типы Ethernet и соответствующие номера протоколов приводятся в следующей таблице.

Таблица 45 Распространенные типы Ethernet и номера протоколов

ТИП ETHERNET	НОМЕР ПРОТОКОЛА
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Наиболее часто используемые порты протокола IP:

Таблица 46 Наиболее часто используемые порты протокола IP

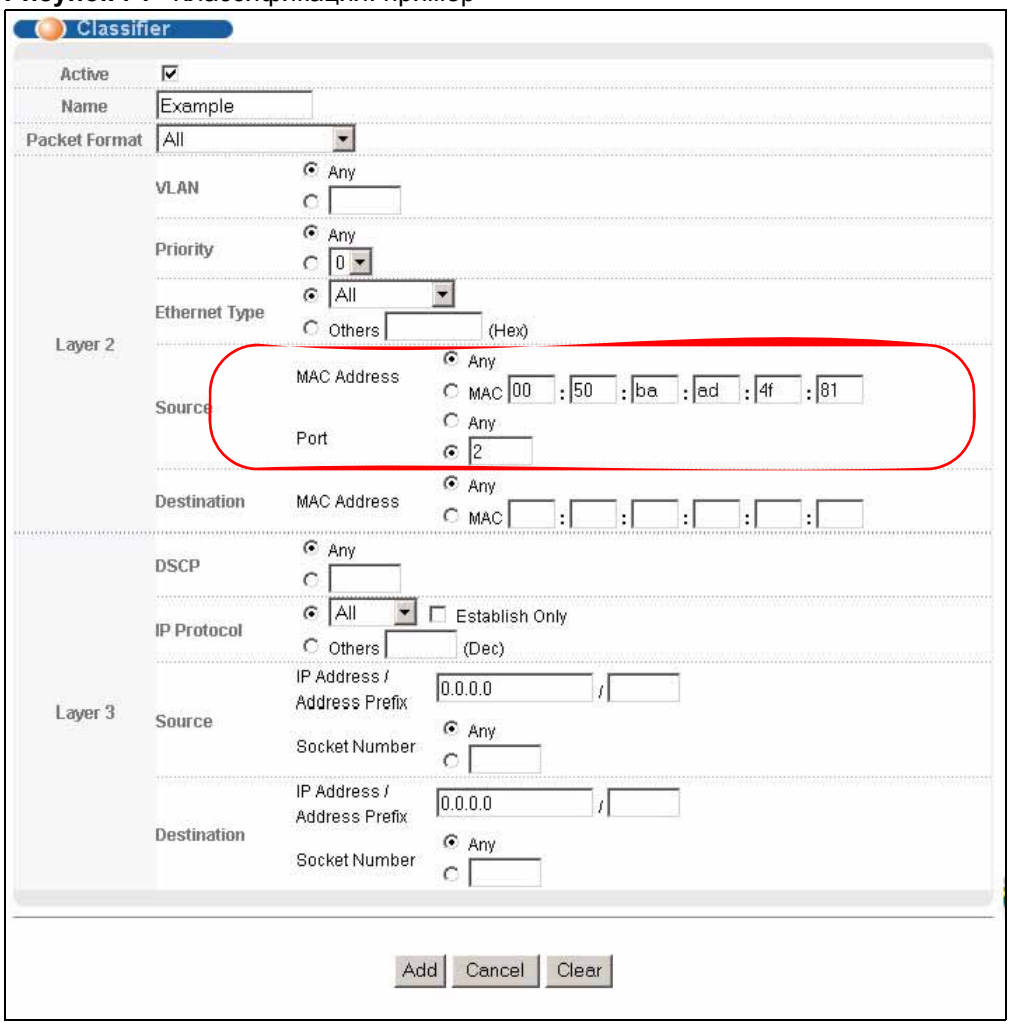
НОМЕР ПОРТА	НАЗВАНИЕ ПОРТА
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Пример использования классификации

На следующем экране показан пример настройки классификации, в котором обнаруживается весь трафик от MAC-адреса 00:50:ba:ad:4f:81, поступающий через порт 2.

После настройки классификации можно настроить политику (на экране **Policy**), чтобы определить действия, выполняемые над этим потоком трафика.

Рисунок 74 Классификация: пример



19

Правила политики

В данной главе описана настройка правил политики.

19.1 Обзор правил политики

С помощью классификации трафик делится на потоки в соответствии с установленными критериями (дополнительную информацию можно найти в гл. 18 на стр. 167). Правила политики обеспечивают надлежащую обработку потоков трафика в сети.

19.1.1 Дифференцированное обслуживание

Дифференцированное обслуживание (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.

19.1.2 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 состоит из двухбитного неиспользуемого поля и 6-битного поля маркера DSCP, которое позволяет определить до 64 уровней обслуживания. Поле DS изображено на следующем рисунке.

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.

DSCP (6 бит)	Не используется (2 бита)

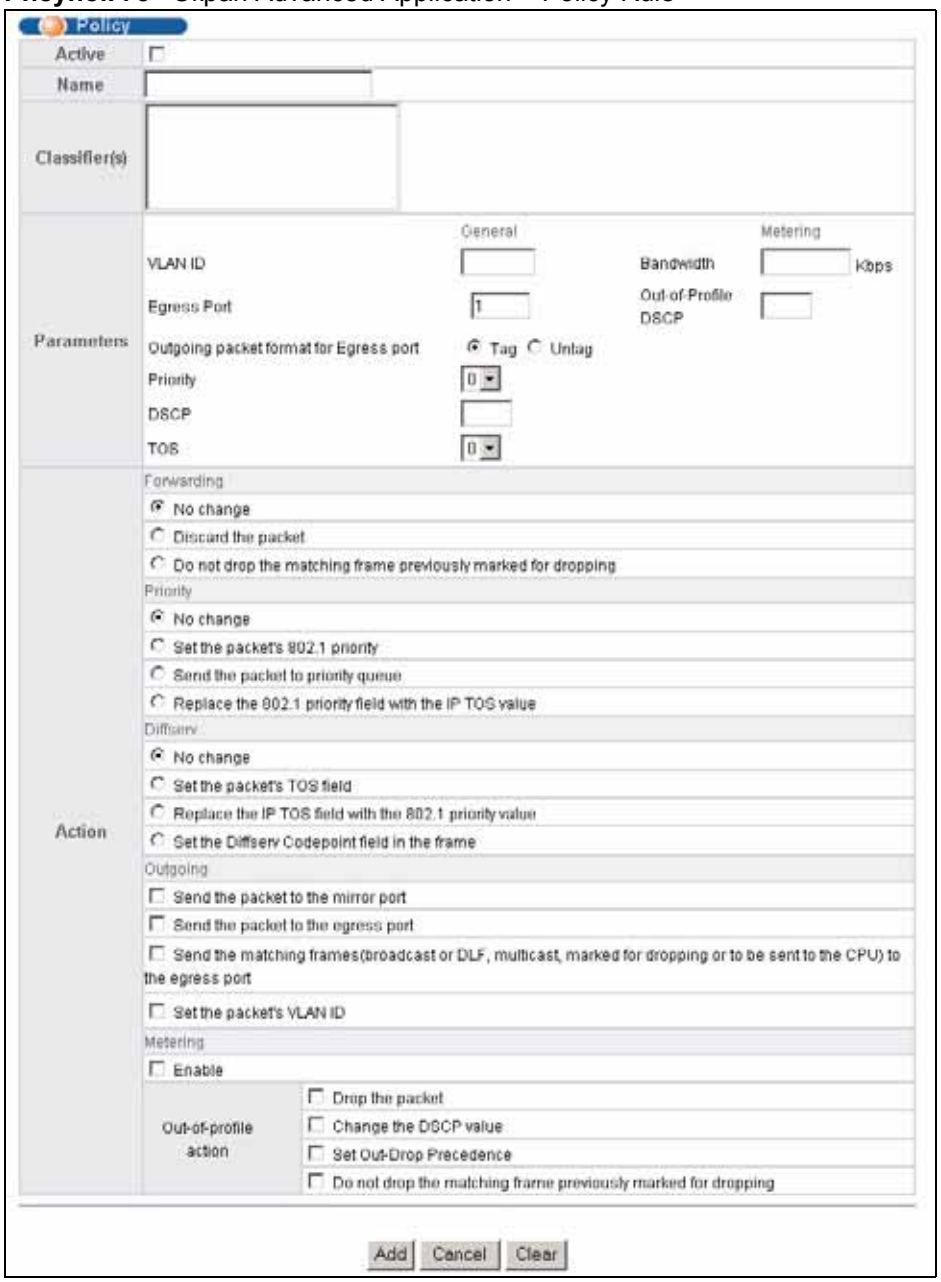
Значение DSCP определяет обработку при пересылке, так называемую обработку на каждом конкретном переходе (PHB, Per-Hop Behavior), которая осуществляется над каждым пакетом при прохождении по сети с поддержкой DiffServ. В зависимости от правила маркирования различные типы трафика могут подвергаться различным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

19.2 Настройка правил политики

Прежде всего необходимо настроить классификацию на экране **Classifier**. Дополнительную информацию можно найти в разд. 18.2 на стр. 167.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Applications > Policy Rule**.

Рисунок 75 Экран Advanced Application > Policy Rule



Поля экрана описаны в следующей таблице.

Таблица 47 Экран Advanced Application > Policy Rule

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить политику.
Name	Введите имя-описание для идентификации.
Classifier(s)	В этом поле отображаются активные правила классификации, настроенные на экране **Classifier**. Выберите правило классификации, к которому применяется данное правило политики. Чтобы выбрать несколько правил классификации, удерживайте при выборе нажатой клавишу [SHIFT].

Таблица 47 Экран Advanced Application > Policy Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Parameters Настройки в следующих полях относятся к данной политике. Необходимо настроить только те поля, которые относятся в настроенным действиям в разделе **Action**.	
General	
VLAN ID	Укажите идентификационный номер VLAN.
Egress Port	Введите номер исходящего порта.
Outgoing packet format for Egress port	Выберите **Tag**, чтобы на указанном исходящем порту к пакетам добавлялся указанный идентификатор VID. В противном случае необходимо выбрать **Untag**.
Priority	Укажите уровень приоритета.
DSCP	Укажите значение DSCP (кодового маркера DiffServ) в диапазоне от 0 до 63.
TOS	Укажите уровень приоритета типа обслуживания (TOS).
Metering	Имеется возможность настроить желаемую пропускную способность, выделяемую для потока трафика. Трафик, поступающий со скоростью сверх максимальной выделенной пропускной способности (в случаях перегрузки сети), называется внепрофильным трафиком.
Bandwidth	Укажите пропускную способность в килобитах в секунду (кбит/с). Введите значение в диапазоне от 1 до 1000000.
Out-of-Profile DSCP	Укажите значение DSCP (в диапазоне от 0 до 63), на которое должно заменяться значение DSCP у внепрофильного трафика.
Action Укажите действия, выполняемые коммутатором над соответствующим классифицированным потоком трафика.	
Forwarding	Выберите **No change** для пересылки пакетов. Выберите **Discard the packet** для отбрасывания пакетов. Выберите **Do not drop the matching frame previously marked for dropping** для сохранения кадров, ранее помеченных на отбрасывание.
Priority	Выберите **No change**, чтобы оставить приоритет кадров без изменения. Выберите **Set the packet's 802.1 priority**, чтобы заменить поле приоритета пакета по стандарту 802.1 на значение, указанное в поле Priority. Выберите **Send the packet to priority queue**, чтобы поместить пакеты в указанную очередь. Выберите **Replace the 802.1 priority field with the IP TOS value**, чтобы заменить поле приоритета пакета по стандарту 802.1 на значение, указанное в поле **TOS**.
Diffserv	Выберите **No change**, чтобы оставить поля TOS и/или DSCP пакетов без изменения. Выберите **Set the packet's TOS field**, чтобы установить для поля TOS значение, указанное в поле **TOS**. Выберите **Replace the IP TOS with the 802.1 priority value**, чтобы заменить поле TOS на значение, указанное в поле **Priority**. Выберите **Set the Diffserv Codepoint field in the frame**, чтобы установить для поля DSCP значение, указанное в поле **DSCP**.

Таблица 47 Экран Advanced Application > Policy Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Outgoing	Выберите **Send the packet to the mirror port**, чтобы передать пакет на зеркальный порт. Выберите **Send the packet to the egress port**, чтобы передать пакет на исходящий порт. Выберите **Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port**, чтобы передать на исходящий порт широковещательные, мультивещательные, DLF-кадры, а также помеченные на отбрасывание кадры и кадры CPU. Выберите **Set the packet's VLAN ID**, чтобы установить идентификатор VLAN пакета равным значению, указанному в поле **VLAN ID**.
Metering	Выберите **Enable**, чтобы активировать ограничение пропускной способности для потоков трафика и затем настроить действия, выполняемые над внепрофильным трафиком.
Out-of-profile action	Выберите действия, выполняемые над внепрофильным трафиком. Выберите **Drop the packet** для отбрасывания внепрофильного трафика. Выберите **Change the DSCP value**, чтобы заменить поле DSCP на значение, указанное в поле **Out of profile DSCP**. Выберите **Set Out-Drop Precedence**, чтобы пометить внепрофильный трафик и отбросить его в случае перегрузки сети. Выберите **Do not drop the matching frame previously marked for dropping** для постановки в очередь кадров, помеченных на отбрасывание.
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 начать настройку на этом экране заново.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.

19.3 Просмотр и редактирование настроек политики

Чтобы просмотреть сводную информацию о настройках политики, перейдите к итоговой таблице в нижней части экрана **Policy**. Чтобы изменить настройки правила, нажмите на номере в поле **Index**.

Рисунок 76 Экран Advanced Application > Policy Rule: итоговая таблица

Поля экрана описаны в следующей таблице.

Таблица 48 Политика: итоговая таблица

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается номер политики. Нажмите на этот номер, чтобы отредактировать политику.
Active	В этом поле отображается **Yes**, если политика активна, и **No**, если политика отключена.

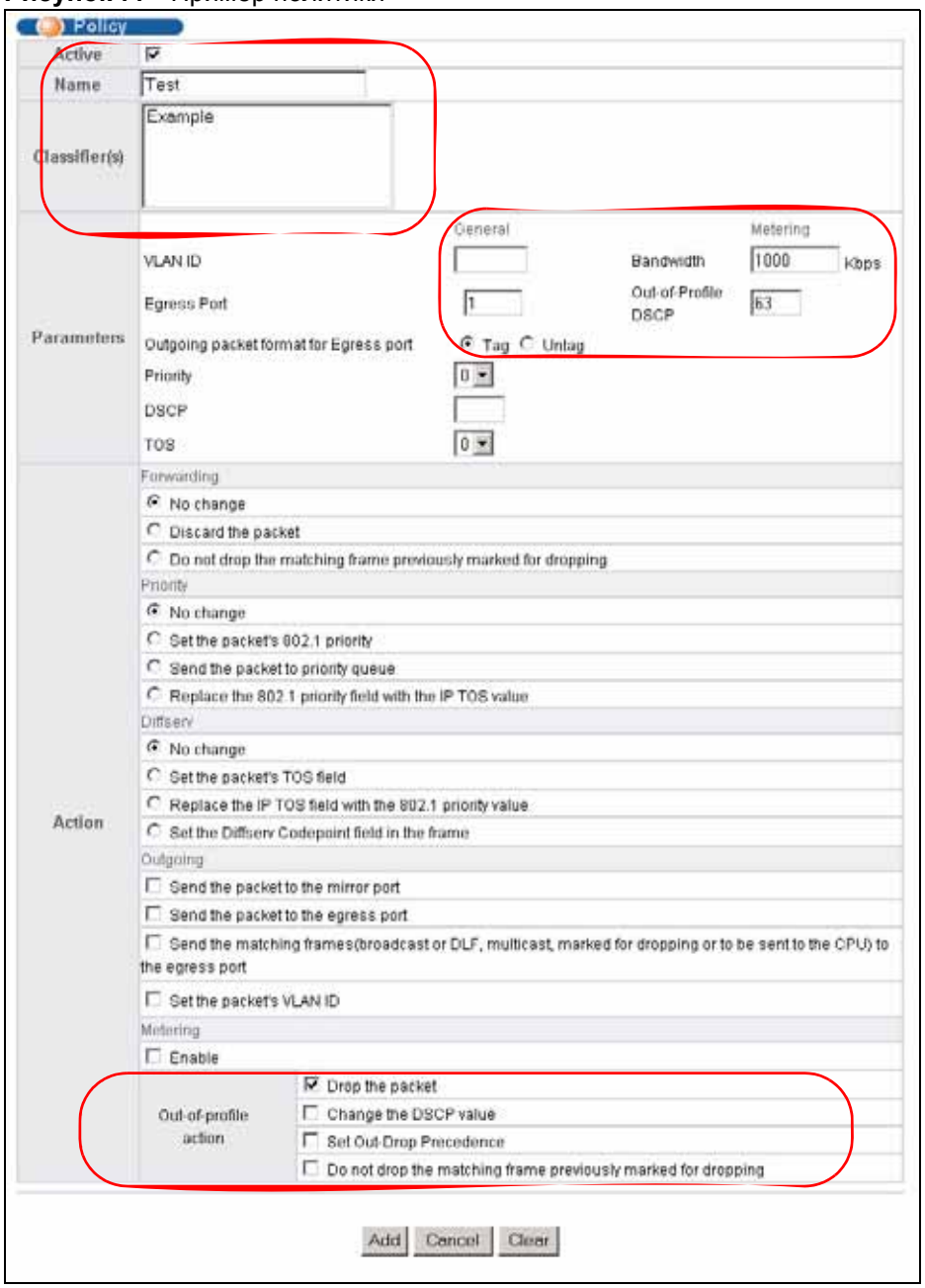
Таблица 48 Политика: итоговая таблица (продолжение)

ПОЛЕ	ОПИСАНИЕ
Name	В этом поле отображается имя, назначенное для данной политики.
Classifier(s)	В этом поле отображаются имена правил классификации, к которым применяется данная политика.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

19.4 Пример политики

На приведенном ниже рисунке показан пример экрана **Policy**, на котором настроена политика ограничения пропускной способности и отбрасывания внепрофильного трафика для потока трафика, классифицированного по правилу **Example** (см. разд. 18.4 на стр. 171).

Рисунок 77 Пример политики



20

Метод организации очередей

В данной главе описаны поддерживаемые методы организации очередей.

20.1 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.

20.1.1 Строгая очередь приоритетов (SP)

Алгоритм строгой очереди приоритетов SP 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.

20.1.2 Взвешенная справедливая постановка в очередь (WFQ)

Алгоритм взвешенной справедливой постановки в очередь (WFQ) позволяет гарантировать для каждой очереди в случае перегрузки минимальную пропускную способность, определяемую весом (долей) очереди (числом, которое указывается в поле Weight – см. рис. 18.1). Алгоритм WFQ запускается только тогда, когда на порт приходит больше трафика, чем он может обработать. Очереди с большим весом получают более высокую гарантированную пропускную способность, чем очереди с малым весом. Этот

механизм организации очереди эффективен потому, что он распределяет всю доступную пропускную способность между различными очередями трафика. По умолчанию очередь Q0 имеет вес 1, очередь Q1 – вес 2, очередь Q2 – вес 3, и так далее. Гарантированная пропускная способность вычисляется следующим образом:

$$\frac{\text{Вес очереди}}{\text{Сумма весов очередей}} \times \text{Скорость порта}$$

Например, при настройках по умолчанию очередь Q0 на порту 1 получает гарантированную пропускную способность:

$$\frac{1}{1+2+3+4+5+6+7+8} \times 100 \text{ Мбит/с} = 3 \text{ Мбит/с}$$

20.1.3 Взвешенное циклическое обслуживание (WRR)

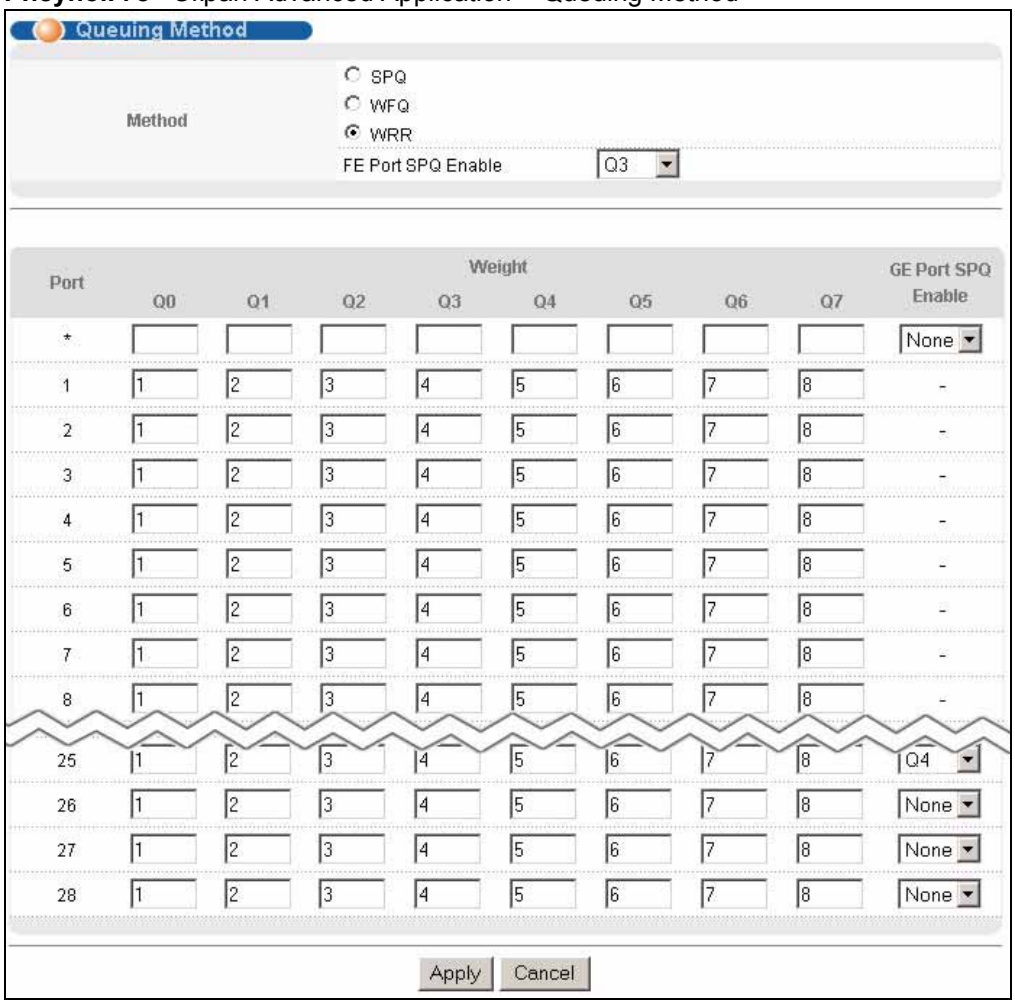
Алгоритм циклического обслуживания обрабатывает очереди по кругу и запускается только тогда, когда на порт приходит больше трафика, чем он может принять. Очереди выделяется некоторая доля пропускной способности вне зависимости от объема трафика, приходящего на этот порт. Затем эта очередь смещается в 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.

20.2 Настройка метода организации очередей

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

Рисунок 78 Экран Advanced Application > Queuing Method



Поля экрана описаны в следующей таблице.

Таблица 49 Экран Advanced Application > Queuing Method

ПОЛЕ	ОПИСАНИЕ
Method	Выберите **SPQ (строгая очередь приоритетов), WFQ (взвешенная справедливая постановка в очередь) или WRR (взвешенное циклическое обслуживание)**. Алгоритм строгой очереди приоритетов 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 – Q7, самый низкий – Q0. Алгоритм взвешенной справедливой постановки в очередь (WFQ) позволяет гарантировать для каждой очереди в случае перегрузки минимальную пропускную способность, определяемую весом (долей) очереди (числом, которое указывается в поле **Weight**). Очереди с большим весом получают более высокую гарантированную пропускную способность, чем очереди с малым весом. Алгоритм взвешенного циклического обслуживания 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.

Таблица 49 Экран Advanced Application > Queuing Method (продолжение)

ПОЛЕ	ОПИСАНИЕ
FE Port SPQ Enable	Данное поле используется только в случае выбора **WFQ** или **WRR**. Выберите очередь (от **Q0** до **Q7**), начиная с которой (включительно) коммутатор будет использовать для портов Ethernet 10/100 Мбит/с алгоритм **строгой очереди приоритетов**. Например, если выбрать **Q5**, то коммутатор будет обслуживать трафик в очередях **Q5**, **Q6** и **Q7** с использованием алгоритма **строгой очереди приоритетов**. Чтобы в любом случае использовать для портов Ethernet 10/100 Мбит/с алгоритмы **WFQ** или **WRR**, выберите в данном поле значение **None**.
Port	В этом поле отображается номер настраиваемого 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.
Вес	В случае выбора метода **WFQ** или **WRR** в этих полях указываются веса очередей. Пропускная способность распределяется между очередями в зависимости от их веса.
GE Port SPQ Enable	Данное поле используется только в случае выбора **WFQ** или **WRR**. Выберите очередь (от **Q0** до **Q7**), начиная с которой (включительно) коммутатор будет использовать для портов Gigabit Ethernet алгоритм **строгой очереди приоритетов**. Например, если выбрать **Q5**, то коммутатор будет обслуживать трафик в очередях **Q5**, **Q6** и **Q7** с использованием алгоритма **строгой очереди приоритетов**. Чтобы в любом случае использовать для портов Gigabit Ethernet алгоритмы **WFQ** или **WRR**, выберите в данном поле значение **None**.
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.

21

Стекирование VLAN

В данной главе описана настройка на коммутаторе стекирования VLAN. Более подробную информацию о виртуальных локальных сетях можно найти в главе о VLAN.

21.1 Обзор стекирования VLAN

С помощью стекирования VLAN провайдер услуг имеет возможность различать сети VLAN различных клиентов, даже если они имеют одинаковые (назначаемые клиентами) идентификаторы VLAN ID.

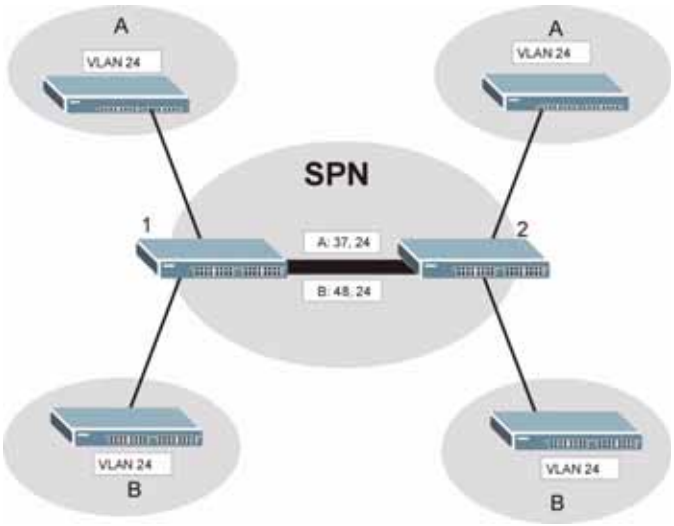
С помощью стекирования VLAN можно добавить внешний тег VLAN к кадрам с внутренними тегами IEEE 802.1Q при их поступлении в сеть. Посредством добавления тегов к уже имеющим теги кадрам (использования «двух тегов») провайдер услуг может управлять максимум 4 094 группами VLAN, каждая из которых может содержать до 4 094 клиентских сетей VLAN. Благодаря этому провайдер услуг может предоставлять дифференцированные услуги в зависимости от конкретной VLAN многим различным клиентам.

Клиентам провайдера услуг могут потребоваться различные виртуальные локальные сети для работы с несколькими приложениями. Клиенты провайдера услуг могут назначать свои собственные внутренние теги VLAN на портах для этих приложений. Каждому клиенту провайдер услуг может присвоить внешний тег VLAN. Таким образом, теги VLAN у различных клиентов не будут перекрываться, а трафик различных клиентов будет по-прежнему изолирован.

21.1.1 Пример стекирования VLAN

На приведенном ниже рисунке **A** и **B** являются клиентами провайдера услуг, использующими VPN-туннели между своими головными офисами и филиалами через сеть провайдера (SPN). Для своих групп VLAN оба клиента выбрали одинаковые теги VLAN. Провайдер услуг может разделить эти две сети VLAN в своей сети, добавляя тег 37 для клиента **A** и тег 48 для клиента **B** на граничном устройстве **1**, и затем удаляя эти теги на граничном устройстве **2** в момент выхода кадров из сети.

Рисунок 79 Пример стекирования VLAN



21.2 Роли портов при стекировании VLAN

Каждый из портов при стекировании VLAN может выполнять одну из трех «ролей»: **Normal** (обычный порт), **Access Port** (порт доступа) и **Tunnel** (туннель, только для гигабитных портов).

- Значение **Normal** соответствует «обычной» (без использования стекирования VLAN) коммутации кадров IEEE 802.1Q.
- Значение **Access Port** устанавливается для входящих портов на граничных устройствах провайдера услуг (**1** и **2** на рисунке с примером стекирования VLAN). При этом входящие кадры обрабатываются как «не имеющие тегов», что дает возможность добавить второй тег VLAN (внешний тег VLAN).

На портах, для которых выбраны режимы **Normal** или **Access Port**, должно быть ОТКЛЮЧЕНО добавление тегов **Tx Tagging** для статических VLAN.

- Значение **Tunnel Port** (доступное только для гигабитных портов) устанавливается для исходящих портов на граничном устройстве сети провайдера услуг. Все принадлежащие клиенту сети VLAN могут быть агрегированы в одну VLAN провайдера услуг (с использованием внешнего тега VLAN, определенного по SP VID).

На портах, для которых выбран режим **Tunnel Port**, должно быть ВКЛЮЧЕНО добавление тегов **Tx Tagging** для статических VLAN.

21.3 Формат тега VLAN

Тег VLAN (при стекировании VLAN провайдером услуг или использовании клиентских сетей IEEE 802.1Q) включает в себя следующие три поля.

Таблица 50 Формат тега VLAN

Type	Priority	VID

Type представляет собой стандартный код типа Ethernet, который идентифицирует кадр и указывает, несет ли кадр информацию тега IEEE 802.1Q. **SP TPID** (идентификатор протокола тега провайдера услуг) представляет собой тип тега для стекирования VLAN провайдером услуг. Многие производители используют значения 0x8100 или 0x9100.

TPID (идентификатор протокола тега) представляет собой тег клиентской сети IEEE 802.1Q.

- Если порт при стекировании VLAN имеет роль **Access Port**, то коммутатор добавляет тег **SP TPID** ко всем входящим кадрам на граничных устройствах провайдера услуг (1 и 2 на рисунке с примером стекирования VLAN).
- Если порт при стекировании VLAN имеет роль **Tunnel**, то коммутатор добавляет тег **SP TPID** только к тем входящим кадрам на граничных устройствах провайдера услуг (1 и 2 на рисунке с примером стекирования VLAN), у которых **SP TPID** отличается от настроенного на коммутаторе. (Если **SP TPID** входящего кадра совпадает с настроенным на коммутаторе, то коммутатор тег не добавляет).

Priority определяется стандартом IEEE 802.1p и позволяет провайдерам услуг приоритезировать трафик в зависимости от класса обслуживания (CoS), оплаченного клиентом.

- На коммутаторе уровни приоритета для внутренних тегов IEEE 802.1Q настраиваются на экране **Port Setup**.
- «0» соответствует самому низкому приоритету, «7» – самому высокому.

VID представляет собой идентификатор VLAN ID. **SP VID** – это идентификатор VID для второго тега VLAN (провайдера услуг).

21.3.1 Формат кадра

Ниже показаны форматы кадра для кадра Ethernet без тега, для кадра с одним тегом 802.1Q (клиентским) и с двумя тегами 802.1Q (провайдера услуг).

Выделенные поля соответствуют настраиваемым на коммутаторе на экране **VLAN Stacking**.

Таблица 51 Формат кадра с одним и двумя тегами 802.11Q

						DA	SA	Len/ Etype	Data	FCS	Кадр Ethernet без тегов
			DA	SA	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	Кадр с клиентским тегом IEEE 802.1Q
DA	SA	**SPTPID**	**Priority**	**VID**	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	Кадр с двумя тегами

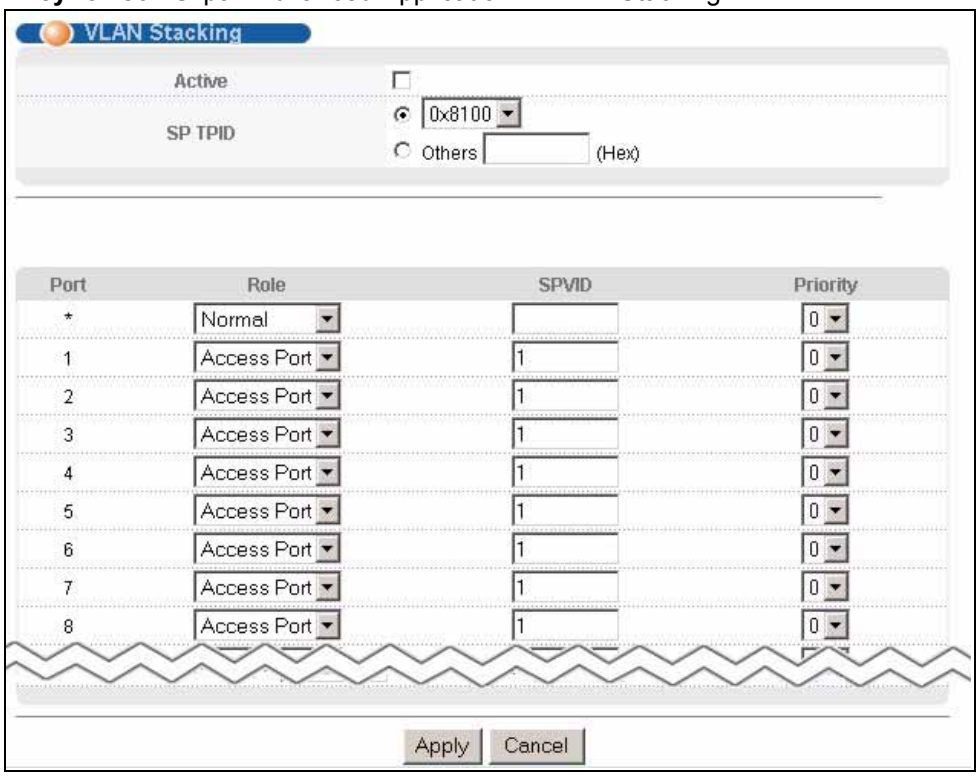
Таблица 52 Кадр 802.1Q

DA	Адрес назначения	Priority	Приоритет 802.1p
SA	Адрес источника	Len/ Etype	Длина и тип кадра Ethernet
(SP)TPID	Идентификатор протокола тега (провайдера услуг)	Data	Данные кадра
VID	Идентификатор VLAN	FCS	Контрольная последовательность кадра

21.4 Настройка стекирования VLAN

Чтобы отобразить следующий экран, нажмите **Advanced Applications > VLAN Stacking**.

Рисунок 80 Экран Advanced Application > VLAN Stacking



Поля экрана описаны в следующей таблице.

Таблица 53 Экран Advanced Application > VLAN Stacking

ПОЛЕ	ОПИСАНИЕ
Active	Установите данный переключатель, чтобы включить на коммутаторе стекирование VLAN.
SP TPID	**SP TPID** представляет собой стандартный код типа Ethernet, идентифицирующий кадр и указывающий, несет ли кадр информацию тега IEEE 802.1Q. Выберите **0x8100** или **0x9100** из ниспадающего списка или выберите пункт **Others** и введите четырехзначное число в шестнадцатеричном виде в диапазоне от 0x0000 до 0xFFFF. 0x указывает на запись в шестнадцатеричном виде. Эти два символа не следует вводить в текстовое поле **Others**.
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.
Role	Выберите **Normal**, чтобы коммутатор игнорировал получаемые (или передаваемые) через данный порт кадры с тегами стекирования VLAN. В этом случае настройки в **SPVID** и **Priority** игнорируются. Выберите **Access Port**, чтобы коммутатор добавлял тег **SP TPID** ко всем входящим кадрам, принимаемым через данный порт. Значение **Access Port** необходимо выбрать для входящих портов на границе сети провайдера услуг. Значение **Tunnel Port** (доступное только для гигабитных портов) устанавливается для исходящих портов на граничном устройстве сети провайдера услуг. Для поддержки стекирования VLAN на порту данный порт должен быть способен пропускать через себя кадры длиной 1526 байт (1522 байта + 4 байта для второго тега).
SPVID	**SPVID** представляет собой идентификатор VLAN провайдера услуг (внешний тег VLAN). Введите идентификатор провайдера услуг (в диапазоне от 1 до 4094) для кадров, принимаемых через данный порт. Дополнительную информацию об идентификаторах VLAN можно найти в гл. 8 на стр. 95.
Priority	На коммутаторе уровни приоритета для внутренних тегов IEEE 802.1Q настраиваются на экране **Port Setup**. «0» соответствует самому низкому приоритету, «7» – самому высокому.
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.

22

Мультивещание

В данной главе описана настройка различных функций мультивещания.

22.1 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.

22.1.1 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).

22.1.2 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.

22.1.3 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.

22.1.4 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.

22.2 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. 22.1 на стр. 191.

Рисунок 81 Экран Advanced Application > Multicast

Поля экрана описаны в следующей таблице.

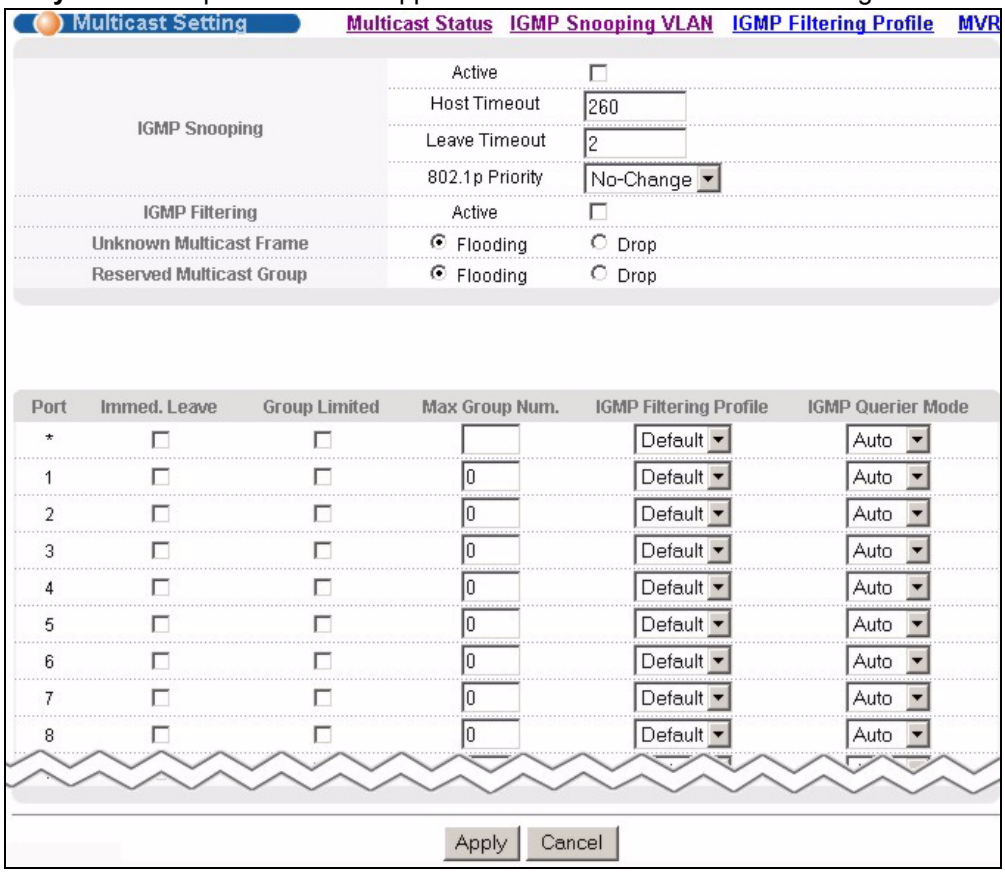
Таблица 54 Экран Multicast Status

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.

22.3 Настройка мультивещания

Чтобы отобразить показанный ниже экран, нажмите **Advanced Applications > Multicast > Multicast Setting**. Более подробную информацию о мультивещании можно найти в разд. 22.1 на стр. 191.

Рисунок 82 Экран Advanced Application > Multicast > Multicast Setting



Поля экрана описаны в следующей таблице.

Таблица 55 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.
Reserved Multicast Group	Адреса мультивещания (в диапазоне с 224.0.0.0 по 224.0.0.255) зарезервированы для использования в локальном масштабе. Например, 224.0.0.1 предназначен для всех хостов в данной подсети, 224.0.0.2 – для всех маршрутизаторов мультивещания в данной подсети и т.д. Пакеты с IP-адресами назначения из данного диапазона маршрутизатором не пересылаются. Дополнительную информацию можно найти на сайте IANA. Выберите действие, выполняемое коммутатором при получении кадра с зарезервированным адресом 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.

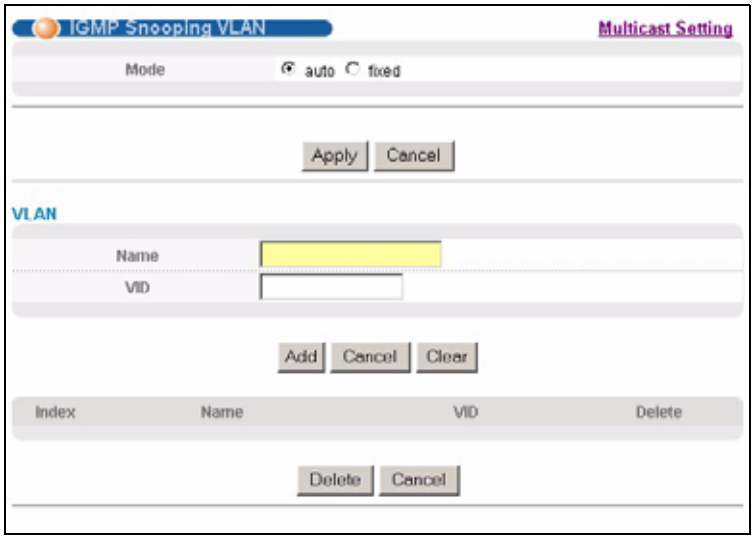
Таблица 55 Экран Advanced Application > Multicast > Multicast Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
Group Limited	Выбор данной опции позволяет ограничить число групп мультивещания, к которым разрешено присоединиться данному порту.
Max Group Num.	Введите число групп мультивещания, к которым разрешено присоединиться данному порту. После регистрации порта в указанном количестве групп мультивещания все последующие Join-сообщения IGMP от данного порта отбрасываются.
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.

22.4 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. 22.1.4 на стр. 192.

Рисунок 83 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN



Поля экрана описаны в следующей таблице.

Таблица 56 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**.

Таблица 56 Экран Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN (продолжение)

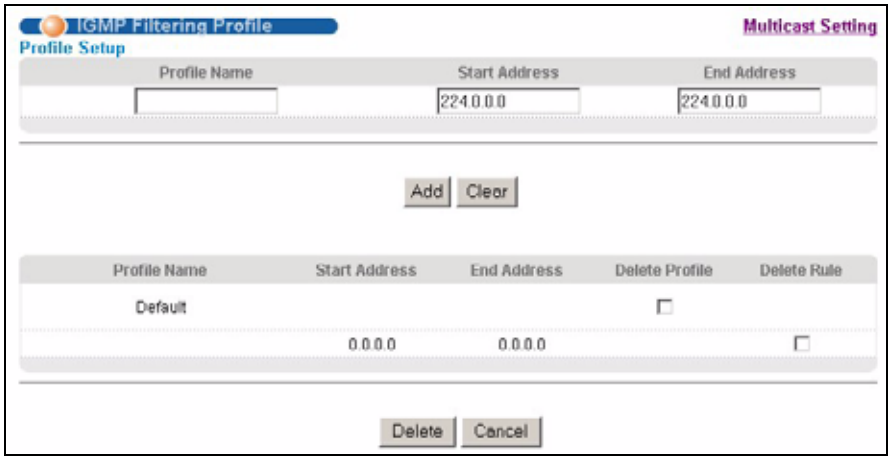
ПОЛЕ	ОПИСАНИЕ
Add	Нажмите **Add**, чтобы добавить запись в итоговую таблицу ниже и сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней 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**.

22.5 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 84 Экран Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile



Поля экрана описаны в следующей таблице.

Таблица 57 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.
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**.

22.6 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 85 Пример сети с поддержкой MVR

22.6.1 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.

22.6.2 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.

22.6.3 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 86 Пример с мультивещанием телевидения посредством MVR

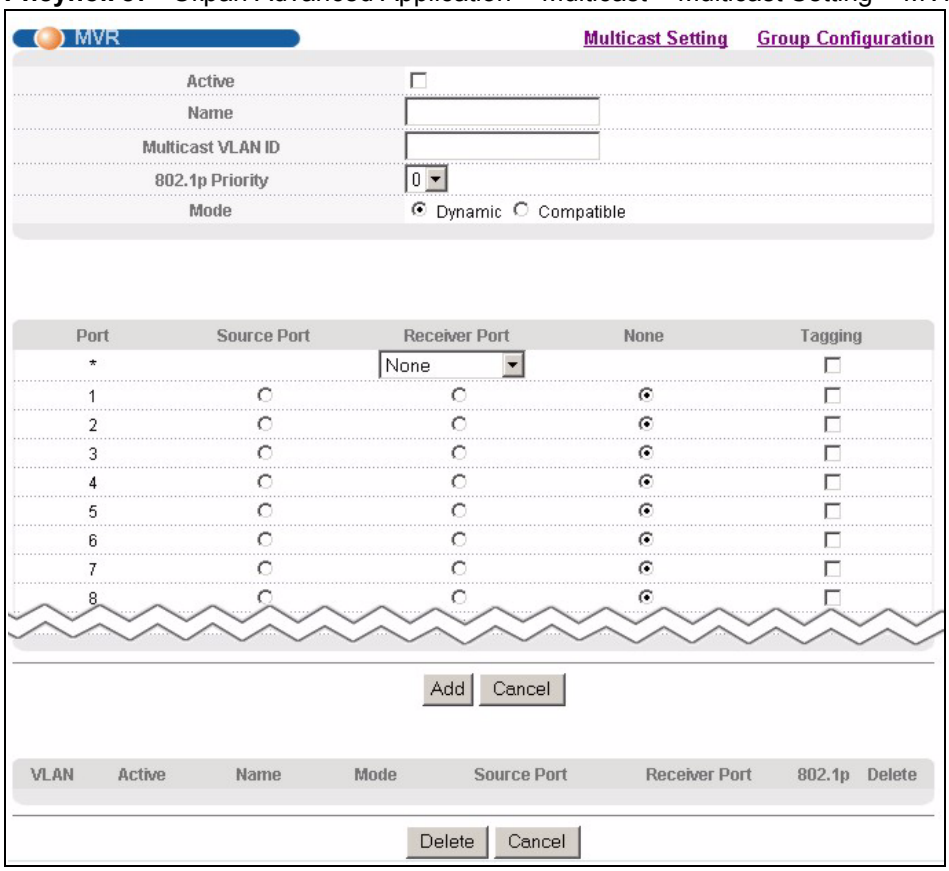
22.7 Общая настройка MVR

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 87 Экран Advanced Application > Multicast > Multicast Setting > MVR



Поля экрана описаны в следующей таблице.

Таблица 58 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 отображаемых ASCII-символов), по которому можно идентифицировать эту запись.
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 58 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**.

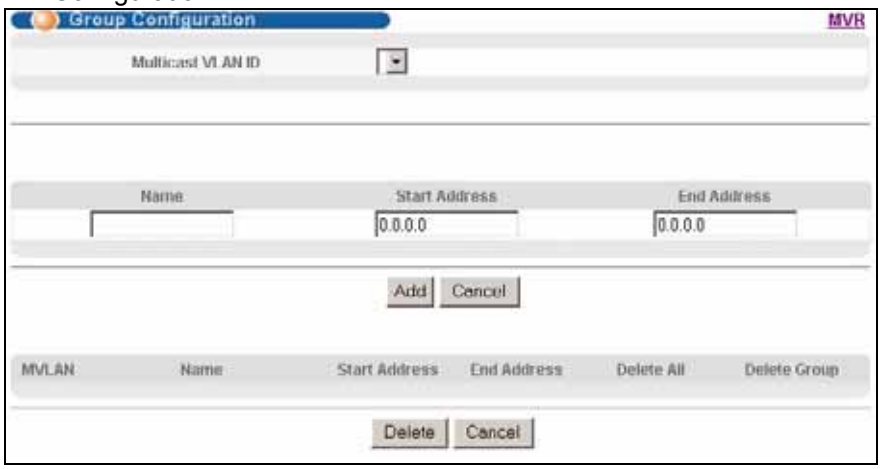
22.8 Настройка группы MVR

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 88 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration



Поля экрана описаны в следующей таблице.

Таблица 59 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. 22.1.1 на стр. 191.
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. 22.1.1 на стр. 191.
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.

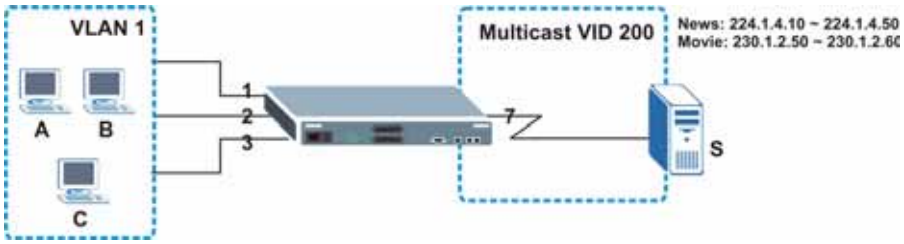
Таблица 59 Экран Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

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.

22.8.1 Пример настройки MVR

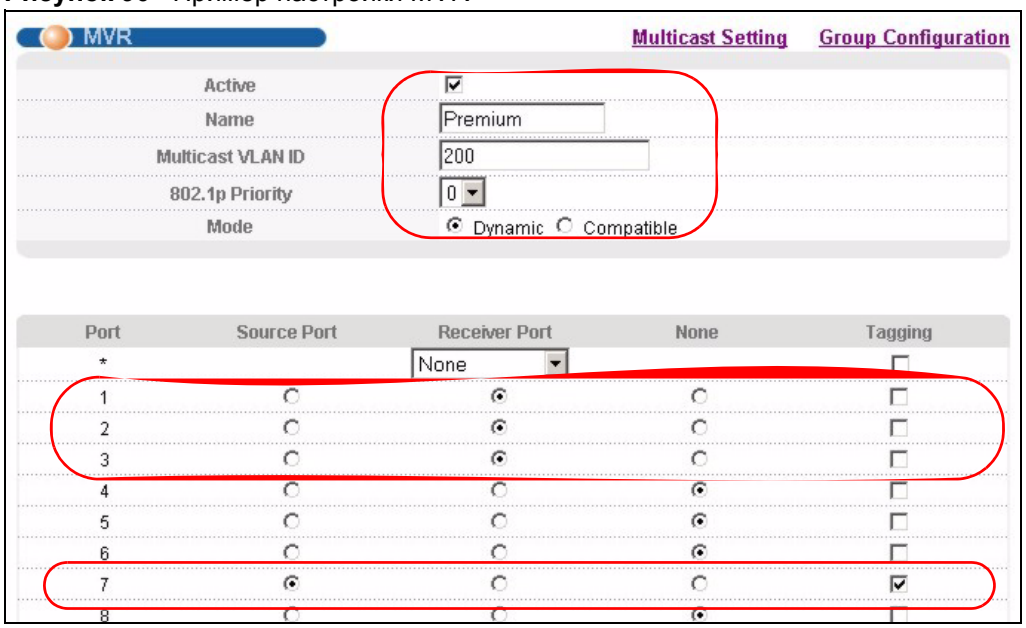
На приведенном ниже рисунке показан пример сети, в которой порты 1, 2 и 3 коммутатора принадлежат VLAN 1. Кроме того, порт 7 принадлежит к группе мультивещания с идентификатором VID 200 для получения трафика мультивещания (каналы **News** и **Movie**) от удаленного сервера потокового мультимедиа, **S**.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

Рисунок 89 Пример настройки MVR



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

Рисунок 90 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 91 Пример настройки групп MVR

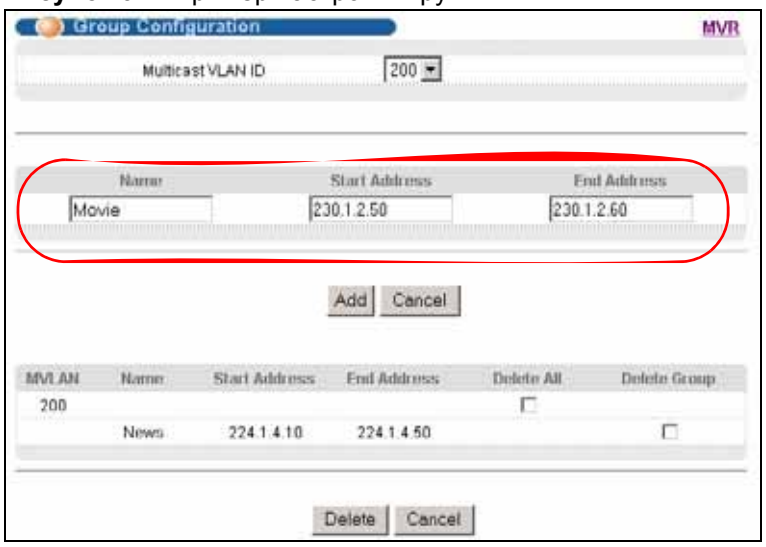
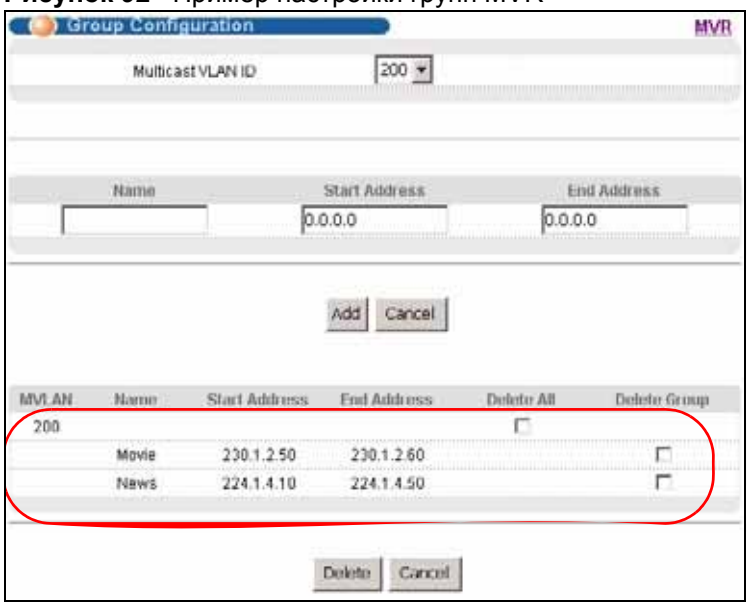


Рисунок 92 Пример настройки групп MVR



23

Аутентификация и учет

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

23.1 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. 23.1.2 на стр. 208) и TACACS+ (Terminal Access Controller Access-Control System Plus, см. разд. 23.1.2 на стр. 208).

Рисунок 93 Сервер AAA

23.1.1 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. 36 на стр. 321).

23.1.2 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 60 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.

23.2 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.

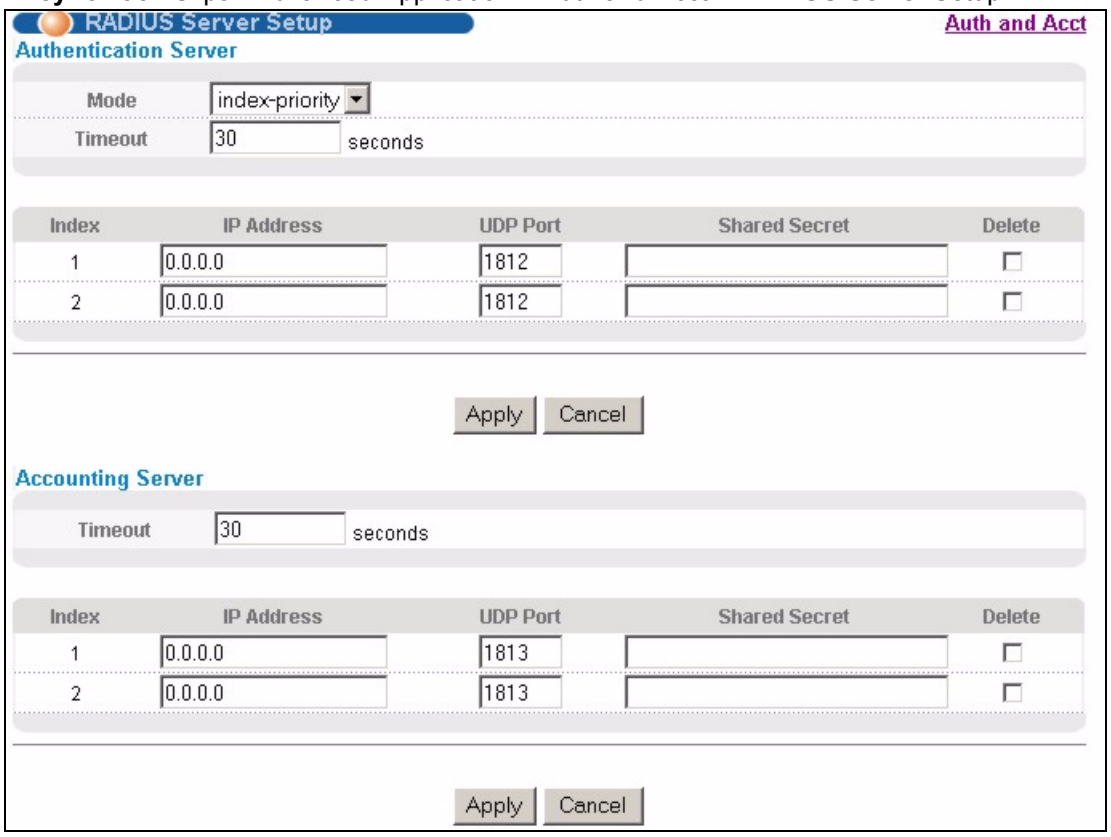
Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Auth and Acct**.

Рисунок 94 Экран Advanced Application > Auth and Acct

23.2.1 Настройка сервера RADIUS

Настройки сервера RADIUS вводятся на показанном ниже экране. Дополнительную информацию о серверах RADIUS можно найти в разд. 23.1.2 на стр. 208, а информацию об атрибутах RADIUS, используемых функциями аутентификации и учета данного коммутатора – в разд. 23.3 на стр. 217.Чтобы отобразить показанный ниже экран, нажмите на ссылке **RADIUS Server Setup** на экране **Authentication and Accounting**.

Рисунок 95 Экран Advanced Application > Auth and Acct > RADIUS Server Setup



Поля экрана описаны в следующей таблице.

Таблица 61 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.

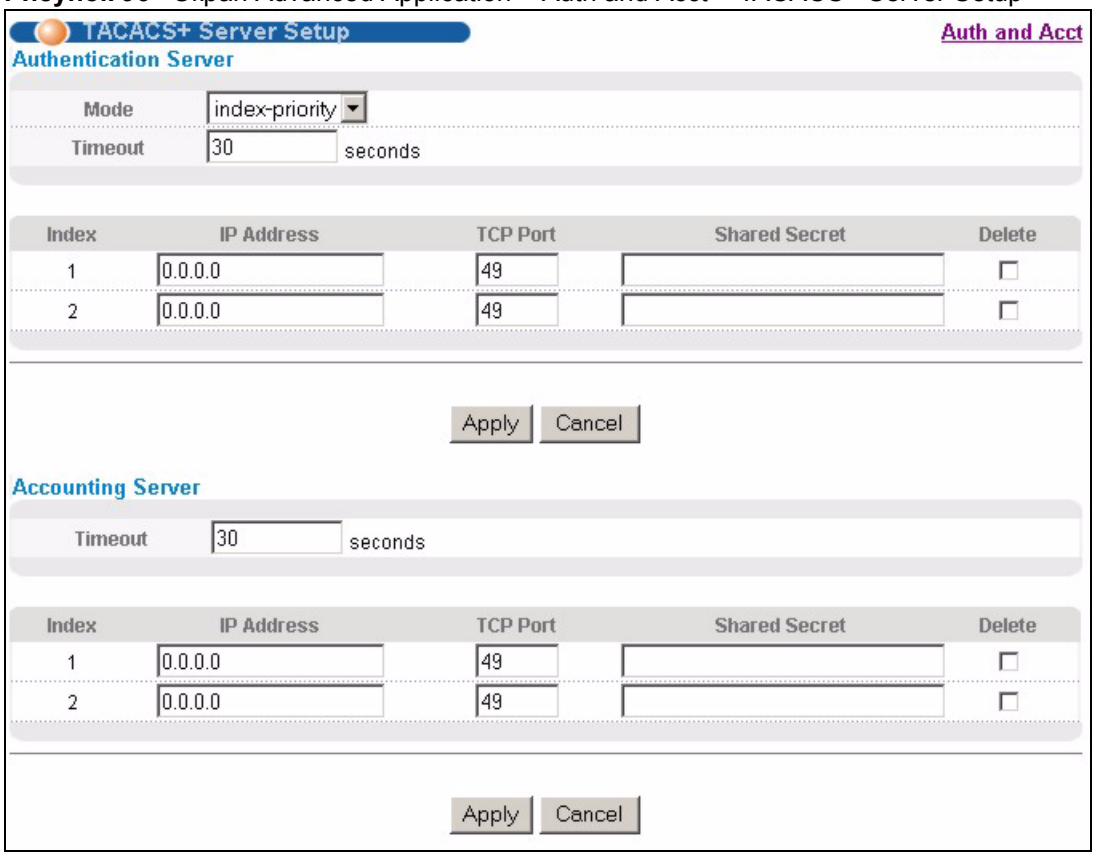
Таблица 61 Экран Advanced Application > Auth and Acct > RADIUS Server Setup

ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер записи о сервере RADIUS (только для чтения).
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 учет на сервере RADIUS производится 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.

23.2.2 Настройка сервера TACACS+

Настройки сервера TACACS+ вводятся на показанном ниже экране. Более подробную информацию о серверах TACACS+ можно найти в разд. 23.1.2 на стр. 208.Чтобы отобразить показанный ниже экран, нажмите на ссылке **TACACS+ Server Setup** на экране **Authentication and Accounting**.

Рисунок 96 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup



Поля экрана описаны в следующей таблице.

Таблица 62 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.

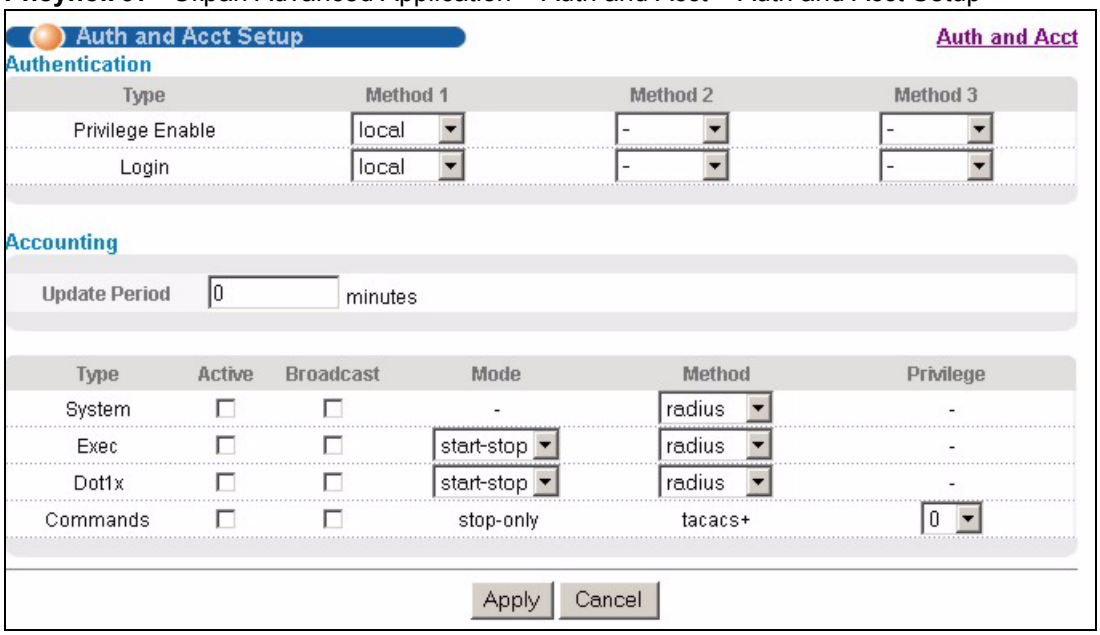
Таблица 62 Экран Advanced Application > Auth and Acct > TACACS+ Server Setup

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 учет на сервере TACACS+ производится 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.

23.2.3 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 97 Экран Advanced Application > Auth and Acct > Auth and Acct Setup



Поля экрана описаны в следующей таблице.

Таблица 63 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. разд. 45.7 на стр. 372). **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 63 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 63 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.

23.2.4 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 разд. 45.7 на стр. 372) 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 64 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.

23.2.4.1 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 65 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.

23.3 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.

23.3.1 Атрибуты, используемые для аутентификации

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

23.3.1.1 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

23.3.1.2 Атрибуты, используемые для входа пользователей

User-Name

User-Password
NAS-Identifier
NAS-IP-Address

23.3.1.3 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

23.3.2 Атрибуты, используемые для учета

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

23.3.2.1 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

23.3.2.2 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 66 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

Таблица 66 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
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

Таблица 67 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

23.3.2.3 Атрибуты, используемые для учета событий IEEE 802.1x

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

Таблица 68 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

Таблица 68 Атрибуты RADIUS – события Exec при выполнении команд с консоли

АТРИБУТ	НАЧАЛО	ПРОМЕЖ. ОБНОВЛЕНИЕ	ЗАВЕРШЕНИЕ
Acct-Input-Octets		Д	Д
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

24

Защита от подмены IP-адресов

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

24.1 Обзор функции защиты от подмены IP-адресов

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

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

При получении коммутатором пакета DHCP или 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 привязок строится коммутатором посредством отслеживания пакетов DHCP (динамическая привязка) и на основе информации, предоставленной администратором вручную (статическая привязка).

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

- Статическая привязка. Используется для создания статических связей в таблице привязок.
- Отслеживание DHCP. Используется для отфильтровывания несанкционированных пакетов DHCP в сети и для динамического построения таблицы привязок.
- Инспекция ARP-пакетов. Используется для отфильтровывания несанкционированных пакетов ARP.

Чтобы использовать динамическую привязку для отфильтровывания несанкционированных ARP-пакетов (типичная ситуация), перед включением инспекции ARP-пакетов необходимо включить отслеживание DHCP.

24.1.1 Обзор отслеживания DHCP

Функция отслеживания DHCP позволяет отфильтровывать несанкционированные DHCP-пакеты в сети и динамически строить таблицу привязок. Благодаря этому можно защитить клиентов от получения IP-адресов от несанкционированных серверов DHCP.

24.1.1.1 Доверенные и не заслуживающие доверия порты

Функция отслеживания DHCP делит все порты на доверенные и не заслуживающие доверия. Данная настройка не зависит от аналогичной настройки доверенных/не заслуживающих доверия портов для функции инспекции ARP-пакетов. Кроме того, можно определить максимальное количество пакетов DHCP, которое может приниматься через каждый из портов (доверенных или не заслуживающих доверия) за секунду.

Доверенные порты подключаются к серверам DHCP или другим коммутаторам. Пакеты DHCP, поступающие через доверенные порты, коммутатор отбрасывает лишь в том случае, если скорость их поступления слишком высока. По информации от доверенных портов коммутатор строит динамическую таблицу привязок.

Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.

Не заслуживающие доверия порты подключаются к абонентам. Пакеты DHCP от не заслуживающих доверия портов отбрасываются коммутатором в следующих случаях:

- Пакет представляет собой пакет сервера DHCP (например, OFFER, ACK или NACK).
- MAC-адрес источника и IP-адрес источника в пакете не соответствуют ни одной из существующих привязок.
- Пакет представляет собой пакет типа RELEASE или DECLINE, и MAC-адрес источника и порт источника не соответствуют ни одной из существующих привязок.
- Скорость поступления пакетов DHCP слишком высока.

24.1.1.2 База данных отслеживания DHCP

Таблица привязок хранится коммутатором в энергозависимой памяти. В случае перезапуска коммутатора он загружает статические привязки из постоянной памяти, однако динамические привязки при этом теряются, т.е. устройства в сети должны повторно направлять DHCP-запросы. В связи с этим рекомендуется настроить базу данных отслеживания DHCP.

База данных отслеживания DHCP позволяет хранить динамические привязки для функций отслеживания DHCP и инспекции ARP-пакетов в файле на внешнем сервере TFTP. Если база данных отслеживания DHCP была настроена, коммутатор загружает динамические привязки из базы данных отслеживания DHCP после перезапуска коммутатора.

Можно настроить имя и расположение файла на внешнем сервере TFTP. Файл имеет следующий формат:

Рисунок 98 Формат файла базы данных отслеживания DHCP

```
<начальная-контрольная-сумма>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<привязка-1> <контрольная-сумма-1>
<привязка-2> <контрольная-сумма-1-2>
...
...
<привязка-n> <контрольная-сумма-1-2-..-n>
END
```

Значение <начальная-контрольная-сумма> позволяет различать привязки, сохраненные в последнем обновлении, от привязок из предыдущих обновлений. Каждая привязка включает в себя 72 байта, пробел и еще одну контрольную сумму, которая используется для проверки привязки в процессе считывания. Если вычисленная контрольная сумма не совпадает с контрольной суммой в файле, данная и все последующие привязки игнорируются.

24.1.1.3 Информация в поле Option 82 при ретрансляции DHCP

Данный коммутатор способен добавлять информацию к тем запросам DHCP, которые им не отбрасываются. Благодаря этому сервер DHCP может получить больше информации об источнике запроса. Данный коммутатор способен добавлять следующую информацию:

- Идентификатор слота (1 байт), идентификатор порта (1 байт), и идентификатор VLAN (2 байта)
- Имя системы (до 32 байт)

Данная информация помещается в поле информации агента поля Option 82 заголовка DHCP в кадрах клиентских запросов DHCP. Дополнительную информацию о поле Option 82 при ретрансляции DHCP можно найти в гл. 33 на стр. 291.

При ответе сервера DHCP коммутатор удаляет информацию из поля информации агента перед пересылкой ответа к первоначальному источнику запроса.

Данные параметры могут быть настроены для каждой исходной VLAN. Они не зависят от настроек ретрансляции DHCP (гл. 33 на стр. 291).

24.1.1.4 Настройка отслеживания DHCP

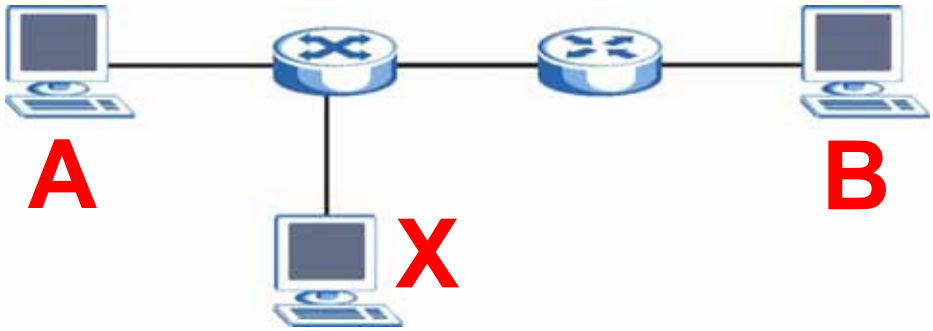
Чтобы настроить на коммутаторе функцию отслеживания DHCP, выполните следующие действия.

1. Включите функцию отслеживания DHCP на коммутаторе.
2. Включите функцию отслеживания DHCP для каждой VLAN, и настройте значение для поля Option 82 при ретрансляции DHCP.
3. Настройте доверенные и не заслуживающие доверия порты, а также укажите максимальное количество пакетов DHCP в секунду, принимаемое через каждый из портов.
4. Настройте статические привязки.

24.1.2 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 99 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.

24.1.2.1 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. 117).

- 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**.

24.1.2.2 Доверенные и не заслуживающие доверия порты

Функция инспекции ARP-пакетов делит все порты на доверенные и не заслуживающие доверия. Данная настройка не зависит от аналогичной настройки доверенных/не заслуживающих доверия портов для функции отслеживания DHCP. Дополнительно можно указать максимальную скорость, с которой коммутатор будет принимать ARP-пакеты через не заслуживающие доверия порты.

Пакеты ARP, приходящие через доверенные порты, коммутатором не отбрасываются ни по какой причине.

От не заслуживающих доверия портов коммутатор отбрасывает ARP-пакеты в следующих случаях:

- Информация об отправителе в ARP-пакете не совпадает с одной из существующих привязок.
- Скорость поступления пакетов ARP слишком высока.

24.1.2.3 Системный журнал Syslog

При пересылке или отбрасывании пакетов ARP коммутатор может отправлять сообщения системного журнала syslog на указанный сервер syslog (гл. 38 на стр. 343). В целях большей эффективности коммутатор может консолидировать сообщения контрольного журнала и отправлять их партиями.

24.1.2.4 Настройка инспекции ARP-пакетов

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

1 Настройте отслеживание DHCP. См. разд. 24.1.1.4 на стр. 223.

Рекомендуется включить отслеживание DHCP как минимум за один день до включения инспекции ARP-пакетов, чтобы у коммутатора было достаточно времени для построения таблицы привязок.

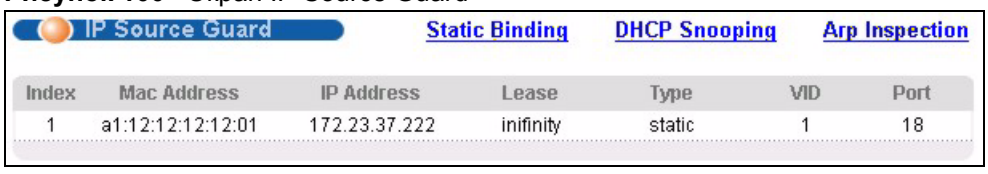
2 Включите функцию инспекции ARP-пакетов в каждой сети VLAN.

3 Настройте доверенные и не заслуживающие доверия порты, а также укажите максимальное количество пакетов ARP в секунду, принимаемое через каждый из портов.

24.2 Защита от подмены IP-адресов

На данном экране можно просмотреть существующие привязки для функций отслеживания DHCP и инспекции ARP-пакетов. На основе привязок функции отслеживания DHCP и инспекции ARP-пакетов различают санкционированные и несанкционированные пакеты. Таблица привязок строится коммутатором посредством отслеживания пакетов DHCP (динамическая привязка) и на основе информации, предоставленной администратором вручную (статическая привязка).Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard**.

Рисунок 100 Экран IP Source Guard



Поля экрана описаны в следующей таблице.

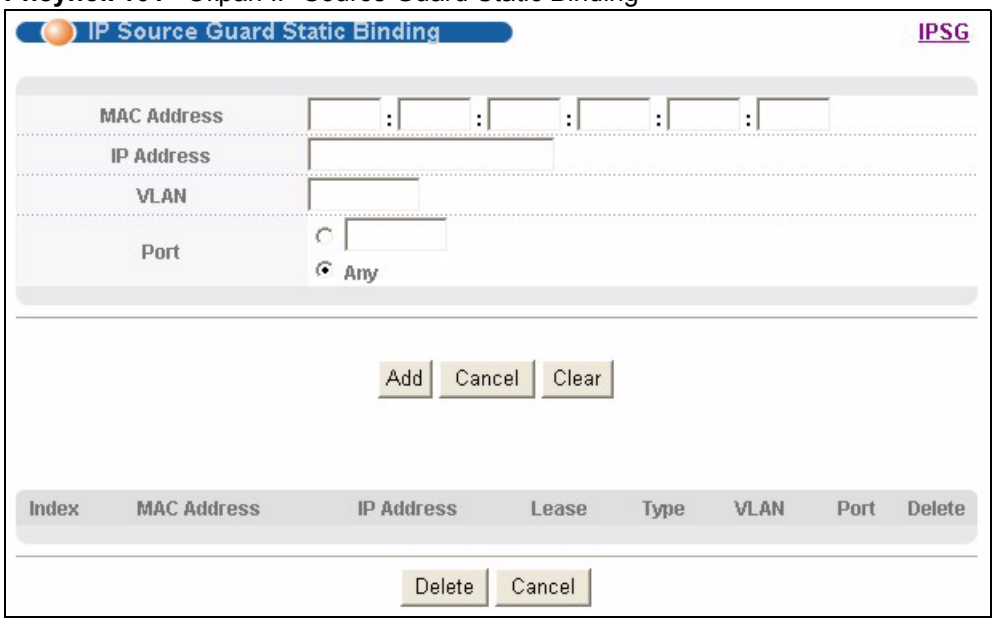
Таблица 69 Экран IP Source Guard

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. **dhcp-snooping**: привязка создана в результате отслеживания пакетов DHCP.
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.

24.3 Статическая привязка для защиты от подмены IP-адресов

На данном экране можно управлять статическими привязками для функций отслеживания DHCP и 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 101 Экран IP Source Guard Static Binding



Поля экрана описаны в следующей таблице.

Таблица 70 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**.
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.

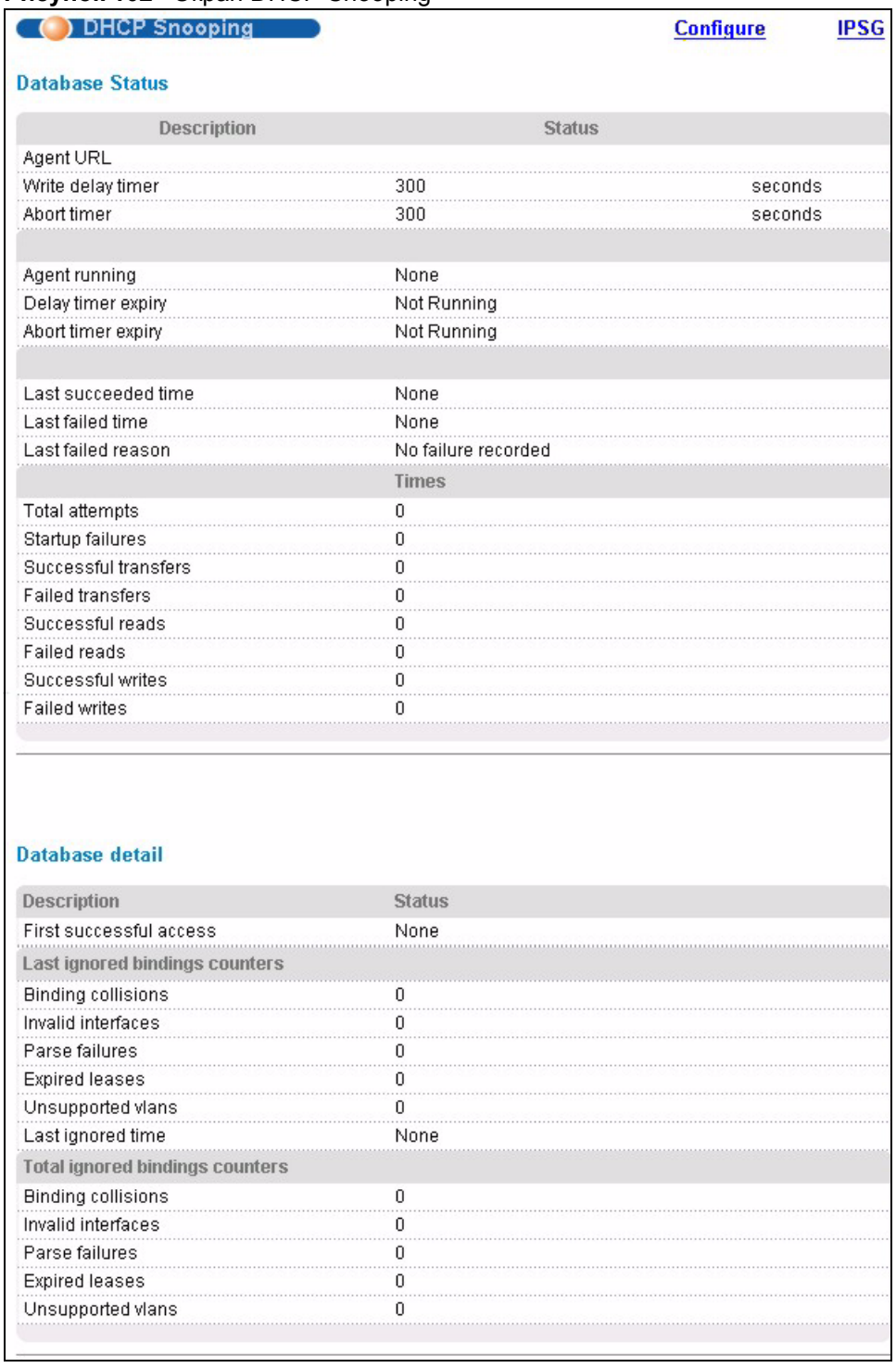
Таблица 70 Экран IP Source Guard Static Binding (продолжение)

ПОЛЕ	ОПИСАНИЕ
Delete	Установите переключатель и нажмите на **Delete**, чтобы удалить выбранную запись.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей **Delete**.

24.4 Отслеживание DHCP

На данном экране можно просмотреть различные статистические данные по базе данных отслеживания DHCP. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping**.

Рисунок 102 Экран DHCP Snooping



DHCP Snooping

Configure IPSG

Database Status

Description	Status	
Agent URL		
Write delay timer	300	seconds
Abort timer	300	seconds
Agent running	None	
Delay timer expiry	Not Running	
Abort timer expiry	Not Running	
Last succeeded time	None	
Last failed time	None	
Last failed reason	No failure recorded	
	Times	
Total attempts	0	
Startup failures	0	
Successful transfers	0	
Failed transfers	0	
Successful reads	0	
Failed reads	0	
Successful writes	0	
Failed writes	0	

Database detail

Description	Status
First successful access	None
Last ignored bindings counters	
Binding collisions	0
Invalid interfaces	0
Parse failures	0
Expired leases	0
Unsupported vlans	0
Last ignored time	None
Total ignored bindings counters	
Binding collisions	0
Invalid interfaces	0
Parse failures	0
Expired leases	0
Unsupported vlans	0

Поля экрана описаны в следующей таблице.

Таблица 71 Экран DHCP Snooping

ПОЛЕ	ОПИСАНИЕ
Database Status	
	В данном разделе отображаются текущие настройки базы данных отслеживания DHCP. Их можно изменить на экране **DHCP Snooping Configure**.См. разд. 24.5 на стр. 232.
Agent URL	В данном поле отображается месторасположение базы данных отслеживания DHCP.
Write delay timer	В данном поле отображается, как долго (в секундах) коммутатор пытается выполнить конкретное обновление базы данных отслеживания DHCP перед отказом от дальнейших попыток.
Abort timer	В данном поле отображается, как долго (в секундах) коммутатор выжидает перед обновлением базы данных отслеживания DHCP после изменения текущих привязок.
	В этом разделе отображается информация о текущем обновлении и следующем обновлении базы данных отслеживания DHCP.
Agent running	В этом поле отображается статус текущего обновления или доступа к базе данных отслеживания DHCP. **none**: коммутатор не обращается к базе данных отслеживания DHCP. **read**: коммутатор осуществляет загрузку динамических привязок из базы данных отслеживания DHCP. **write**: коммутатор осуществляет обновление базы данных отслеживания DHCP.
Delay timer expiry	В данном поле отображается, сколько еще (в секундах) коммутатор будет пытаться выполнить текущее обновление перед отказом от дальнейших попыток. Если коммутатор в данный момент не выполняет обновления базы данных отслеживания DHCP, в этом поле отображается **Not Running**.
Abort timer expiry	В данном поле отображается, через какой промежуток времени (в секундах) коммутатор выполнит очередное обновление базы данных отслеживания DHCP. Если текущие привязки с момента последнего обновления не изменялись, в этом поле отображается **Not Running**.
	В данном разделе отображается информация о последнем обновлении коммутатором базы данных отслеживания DHCP.
Last succeeded time	В этом поле отображается время последнего успешного обновления коммутатором базы данных отслеживания DHCP.
Last failed time	В этом поле отображается время последнего неудавшегося обновления коммутатором базы данных отслеживания DHCP.
Last failed reason	В этом поле отображается причина последнего неудавшегося обновления коммутатором базы данных отслеживания DHCP.
	В данном разделе отображается историческая информация о количестве успешных и неудавшихся попыток считывания или обновления коммутатором базы данных отслеживания DHCP.
Total attempts	В этом поле отображается общее количество попыток обращения коммутатором к базе данных отслеживания DHCP по любым причинам.
Startup failures	В данном поле отображается количество случаев, когда коммутатору не удалось создать или считать базу данных отслеживания DHCP при запуске коммутатора или настройки нового URL для базы данных отслеживания DHCP.

Таблица 71 Экран DHCP Snooping (продолжение)

ПОЛЕ	ОПИСАНИЕ
Successful transfers	В данном поле отображается количество случаев успешного считывания привязок или обновления привязок коммутатором в базе данных отслеживания DHCP.
Failed transfers	В данном поле отображается количество случаев неудавшегося считывания привязок или обновления привязок коммутатором в базе данных отслеживания DHCP.
Successful reads	В этом поле отображается количество успешных считываний привязок коммутатором из базы данных отслеживания DHCP.
Failed reads	В этом поле отображается количество неудавшихся считываний привязок коммутатором из базы данных отслеживания DHCP.
Successful writes	В этом поле отображается количество успешных обновлений привязок коммутатором в базе данных отслеживания DHCP.
Failed writes	В этом поле отображается количество неудавшихся обновлений привязок коммутатором в базе данных отслеживания DHCP.
Database detail	
First successful access	В этом поле отображается время первого обращения коммутатора к базе данных отслеживания DHCP по любой причине.
Last ignored bindings counters	В этом разделе отображается количество случаев и причины, по которым коммутатором были проигнорированы привязки при последней попытке считывания привязок из базы данных отслеживания DHCP. Эти счетчики можно сбросить посредством перезапуска коммутатора или с использованием команд интерфейса командной строки.См. гл. 45 на стр. 369.
Binding collisions	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине наличия в коммутаторе привязки с тем же самым MAC-адресом и идентификатором VLAN ID.
Invalid interfaces	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине того, что номер порта соответствует доверенному интерфейсу или больше не существует.
Parse failures	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине невозможности для коммутатор выделить данные для привязки из базы данных привязок DHCP.
Expired leases	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине окончания срока аренды.
Unsupported vlans	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине прекращения существования сети с указанным VLAN ID.
Last ignored time	В этом поле отображается время последнего игнорирования коммутатором привязок из базы данных отслеживания DHCP по любой причине.
Total ignored bindings counters	В этом разделе отображается количество случаев и причины, по которым коммутатором были проигнорированы привязки при считывании привязок из базы данных отслеживания DHCP за все время. Эти счетчики можно сбросить посредством перезапуска коммутатора или с использованием команд интерфейса командной строки.См. гл. 45 на стр. 369.
Binding collisions	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине наличия в коммутаторе привязки с тем же самым MAC-адресом и идентификатором VLAN ID.

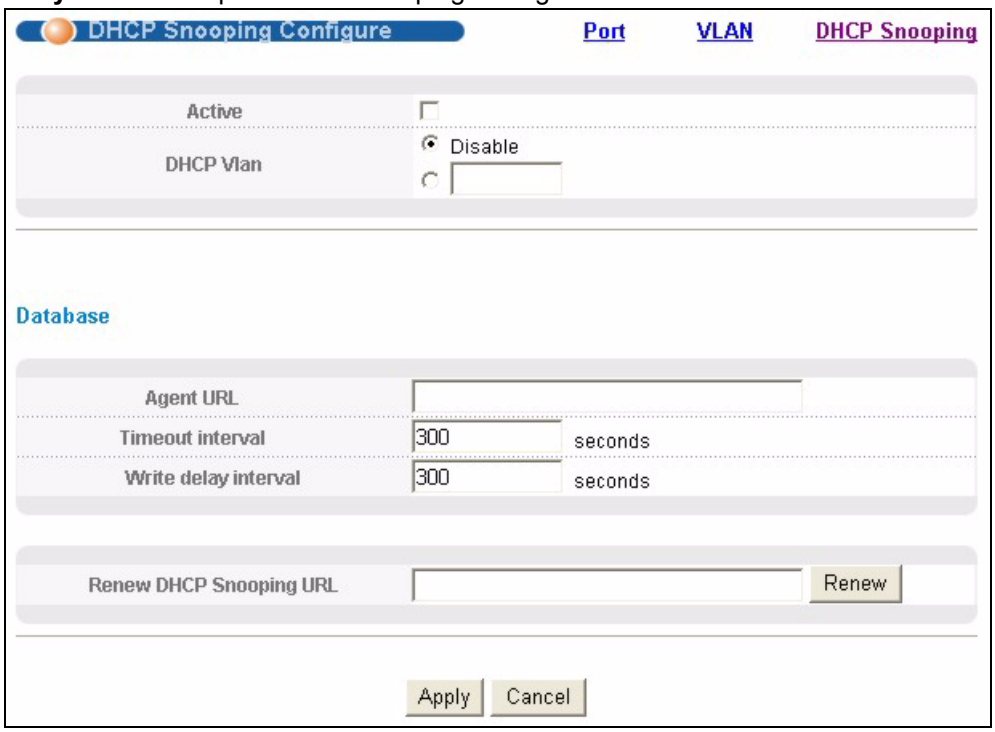
Таблица 71 Экран DHCP Snooping (продолжение)

ПОЛЕ	ОПИСАНИЕ
Invalid interfaces	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине того, что номер порта соответствует доверенному интерфейсу или больше не существует.
Parse failures	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине невозможности для коммутатор выделить данные для привязки из базы данных привязок DHCP.
Expired leases	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине окончания срока аренды.
Unsupported vlans	В этом поле отображается количество привязок, которые были проигнорированы коммутатором по причине прекращения существования сети с указанным VLAN ID.

24.5 Настройка отслеживания DHCP

С помощью данного экрана можно включить отслеживание DHCP на коммутаторе (но не на конкретных VLAN), указать сеть VLAN, в которой располагается DHCP-сервер по умолчанию, а также настроить базу данных отслеживания DHCP. База данных отслеживания DHCP позволяет хранить текущие привязки на защищенном внешнем сервере TFTP, чтобы они были доступны после перезапуска. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Рисунок 103 Экран DHCP Snooping Configure



Поля экрана описаны в следующей таблице.

Таблица 72 Экран DHCP Snooping Configure

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на коммутаторе функцию отслеживания DHCP. После этого необходимо включить функцию отслеживания DHCP в конкретной сети VLAN и указать доверенные порты. Примечание: Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.
DHCP Vlan	Выберите идентификатор VLAN ID, если коммутатор должен пересылать пакеты DHCP к серверам DHCP в конкретной VLAN. Примечание: Для этой VLAN необходимо будет также включить отслеживание DHCP. Чтобы помочь серверам DHCP различать запросы DHCP от различных сетей VLAN, на экране **DHCP Snooping VLAN Configure** можно включить использование поля **Option82** (разд. 24.5.2 на стр. 235). Выберите **Disable**, если от коммутатора не требуется пересылки пакетов DHCP в конкретную сеть VLAN.
Database	Если значение **Timeout interval** превышает значение **Write delay interval**, то следующее плановое обновление может произойти до успешного завершения или тайм-аута текущего обновления. В этом случае коммутатор выжидает с началом следующего обновления до завершения текущего.
Agent URL	Введите расположение базы данных отслеживания DHCP. Расположение должно быть указано в следующем виде: tftp://{имя домена или IP-адрес}/каталог, если необходимо/имя файла; например, tftp://192.168.10.1/database.txt.
Timeout interval	Введите, как долго (от 10 до 65535 секунд) коммутатор будет пытаться выполнить конкретное обновление базы данных отслеживания DHCP перед отказом от дальнейших попыток.
Write delay interval	Введите, как долго (от 10 до 65535 секунд) коммутатор будет выжидать перед обновлением базы данных отслеживания DHCP после первого изменения текущих привязок с момента обновления. После определения времени следующего обновления все дополнительные изменения в текущих привязках включаются в это обновление автоматически.
Renew DHCP Snooping URL	Введите расположение базы данных отслеживания DHCP и нажмите на **Renew**, чтобы коммутатор загрузил ее. Таким образом можно загрузить динамические привязки из другой базы данных отслеживания DHCP, чем указанная в поле **Agent URL**. При загрузке динамических привязок из базы данных отслеживания DHCP коммутатор предварительно не отбрасывает существующие динамические привязки. В случае конфликта коммутатор сохраняет динамические привязки в энергозависимой памяти и изменяет показания счетчика **Binding collisions** на экране **DHCP Snooping** (разд. 24.4 на стр. 228).

Таблица 72 Экран DHCP Snooping Configure (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	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

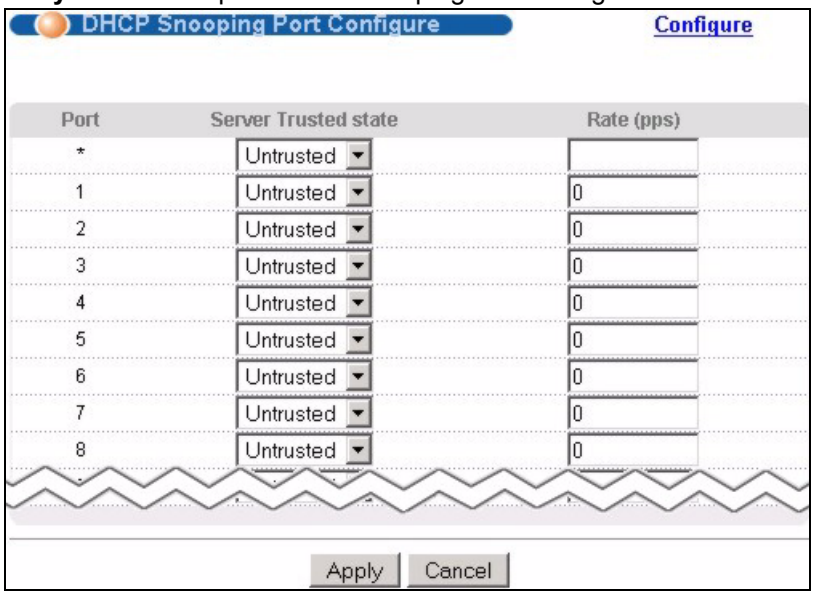
24.5.1 Настройка портов отслеживания DHCP

На данном экране можно определить порты как доверенные и не заслуживающие доверия для функции отслеживания DHCP.

Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.

Кроме того, можно определить максимальное количество пакетов DHCP, которое может приниматься через каждый из портов (доверенных или не заслуживающих доверия) за секунду. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Рисунок 104 Экран DHCP Snooping Port Configure



Поля экрана описаны в следующей таблице.

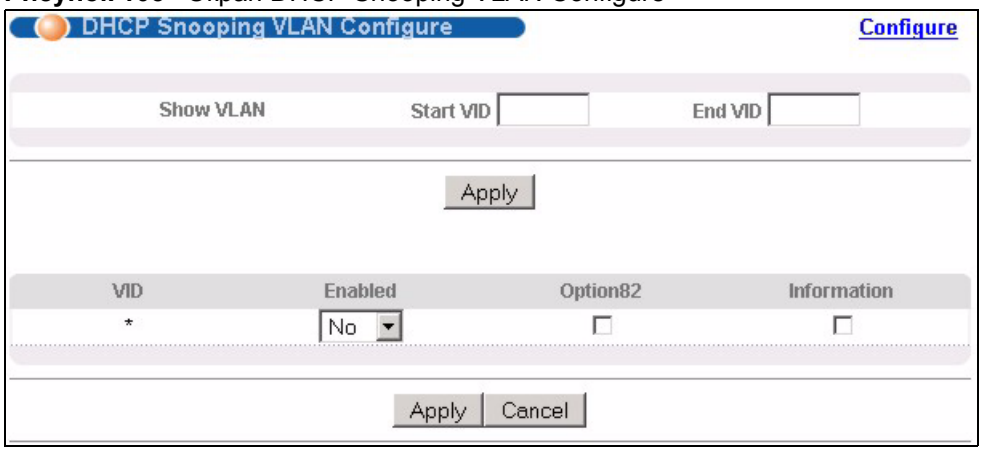
Таблица 73 Экран DHCP Snooping Port Configure

ПОЛЕ	ОПИСАНИЕ
Port	В этом поле отображается номер порта. При настройке порта * эти настройки применяются ко всем портам.
Server Trusted state	Выберите, будет ли данный порт считаться доверенным (**Trusted**) или не заслуживающим доверия (**Untrusted**). Доверенные порты подключаются к серверам DHCP или другим коммутаторам, поэтому коммутатор отбрасывает пакеты DHCP от доверенных портов лишь в том случае, если скорость их поступления слишком высока. Не заслуживающие доверия порты подключаются к абонентам, и коммутатор отбрасывает пакеты DHCP от не заслуживающих доверия портов в следующих случаях: • Пакет представляет собой пакет сервера DHCP (например, OFFER, ACK или NACK). • MAC-адрес источника и IP-адрес источника в пакете не соответствуют ни одной из существующих привязок. • Пакет представляет собой пакет типа RELEASE или DECLINE, и MAC-адрес источника и порт источника не соответствуют ни одной из существующих привязок. • Скорость поступления пакетов DHCP слишком высока.
Rate (pps)	Укажите максимальное число пакетов DHCP (1-2048), которое коммутатор может принимать через каждый из портов за секунду. Все пакеты DHCP сверх указанного лимита коммутатором отбрасываются. Значение 0 позволяет отключить данный лимит, что рекомендуется сделать для доверенных портов.
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.

24.5.2 Настройка VLAN отслеживания DHCP

На данном экране можно включить отслеживание DHCP в каждой из VLAN и указать, должен ли коммутатор добавлять информацию агента ретрансляции DHCP в поле option 82 (гл. 33 на стр. 291) к запросам DHCP, которые коммутатор ретранслирует к серверу DHCP для каждой из VLAN. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Рисунок 105 Экран DHCP Snooping VLAN Configure



Поля экрана описаны в следующей таблице.

Таблица 74 Экран DHCP Snooping VLAN Configure

ПОЛЕ	ОПИСАНИЕ
Show 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 отслеживание DHCP в данной сети VLAN. Также необходимо включить функцию отслеживания DHCP на коммутаторе и указать доверенные порты. Примечание: Если включить отслеживание DHCP и не определить ни одного доверенного порта, коммутатор будет отбрасывать все запросы DHCP.
Option82	Установите этот переключатель, чтобы коммутатор добавлял номер слота, номер порта и идентификатор VLAN ID к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN. Сеть VLAN DHCP указывается на экране **DHCP Snooping Configure**.См. разд. 24.5 на стр. 232.
Information	Установите этот переключатель, чтобы коммутатор добавлял имя системы к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN. Имя системы указывается на экране **General Setup**.См. гл. 7 на стр. 79. Сеть VLAN DHCP указывается на экране **DHCP Snooping Configure**.См. разд. 24.5 на стр. 232.

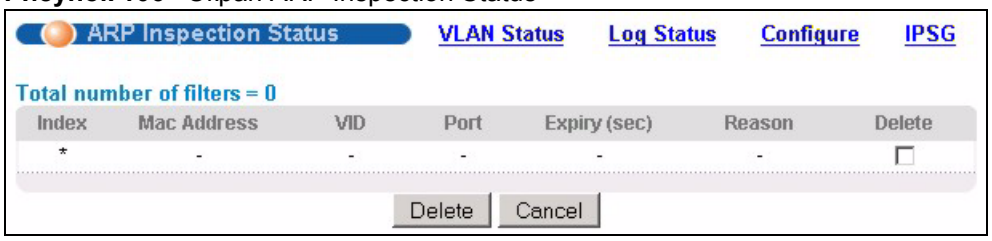
Таблица 74 Экран DHCP Snooping VLAN Configure (продолжение)

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	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

24.6 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 106 Экран ARP Inspection Status



Поля экрана описаны в следующей таблице.

Таблица 75 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**).

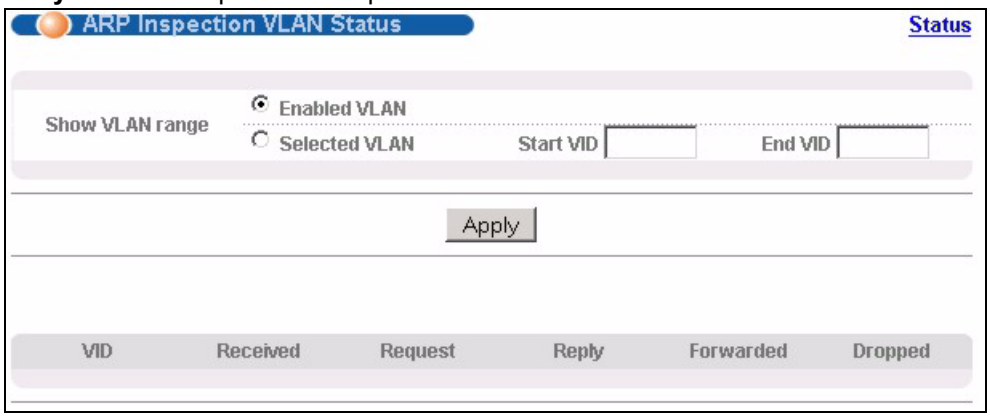
Таблица 75 Экран ARP Inspection Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
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**.

24.6.1 Состояние сети VLAN для инспекции ARP-пакетов

На данном экране можно просмотреть различные статистические данные по пакетам ARP в каждой из сетей VLAN. Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Рисунок 107 Экран ARP Inspection VLAN Status



Поля экрана описаны в следующей таблице.

Таблица 76 Экран ARP Inspection VLAN Status

ПОЛЕ	ОПИСАНИЕ
Show VLAN range	В данном разделе определяются виртуальные локальные сети VLAN, которые будут отображаться в разделе ниже.
Enabled VLAN	Выберите этот переключатель, чтобы отобразить в разделе ниже все виртуальные локальные сети VLAN, на которых включена инспекция ARP-пакетов.
Selected VLAN	Выберите данный переключатель, чтобы отобразить в разделе ниже все виртуальные локальные сети VLAN из указанного диапазона. После этого введите наименьший идентификатор VLAN ID (в поле **Start VID**) и наибольший идентификатор VLAN ID (в поле **End VID**) для требуемого диапазона.
Apply	Нажмите на данную кнопку, чтобы отобразить введенный диапазон сетей VLAN в разделе ниже.

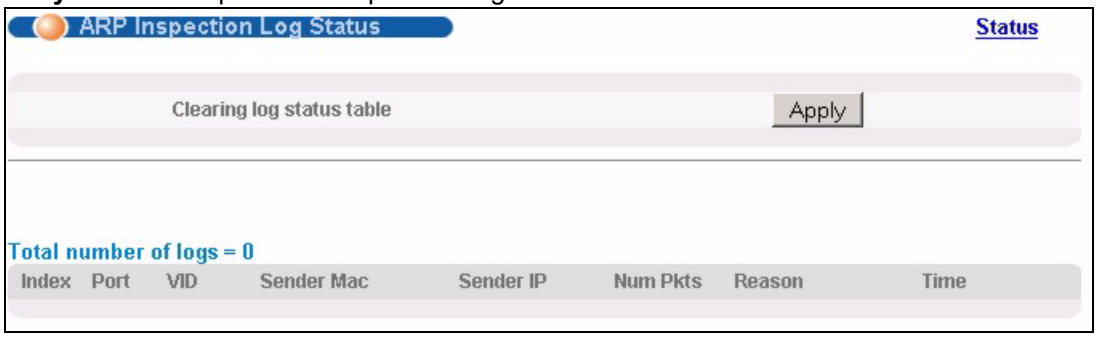
Таблица 76 Экран ARP Inspection VLAN Status

ПОЛЕ	ОПИСАНИЕ
VID	В данном поле отображаются идентификаторы VLAN ID каждой из сетей VLAN из выбранного выше диапазона.
Received	В этом поле отображается общее количество ARP-пакетов, полученных из данной VLAN с момента последнего перезапуска коммутатора.
Request	В этом поле отображается общее количество ARP-пакетов типа Request, полученных из данной VLAN с момента последнего перезапуска коммутатора.
Reply	В этом поле отображается общее количество ARP-пакетов типа Reply, полученных из данной VLAN с момента последнего перезапуска коммутатора.
Forwarded	В этом поле отображается общее количество ARP-пакетов, направленных коммутатором в данную VLAN с момента последнего перезапуска коммутатора.
Dropped	В этом поле отображается общее количество ARP-пакетов для данной VLAN, отброшенных коммутатором с момента последнего перезапуска коммутатора.

24.6.2 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 108 Экран ARP Inspection Log Status



Поля экрана описаны в следующей таблице.

Таблица 77 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.

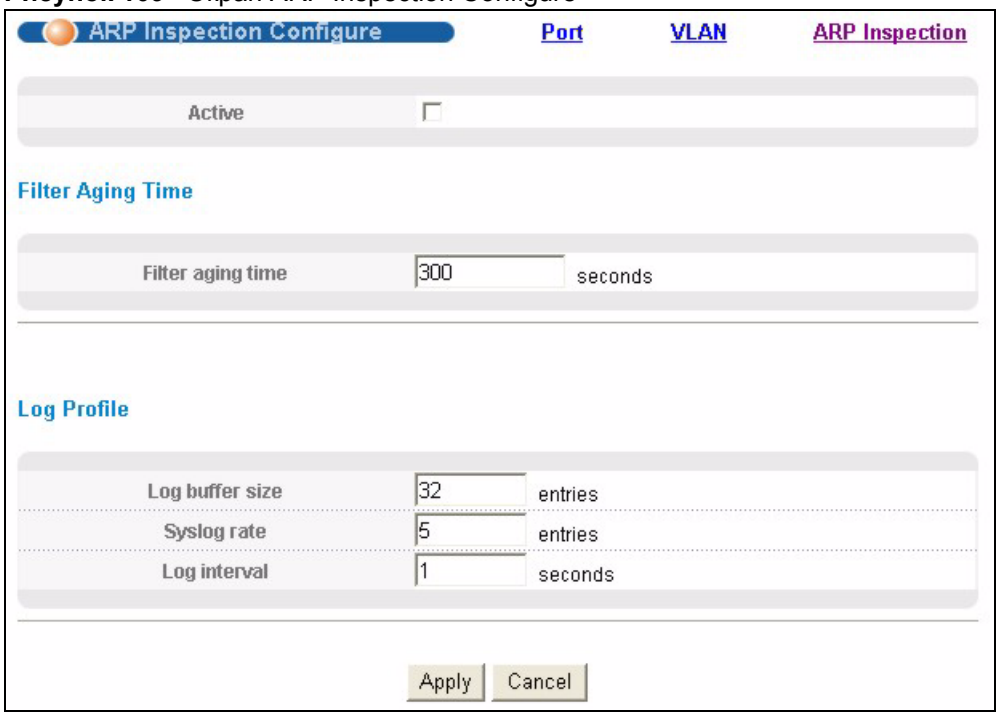
Таблица 77 Экран ARP Inspection Log Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
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. 24.7 на стр. 240.
Reason	В этом поле отображается причина, по которой было сгенерировано сообщение контрольного журнала. **dhcp deny**: ARP-пакет был отброшен из-за нарушения динамической привязки MAC-адреса и идентификатора VLAN ID. **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. **dhcp permit**: Коммутатор переслал ARP-пакет, так как была найдена динамическая привязка. **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. 24.7.2 на стр. 244.
Time	В этом поле отображается время, в которое было сгенерировано сообщение контрольного журнала.

24.7 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 109 Экран ARP Inspection Configure



Поля экрана описаны в следующей таблице.

Таблица 78 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. 24.6.2 на стр. 239.

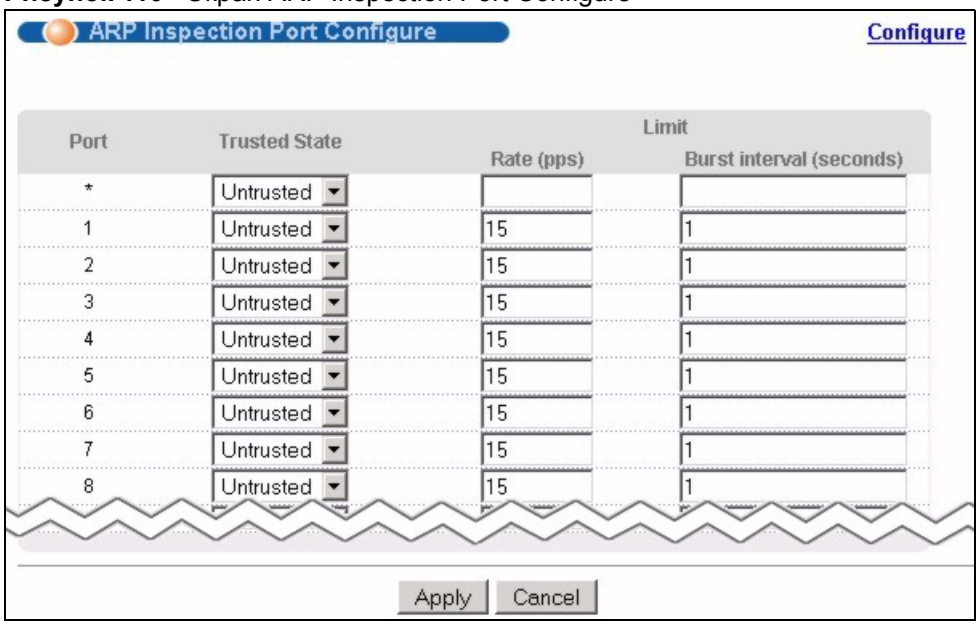
Таблица 78 Экран ARP Inspection Configure (продолжение)

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. 38 на стр. 343). 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.

24.7.1 Настройка портов для инспекции ARP-пакетов

На данном экране можно определить порты как доверенные и не заслуживающие доверия для функции инспекции ARP-пакетов. Дополнительно можно указать максимальную скорость, с которой коммутатор будет принимать ARP-пакеты через каждый из не заслуживающих доверия портов.Чтобы отобразить показанный ниже экран, выберите **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Рисунок 110 Экран ARP Inspection Port Configure



Поля экрана описаны в следующей таблице.

Таблица 79 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. От не заслуживающих доверия портов коммутатор отбрасывает ARP-пакеты в следующих случаях: • Информация об отправителе в ARP-пакете не совпадает с одной из существующих привязок. • Скорость поступления пакетов ARP слишком высока. Можно указать максимальную скорость, с которой будут приниматься ARP-пакеты через не заслуживающие доверия порты.
Limit	Для доверенных портов данные настройки безразличны
Rate (pps)	Укажите максимальную скорость (1-2048 пакетов в секунду), с которой коммутатор будет принимать ARP-пакеты через каждый из портов. Все пакеты ARP сверх указанного лимита коммутатором отбрасываются. Значение 0 позволяет отключить данный лимит.
Burst interval (seconds)	Под этим значением понимается период времени, в течение которого контролируется скорость поступления ARP-пакетов через каждый порт. Например, если скорость установлена равной 15 пакетам в секунду, а данный интервал – 1 секунде, то коммутатор принимает максимум 15 ARP-пакетов за каждый из интервалов продолжительностью в одну секунду. Если интервал установить равным 5 секундам, то коммутатор будет принимать максимум 75 ARP-пакетов в течение каждого пятисекундного интервала. Введите продолжительность интервала оценки (1-15 секунд).

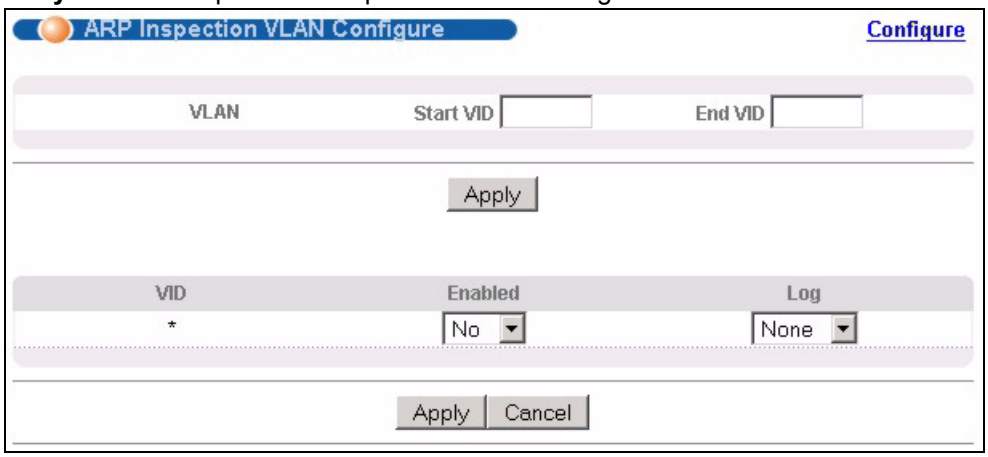
Таблица 79 Экран ARP Inspection Port Configure (продолжение)

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	Нажатие на данную кнопку сбрасывает параметры на данном экране к последним сохраненным значениям.

24.7.2 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 111 Экран ARP Inspection VLAN Configure



Поля экрана описаны в следующей таблице.

Таблица 80 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.

Таблица 80 Экран ARP Inspection VLAN Configure (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.

25

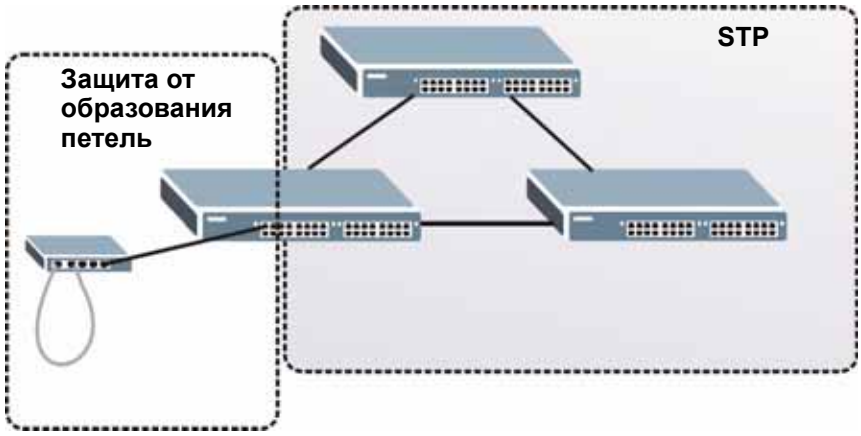
Защита от образования петель

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

25.1 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 112 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.

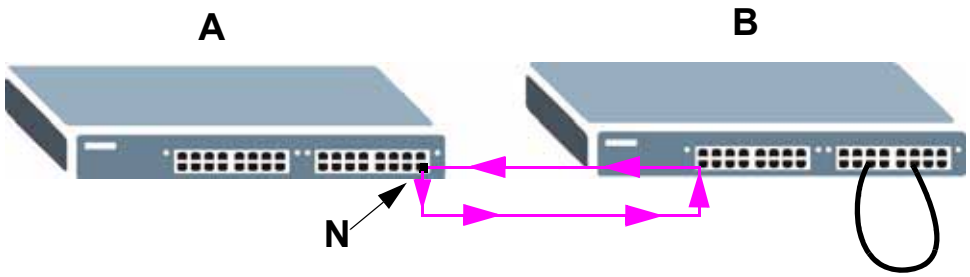
При подключении коммутатора (без петли) к коммутатору с петлей проблемы последнего отражаются на первом следующим образом:

- 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.

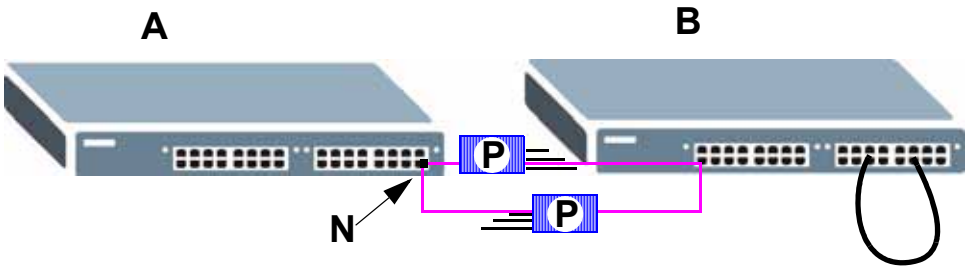
Рисунок 113 Коммутатор с петлей



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.

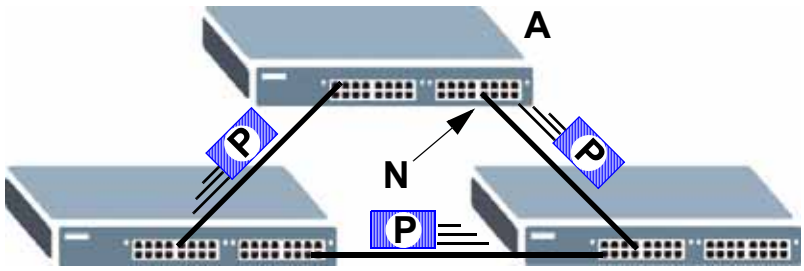
На приведенном ниже рисунке показан коммутатор **A** с активированной на порту **N** функцией защиты от образования петель, который отправляет пробный пакет **P** на коммутатор **B**. Так как на коммутаторе **B** имеется петля, пробный пакет **P** возвращается на порт **N** коммутатора **A**. Для защиты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

Рисунок 114 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 115 Защита от образования петель – петля в сети



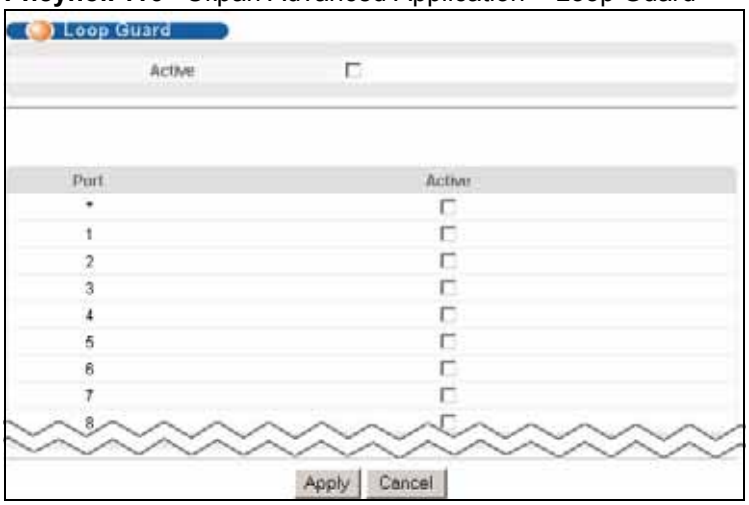
После устранения проблемы с петлей в сети отключенный порт можно снова активировать через Web-конфигуратор (см. разд. 7.7 на стр. 89) или интерфейс командной строки (см. разд. 45.12.4 на стр. 428).

25.2 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, MRSTP или MSTP).

Рисунок 116 Экран Advanced Application > Loop Guard



Поля экрана описаны в следующей таблице.

Таблица 81 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

26

Статические маршруты

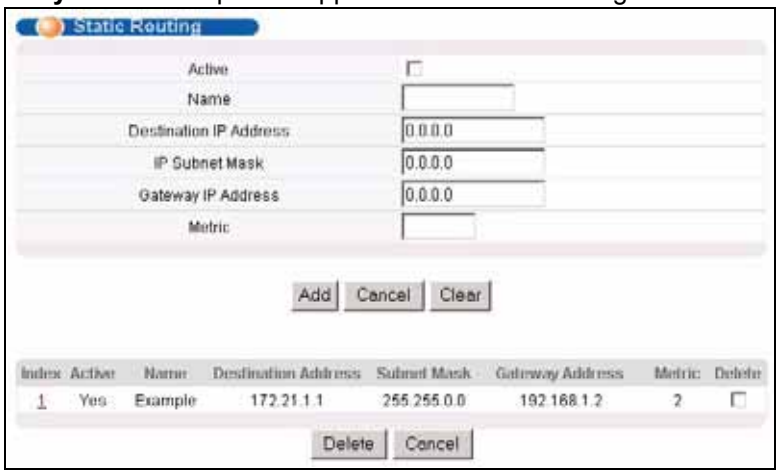
В данной главе описана настройка статических маршрутов.

26.1 Настройка статических маршрутов

Статические маршруты указывают коммутатору, куда следует направлять IP-трафик при ручной настройке параметров протокола TCP/IP.

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

Рисунок 117 Экран IP Application > Static Routing



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

Таблица 82 Экран IP Application > Static Routing

ПОЛЕ	ОПИСАНИЕ
Active	В этом поле можно активировать/деактивировать данный статический маршрут.
Name	Введите имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать эту запись.
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.

Таблица 82 Экран IP Application > Static Routing (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.
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**.

27

RIP

В данной главе описана настройка протокола маршрутной информации RIP (Routing Information Protocol).

27.1 Обзор протокола RIP

Протокол маршрутной информации RIP позволяет маршрутизирующим устройствам обмениваться информацией о маршрутах с другими маршрутизаторами. Отправка и получение пакетов RIP контролируется полем **Direction**. Когда это поле установлено равным:

- **Both** – коммутатор периодически осуществляет широковещательную рассылку своей таблицы маршрутизации и использует всю получаемую информацию RIP.
- **Incoming** – коммутатор не рассылает никаких пакетов RIP, однако принимает все поступающие пакеты RIP.
- **Outgoing** – коммутатор рассылает пакеты RIP, но не принимает никаких поступающих пакетов RIP.
- **None** – коммутатор не рассылает никаких пакетов RIP и игнорирует все поступающие пакеты RIP.

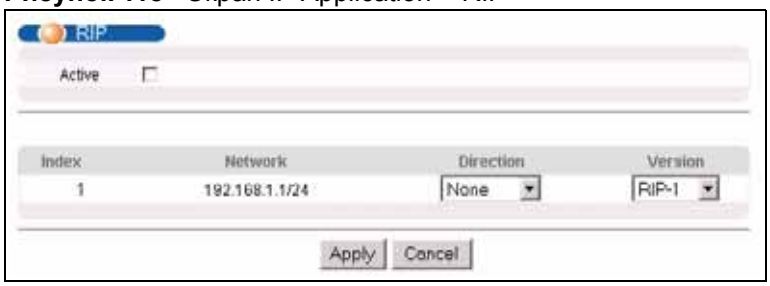
Формат и способ широковещательной рассылки пакетов RIP коммутатором (при приеме им распознаются оба формата) управляются полем **Version**. **RIP-1** представляет собой универсальный, повсеместно поддерживаемый формат; однако RIP-2 позволяет передавать больший объем информации. **RIP-1** скорее всего подойдет для большинства сетей, за исключением случаев нестандартной сетевой топологии.

Как в случае выбора **RIP-2B**, так и в случае выбора **RIP-2M** рассылка информации о маршрутах осуществляется в формате RIP-2; различие заключается в том, что при выборе **RIP-2B** используется широковещательная рассылка в подсети, тогда как при выборе **RIP-2M** используется мультивещание.

27.2 Настройка RIP

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application** > **RIP**. Настроить новую запись вручную невозможно. Каждая из записей в таблице создается автоматически при настройке нового IP-домена на экране **IP Setup** (см. разд. 7.6 на стр. 86).

Рисунок 118 Экран IP Application > RIP



Поля экрана описаны в следующей таблице.

Таблица 83 Экран IP Application > RIP

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить протокол RIP на коммутаторе.
Index	В этом поле отображается порядковый номер IP-интерфейса.
Network	В этом поле отображается IP-интерфейс, настроенный на коммутаторе. Дополнительную информацию о настройке IP-доменов можно найти в описании экрана IP Setup.
Direction	Выберите направления работы RIP из ниспадающего списка. Возможные значения: **Outgoing**, **Incoming**, **Both** и **None**.
Version	Выберите версию RIP из ниспадающего списка. Возможные значения: **RIP-1**, **RIP-2B** и **RIP-2M**.
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

OSPF

В данной главе описан протокол «предпочтения кратчайшего пути» OSPF (Open Shortest Path First) и описан порядок настройки OSPF.

28.1 Обзор протокола OSPF

Протокол «предпочтения кратчайшего пути» OSPF представляет собой протокол маршрутизации по состоянию канала, предназначенный для распространения информации о маршрутах в пределах автономной системы (AS). Под автономной системой понимается группа сетей, использующих общий протокол маршрутизации для обмена информацией о маршрутах.

OSPF обладает рядом преимуществ по сравнению с традиционными векторными протоколами (такими как RIP). Основные различия между протоколами OSPF и RIP показаны в следующей таблице.

Таблица 84 OSPF и RIP

	OSPF	**RIP**
Размер сети	Большие	Малые (до 15 маршрутизаторов)
Метрики	Пропускная способность, количество переходов, производительность, время передачи туда и обратно и надежность.	Количество переходов
Сходимость	Быстрая	Медленная

28.1.1 Автономные системы и области OSPF

Автономная система OSPF может быть разделена на логические области. Каждая область представляет группу смежных сетей. Все области подключаются к магистрали (также называемой областью 0). Магистраль представляет собой транзитную область для маршрутизации пакетов между двумя областями. Тупиковая область на границе автономной системы не является транзитной областью, так как к ней имеется только одно подключение.

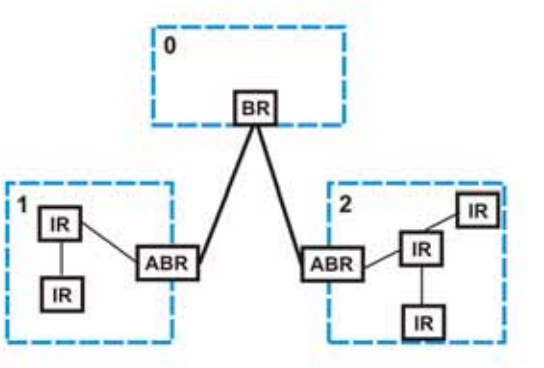
Четыре класса маршрутизаторов OSPF описаны в следующей таблице.

Таблица 85 OSPF: типы маршрутизаторов

ТИП	ОПИСАНИЕ
Внутренний маршрутизатор (IR)	Внутренним или внутриобластным маршрутизатором называется маршрутизатор в области.
Граничный маршрутизатор области (ABR)	Граничный маршрутизатор области подключается к двум или нескольким областям.
Магистральный маршрутизатор (BR)	Магистральный маршрутизатор имеет интерфейс к магистрали.
Граничный маршрутизатор автономной системы	Граничный маршрутизатор автономной системы обменивается информацией о маршрутах с другими автономными системами.

Пример сети OSPF показан на следующем рисунке. Магистраль находится в области 0 с магистральным маршрутизатором. Внутренние маршрутизаторы находятся в области 1 и области 2. Граничные маршрутизаторы области подключают области 1 и 2 к магистрали.

Рисунок 119 Пример сети OSPF



28.1.2 Как работает протокол OSPF

Устройства уровня 3 обмениваются информацией о маршрутах для построения синхронизированной базы данных состояний каналов в рамках одной автономной системы или одной области. Для этого они обмениваются сообщениями Hello, чтобы подтвердить наличие соседних устройств (уровня 3), а затем – описаниями базы данных (DD), позволяющими построить базу данных состояний каналов. База данных состояний каналов непрерывно обновляется посредством объявлений о состоянии канала LSA (Link State Advertisement).

База данных состояний каналов содержит записи, которые включают в себя идентификаторы маршрутизаторов, связанные с ним каналы и стоимости путей. Каждое из устройств может использовать базу данных состояний каналов и алгоритм Дейкстра для вычисления путей к пунктам назначения в сети с наименьшей стоимостью.

28.1.3 Интерфейсы и виртуальные каналы

Под интерфейсом в OSPF понимается канал между устройством уровня 3 и сетью OSPF. С интерфейсом связывается информация о состоянии, IP-адрес и маска подсети. При настройке интерфейса OSPF прежде всего для интерфейса включается передача трафика OSPF, а затем интерфейс добавляется к области.

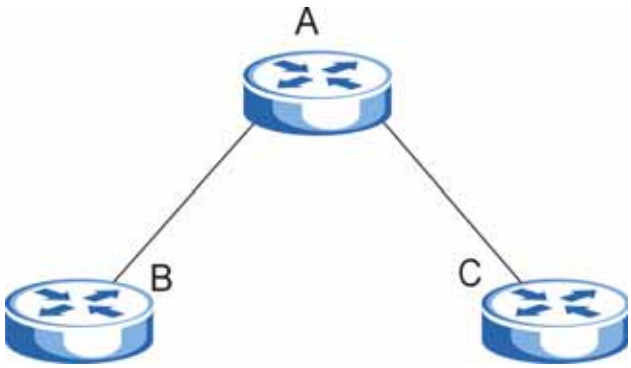
Чтобы определить/поддерживать связность между немагистральной областью и магистралью, можно настроить виртуальный канал. Виртуальный канал должен быть настроен на обоих устройствах уровня 3, в немагистральной области и в магистрали.

28.1.4 OSPF и выборы маршрутизатора

Протокол OSPF предусматривает механизм автоматического выбора назначенного маршрутизатора (Designated Router, DR) и резервного назначенного маршрутизатора (Backup Designated Router, BDR) для сегментов сети. Маршрутизаторы DR и BDR следят за обновлениями состояний каналов в своей области и обеспечивают рассылку объявлений LSA в оставшуюся часть сети.

В большинстве случаев выбранные по умолчанию маршрутизаторы DR/BDR вполне подходят, однако в некоторых случаях данным процессом необходимо управлять. В примере на показанном ниже рисунке только маршрутизатор **A** имеет прямое подключение ко всем другим маршрутизаторам в сегменте сети. Маршрутизаторы **B** и **C** не имеют прямого подключения друг к другу. Поэтому недопустимо, чтобы они были выбраны в качестве маршрутизаторов DR или BDR. Только маршрутизатор A должен стать назначенным маршрутизатором DR.

Рисунок 120 Пример выборов маршрутизатора в OSPF



Управлять выборами маршрутизатора в качестве DR или BDR можно, назначая приоритеты интерфейсам. Назначенным маршрутизатором DR становится маршрутизатор с наивысшим приоритетом, тогда как маршрутизатор с приоритетом 0 вообще не участвует в выборах маршрутизатора. В примере на рис. 120 на стр. 259 можно назначить приоритет 0 маршрутизаторам **B** и **C**, запретив им таким образом становится маршрутизаторами DR или BDR, и назначить приоритет 1 маршрутизатору **A**, что гарантирует его выборы в качестве DR.

28.1.5 Настройка OSPF

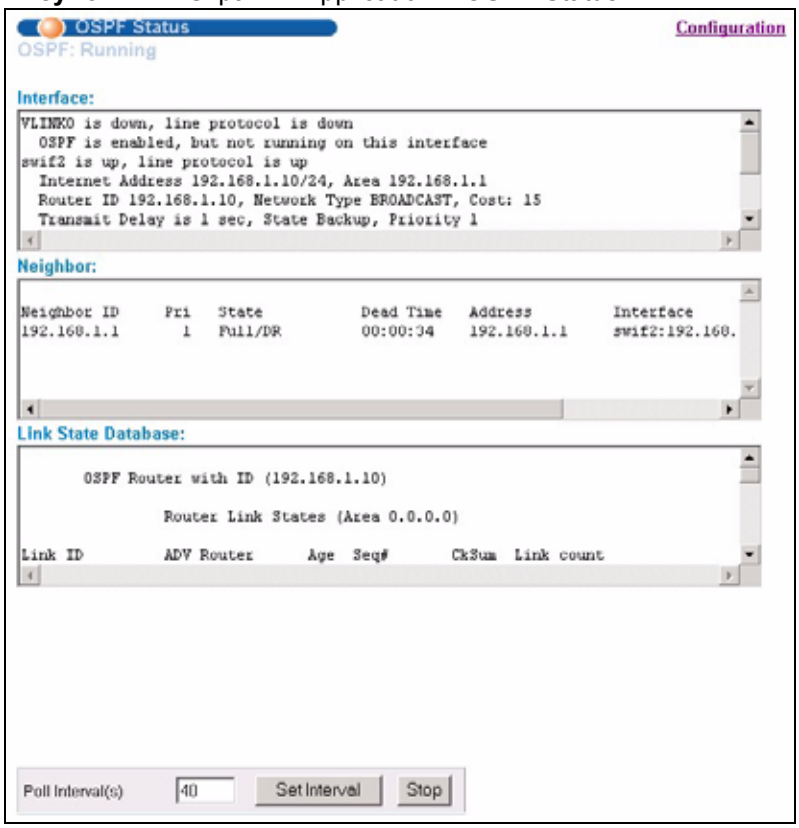
Чтобы настроить на коммутаторе протокол OSPF, необходимо выполнить следующие задачи:

1. Включить протокол OSPF
2. Создать области OSPF
3. Создать и связать интерфейсы с областью
4. Создать виртуальные каналы для поддержания связности с магистралью.

28.2 Состояние OSPF

На данном экране можно просмотреть текущее состояние OSPF. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application** > **OSPF**. Более подробную информацию об OSPF можно найти в разд. 28.1 на стр. 257.

Рисунок 121 Экран IP Application > OSPF Status



Поля экрана описаны в следующей таблице.

Таблица 86 Экран IP Application > OSPF Status

ПОЛЕ	ОПИСАНИЕ
OSPF	В данном поле отображается, включен протокол OSPF (**Running**) или нет (**Down**).
Interface	Текстовое поле, описывающее состояние OSPF по интерфейсам коммутатора.

Таблица 86 Экран IP Application > OSPF Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
Neighbor	Текстовое поле, описывающее состояние соседнего маршрутизатора, участвующего в сети OSPF.
Link State Database	Текстовое поле, отображающее информацию о базе данных состояний каналов, в которую попадает информация из LSA.
Poll Interval(s)	В этом поле отображается, как часто (в секундах) происходит обновление данного экрана. Чтобы изменить интервал обновления, можно ввести новое число в это текстовое поле и нажать на кнопку **Set Interval**.
Stop	Нажатие на **Stop** останавливает опрос состояния OSPF.

Некоторые из наиболее часто отображаемых полей описаны в следующей таблице.

Таблица 87 Экран OSPF Status: наиболее часто отображаемые поля

ПОЛЕ	ОПИСАНИЕ
Interface	
Internet Address	В этом поле отображается IP-адрес и количество единичных битов в маске подсети для домена IP-маршрутизации.
Area	В этом поле отображается идентификатор области.
Router ID	В этом поле отображается уникальный идентификатор коммутатора.
Transmit Delay	В этом поле отображается задержка передачи в секундах.
State	В данном поле отображается статус коммутатора (**backup** – резервный выделенный маршрутизатор, или **DR** – выделенный маршрутизатор).
Priority	В этом поле отображается приоритет коммутатора. Данное значение используется при выборах назначенного маршрутизатора.
Designated Router	В этом поле отображается идентификатор назначенного маршрутизатора.
Backup Designated Router	В этом поле отображается идентификатор резервного назначенного маршрутизатора.
Time Intervals Configured	В этом поле отображаются настроенные интервалы времени (в секундах).
Neighbor Count	В этом поле отображается количество соседних маршрутизаторов.
Adjacent Neighbor Count	В этом поле отображается количество соседних маршрутизаторов, которые являются смежными по отношению к коммутатору.
Neighbor	
Neighbor ID	В этом поле отображается идентификатор соседнего маршрутизатора.
Pri	В этом поле отображается приоритет соседнего маршрутизатора. Данное значение используется при выборах назначенного маршрутизатора.
State	В данном поле отображается статус соседнего маршрутизатора (**backup** – резервный выделенный маршрутизатор, или **DR** – выделенный маршрутизатор).
Dead Time	В этом поле отображается время нечувствительности в секундах.
Address	В этом поле отображается IP-адрес соседнего маршрутизатора.
Interface	В этом поле отображается MAC-адрес устройства.
Link State Database	
Link ID	В этом поле отображается идентификатор маршрутизатора или подсети.

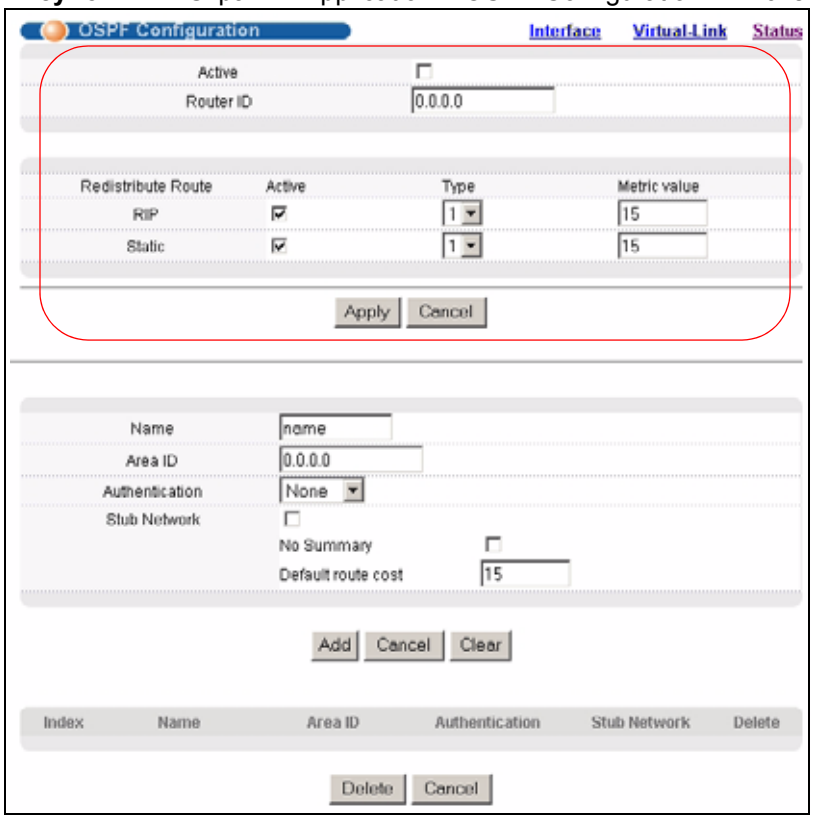
Таблица 87 Экран OSPF Status: наиболее часто отображаемые поля (продолжение)

ПОЛЕ	ОПИСАНИЕ
ADV Router	В этом поле отображается IP-адрес устройства уровня 3, которое рассылает объявления LSA.
Age	В этом поле отображается время (в секундах) с момента последней отправки объявления LSA.
Seq #	В этом поле отображается порядковый номер канала в объявлении LSA.
Checksum	В этом поле отображается значение контрольной суммы объявления LSA.
Link Count	В этом поле отображается количество каналов в объявлении LSA.

28.3 Настройка OSPF

На этом экране можно активировать OSPF и ввести общие настройки. Чтобы отобразить показанный ниже экран **OSPF Configuration**, выберите **IP Application** > **OSPF** и нажмите на ссылку **Configuration**. Более подробную информацию об OSPF можно найти в разд. 28.1 на стр. 257.

Рисунок 122 Экран IP Application > OSPF Configuration: включение и общие настройки



Поля экрана описаны в следующей таблице.

Таблица 88 Экран IP Application > OSPF Configuration: включение и общие настройки

ПОЛЕ	ОПИСАНИЕ
Active	По умолчанию протокол OSPF отключен. Чтобы включить его, установите данный переключатель.
Router ID	Router ID представляет собой уникальный идентификатор коммутатора для протокола OSPF. Введите уникальный идентификатор (для которого используется формат IP-адреса в виде десятичных чисел, разделенных точками) коммутатора.
Redistribute Route	Механизм перераспределения маршрутов позволяет коммутатору импортировать и прозрачным образом транслировать в сеть OSPF маршруты, полученные с использованием других протоколов маршрутизации (**RIP** и **статических маршрутов**).
Active	Установите данный переключатель, чтобы включить механизм перераспределения маршрутов для маршрутов, полученных с использованием указанного протокола.
Type	Выберите **1** для протоколов маршрутизации (таких как RIP), у которых внешние метрики напрямую сопоставимы с внутренней стоимостью OSPF. При выборе пути внутренняя стоимость OSPF добавляется граничным маршрутизатором AB к внешним метрикам. Выберите **2** для протоколов маршрутизации, у которых внешние метрики несопоставимы со стоимостью OSPF. В этом случае при выборе пути к пункту назначения граничным маршрутизатором AB учитывается внешняя стоимость.
Metric Value	Введите стоимость маршрута (в диапазоне от 0 до 16777214). По умолчанию для метрики установлено значение 15.
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.

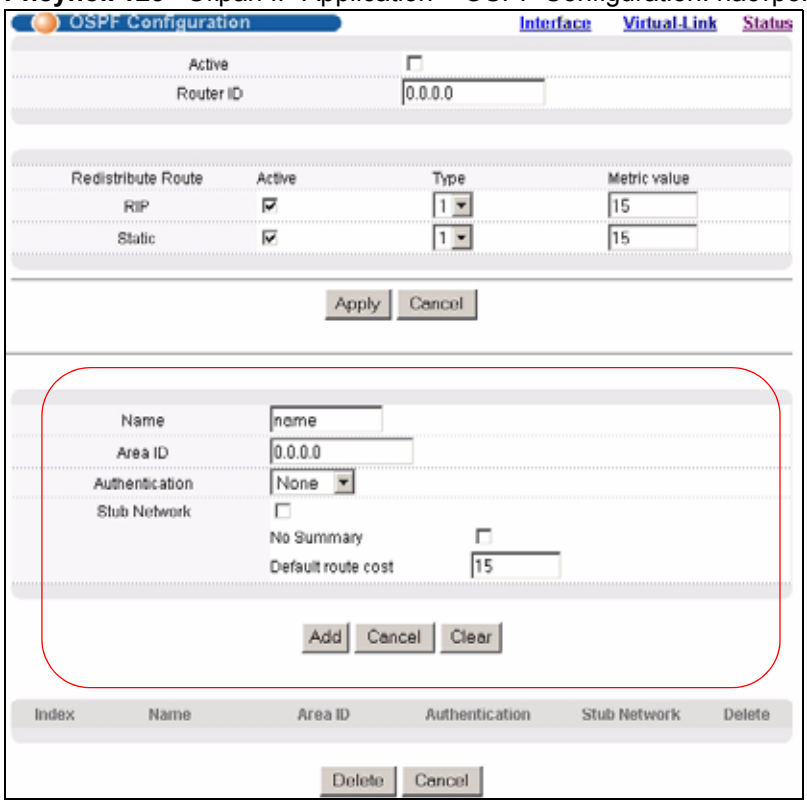
28.4 Настройка областей OSPF

Чтобы коммутатор принимал информацию о маршрутах только от доверенных устройств уровня 3, на нем необходимо включить аутентификацию. OSPF поддерживает три режима аутентификации:

- None – аутентификация не используется.
- Simple – аутентификация объявлений о состоянии канала с использованием пароля из 8 ASCII- символов.
- MD5 – аутентификация объявлений о состоянии канала с использованием пароля из 16 ASCII-символов.

Чтобы настроить область, необходимо заполнить соответствующие поля на экране **OSPF Configuration**.

Рисунок 123 Экран IP Application > OSPF Configuration: настройка области



Поля экрана описаны в следующей таблице.

Таблица 89 Экран IP Application > OSPF Configuration: настройка области

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать эту запись.
Area ID	Введите 32-разрядный идентификатор (для которого используется формат IP-адреса в виде десятичных чисел, разделенных точками), уникальным образом идентифицирующий область. Значение **0.0.0.0** указывает, что данная область является магистралью (областью 0). На коммутаторе можно настроить только одну магистраль.
Authentication	Выберите режим аутентификации (**Simple** или **MD5**), чтобы включить аутентификацию. Установленное по умолчанию значение **None** соответствует отключенной аутентификации. Как правило, для интерфейсов и виртуальных интерфейсов должен использоваться тот же режим аутентификации, что и у соответствующей области. В случае, если у интерфейсов и виртуальных интерфейсов используется отличный от соответствующей области режим аутентификации, применяются режимы аутентификации, настроенные для интерфейсов и виртуальных интерфейсов.
Stub Network	Установите этот переключатель, если данная область является тупиковой. Если в поле **Area ID** выбрано значение **0.0.0.0**, значения полей **Stub Area** игнорируются.
No Summary	Установите этот переключатель, если коммутатор не должен отправлять/принимать объявления LSA.

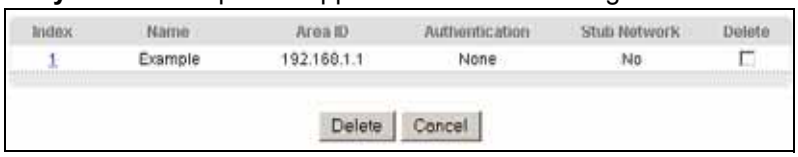
Таблица 89 Экран IP Application > OSPF Configuration: настройка области

ПОЛЕ	ОПИСАНИЕ
Default Route Cost	Укажите стоимость (в диапазоне от 0 до 16777214), используемую для добавления маршрута по умолчанию в тупиковой области для маршрутизаторов, которые являются внешними по отношению к домену OSPF. Если не указывать стоимость маршрута, маршрут по умолчанию не добавляется.
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.

28.4.1 Просмотр таблицы с информацией об областях OSPF

Итоговая таблица со всеми настроенными областями OSPF отображается в нижней части экрана **OSPF Configuration**.

Рисунок 124 Экран IP Application > OSPF Configuration: итоговая таблица



Поля экрана описаны в следующей таблице.

Таблица 90 Экран IP Application > OSPF Configuration: итоговая таблица

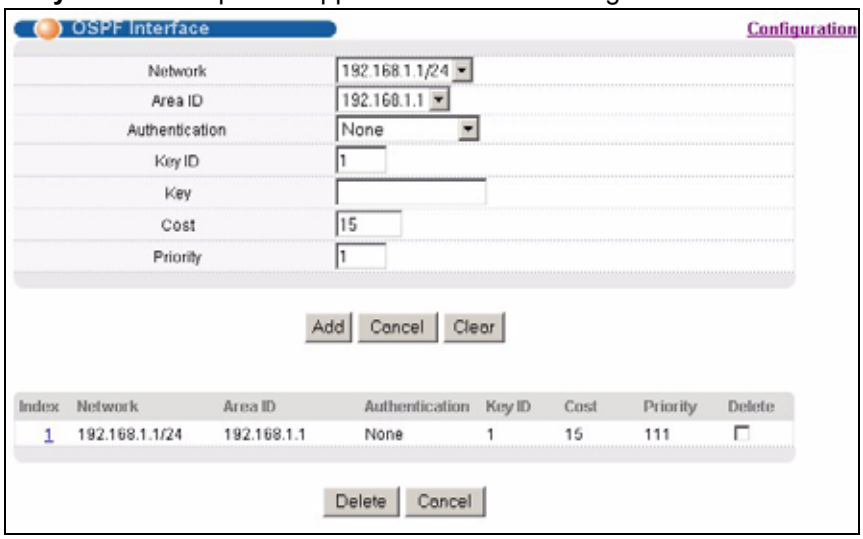
ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер области.
Name	В этом поле отображается имя-описание области.
Area ID	В этом поле отображается идентификатор области (для которого используется формат IP-адреса в виде десятичных чисел, разделенных точками), уникальным образом идентифицирующий область. Область с идентификатором **0.0.0.0** обозначает магистраль.
Authentication	В этом поле отображается используемый режим аутентификации (**None**, **Simple** или **MD5**).
Stub Network	В данном поле отображается информация о том, является ли данная область тупиковой (**Yes**) или нет (**No**).
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

28.5 Настройка интерфейсов OSPF

Чтобы настроить интерфейс OSPF, предварительно необходимо создать домен IP-маршрутизации на экране **IP Setup** (более подробную информацию можно найти в разд. 7.6 на стр. 86). Запись для интерфейса OSPF создается автоматически при создании домена IP-маршрутизации. Более подробную информацию об OSPF можно найти в разд. 28.1 на стр. 257.

Чтобы отобразить экран **OSPF Interface**, нажмите на экране **OSPF Configuration** ссылку **Interface**.

Рисунок 125 Экран IP Application > OSPF Configuration > OSPF Interface



Поля экрана описаны в следующей таблице.

Таблица 91 Экран IP Application > OSPF Configuration > OSPF Interface

ПОЛЕ	ОПИСАНИЕ
Network	Выберите IP-интерфейс.
Area ID	Выберите идентификатор области (для которого используется формат IP-адреса в виде десятичных чисел, разделенных точками), которую необходимо связать с данным интерфейсом.
Authentication	Примечание: Для всех интерфейсов OSPF в одной области необходимо использовать одинаковый режим аутентификации. Выберите режим аутентификации. Возможные варианты: **Same-as-Area** (тот же, что и в области), **None** (по умолчанию), **Simple** и **MD5**. Для участия в сети OSPF необходимо настроить одинаковый с соответствующей областью режим аутентификации и/или пароль. Выберите **Same-as-Area**, чтобы использовать тот же режим аутентификации, что и в области, и введите значения нужных полей. Выберите **None**, чтобы отключить аутентификацию. Это значение выбрано по умолчанию. Выберите **Simple** и введите значение в поле **Key**, чтобы использовать для аутентификации пакетов OSPF, передаваемых через данный интерфейс, аутентификацию по простому паролю. Выберите **MD5** и введите значения в поля **Key ID** и **Key**, чтобы использовать для аутентификации пакетов OSPF, передаваемых через данный интерфейс, аутентификацию по алгоритму MD5.
Key ID	В случае выбора **MD5** в поле **Authentication** следует указать в данном поле идентификационный номер для аутентификации, который необходимо использовать.

Таблица 91 Экран IP Application > OSPF Configuration > OSPF Interface (продолжение)

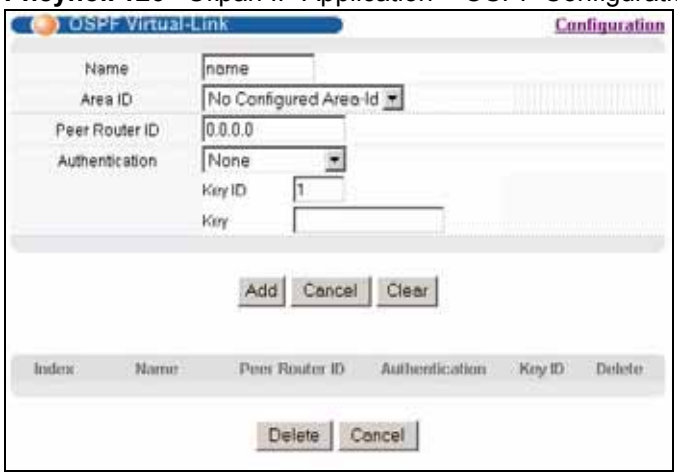
ПОЛЕ	ОПИСАНИЕ
Key	В случае выбора **Simple** в поле **Authentication** введите в данное поле пароль длиной восемь символов. Все введенные символы после восьмого будут проигнорированы. В случае выбора **MD5** в поле **Authentication** введите в данное поле пароль длиной 16 символов.
Cost	Стоимость интерфейса, используемая для вычисления таблицы маршрутизации. Введите значение в диапазоне от 0 до 65535. По умолчанию стоимость интерфейса устанавливается равной 15.
Priority	Приоритет, назначенный интерфейсу, используется при выборах маршрутизатора, который станет назначенным маршрутизатором (DR) или резервным назначенным маршрутизатором (BDR). Можно ввести значение в диапазоне от 0 до 255. Значение приоритета, равное 0, исключает маршрутизатор из участия в выборах маршрутизатора.
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 интерфейса.
Network	В этом поле отображается информация IP-интерфейса.
Area ID	В этом поле отображается идентификатор области (для которого используется формат IP-адреса в виде десятичных чисел, разделенных точками), связанной с данным интерфейсом.
Authentication	В этом поле отображается используемый режим аутентификации (**Same-as-Area**, **None**, **Simple** или **MD5**).
Key ID	Если в поле **Authentication** указано значение **MD5**, в данном поле отображается идентификационный номер используемого ключа.
Cost	В данном поле отображается стоимость интерфейса, используемая для вычисления таблицы маршрутизации.
Priority	В этом поле отображается приоритет данного интерфейса OSPF.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

28.6 Виртуальные каналы OSPF

На данном экране можно просмотреть и настроить параметры виртуальных каналов. Более подробную информацию об OSPF можно найти в разд. 28.1 на стр. 257.

Чтобы отобразить показанный ниже экран, нажмите на экране **OSPF Configuration** на ссылку **Virtual-Link**.

Рисунок 126 Экран IP Application > OSPF Configuration > OSPF Virtual Link



Поля экрана описаны в следующей таблице.

Таблица 92 Экран IP Application > OSPF Configuration > OSPF Virtual Link

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать эту запись.
Area ID	Выберите идентификатор области (для которого используется формат IP-адреса в виде десятичных чисел, разделенных точками), которую необходимо связать с данным интерфейсом.
Peer Router ID	Введите идентификатор граничного маршрутизатора-партнера.
Authentication	Примечание: Для всех виртуальных интерфейсов в одной области необходимо использовать одинаковый режим аутентификации. Выберите режим аутентификации. Возможные варианты: **Same-as-Area** (тот же, что и в области), **None** (по умолчанию), **Simple** и **MD5**. Чтобы обмениваться пакетами OSPF с граничным маршрутизатором-партнером, необходимо настроить одинаковый с соответствующим граничным маршрутизатором-партнером режим аутентификации и/или пароль. Выберите **Same-as-Area**, чтобы использовать тот же режим аутентификации, что и в области, и введите значения нужных полей. Выберите **None**, чтобы отключить аутентификацию. Это значение выбрано по умолчанию. Выберите **Simple**, чтобы использовать для аутентификации пакетов OSPF, передаваемых через данный интерфейс, аутентификацию по простому паролю. Выберите **MD5**, чтобы использовать для аутентификации пакетов OSPF, передаваемых через данный интерфейс, аутентификацию по алгоритму MD5.
Key ID	В случае выбора **MD5** в поле **Authentication** следует указать в данном поле идентификационный номер для аутентификации, который необходимо использовать.
Key	В случае выбора **Simple** в поле **Authentication** введите в данное поле пароль длиной восемь символов. В случае выбора **MD5** в поле **Authentication** введите в данное поле пароль длиной 16 символов.

Таблица 92 Экран IP Application > OSPF Configuration > OSPF Virtual Link

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 записи.
Name	В этом поле отображается имя-описание виртуального канала.
Peer Router ID	В этом поле отображается идентификатор граничного маршрутизатора-партнера (для которого используется формат IP-адреса в виде десятичных чисел, разделенных точками).
Authentication	В этом поле отображается используемый режим аутентификации (**Same-as-Area**, **None**, **Simple** или **MD5**).
Key ID	Если в поле **Authentication** указано значение **MD5**, в данном поле отображается идентификационный номер используемого ключа.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

29

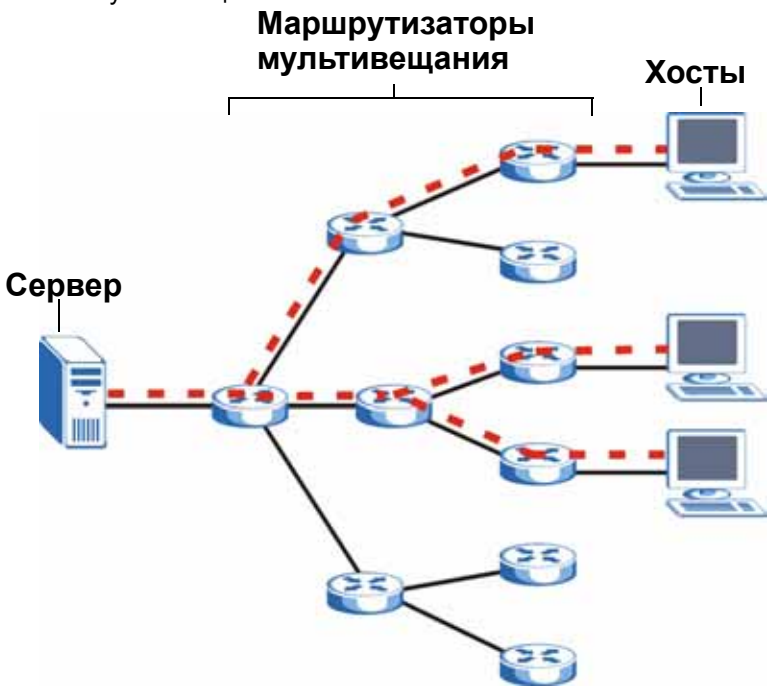
IGMP

В данной главе описана настройка коммутатора в качестве маршрутизатора мультивещания. Дополнительную информацию об отслеживании многоадресного трафика IGMP можно найти также в разд. 22.4 на стр. 195.

29.1 Обзор протокола IGMP

IP-мультивещание представляет собой стандарт IETF, описывающий рассылку данных нескольким получателям. Сессия мультивещания и взаимосвязи между сервером мультивещания, маршрутизаторами мультивещания и хостами мультивещания показаны на следующем рисунке. Сервер мультивещания осуществляет передачу мультивещательных пакетов, которые передаются маршрутизаторами мультивещания хостам мультивещания.

Рисунок 127 IP-мультивещание



Хост может принять решение о присоединении или выходе из группы мультивещания в любой момент. Кроме того, хост может быть членом нескольких групп мультивещания. Группы мультивещания идентифицируются по IP-адресам из диапазона класса D (от 224.0.0.0 до 239.255.255.255). Сервер мультивещания отправляет пакеты, адресуемые конкретной группе мультивещания (на IP-адрес мультивещания).

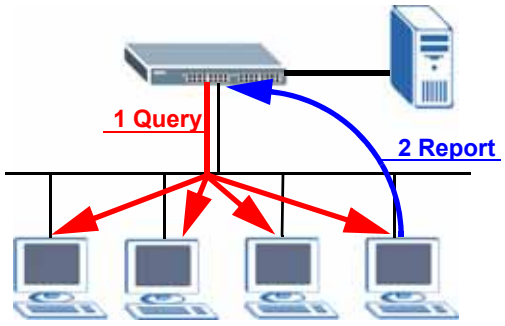
Хосты мультивещания информируют маршрутизаторы мультивещания о своем участии в группах мультивещания с использованием межсетевого протокола управления группами (Internet Group Management Protocol, IGMP). Маршрутизаторы мультивещания могут использовать IGMP для периодического опроса хостов мультивещания о желании получать передачи от сервера мультивещания. Другими словами, маршрутизаторы мультивещания проверяют, являются ли какие-либо из хостов в их сети членами определенной группы мультивещания.

Данный коммутатор поддерживает протоколы IGMP версии 1 (**IGMP-v1**), версии 2 (**IGMP-v2**) и версии 3 (**IGMP-v3**). Информацию о протоколе IGMP версий 1, 2 и 3 можно найти соответственно в стандартах RFC 1112, RFC 2236 и RFC 3376. При запуске коммутатор опрашивает все непосредственно подключенные к нему сети для сбора информации об участии в группах мультивещания. После этого коммутатор периодически обновляет эту информацию.

29.1.1 Как работает протокол IGMP

В данном разделе описывается работа протокола IGMP и изменения, которые были внесены в него с версии 1 по версию 3. IGMP версии 1 определяет порядок проверки маршрутизатором мультивещания факта участия каких-либо хостов мультивещания в определенной группе мультивещания. Для проверки участия в группе маршрутизатором рассылаются пакеты IGMP типа Query. Хосты, которые являются членами группы мультивещания, отвечают пакетами IGMP типа Report. Они также называются запросами на присоединение к группе. После этого маршрутизатор сохраняет список всех сетей, в которых имеются члены данной группы мультивещания, и направляет мультивещательный трафик в эти сети.

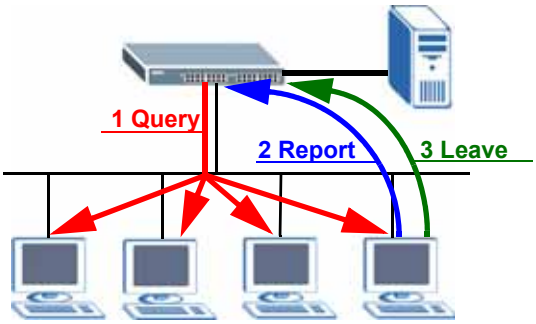
Рисунок 128 Пример работы IGMP версии 1



Основное отличие протокола IGMP версии 2 – наличие в нем механизма, с помощью которого член группы мультивещания может уведомить маршрутизатор мультивещания о своем выходе из группы мультивещания (пакет типа Leave). После этого маршрутизатор мультивещания направляет запрос IGMP типа Query для соответствующей группы, чтобы проверить, остались ли в ней еще какие-либо участники. Если маршрутизатор мультивещания не получает от каких-либо членов

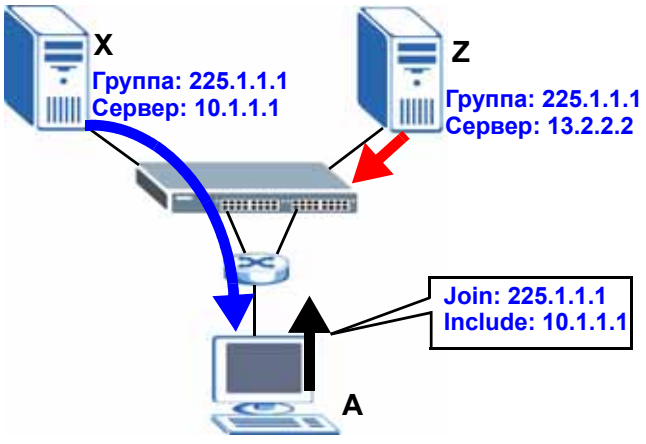
ответа IGMP типа Report, то пересылка мультивещательного трафика для данной группы им прекращается. Это сокращает период сходимости после покидания группы, то есть период времени, в течение которого маршрутизатор мультивещания полагает, что в конкретной сети еще остаются члены данной группы. Это, в свою очередь, уменьшает объемы мультивещательного трафика, проходящего через маршрутизатор мультивещания.

Рисунок 129 Пример работы IGMP версии 2



IGMP версии 3 позволяет хосту мультивещания присоединяться к группе мультивещания и указывать, от какого источника (сервера мультивещания) он желает получать мультивещательные пакеты. Или напротив, хост мультивещания может указать, от каких серверов мультивещания он не желает получать мультивещательные пакеты На приведенном ниже рисунке сервер мультивещания **X** (IP-адрес **10.1.1.1**) и сервер мультивещания **Z** (IP-адрес **13.2.2.2**) оба передают трафик в одну и ту же группу мультивещания, идентификатором которой является IP-адрес мультивещания **225.1.1.1**. Использующий IGMP версии 3 хост мультивещания **A** может присоединиться к группе мультивещания **225.1.1.1** и указать, что он желает получать мультивещательные пакеты только от сервера **X**.

Рисунок 130 Пример работы IGMP версии 3



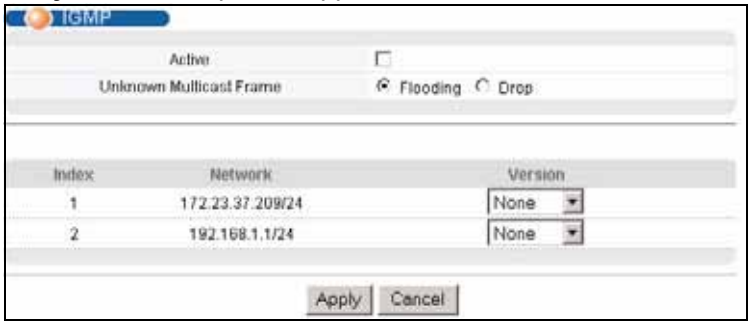
29.2 IGMP на основе портов

Данный коммутатор отправляет пакеты IGMP типа Query на все порты. После этого коммутатор ожидает получения пакетов IGMP типа Report, и записывает, через какие порты были получены эти сообщения. После этого широковещательный трафик направляется только на те порты, через которые были приняты запросы на присоединение к группе мультивещания.

29.3 Настройка IGMP

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application** > **IGMP**. Каждая из записей в таблице создается автоматически при настройке нового IP-домена на экране **IP Setup** (см. разд. 7.6 на стр. 86).

Рисунок 131 Экран IP Application > IGMP



Поля экрана описаны в следующей таблице.

Таблица 93 Экран IP Application > IGMP

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить протокол IGMP на коммутаторе. Примечание: Включить одновременно отслеживание многоадресного трафика IGMP и протокол IGMP невозможно. Более подробную информацию об отслеживании многоадресного трафика IGMP можно найти в разд. 22.4 на стр. 195.
Unknown Multicast Frame	Выберите действие, выполняемое коммутатором при получении неизвестного кадра мультивещания. Под неизвестными кадрами мультивещания понимаются адресованные в те группы мультивещания, для которых коммутатором не зарегистрировано ни одного участника. **Drop** – отбрасывание кадра. **Flooding** – пересылка кадра на все порты.
Index	В этом поле отображается порядковый номер записи.
Network	В этом поле отображается IP-домен, настроенный на коммутаторе. Более подробную информацию о настройке IP-доменов можно найти в разд. 7.6 на стр. 86.

Таблица 93 Экран IP Application > IGMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Version	Выберите версию IGMP из ниспадающего списка. Возможные значения: **IGMP-v1**, **IGMP-v2**, **IGMP-v3** и **None**. Как правило, при желании включить на коммутаторе протокол IGMP следует выбрать **IGMP-v3**, так как он совместим с более старыми версиями. Более ранние версии IGMP (**IGMP-v2** или **IGMP-v1**) необходимо выбирать лишь в тех случаях, когда хосты мультивещания в вашей сети не распознают сообщения типа Query версии 3 или версии 2 протокола IGMP.
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.

30

DVMRP

Данная глава знакомит с протоколом маршрутизации мультивещания «вектор-длина» и описывает порядок его настройки.

30.1 Обзор протокола DVMRP

Протокол маршрутизации мультивещания «вектор-длина» DVMRP (Distance Vector Multicast Routing Protocol) представляет собой протокол, используемый для маршрутизации данных мультивещания в пределах автономной системы (AS). Данная реализация DVMRP базируется на спецификации draft-ietf-idmr-dvmrp-v3-10. DVMRP обеспечивает поддержку передачи мультивещательного трафика на коммутаторах уровня 3, использующих протокол IPv4 (с поддержкой IP-мультивещания) и протокол IGMP. Метрикой DVMRP является количество переходов, равное 32.

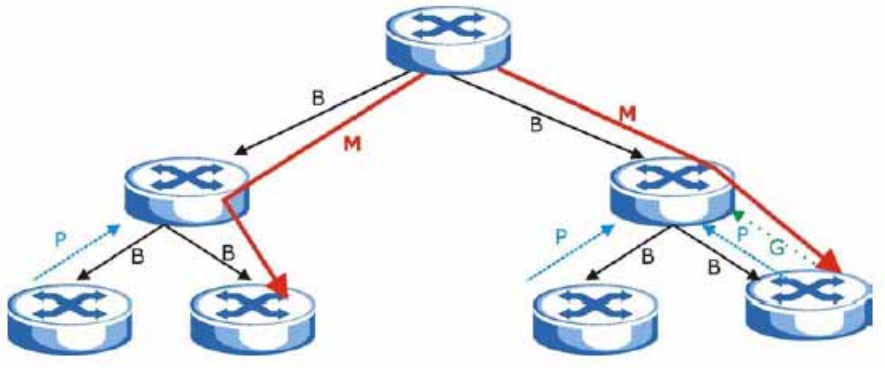
Для присоединения и выхода из групп мультивещания используется протокол IGMP. При включении DVMRP протокол IGMP должен быть включен; в противном случае будет выдано сообщение, показанное на рис. 134 на стр. 279.

30.2 Как работает протокол DVMRP

Для построения дерева доставки IP-мультивещания в протоколе DVMRP используется алгоритм мультивещания по обратному пути Reverse Path Multicasting (RPM). Пакеты мультивещания передаются по ветвям построенного дерева мультивещания. DVMRP динамически получает информацию об участии хостов в группах с использованием протокола IGMP. В зависимости от участия в отдельных группах построенные деревья динамически обновляются.

1. Изначально мультивещательный пакет-объявление передается в широковещательном (broadcast) режиме («B» на показанном ниже рисунке).
2. Устройства уровня 3 с поддержкой DVMRP, в сетях которых отсутствуют хосты, принадлежащие к данной группе мультивещания, передают обратно отсекающее (prune) сообщение («P»).
3. Если позднее к группе мультивещания присоединяется какой-либо хост, на родительский интерфейс передается присоединительное (graft) сообщение («G»), отменяющее отсекающее сообщение.
4. Окончательный поток мультивещания («M») после отсечения и присоединения показан на следующем рисунке.

Рисунок 132 Как работает протокол DVMRP



30.2.1 Терминология DVMRP

Для обнаружения соседних устройств DVMRP применяются пакеты DVMRP типа Probe.

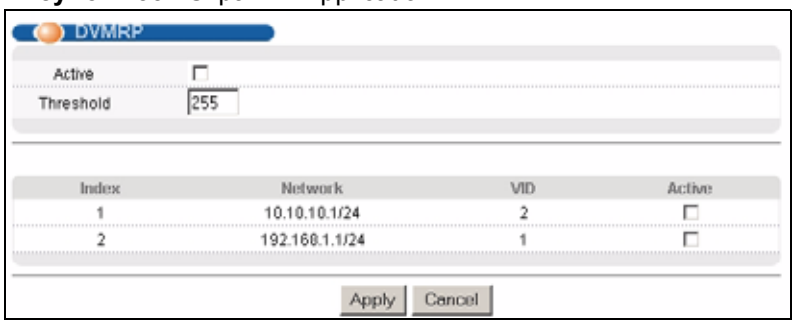
Для обмена информацией о маршрутах к источнику DVMRP используются пакеты DVMRP типа Report. С помощью данных пакетов строится таблица маршрутизации мультивещания DVMRP, на основе которой строятся деревья к источникам, а также выполняются проверки алгоритма мультивещания по обратному пути (RPF) для входящих мультивещательных пакетов. Проверки RPF предотвращают отфильтровывание дублирующихся пакетов при наличии петель в топологии сети.

Пакеты DVMRP типа Prune отсекают деревья доставки мультивещания. Пакеты DVMRP типа Graft позволяют вновь присоединить ветвь к дереву доставки мультивещания.

30.3 Настройка DVMRP

Протокол DVMRP необходимо настроить на коммутаторе, если он будет использоваться в качестве маршрутизатора мультивещания (так называемого «mrouter»). Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application > DVMRP**.

Рисунок 133 Экран IP Application > DVMRP



Поля экрана описаны в следующей таблице.

Таблица 94 Экран IP Application > DVMRP

ПОЛЕ	ОПИСАНИЕ
Active	Установите переключатель **Active**, чтобы включить DVMRP на коммутаторе. Это необходимо лишь в том случае, если коммутатор должен работать в качестве маршрутизатора мультивещания.
Threshold	Пороговое значение соответствует максимальному времени жизни пакета (TTL). С помощью TTL ограничиваются масштабы мультивещания. Чтобы не загружать веерной рассылкой мультивещательного трафика устройства уровня 3, отстоящие на много переходов от источника, данное значение следует уменьшить. Данное значение применяется лишь к мультивещательному трафику, который рассылается данным коммутатором.
Index	Порядковый номер конфигурации DVMRP для домена IP-маршрутизации, определенного в поле **Network**. Максимально возможное число конфигураций DVMRP соответствует максимальному числу доменов IP-маршрутизации, поддерживаемых коммутатором. Дополнительную информацию о доменах IP-маршрутизации можно найти в разд. 7.6 на стр. 86.
Network	IP-адрес и маска подсети домена IP-маршрутизации, настроенные на экране **IP Setup.**
VID	DVMRP невозможно включить для одной группы VLAN в различных доменах IP-маршрутизации, то есть использовать одинаковый VID для различных конфигураций DVMRP не допускается (см. рис. 136 на стр. 280).
Active	Установите переключатель **Active**, чтобы включить DVMRP в данном домене IP-маршрутизации.
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.

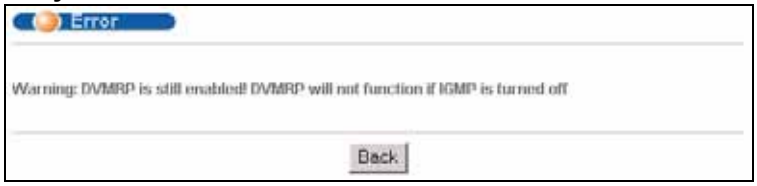
30.3.1 Сообщения об ошибках при настройке DVMRP

При включении DVMRP протокол IGMP/RIP должен быть включен; в противном случае будет выдано сообщение, показанное на следующем рисунке.

Рисунок 134 DVMRP: ошибка «IGMP/RIP не включен»

Если отключить IGMP, оставив активным DVMRP, будет выдано следующее предупреждение.

Рисунок 135 DVMRP: ошибка «невозможно отключить IGMP»



Конфигурация DVMRP для каждого из доменов IP-маршрутизации должна относиться к отдельной группе VLAN; в противном случае будет выдан следующий экран.

Рисунок 136 DVMRP: ошибка «дублирование VID»

30.4 Значения таймеров DVMRP по умолчанию

Используемые по умолчанию настройки таймеров DVMRP приводятся ниже.

Таблица 95 DVMRP: значения таймеров по умолчанию

ПОЛЕ DVMRP	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ
Интервал опроса (Probe)	10 с
Интервал ответа (Report)	35 с
Время жизни маршрута	140 с
Время жизни отсечения (Prune)	Переменное (менее двух часов)
Время повтора отсечения (Prune)	3 с с экспоненциальным уменьшением
Время повтора присоединения (Graft)	5 с с экспоненциальным уменьшением

31

IP-мультивещание

В данной главе описаны настройки на экране **IP Multicast**.

31.1 Обзор IP-мультивещания

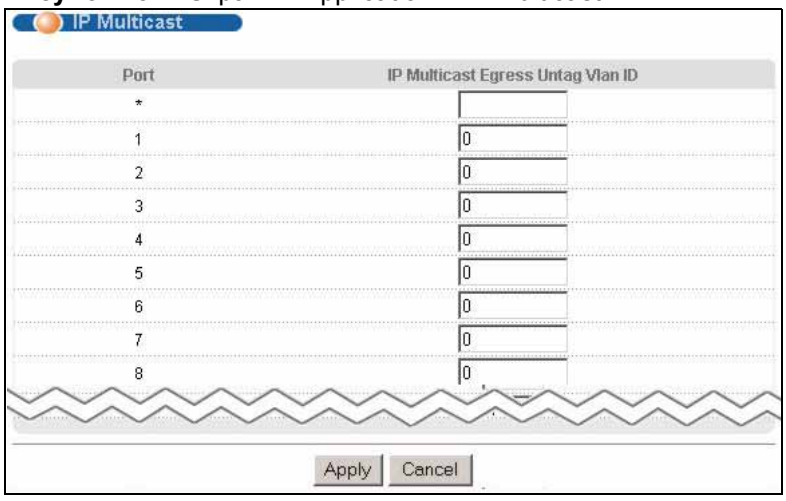
Обычно передача IP-пакетов происходит одним из двух способов: в режиме одноадресной передачи (от одного отправителя к одному получателю) или в режиме широковещания (от одного отправителя всем получателям в сети). IP-мультивещание (или групповая передача) представляет собой третий способ доставки IP-пакетов определенной группе хостов в сети – но не всем.

На коммутаторе можно настроить удаление тегов VLAN из пакетов IP-мультивещания, пересылаемых коммутатором. Благодаря этому коммутатор может пересылать пакеты Ethernet на устройства, не поддерживающие VLAN.

31.2 Настройка мультивещания

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

Рисунок 137 Экран IP Application > IP Multicast



Поля экрана описаны в следующей таблице.

Таблица 96 Экран IP Application > IP Multicast

ПОЛЕ	ОПИСАНИЕ
Port	В этом поле отображается номер порта (только для чтения).
*	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.
IP Multicast Egress Untag Vlan ID	Данный коммутатор удаляет теги VLAN из пакетов IP-мультивещания, принадлежащих указанной VLAN, до передачи через данный порт. Введите в это поле идентификатор группы VLAN. Чтобы коммутатор не удалял теги VLAN из пакетов, введите **0**.
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.

32

Дифференцированное обслуживание

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

32.1 Обзор механизма DiffServ

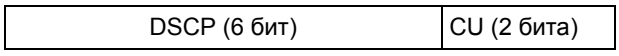
Механизмы управления качеством обслуживания (QoS) позволяют установить приоритеты для потоков трафика из источника в пункт назначения. Все пакеты в потоке получают одинаковый приоритет. Чтобы установить различные приоритеты для различных типов пакетов, можно использовать классы обслуживания (CoS).

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.

32.1.1 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 138 DiffServ: поле Differentiated Service



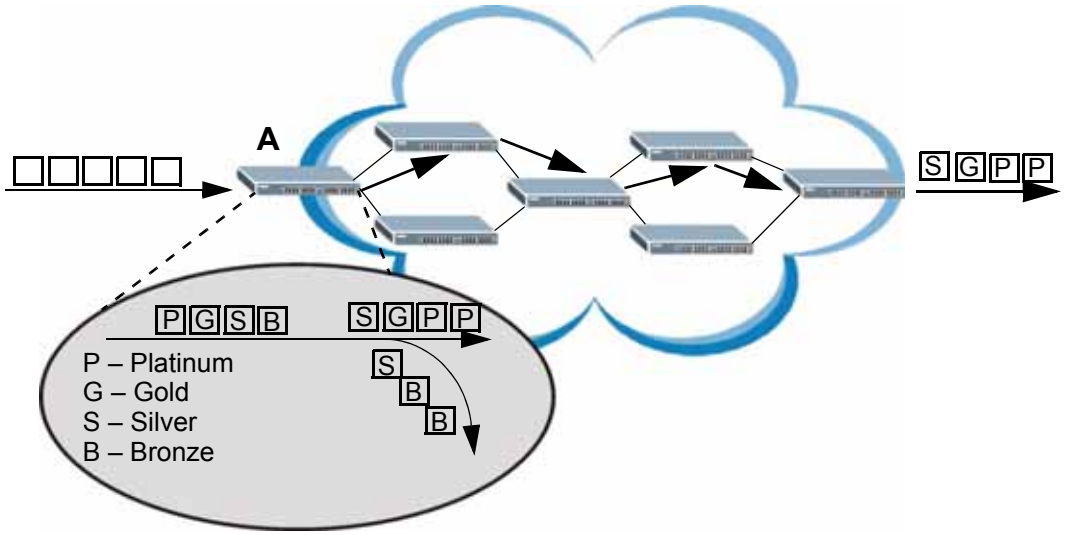
Маркер DSCP обратно совместим с тремя битами приоритета в октете ToS, благодаря чему сетевое устройство с поддержкой ToS, но без поддержки DiffServ не будет конфликтовать с отображением маркера DSCP.

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.

32.1.2 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. 139) 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 139 Сеть с поддержкой DiffServ



32.2 Ограничение трафика с использованием маркеров TRTCM

Функция ограничения трафика позволяет ограничить скорость входящего или исходящего трафика в зависимости от класса трафика с использованием определяемых пользователем критериев. Методы ограничения трафика оценивают потоки трафика на основе определяемых пользователем критериев и идентифицируют трафик как отвечающий критериям, превышающий критерии или нарушающий критерии.

Маркеры TRTCM (Two Rate Three Color Marker, определенные в RFC 2698) – один из типов ограничения трафика, в котором идентификация пакетов осуществляется на основании сравнения с двумя установленным пользователем скоростями: гарантированной скорости передачи информации (CIR) и пиковой скорости передачи информации (PIR). CIR определяет среднюю скорость, с которой пакеты допускаются в сеть. Значение PIR выбирается большим или равным CIR. Значения CIR и PIR базируются на гарантированной и максимальной пропускной способности, соответственно, согласованных между провайдером услуг и клиентом.

При использовании метода Two Rate Three Color (две скорости, три цвета) поступающие пакеты оцениваются и маркируются одним из трех цветов, определяющие приоритеты при отбрасывании пакетов. Высокий уровень приоритета при отбрасывании пакетов обозначается красным, средний уровень – желтым, а низкий – зеленым. После настройки TRTCM и включения DiffServ над пакетами с цветовой маркировкой выполняются следующие действия:

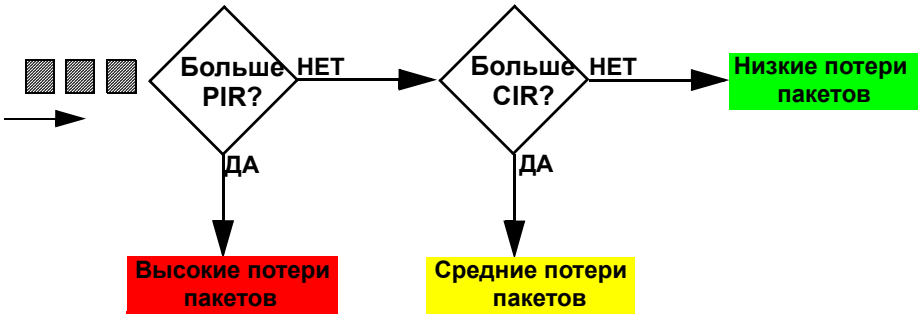
- Красные пакеты (с высоким приоритетом отбрасывания) отбрасываются.
- Желтые пакеты (со средним приоритетом отбрасывания) отбрасываются в случае перегрузки в сети.
- Зеленые пакеты (с низким приоритетом отбрасывания) пересылаются.

TRTCM может работать в одном из двух режимов: без учета цвета и с учетом цвета. В режиме без учета цвета (color-blind) маркировка пакетов осуществляется посредством их оценки относительно параметров PIR и CIR, независимо от предыдущей маркировки. В режиме с учетом цвета (color-aware) маркировка пакетов осуществляется с учетом как текущего цвета, так и оценки относительно параметров PIR и CIR. Если пакеты не подпадают под маркировку ни одним из цветов, они передаются в неизменном виде.

32.2.1 TRTCM – режим без учета цвета

Все пакеты оцениваются по скорости PIR. Пакеты, поступающие со скоростью свыше PIR, помечаются красным. В противном случае пакеты оцениваются по скорости CIR. Пакеты, поступающие со скоростью свыше CIR, помечаются желтым. Все остальные пакеты (поступающие со скоростью ниже CIR) помечаются зеленым.

Рисунок 140 TRTCM – режим без учета цвета

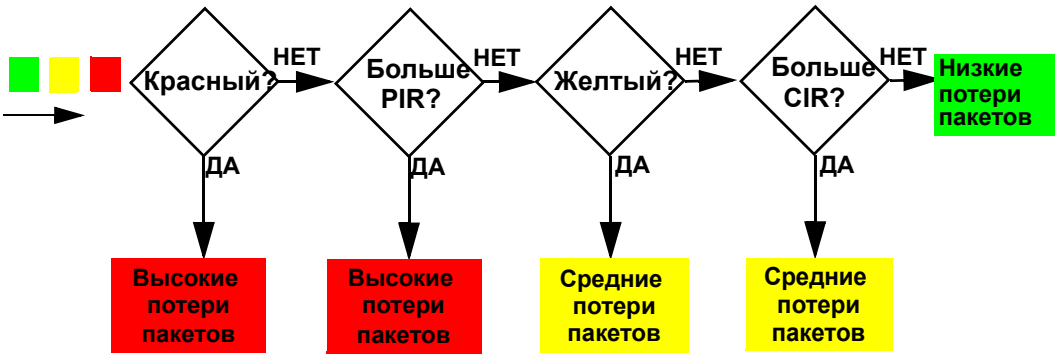


32.2.2 TRTCM – режим с учетом цвета

В режиме с учетом цвета при оценке пакетов учитывается ранее назначенный приоритет отбрасывания. TRTCM может увеличить приоритет отбрасывания пакетов, однако не может его уменьшить. Пакеты, ранее помеченные красным или желтым, могут быть промаркированы цветом с тем же самым или более высоким приоритетом отбрасывания.

Пакеты, промаркированные красным (с высоким приоритетом отбрасывавания), остаются красными без оценки относительно параметров PIR и CIR. Пакеты, промаркированные желтым, могут быть промаркированы красным или остаться желтыми, в связи с чем они оцениваются только относительно PIR. Только пакеты, промаркированные зеленым, оцениваются относительно PIR и затем, если их скорость меньше PIR, оцениваются относительно CIR.

Рисунок 141 TRTCM – режим с учетом цвета

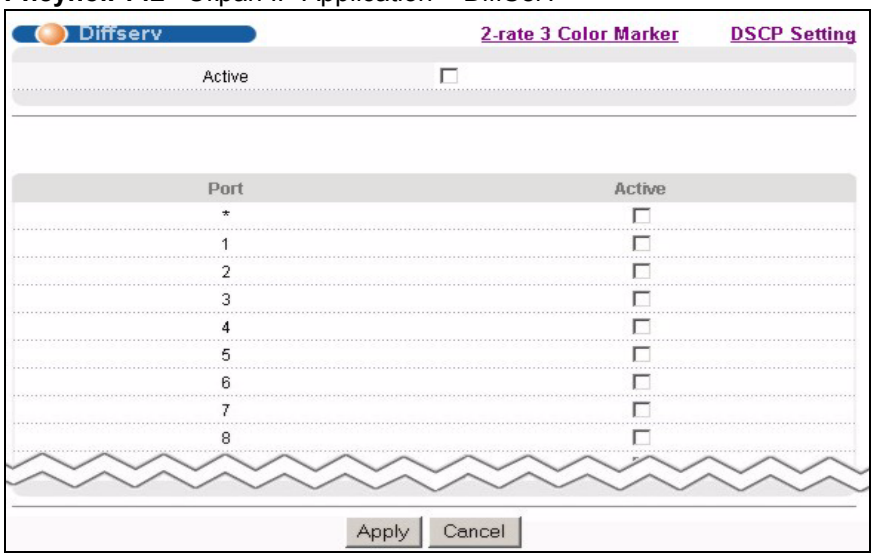


32.3 Активация механизма DiffServ

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 142 Экран IP Application > DiffServ



Поля экрана описаны в следующей таблице.

Таблица 97 Экран IP Application > DiffServ

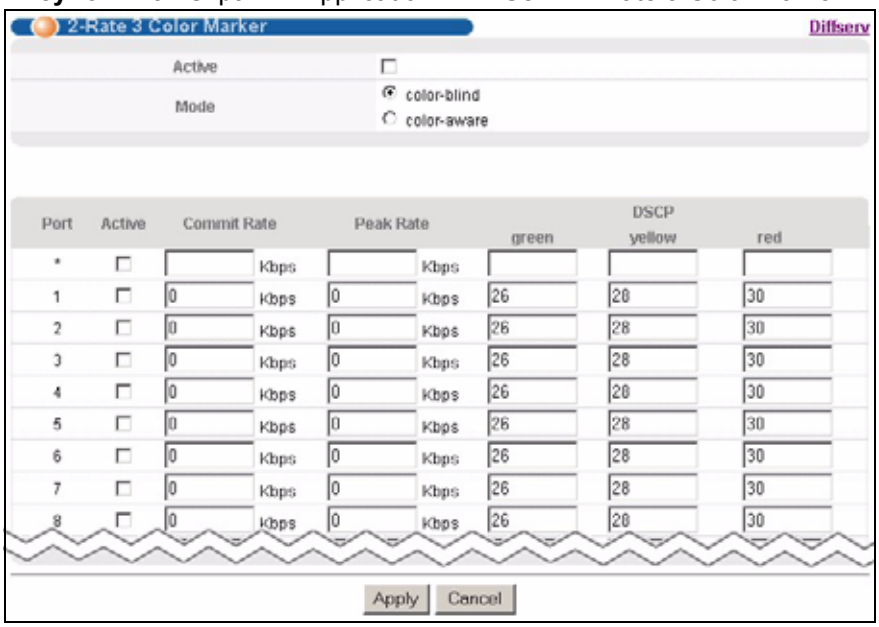
ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить поддержку DiffServ на коммутаторе.
Port	В этом поле отображается порядковый номер порта коммутатора.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов 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.

32.3.1 Настройка маркировки TRTCM

Настройка маркировки TRTCM осуществляется на следующем экране. Чтобы отобразить показанный ниже экран, нажмите на экране **DiffServ** ссылку **2-rate 3 Color Marker**.

Включить одновременно TRTCM и управление пропускной способностью невозможно.

Рисунок 143 Экран IP Application > DiffServ > 2-rate 3 Color Marker



Поля экрана описаны в следующей таблице.

Таблица 98 Экран IP Application > DiffServ > 2-rate 3 Color Marker

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить на коммутаторе маркировку TRTCM (Two Rate Three Color Marker). Данный коммутатор оценивает и маркирует пакеты с использованием настроек TRTCM. Примечание: Чтобы коммутатор отбрасывал пакеты с красной маркировкой (высоким приоритетом отбрасывания), необходимо также включить **DiffServ** на коммутаторе и на отдельных портах.
Mode	Выберите **color-blind**, чтобы коммутатор обрабатывал все поступающие пакеты как не имеющие цветовой маркировки. При этом все поступающие пакеты оцениваются на основе параметров CIR и PIR. Выберите **color-aware**, чтобы пакеты маркировались с учетом предыдущей маркировки. При этом все поступающие оцениваются на основе существующей цветовой маркировки. Поступающие пакеты без цветовой маркировкой проходят через коммутатор.
Port	В этом поле отображается порядковый номер порта коммутатора.

Таблица 98 Экран IP Application > DiffServ > 2-rate 3 Color Marker (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.
Active	Установите этот переключатель, чтобы активировать TRTCM на порту.
Commit Rate	Укажите гарантированную скорость передачи информации (CIR) для данного порта.
Peak Rate	Укажите пиковую скорость передачи информации (PIR) для данного порта.
DSCP	В данном разделе можно указать, какие значения кодовых маркеров DSCP должны назначаться пакетам в зависимости от их цвета, который они получают в результате обработки TRTCM.
green	Укажите значение DSCP, которое назначается пакетам с низким приоритетом отбрасывания.
yellow	Укажите значение DSCP, которое назначается пакетам со средним приоритетом отбрасывания.
red	Укажите значение DSCP, которое назначается пакетам с высоким приоритетом отбрасывания.
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.

32.4 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.

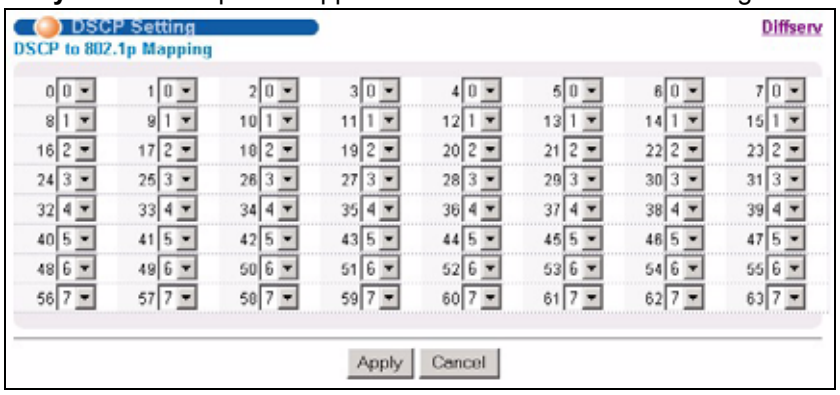
Таблица 99 Отображение маркеров DSCP на приоритеты IEEE 802.1p по умолчанию

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

32.4.1 Настройка DSCP

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

Рисунок 144 Экран IP Application > DiffServ > DSCP Setting



Поля экрана описаны в следующей таблице.

Таблица 100 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.

33

DHCP

В данной главе описана настройка функции DHCP.

33.1 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 сервера DHCP или агента ретрансляции DHCP. При настройке в качестве сервера коммутатор предоставляет клиентам настройки TCP/IP. При настройке коммутатора в качестве агента ретрансляции коммутатор пересылает запросы DHCP на сетевой сервер DHCP. Если не настраивать коммутатор в качестве сервера или агента ретрансляции DHCP, сервер DHCP должен находиться широковещательном домене клиентских компьютеров или клиентские компьютеры должны настраиваться вручную.

33.1.1 Режимы DHCP

Данный коммутатор можно настроить в качестве сервера DHCP или в качестве агента ретрансляции DHCP.

- В случае настройки коммутатора в качестве сервера DHCP на нем необходимо будет настроить пулы IP-адресов вместе с масками подсетей, адресами серверов DNS и шлюзов по умолчанию, которые будут назначаться компьютерам в локальной сети.
- 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.

33.1.2 Варианты настройки DHCP

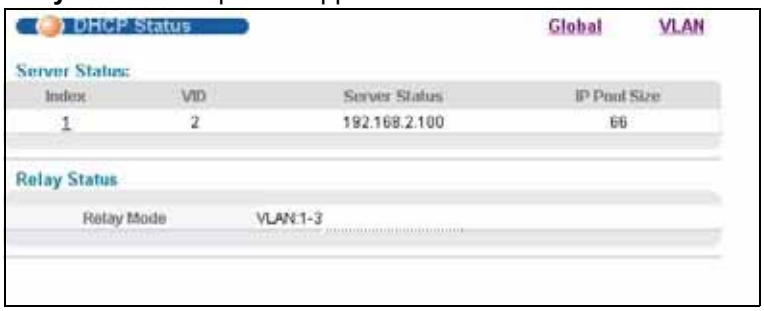
Настройки DHCP на коммутатор осуществляются на экранах **Global** и **VLAN**. Выбор экрана для настройки зависит от тех служб DHCP, которые должны быть предоставлены клиентам DHCP в сети. При выборе руководствуйтесь следующими критериями:

- **Global** – коммутатор пересылает все запросы DHCP на один и тот же сервер DHCP.
- **VLAN** – коммутатор настраивается на уровне отдельной VLAN. Данный коммутатор может быть настроен в качестве сервера DHCP для одной из сетей VLAN и одновременно этот коммутатор может работать в качестве агента ретрансляции запросов DHCP для клиентов в другой VLAN.

33.2 Состояние DHCP

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

Рисунок 145 Экран IP Application > DHCP Status



Поля экрана описаны в следующей таблице.

Таблица 101 Экран IP Application > DHCP Status

ПОЛЕ	ОПИСАНИЕ
Server Status	В данном разделе отображаются настройки, относящиеся к режиму сервера DHCP на коммутаторе.
Index	Порядковый номер.
VID	В этом поле отображается идентификационный номер VLAN, для которой коммутатор будет работать в качестве сервера DHCP.
Server Status	В этом поле отображается начальный IP-адрес для клиентов DHCP.
IP Pool Size	В этом поле отображается количество IP-адресов, которые могут быть назначены клиентам.
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.

33.3 Детали состояния сервера DHCP

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **IP Application** > **DHCP** и затем нажмите на порядковом номере настройки сервера DHCP. На этом экране можно просмотреть подробную информацию о настройках сервера DHCP на коммутаторе.

Рисунок 146 Экран IP Application > DHCP > DHCP Server Status Detail

Поля экрана описаны в следующей таблице.

Таблица 102 Экран IP Application > DHCP Server Status Detail

ПОЛЕ	ОПИСАНИЕ
Start IP Address	В этом поле отображается начальный IP-адрес пула IP-адресов, настроенных на данном экземпляре сервера DHCP.
End IP Address	В этом поле отображается конечный IP-адрес пула IP-адресов, настроенных на данном экземпляре сервера DHCP.
Subnet Mask	В этом поле отображается маска подсети для клиентов, назначаемая данным экземпляром сервера DHCP.
Default Gateway	В этом поле отображается адрес шлюза по умолчанию для клиентов, назначаемый данным экземпляром сервера DHCP.
Primary DNS Server	В этом поле отображается адрес основного сервера DNS для клиентов, назначаемый данным экземпляром сервера DHCP.
Secondary DNS Server	В этом поле отображается адрес вспомогательного сервера DNS для клиентов, назначаемый данным экземпляром сервера DHCP.
Address Leases	В данном разделе отображается информация об IP-адресах, выданных клиентам данным сервером DHCP.
Index	В этом поле отображается порядковый номер каждого запроса DHCP, обработанного коммутатором.
IP Address	IP-адрес, выданный клиенту DHCP.
Timer	В этом поле отображается время, оставшееся до момента возобновления своего IP-адреса клиентом DHCP.
Hardware Address	В этом поле отображается MAC-адрес клиента DHCP. В этом поле может также отображаться надпись **SELF OCCUPIED ADDRESS**, если IP-адрес не может быть использован для DHCP ввиду того, что он уже назначен самому коммутатору.
Hostname	В этом поле отображается имя системы клиента.

33.4 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.

33.4.1 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:

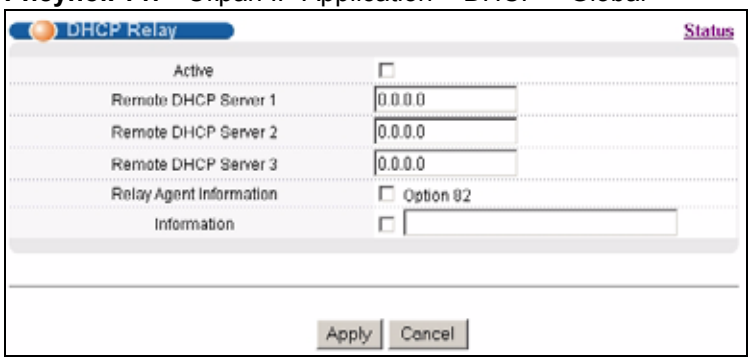
Таблица 103 Информация агента ретрансляции

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.**

33.4.2 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 147 Экран IP Application > DHCP > Global



Поля экрана описаны в следующей таблице.

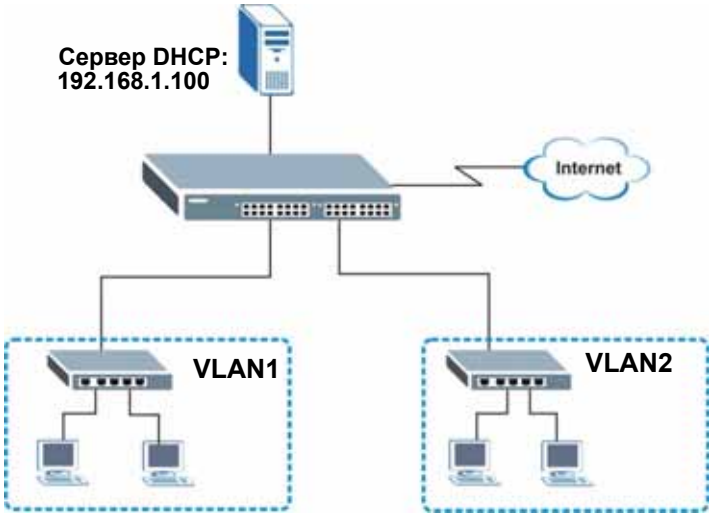
Таблица 104 Экран IP Application > DHCP > Global

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.
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.

33.4.3 Пример настройки глобальной ретрансляции DHCP

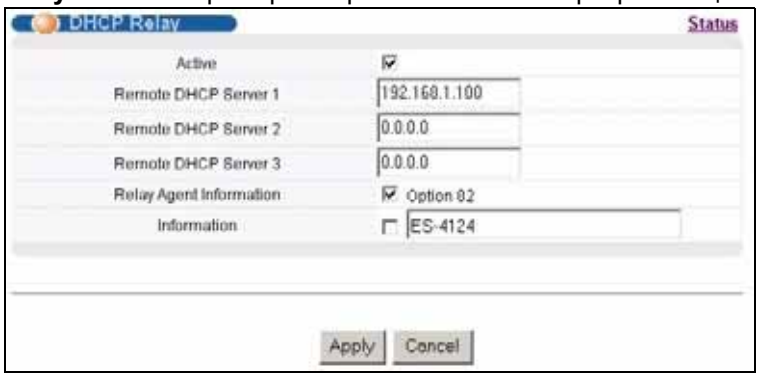
На приведенном ниже рисунке показан пример сети, в которой коммутатор используется для ретрансляции запросов DHCP в доменах **VLAN1** и **VLAN2**. В сети имеется только один сервер DHCP, который обслуживает клиентов DHCP в обоих доменах.

Рисунок 148 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 149 Пример настройки глобальной ретрансляции DHCP

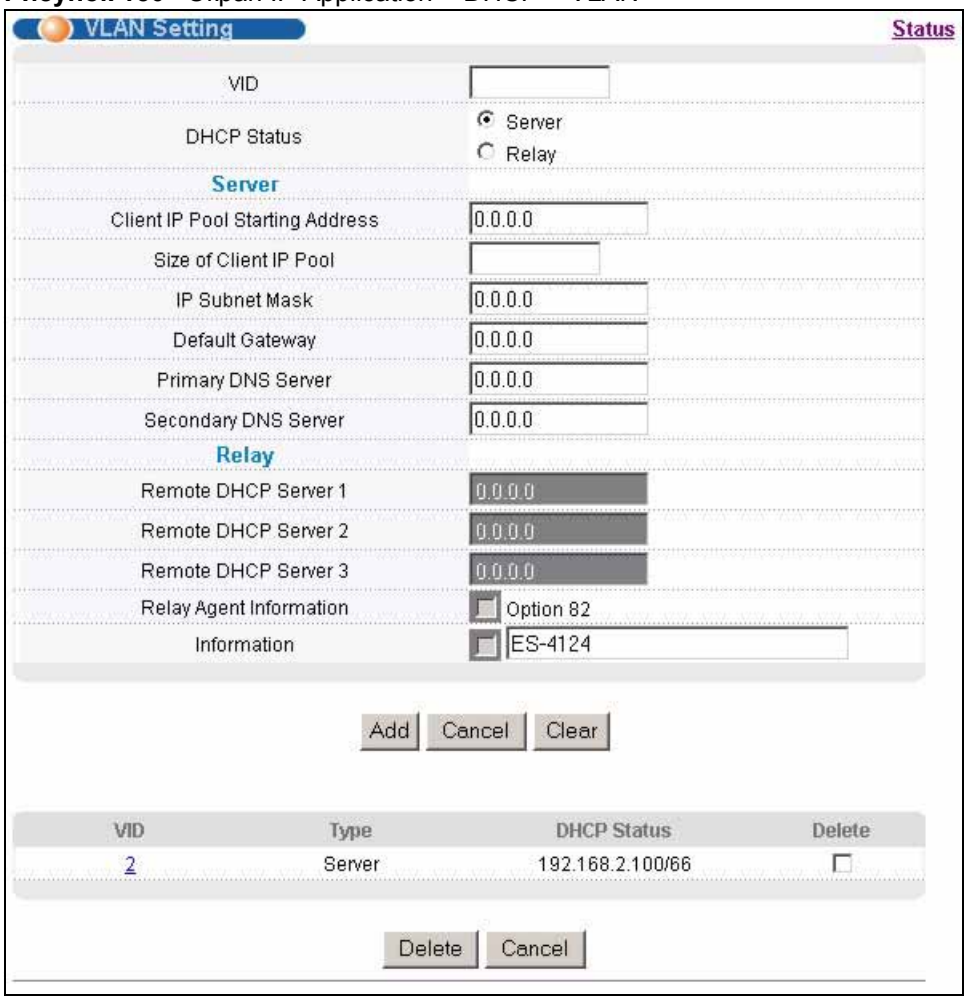


33.5 Настройка DHCP для конкретных VLAN

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. 86.

Рисунок 150 Экран IP Application > DHCP > VLAN



Поля экрана описаны в следующей таблице.

Таблица 105 Экран IP Application > DHCP > VLAN

ПОЛЕ	ОПИСАНИЕ
VID	Введите идентификатор VLAN, к которой относятся данные настройки DHCP.
DHCP Status	Выберите, должен ли коммутатор работать в качестве сервера DHCP (**Server**) или агента ретрансляции (**Relay**) для указанного VID. В случае выбора **Server** все поля, относящиеся к настройке агента ретрансляции DHCP, становятся затененными (недоступными), и наоборот.
Server	В этом разделе можно настроить коммутатор для работы в качестве сервера DHCP для указанной VLAN.
Client IP Pool Starting Address	Укажите первый из серии последовательных IP-адресов в пуле.
Size of Client IP Pool	Укажите размер пула, то есть количество IP-адресов в пуле. Данный коммутатор может назначать клиентам DHCP от 1 to 253 IP-адресов.
IP Subnet Mask	Введите маску подсети для клиентского пула IP-адресов.
Default Gateway	Введите IP-адрес шлюза по умолчанию.

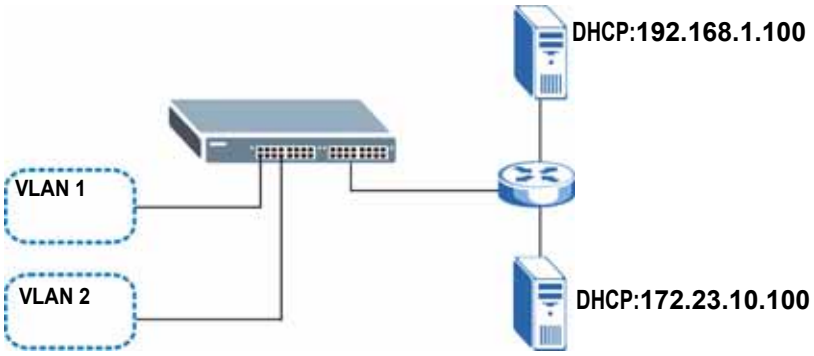
Таблица 105 Экран IP Application > DHCP > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Primary/ Secondary DNS Server	Введите IP-адреса серверов DNS. Настройки серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Relay	В этом разделе можно настроить коммутатор для работы в качестве агента ретрансляции DHCP для указанной VLAN.
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.
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 режим DHCP: **Server** или **Relay**.
DHCP Status	Для конфигурации сервера DHCP в этом поле отображается начальный IP-адрес и размер пула IP-адресов. При настройке в качестве агента ретрансляции DHCP 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**.

33.5.1 Пример: Ретрансляция DHCP для двух VLAN

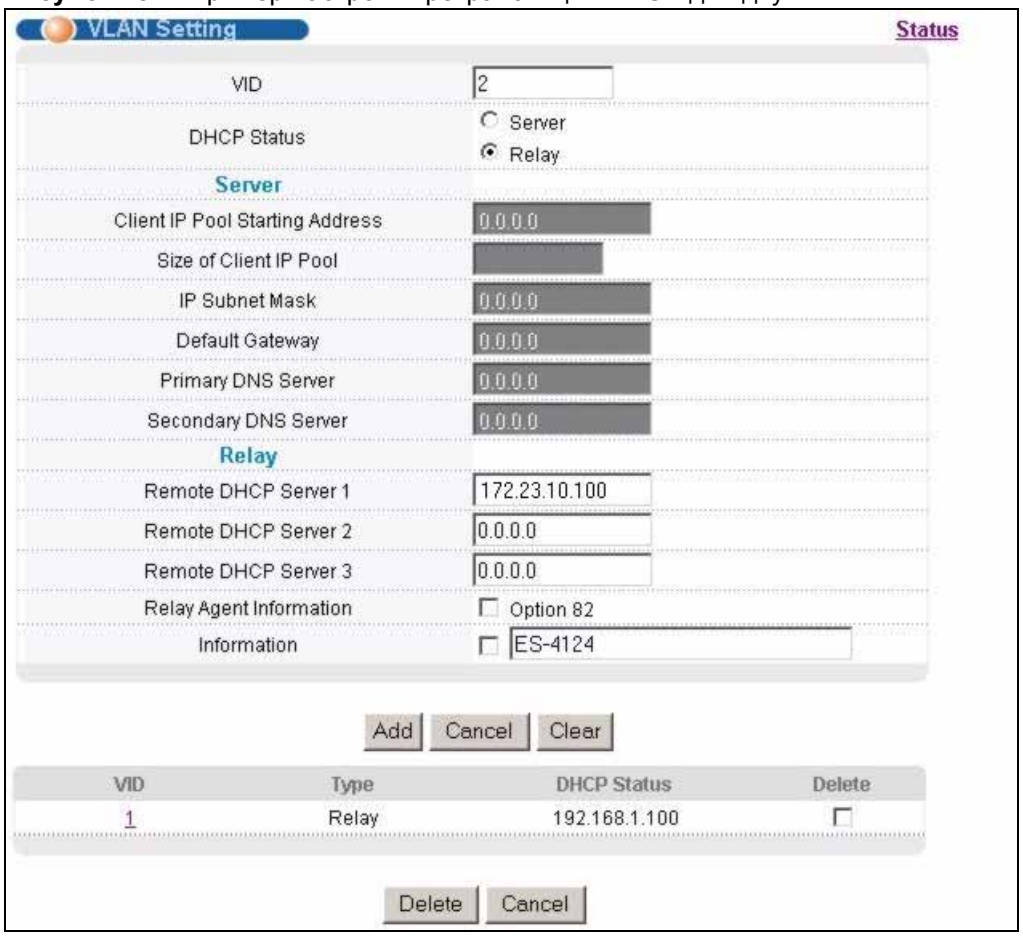
В следующем примере показана сеть группы зданий с двумя виртуальными локальными сетями VLAN (VID 1 и 2). Для обслуживания каждой из сетей VLAN установлено два сервера DHCP. В системе настроена ретрансляция запросов DHCP из комнат общежития (VLAN 1) на сервер DHCP с IP-адресом 192.168.1.100. Запросы из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

Рисунок 151 Ретрансляция DHCP для двух VLAN



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

Рисунок 152 Пример настройки ретрансляции DHCP для двух VLAN



34

VRRP

В данной главе описана настройка и мониторинг на коммутаторе протокола резервирования виртуального маршрутизатора (VRRP).

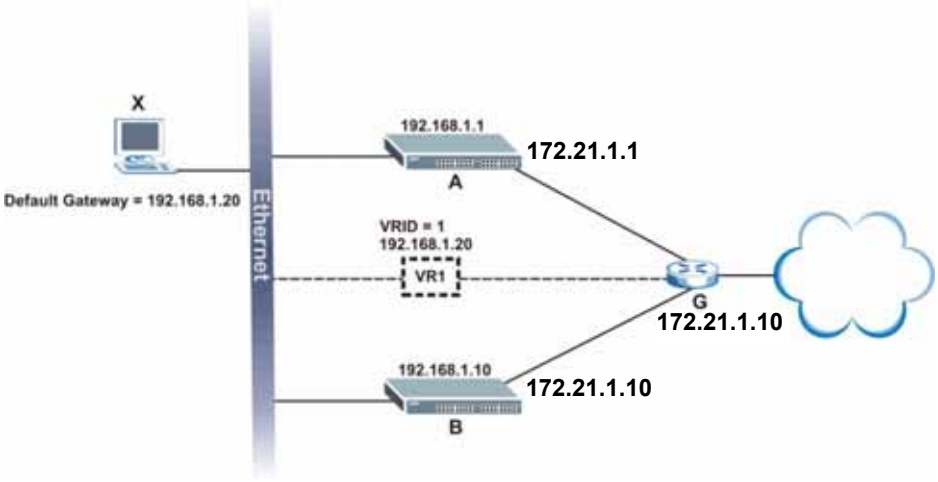
34.1 Обзор протокола VRRP

На каждом из хостов в сети указывается статический адрес шлюза по умолчанию (данного коммутатора), на который отправляются пакеты. Таким образом, шлюз по умолчанию может стать критическим элементом, отказ которого приводит к отказу всей сети. Протокол резервирования виртуального маршрутизатора (VRRP), определенный в RFC 2338, позволяет создать резервные шлюзы, чтобы шлюз по умолчанию был всегда доступен для хостов.

При использовании VRRP определяется виртуальный маршрутизатор (VR), который представляет несколько физических устройств уровня 3. IP-адрес связывается с виртуальным маршрутизатором. Устройство уровня 3, IP-которого совпадает с IP-адресом виртуального маршрутизатор, называется предпочтительным главным маршрутизатором, тогда как другие устройства уровня 3 называются резервными маршрутизаторами. Трафик, направляемый на виртуальный маршрутизатор, пересылается главным маршрутизатором. Если главный маршрутизатор становится недоступным, роль главного маршрутизатора возлагается на резервный маршрутизатор, который исполняет ее до тех пор, пока главный маршрутизатор не заработает снова.

На рисунке ниже показан пример сети VRRP, в которой коммутаторы (**A** и **B**) реализуют один виртуальный маршрутизатор **VR1**, гарантируя наличие канала связи от хоста **X** к шлюзу **G**. На хосте **X** в качестве шлюза по умолчанию установлен адрес **VR1** (192.168.1.20). Если более высокий приоритет имеет коммутатор **A**, он становится главным маршрутизатором. Коммутатор **B** с меньшим приоритетом, выполняет роль резервного маршрутизатора.

Рисунок 153 VRRP: пример 1

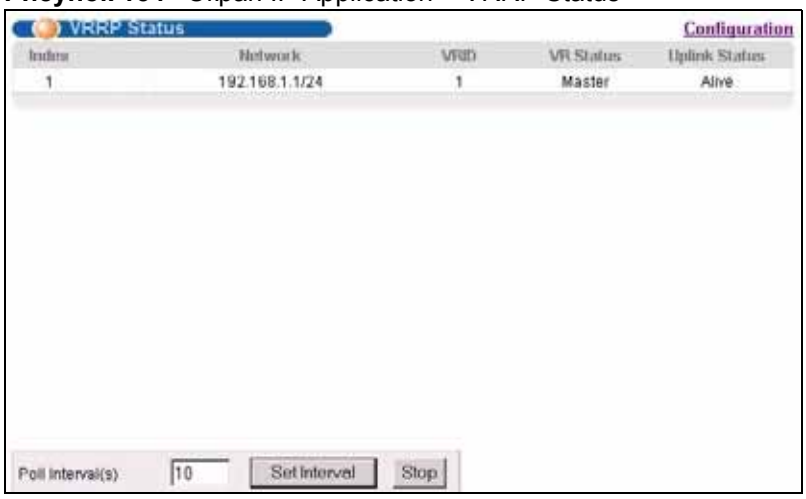


Если коммутатор **A** (главный маршрутизатор) становится недоступным, вступает в действие коммутатор **B**. В этом случае трафик обрабатывается коммутатором **B**.

34.2 Состояние VRRP

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

Рисунок 154 Экран IP Application > VRRP Status



Поля экрана описаны в следующей таблице.

Таблица 106 Экран IP Application > VRRP Status

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер записи.
Network	В этом поле отображается IP-адрес и число единичных бит в маске подсети для домена IP-маршрутизации, с которым связан данный виртуальный маршрутизатор.
VRID	В этом поле отображается идентификационный номер виртуального маршрутизатора.

Таблица 106 Экран IP Application > VRRP Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
VR Status	В этом поле отображается состояние виртуального маршрутизатора. Значение **Master** означает, что данный коммутатор выполняет роль главного маршрутизатора. Значение **Backup** означает, что данный коммутатор выполняет роль резервного маршрутизатора. Значение **Init** отображается в процессе инициализации протокола VRRP на данном коммутаторе, а также в тех случаях, когда канал к шлюзу недоступен (в поле **Uplink Status** отображается **Dead**).
Uplink Status	В этом поле отображается состояние канала между данным коммутатором и шлюзом. Значение **Alive** означает, что канал между данным коммутатором и шлюзом работает. В противном случае в этом поле отображается **Dead**. При проверке коммутатором состояния канала в этом поле отображается **Probe**.
Poll Interval(s)	В этом поле отображается, как часто (в секундах) происходит обновление данного экрана. Чтобы изменить интервал обновления, можно ввести новое число в это текстовое поле и нажать на кнопку **Set Interval**.
Stop	Нажатие на **Stop** останавливает сбор статистики.

34.3 Настройка VRRP

В приведенных ниже разделах описаны различные части экрана настройки **VRRP Configuration**.

34.3.1 Настройка IP-интерфейса

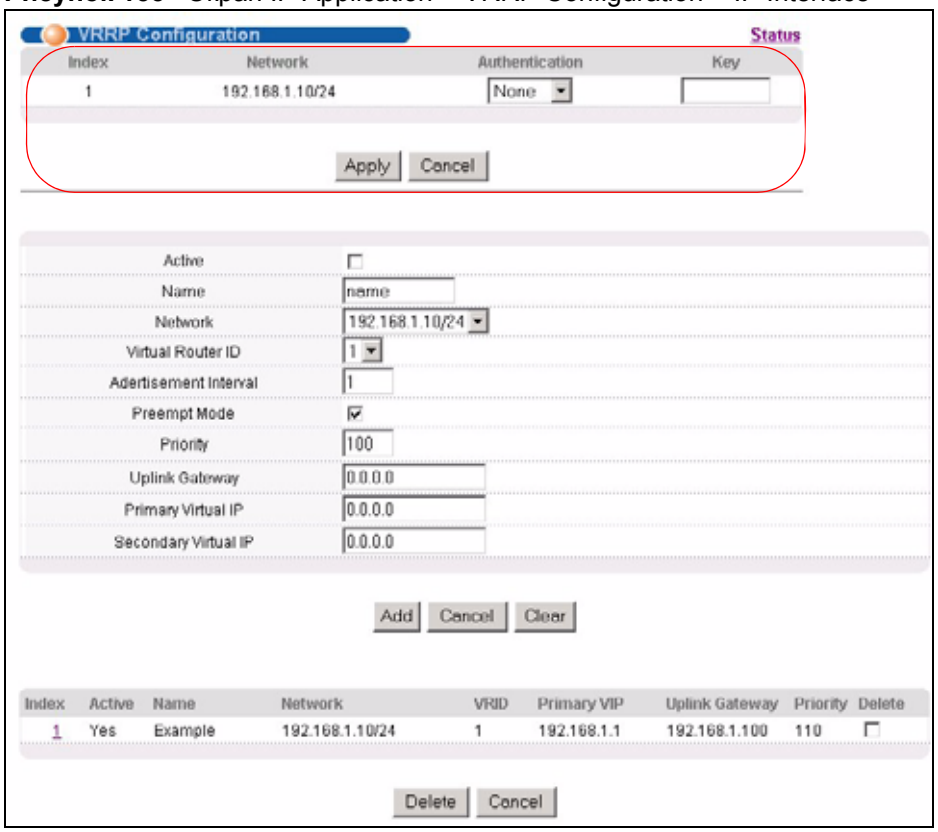
Перед началом настройки VRRP необходимо сначала создать IP-интерфейс (или домен маршрутизации) на экране **IP Setup** (более подробную информацию можно найти в разд. 7.6 на стр. 86).

Чтобы отобразить показанный ниже экран **VRRP Configuration**, выберите **IP Application**, **VRRP** и нажмите на ссылку **Configuration**.

VRRP можно настроить только на интерфейсах с уникальными идентификаторами VLAN ID.

Домены маршрутизации с одним и тем же идентификатором VLAN ID в показанной ниже таблице не отображаются.

Рисунок 155 Экран IP Application > VRRP Configuration > IP Interface



Поля экрана описаны в следующей таблице.

Таблица 107 Экран IP Application > VRRP Configuration > IP Interface

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер записи.
Network	В этом поле отображается IP-адрес и количество единичных битов в маске подсети для домена IP-маршрутизации.
Authentication	Выберите **None**, чтобы отключить аутентификацию. Это значение выбрано по умолчанию. Выберите **Simple**, чтобы использовать для аутентификации пакетов VRRP, передаваемых через данный интерфейс, аутентификацию по простому паролю.
Key	В случае выбора **Simple** в поле **Authentication** введите в данное поле пароль (не более восьми печатных символов ASCII).
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 отменить все изменения в таблице.

34.3.2 Параметры VRRP

В данном разделе описаны параметры VRRP.

34.3.2.1 Интервал объявлений

Чтобы информировать резервные маршрутизаторы о своей нормальной работе, главный маршрутизатор рассылает сообщения Hello. Интервалом объявлений называется период времени между рассылкой сообщений Hello. По умолчанию сообщения Hello рассылаются каждую секунду.

Если резервные маршрутизаторы не получают сообщения Hello от главного маршрутизатора по истечении указанного интервала, главный маршрутизатор считается прекратившим работу. В этом случае главным маршрутизатором становится резервный маршрутизатор с наивысшим приоритетом.

На всех маршрутизаторах, включенных в состав виртуального маршрутизатора, должен быть установлен одинаковый интервал объявлений.

34.3.2.2 Приоритет

Настройка уровня приоритета (в диапазоне от 1 до 254) позволяет установить, какой из резервных маршрутизаторов должен брать на себя роль главного в случае прекращения работы последнего. Таким маршрутизатором становится резервный маршрутизатор с наивысшим приоритетом. Приоритет маршрутизатора VRRP, которому принадлежат связанные с виртуальным маршрутизатором IP-адреса, устанавливается равным 255.

34.3.2.3 Режим вытеснения

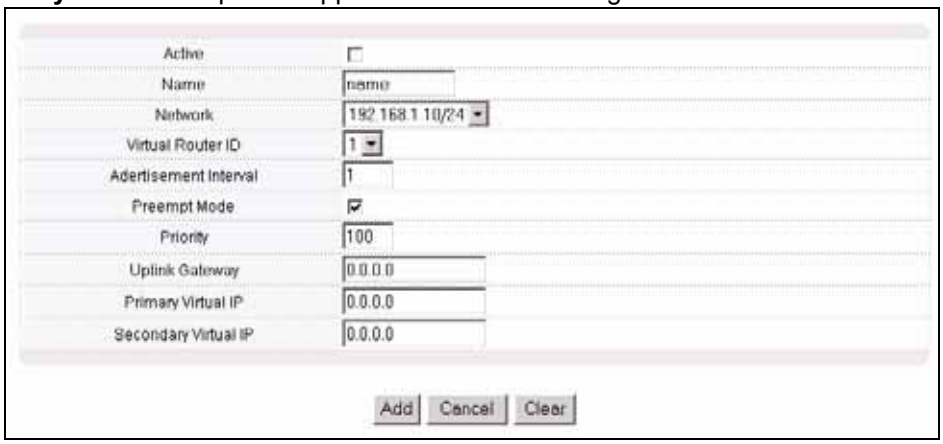
Если главный маршрутизатор становится недоступным, его роль берет на себя резервный маршрутизатор. Однако, в случае присоединения к сети еще одного резервного маршрутизатора с более высоким приоритетом он вытеснит резервный маршрутизатор с меньшим приоритетом, который стал главным. Чтобы предотвратить подобную ситуацию, можно отключить режим вытеснения.

Устройство уровня 3 с тем же IP-адресом, что и у виртуального маршрутизатора, по умолчанию становится главным маршрутизатором независимо от режима вытеснения.

34.3.3 Настройка параметров VRRP

После настройки IP-интерфейса необходимо настроить параметры VRRP на экране **VRRP Configuration**.

Рисунок 156 Экран IP Application > VRRP Configuration > VRRP Parameters



Поля экрана описаны в следующей таблице.

Таблица 108 Экран IP Application > VRRP Configuration > VRRP Parameters

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить данную запись VRRP.
Name	Введите имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать эту запись.
Network	Выберите IP-домен, к которому относится данная запись VRRP.
Virtual Router ID	Выберите номер виртуального маршрутизатора (от 1 до 7), для которого создается данная запись VRRP. В одной сети можно настроить не более семи виртуальных маршрутизаторов.
Advertisement Interval	Укажите интервал времени в секундах между передачей сообщений Hello. По умолчанию установлено значение **1**.
Preempt Mode	Установите этот переключатель, чтобы активировать режим вытеснения.
Priority	Введите число (в диапазоне от 1 до 254), обозначающее уровень приоритета. Чем больше число, тем выше приоритет. По умолчанию данное поле имеет значение **100**.
Uplink Gateway	Введите IP-адрес шлюза в виде десятичных чисел, разделенных точками. Данный коммутатор проверяет канал связи с этим шлюзом.
Primary Virtual IP	Введите IP-адрес основного виртуального маршрутизатора в виде десятичных чисел, разделенных точками.
Secondary Virtual IP	Данное поле является необязательным. Введите IP-адрес вспомогательного виртуального маршрутизатора в виде десятичных чисел, разделенных точками. В случае ввода **0.0.0.0** данное поле игнорируется.
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 отменить все изменения в таблице.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.

34.3.4 Настройка параметров VRRP

Итоговые настройки VRRP отображаются в нижней части экрана.

Рисунок 157 Экран VRRP Configuration: итоговая таблица

Поля экрана описаны в следующей таблице.

Таблица 109 Настройка VRRP: параметры VRRP

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер записи.
Active	В этом поле указано, включена ли соответствующая запись VRRP (**Yes**) или отключена (**No**).
Name	В этом поле отображается имя-описание записи.
Network	В этом поле отображается IP-адрес и маска подсети для интерфейса.
VRID	В этом поле отображается идентификационный номер виртуального маршрутизатора.
Primary VIP	В этом поле отображается IP-адрес основного виртуального маршрутизатора.
Uplink Gateway	В этом поле отображается IP-адрес шлюза.
Priority	В этом поле отображается уровень приоритета (от 1 до 255) для записи.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

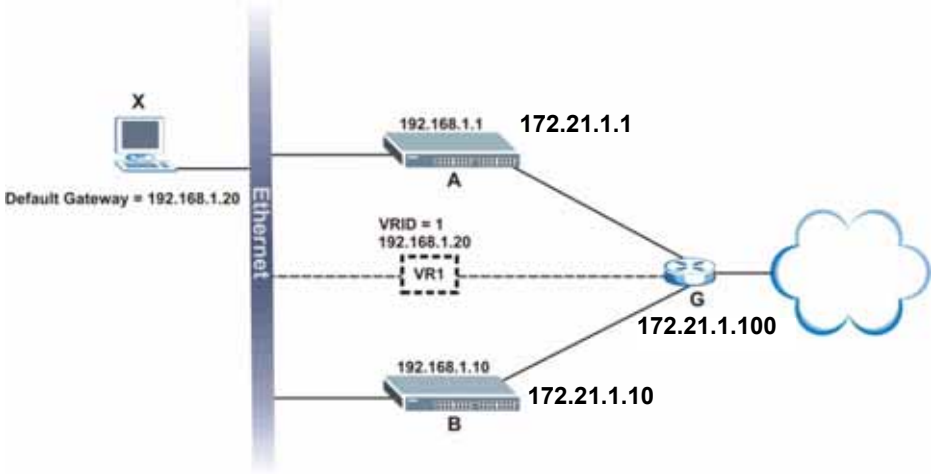
34.4 Примеры настройки VRRP

В следующих разделах описаны два примера настройки VRRP на коммутаторе.

34.4.1 Пример с одной подсетью

На приведенном ниже рисунке показана простая сеть VRRP, включающая в себя только один виртуальный маршрутизатор **VR1** (VRID =1) и два коммутатора. Сеть подключена к распределенной сети WAN через шлюз **G** (172.21.1.100). На хост-компьютере **X** в качестве шлюза по умолчанию настроен виртуальный маршрутизатор **VR1**.

Рисунок 158 Пример настройки VRRP: сеть с одним виртуальным маршрутизатором



Коммутатор **A** необходимо настроить в качестве главного маршрутизатора. Установите на экранах **VRRP Configuration** коммутаторов следующие параметры VRRP, как показано на рисунках ниже.

Рисунок 159 Пример настройки VRRP 1: значения параметров VRRP для коммутатора A

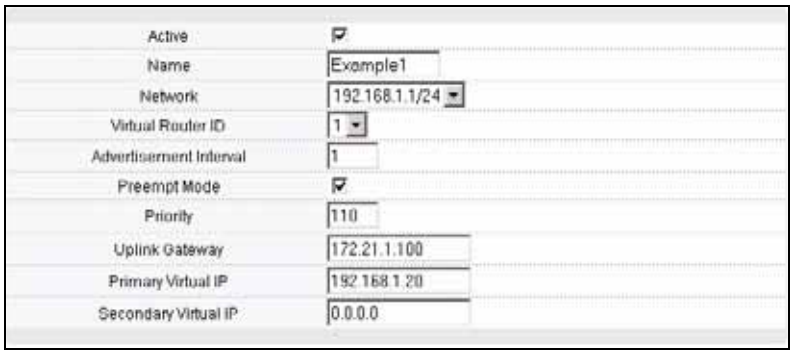
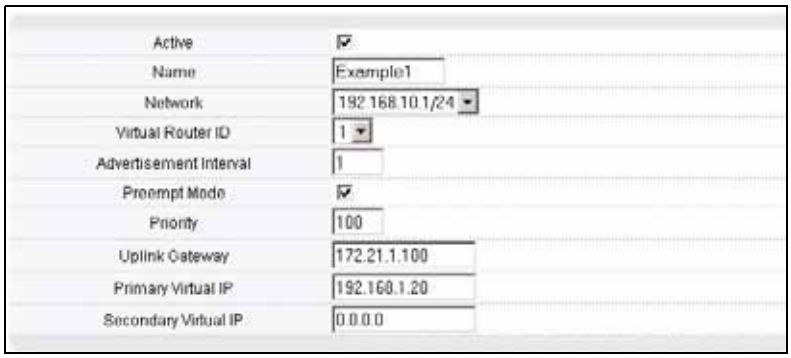


Рисунок 160 Пример настройки VRRP 1: значения параметров VRRP для коммутатора B



После настройки и сохранения конфигураций VRRP экраны **VRRP Status** коммутаторов будут выглядеть следующим образом.

Рисунок 161 Пример настройки VRRP 1: состояние VRRP на коммутаторе A

VRRP Status — Configuration

Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.1/24	1	Master	Alive

Рисунок 162 Пример настройки VRRP 1: состояние VRRP на коммутаторе B

VRRP Status — Configuration

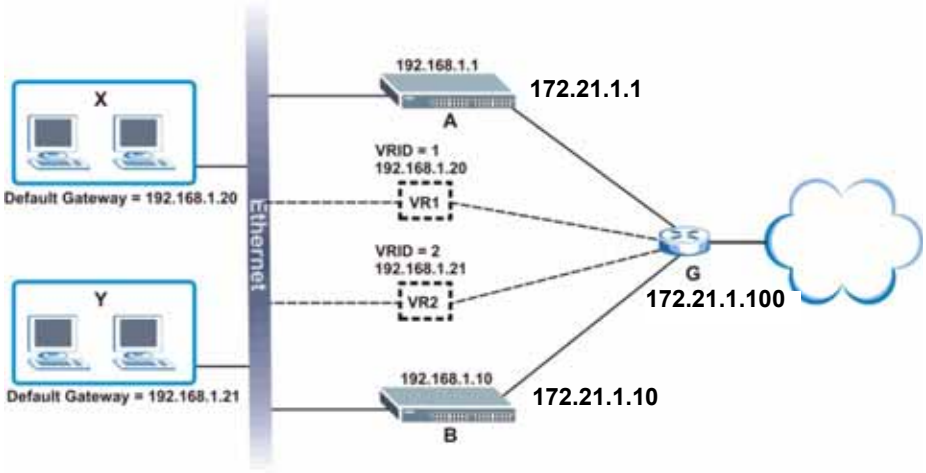
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.10/24	1	Backup	Alive

34.4.2 Пример с двумя подсетями

На приведенном ниже рисунке показан пример сети, в которой трафик делится между двумя коммутаторами. На хостах в двух сетевых группах настроены различные шлюзы по умолчанию. На каждом из коммутаторов необходимо настроить поддержку виртуального маршрутизатора в качестве резервного с использованием VRRP.

То есть необходимо настроить коммутатор **A** в качестве главного маршрутизатора для виртуального маршрутизатора **VR1**, и в качестве резервного – для виртуального маршрутизатора **VR2**. Коммутатор **B**, напротив, является главным для маршрутизатора **VR2** и резервным – для **VR1**.

Рисунок 163 Пример настройки VRRP: сеть с двумя виртуальными маршрутизаторами



Оставив без изменения конфигурацию VRRP от примера 1 для виртуального маршрутизатора **VR1** (см. разд. 34.4.2 на стр. 309), необходимо произвести настройки для виртуального маршрутизатора VR2 на экране **VRRP Configuration** каждого из коммутаторов. Настроить параметры VRRP на коммутаторах необходимо следующим образом, как показано на рисунках.

Рисунок 164 Пример настройки VRRP 2: значения параметров VRRP для VR2 на коммутаторе A

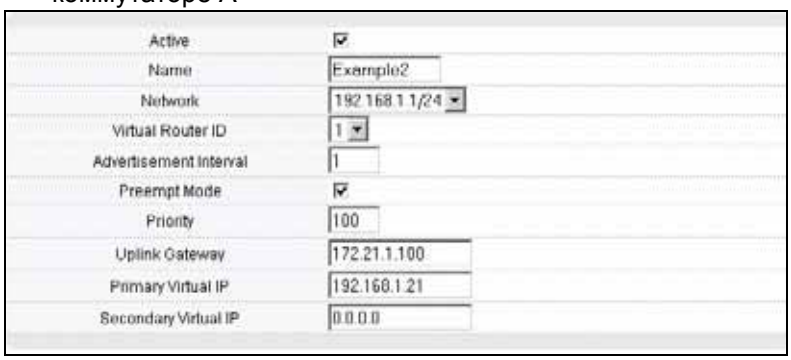
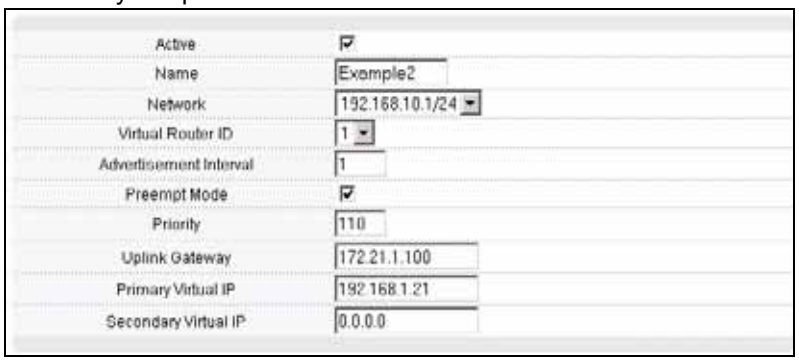


Рисунок 165 Пример настройки VRRP 2: значения параметров VRRP для VR2 на коммутаторе B



После настройки и сохранения конфигураций VRRP экраны **VRRP Status** коммутаторов будут выглядеть следующим образом.

Рисунок 166 Пример настройки VRRP 2: состояние VRRP на коммутаторе A

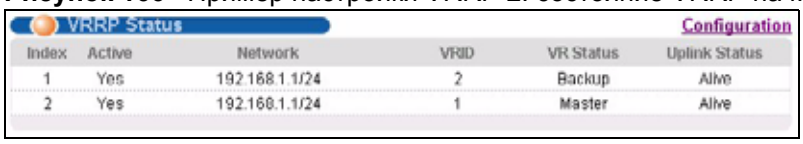
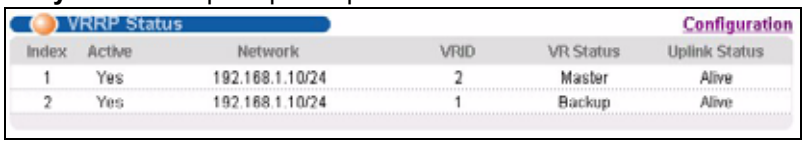


Рисунок 167 Пример настройки VRRP 2: состояние VRRP на коммутаторе B



Часть V
Управление

35

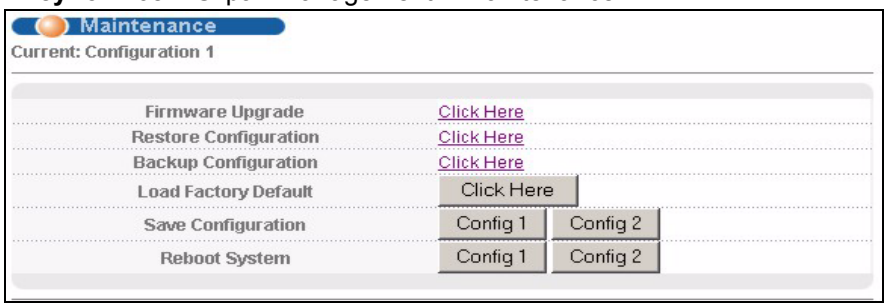
Обслуживание

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

35.1 Экран обслуживания

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

Рисунок 168 Экран Management > Maintenance



Поля экрана описаны в следующей таблице.

Таблица 110 Экран Management > Maintenance

ПОЛЕ	ОПИСАНИЕ
Current	В этом поле отображается, какая конфигурация используется коммутатором в данный момент (**Configuration 1** или **Configuration 2**).
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 110 Экран Management > Maintenance (продолжение)

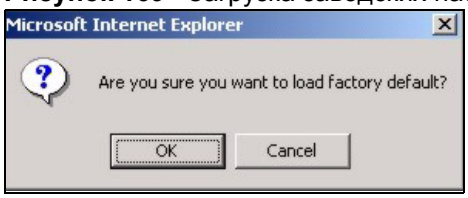
ПОЛЕ	ОПИСАНИЕ
Save Configuration	Нажмите **Config 1** для сохранения текущей конфигурации в качестве **Configuration 1** коммутатора. Нажмите **Config 2** для сохранения текущей конфигурации в качестве **Configuration 2** коммутатора.
Reboot System	Нажмите **Config 1** для перезагрузки системы с использованием на коммутаторе конфигурации **Configuration 1**. Нажмите **Config 2** для перезагрузки системы с использованием на коммутаторе конфигурации **Configuration 2**. Примечание: Не забывайте нажимать на кнопку **Save** на экранах настройки при изменении текущей конфигурации коммутатора.

35.2 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 169 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).

35.3 Сохранение конфигурации

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

Нажмите **Config 2** для сохранения текущей конфигурации в качестве **Configuration 2** 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.

35.4 Перезагрузка системы

Опция **Reboot System** позволяет перезагрузить коммутатор, не отключая питание физически. Кроме того, при перезагрузке можно выбрать конфигурацию один (**Config 1**) или конфигурацию два (**Config 2**). 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 170 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.

Чтобы перезагрузить коммутатор с использованием второй конфигурации, нажмите **Config 2** и выполните действия 1 и 2.

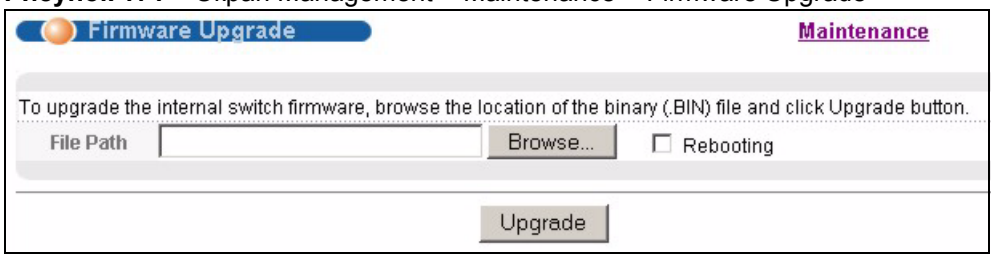
35.5 Обновление встроенного программного обеспечения

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 171 Экран Management > Maintenance > Firmware Upgrade



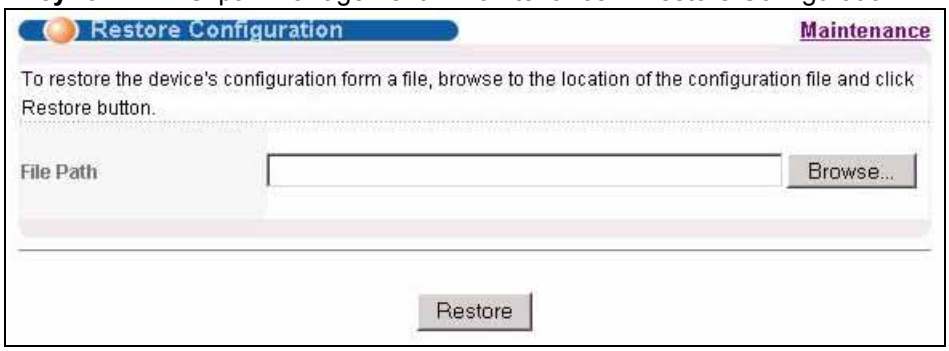
Введите путь и имя файла встроенного программного обеспечения, который необходимо загрузить в коммутатор, в текстовом поле **File Path**, или нажмите **Browse**, чтобы найти его вручную. Установите переключатель **Rebooting**, если необходимо перезагрузить коммутатор и применить новое встроенное программное 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.

35.6 Восстановление файла конфигурации

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

Рисунок 172 Экран Management > Maintenance > Restore Configuration



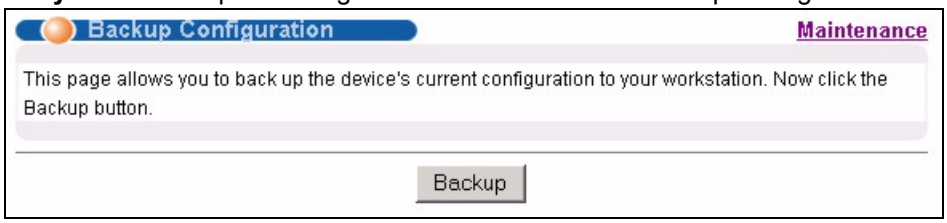
Введите путь и имя файла конфигурации, который необходимо восстановить, в текстовом поле **File Path**, или нажмите **Browse**, чтобы открыть экран **Choose File** и найти его вручную. После ввода пути к файлу нажмите **Restore**. Файл конфигурации в коммутаторе имеет имя «config», поэтому файл резервной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

35.7 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 173 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.

35.8 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.

35.8.1 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 111 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.

35.8.1.1 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.

35.8.2 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. 111 на стр. 317.
7. Чтобы покинуть строку ftp-команд, введите `quit`.

35.8.3 FTP-клиенты с графическим пользовательским интерфейсом

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

Таблица 112 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).

35.8.4 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.

36

Контроль доступа

В данной главе описан контроль доступа к коммутатору.

36.1 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 113 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 разд. 45.12.2 на стр. 379.

36.2 Главный экран контроля доступа

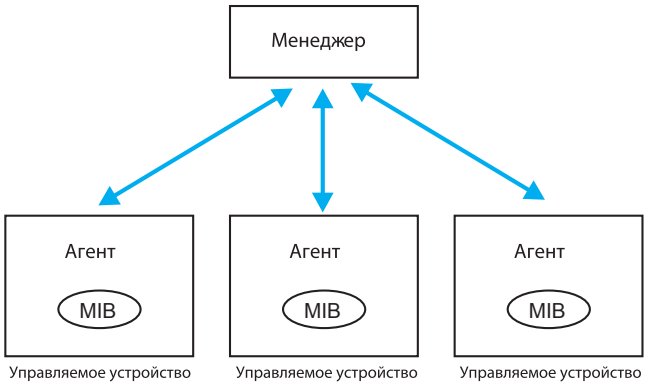
Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management > Access Control**.

Рисунок 174 Экран Management > Access Control

36.3 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 175 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 (коммутатор). 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 114 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 114 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.

36.3.1 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.

36.3.2 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

36.3.3 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 «**1.3.6.1.4.1.890.1.5.8.24**», определены в частных MIB. Все прочие OID определены в стандартных MIB.

Таблица 115 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	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при понижении или повышении скорости вентилятора так, что она выходит из нормального рабочего диапазона.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	Эта команда Trap отправляется при возвращении скорости вентилятора в нормальный рабочий диапазон.
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при понижении или повышении температуры так, что она выходит из нормального рабочего диапазона.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	Эта команда Trap отправляется при возвращении температуры в нормальный рабочий диапазон.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при понижении или повышении напряжения так, что оно выходит из нормального рабочего диапазона.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	Эта команда Trap отправляется при возвращении напряжения в нормальный рабочий диапазон.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при автоматическом сбросе коммутатора.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	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	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при неполучении коммутатором времени и даты от сервера времени.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	Эта команда Trap отправляется при получении коммутатором времени и даты от сервера времени.

Таблица 115 Системные команды Trap протокола SNMP (System) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при блокировке порта для защиты от вторжения.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при блокировке порта функцией защиты от образования петель.

Таблица 116 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	1.3.6.1.4.1.890.1.5.8.24.31.2.2	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	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при разрыве Ethernet-соединения.
autonegotiation	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется в случае, когда интерфейсу Ethernet не удается автоматически согласовать параметры соединения с другим интерфейсом Ethernet.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	Эта команда Trap отправляется в случае, когда интерфейсу Ethernet удается автоматически согласовать параметры соединения с другим интерфейсом Ethernet.

Таблица 117 Команды Trap протокола SNMP для аутентификации, авторизации и учета (AAA)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
authentication	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	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при невозможности аутентификации из-за неправильного имени пользователя и/или пароля.
	RADIUSNotReachableEvent On	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при отсутствии ответа от сервера RADIUS.
	RADIUSNotReachableEvent Clear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	Эта команда Trap отправляется при недоступности сервера RADIUS.
accounting	RADIUSNotReachableEvent On	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при отсутствии ответа от сервера учета RADIUS.
	RADIUSNotReachableEvent Clear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	Эта команда Trap отправляется при недоступности сервера учета RADIUS.

Таблица 118 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.

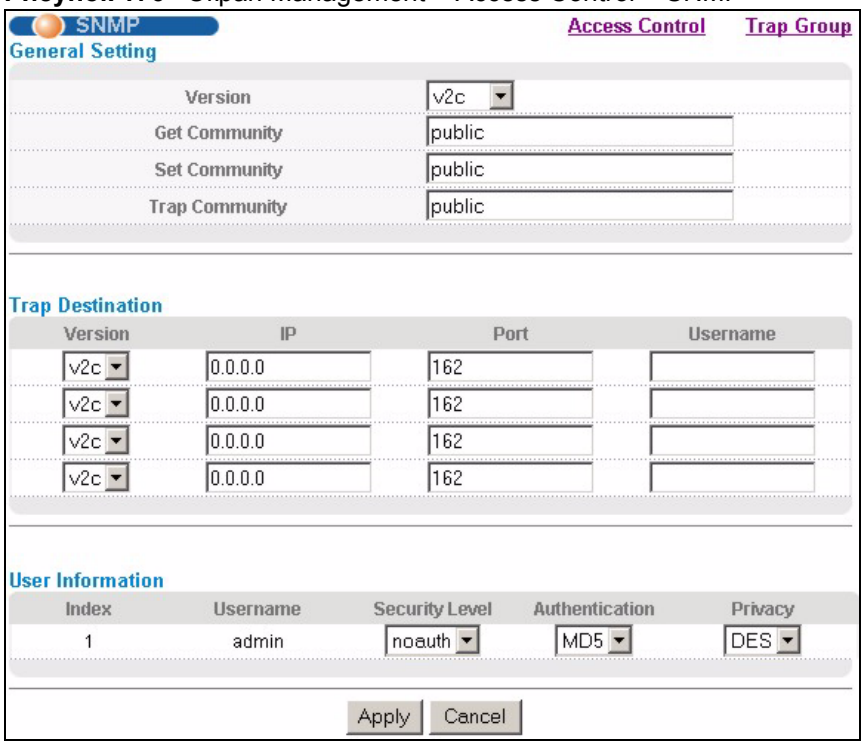
Таблица 119 Команды Trap протокола SNMP для коммутатора (Switch)

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.
	MRSTPNewRoot	1.3.6.1.4.1.890.1.5.8.24.43.2.1	Эта команда Trap отправляется при изменении корневого коммутатора MRSTP.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.8.24.107.70.1	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.
	MRSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.24.43.2.2	Эта команда Trap отправляется при изменении топологии MRSTP.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.24.107.70.2	Эта команда Trap отправляется при изменении топологии MSTP.
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.8.24.31.2.1	Эта команда Trap отправляется при использовании более 99% таблицы MAC-адресов.
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.8.24.31.2.2	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.

36.3.4 Настройка SNMP

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

Рисунок 176 Экран Management > Access Control > SNMP



Поля экрана описаны в следующей таблице.

Таблица 120 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 120 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.

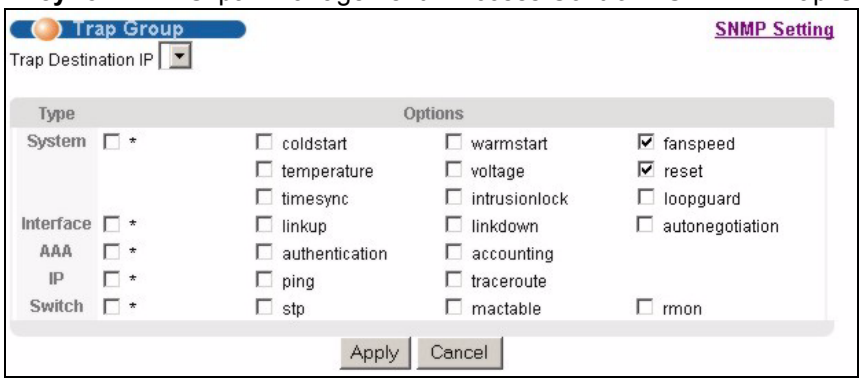
Таблица 120 Экран Management > Access Control > SNMP (продолжение)

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.

36.3.5 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 177 Экран Management > Access Control > SNMP > Trap Group



Поля экрана описаны в следующей таблице.

Таблица 121 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. 36.3.3 на стр. 323. 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 121 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.

36.3.6 Настройка учетных записей пользователей

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

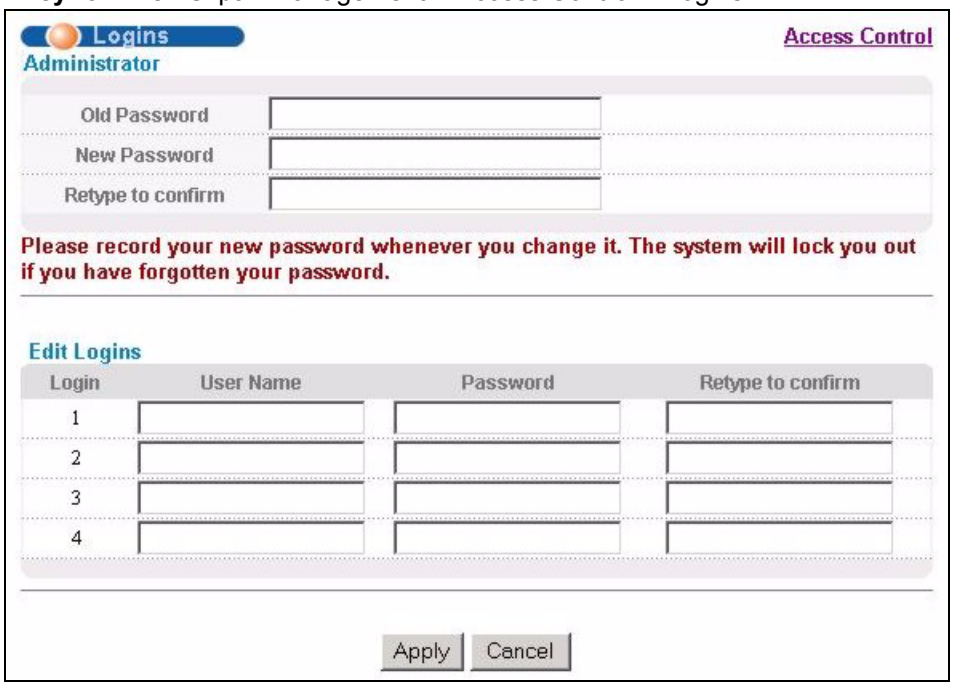
- Администратор – это пользователь, который может как просматривать, так и вносить изменения в настройки коммутатора. Имя пользователя для администратора не может быть изменено – это всегда **admin**. Пароль по умолчанию – **1234**.

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 открыть приведенный ниже экран, нажмите **Management > Access Control > Logins**.

Рисунок 178 Экран Management > Access Control > Logins



Поля экрана описаны в следующей таблице.

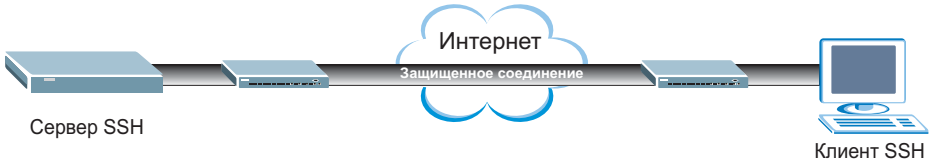
Таблица 122 Экран Management > Access Control > Logins

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. У этих пользователей будут права только на чтение. Более высокие привилегии могут назначаться пользователям через интерфейс командной строки.Дополнительную информацию об изменении привилегий можно найти в гл. 45 на стр. 369.	
User Name	Введите имя пользователя (до 32 символов ASCII).
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.

36.4 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 179 Пример связи по протоколу SSH



36.5 Как работает протокол SSH

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

Рисунок 180 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).

36.6 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.

36.6.1 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).

36.7 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).

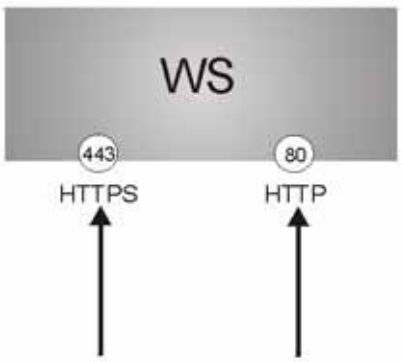
Этот протокол работает на основе сертификатов, открытых и секретных ключей.

Протокол HTTPS на коммутаторе используется для получения защищенного доступа к коммутатору через Web-конфигуратор. Протокол SSL предусматривает, что SSL-сервер (коммутатор) должен всегда предоставлять свою аутентификационную информацию SSL-клиенту (компьютеру, который запрашивает HTTPS-соединение с коммутатором), тогда как SSL-клиент должен проходить аутентификацию только по требованию SSL-сервера. Аутентификация клиентских сертификатов необязательна, и если она выбрана, то SSL-клиент должен отправить коммутатору сертификат. За сертификатом для браузера следует обращаться к поставщику сертификатов, являющемуся доверенным поставщиком сертификатов для коммутатора.

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 181 Реализация протокола HTTPS



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

36.8 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.

36.8.1 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 182 Диалоговое окно Security Alert (Internet Explorer)

36.8.2 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 183 Сертификат безопасности 1 (Netscape)

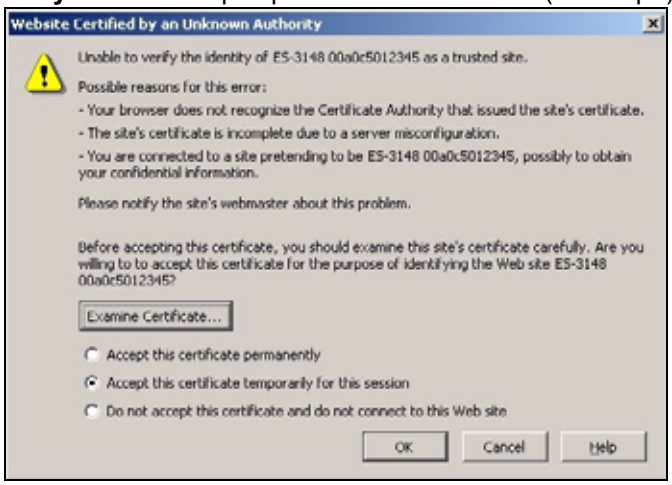
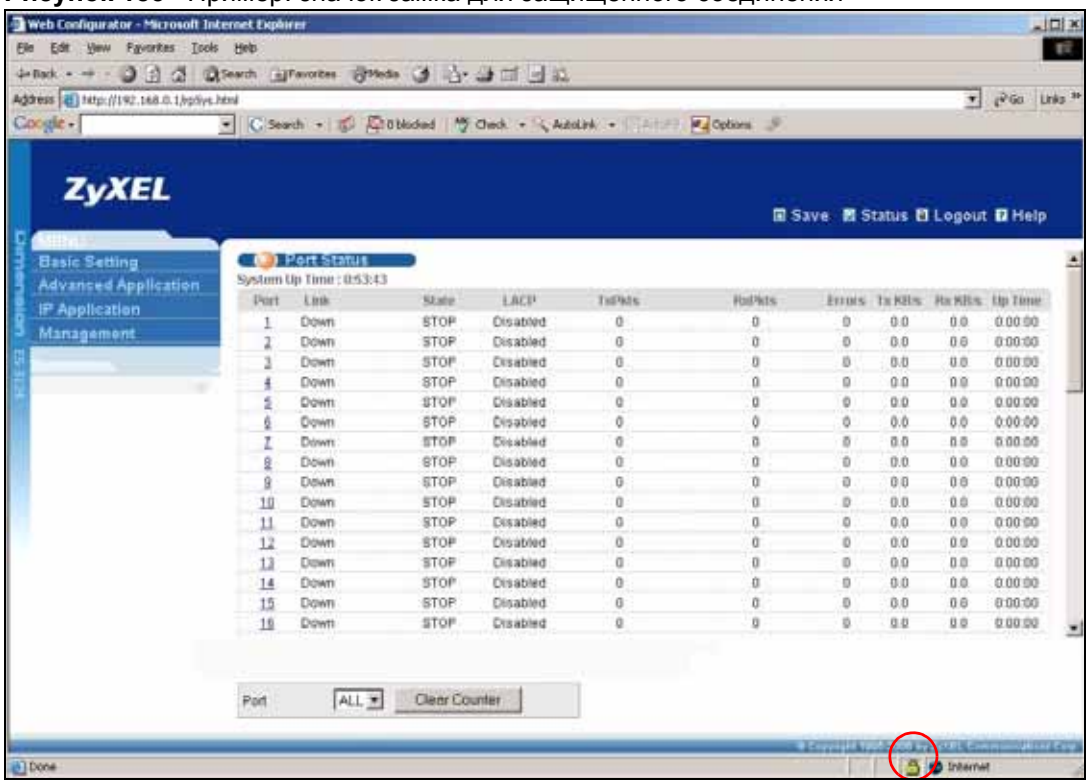


Рисунок 184 Сертификат безопасности 2 (Netscape)

36.8.3 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.

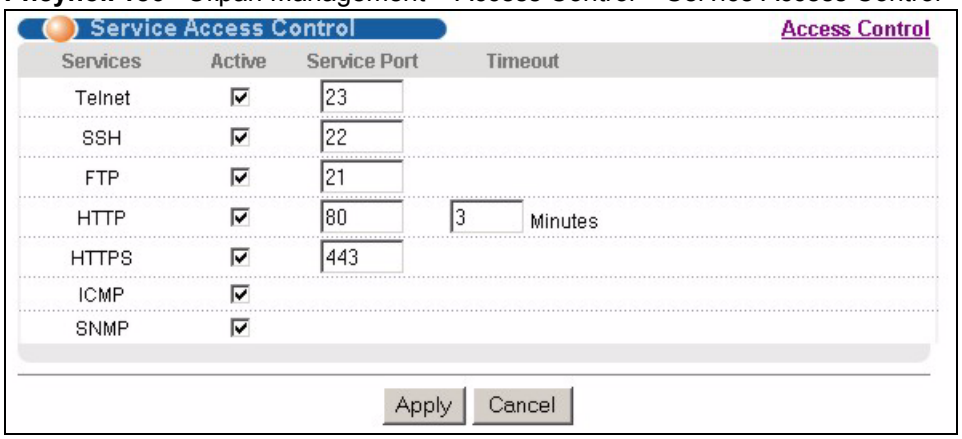
Рисунок 185 Пример: значок замка для защищенного соединения



36.9 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 186 Экран Management > Access Control > Service Access Control



Поля экрана описаны в следующей таблице.

Таблица 123 Экран Management > Access Control > Service Access Control

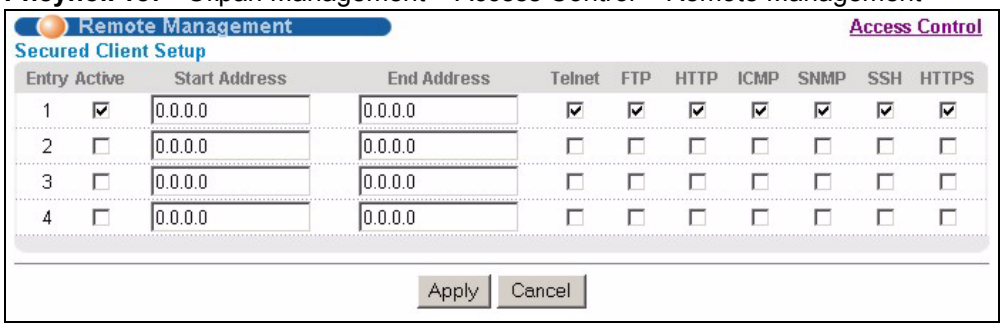
ПОЛЕ	ОПИСАНИЕ
Services	В этом столбце перечислены службы, с помощью которых можно получить доступ к коммутатору.
Active	Установите этот переключатель, чтобы разрешить соответствующей службе получать доступ к коммутатору.
Service Port	Номер порта службы по умолчанию для Telnet, SSH, FTP, HTTP или HTTPS; 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 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.

36.10 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 187 Экран Management > Access Control > Remote Management



Поля экрана описаны в следующей таблице.

Таблица 124 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.

37

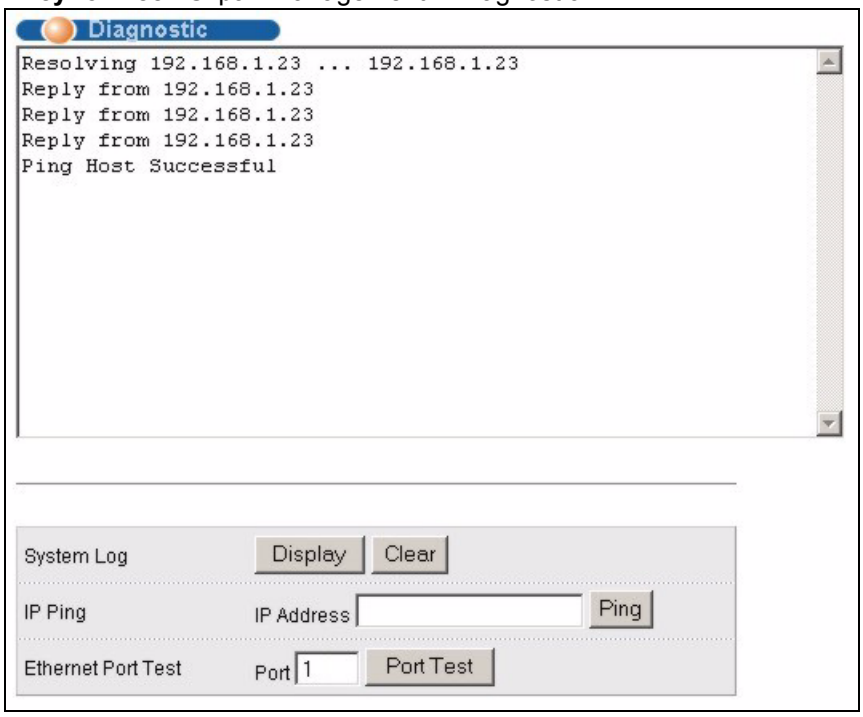
Диагностика

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

37.1 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 188 Экран Management > Diagnostic



Поля экрана описаны в следующей таблице.

Таблица 125 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.

38

Системный журнал Syslog

В данной главе описаны экраны системного журнала Syslog.

38.1 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.

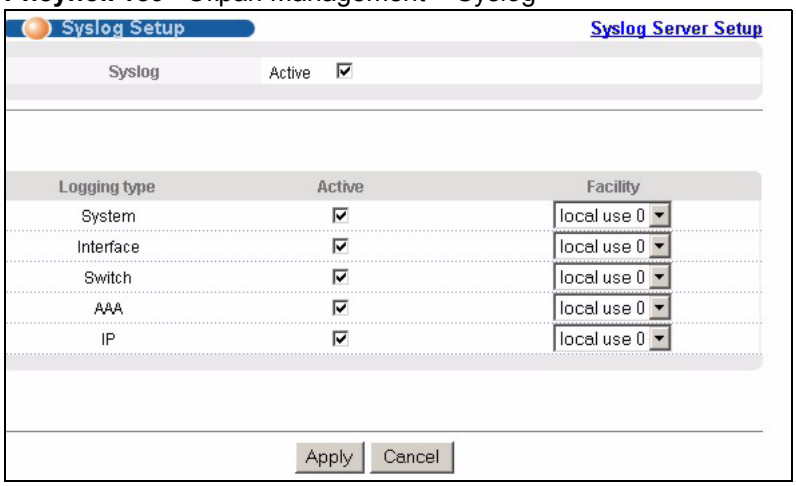
Таблица 126 Уровни серьезности Syslog

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.

38.2 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 189 Экран Management > Syslog



Поля экрана описаны в следующей таблице.

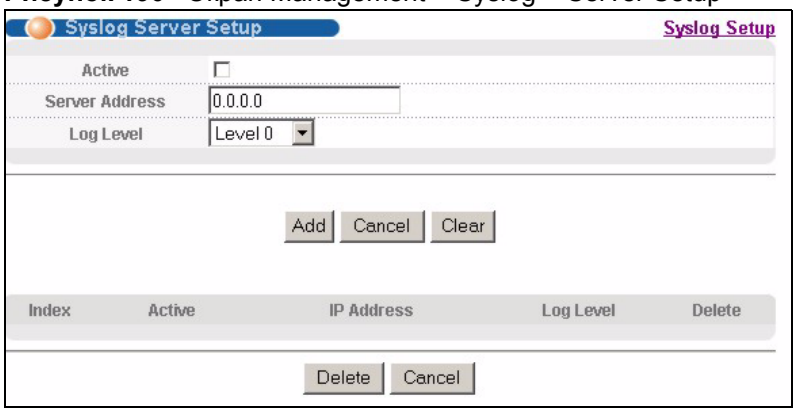
Таблица 127 Экран Management > Syslog

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.

38.3 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 190 Экран Management > Syslog > Server Setup



Поля экрана описаны в следующей таблице.

Таблица 128 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.

39

Управление кластерами

В данной главе описано управление кластерами.

39.1 Обзор управления кластерами

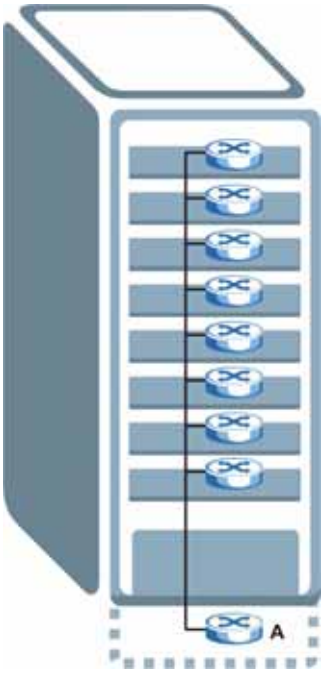
Управление кластерами позволяет управлять несколькими коммутаторами через один коммутатор, называемый менеджером кластера. Чтобы коммутаторы могли взаимодействовать друг с другом, они должны быть подключены напрямую и принадлежать к одной группе VLAN.

Таблица 129 Спецификации управления кластерами ZyXEL

Максимальное количество членов кластера	24
Модели членов кластера	Должны быть совместимы с реализацией управления кластерами ZyXEL.
Менеджер кластера	Это 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 191 Пример реализации кластера

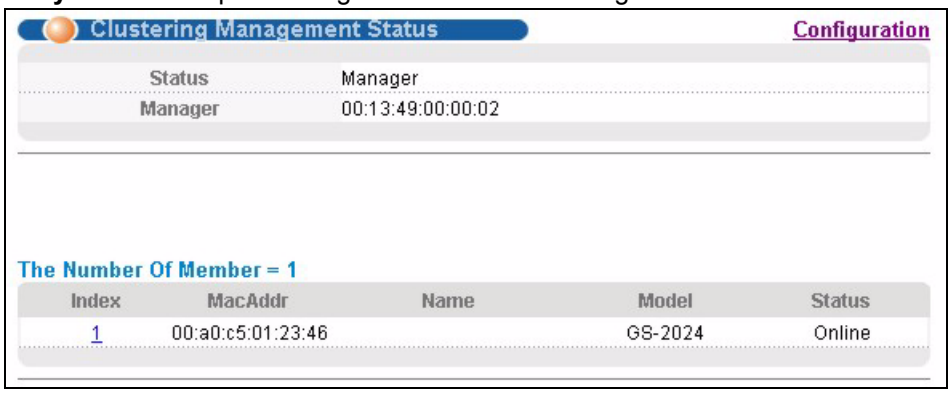


39.2 Состояние управления кластером

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

У кластера может быть только один менеджер.

Рисунок 192 Экран Management > Cluster Management



Поля экрана описаны в следующей таблице.

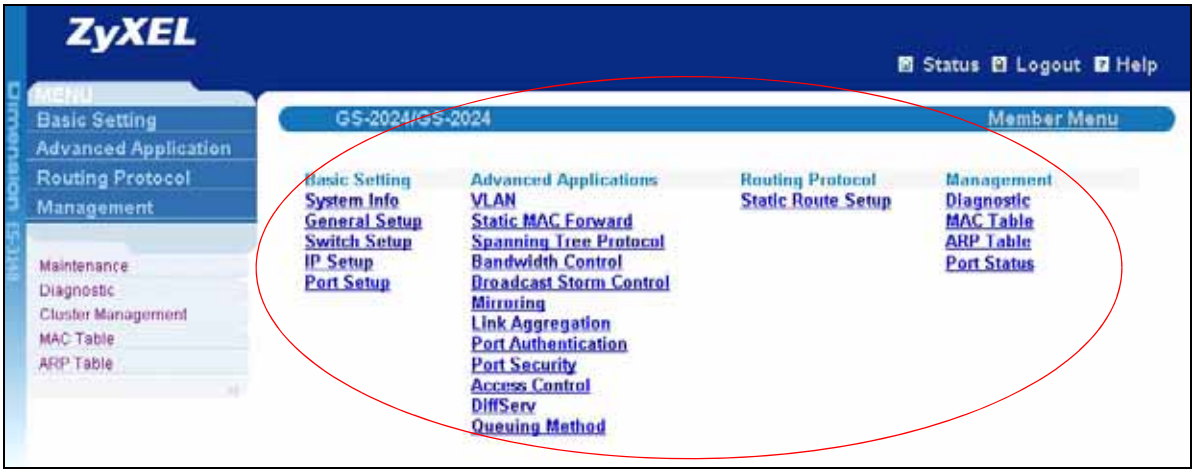
Таблица 130 Экран Management > Cluster Management

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. 193 на стр. 349).
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)

39.2.1 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 193 Управление кластером: экран Web-конфигуратора члена кластера



39.2.1.1 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 194 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 (192.168.0.1:(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.

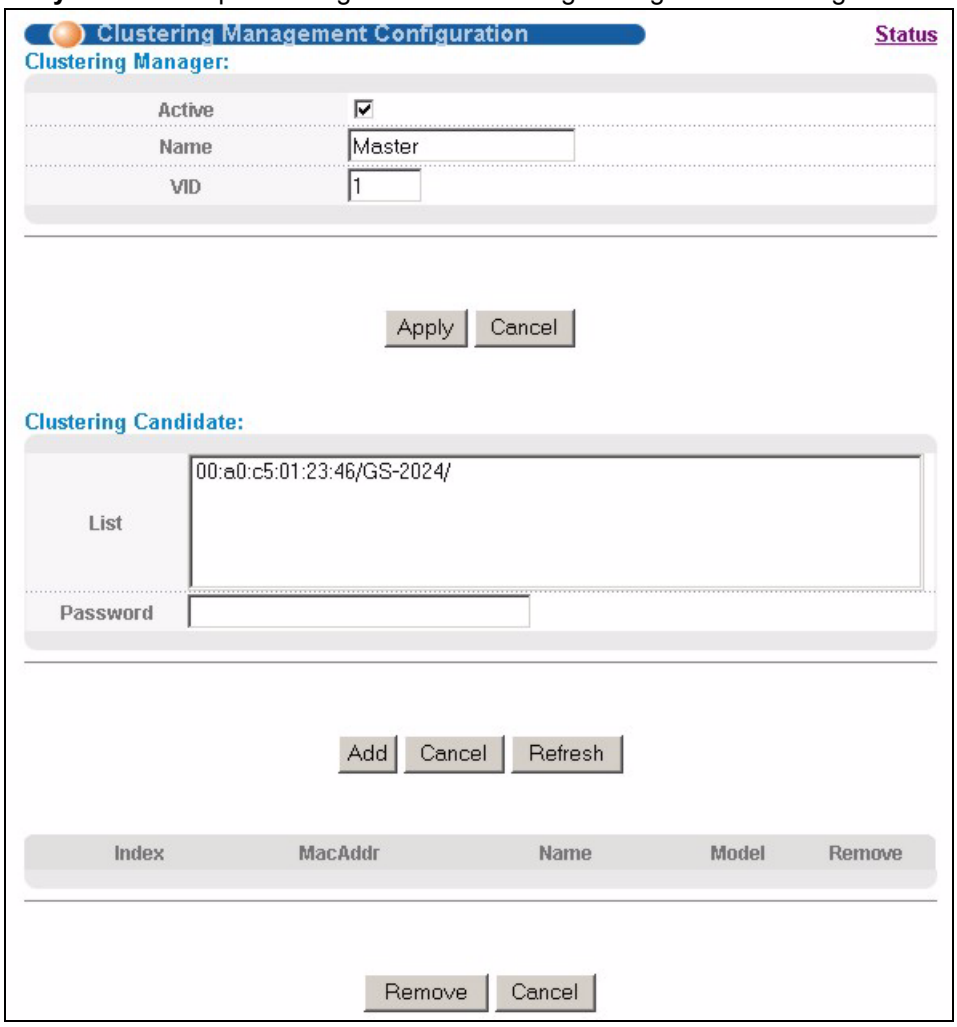
Таблица 131 Пример загрузки встроенного программного обеспечения на член кластера посредством FTP

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.

39.3 Настройка управления кластерами

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

Рисунок 195 Экран Management > Clustering Management > Configuration



Поля экрана описаны в следующей таблице.

Таблица 132 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 132 Экран Management > Clustering Management > Configuration

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 132 Экран Management > Clustering Management > Configuration

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.

40

Таблица MAC-адресов

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

40.1 Обзор таблицы MAC-адресов

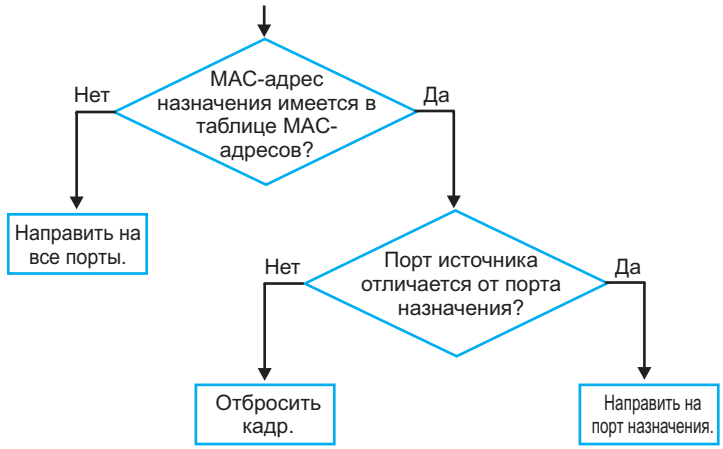
На экране настройки таблицы MAC-адресов **MAC Table** (которую еще называют базой данных фильтрации) можно увидеть, каким образом кадры пересылаются или фильтруются на портах коммутатора. На этом экране отображается, на какой порт (порты) передается MAC-адрес какого устройства, принадлежащего к какой 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.

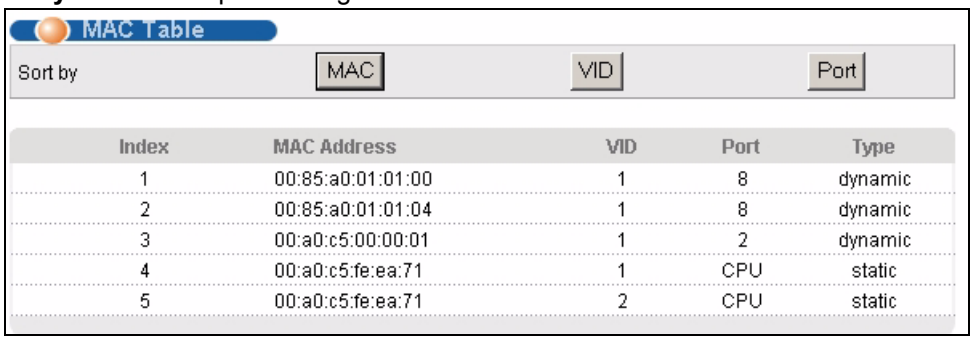
Рисунок 196 Схема работы таблицы MAC-адресов



40.2 Просмотр таблицы MAC-адресов

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

Рисунок 197 Экран Management > MAC Table



Поля экрана описаны в следующей таблице.

Таблица 133 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 133 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**).

41

Таблица IP-адресов

В данной главе описана таблица IP-адресов.

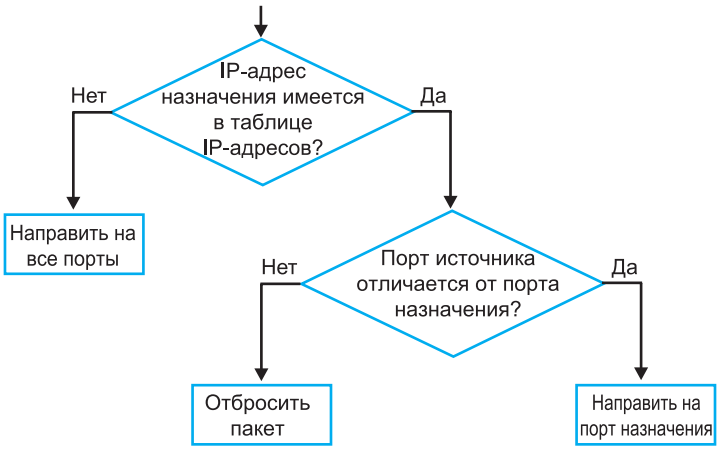
41.1 Обзор таблицы IP-адресов

На экране **IP Table** отображается информация о пересылке или фильтрации пакетов на портах коммутатора. На этом экране отображается, на какой порт (порты) передается IP-адрес какого устройства, принадлежащего к какой из групп VLAN (если они определены), и является ли IP-адрес динамическим (полученным коммутатором) или статическим (принадлежащим коммутатору).

Чтобы определить, куда направлять пакеты, коммутатор пользуется таблицей IP-адресов. См. следующий рисунок.

1. Данный коммутатор изучает полученный пакет и запоминает порт, на который пришел этот IP-адрес источника.
2. Затем коммутатор проверяет, соответствует ли IP-адрес назначения этого пакета IP-адресу источника, уже имеющемуся в таблице IP-адресов.
   - Если коммутатору уже известен порт для этого IP-адреса, то он направляет пакет на этот порт.
   - Если коммутатору еще не известен порт для этого IP-адреса, то пакет направляется на все порты сразу. Если таким образом направляется слишком много кадров, то происходит перегрузка сети.
   - Если коммутатору уже известен порт для IP-адреса, и порт назначения совпадает с портом источника, то этот пакет отбрасывается.

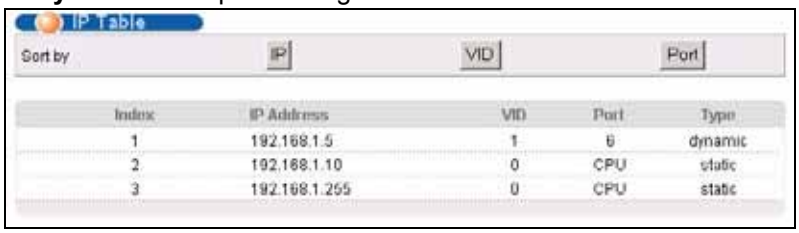
Рисунок 198 Схема работы таблицы IP-адресов



41.2 Просмотр таблицы IP-адресов

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

Рисунок 199 Экран Management > IP Table



Поля экрана описаны в следующей таблице.

Таблица 134 Экран Management > IP 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.
IP	Нажмите эту кнопку, чтобы отсортировать данные по IP-адресу.
VID	Нажмите эту кнопку, чтобы отсортировать данные по группе VLAN.
Port	Нажмите эту кнопку, чтобы отсортировать данные по номеру порта.
Index	В этом поле отображается порядковый номер.
IP Address	IP-адрес устройства, с которого поступают входящие пакеты.
VID	Группа VLAN, к которой принадлежит данный пакет.
Port	Номер порта, с которого был получен указанный выше IP-адрес. Для IP-адресов, принадлежащих коммутатору, в этом поле отображается **CPU**.
Type	В этом поле отображается тип IP-адреса – **dynamic** (динамический, то есть полученный коммутатором) или **static** (статический, принадлежащий коммутатору).

42

Таблица ARP

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

42.1 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.

42.1.1 Как работает протокол ARP

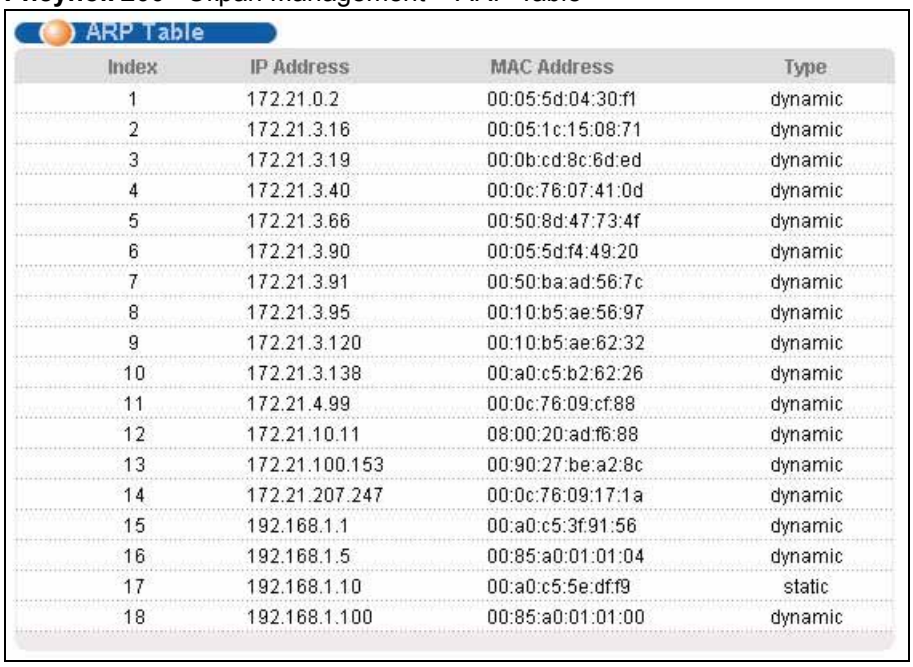
Когда входящий пакет, предназначенный для хост-устройства в локальной сети, прибывает на коммутатор, программа протокола ARP на коммутаторе ищет его в таблице ARP и, если адрес обнаружен, отправляет пакет на устройство.

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.

42.2 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 200 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 135 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**).

43

Таблица маршрутизации

В данной главе описана таблица маршрутизации.

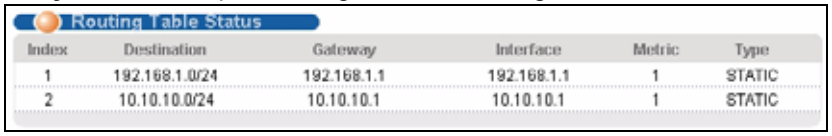
43.1 Обзор

В таблице маршрутизации содержится информация о маршрутах к сетям, доступным для коммутатора. Данный коммутатор автоматически обновляет таблицу маршрутизации с использованием информации RIP, получаемой от других устройств Ethernet.

43.2 Просмотр таблицы маршрутизации

На данном экране можно просмотреть информацию в таблице маршрутизации. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **Routing Table**.

Рисунок 201 Экран Management > Routing Table



Поля экрана описаны в следующей таблице.

Таблица 136 Экран Management > Routing Table

ПОЛЕ	ОПИСАНИЕ
Index	В этом поле отображается порядковый номер.
Destination	В этом поле отображается домен IP-маршрутизации пункта назначения.
Gateway	В этом поле отображается IP-адрес шлюза.
Interface	В этом поле отображается IP-адрес интерфейса.
Metric	В этом поле отображается стоимость маршрута.
Type	В этом поле отображается способ получения маршрута; **OSPF** – добавлен в качестве интерфейса OSPF, **RIP** – получен из поступающих пакетов RIP или **STATIC** – добавлен в виде статической записи.

44

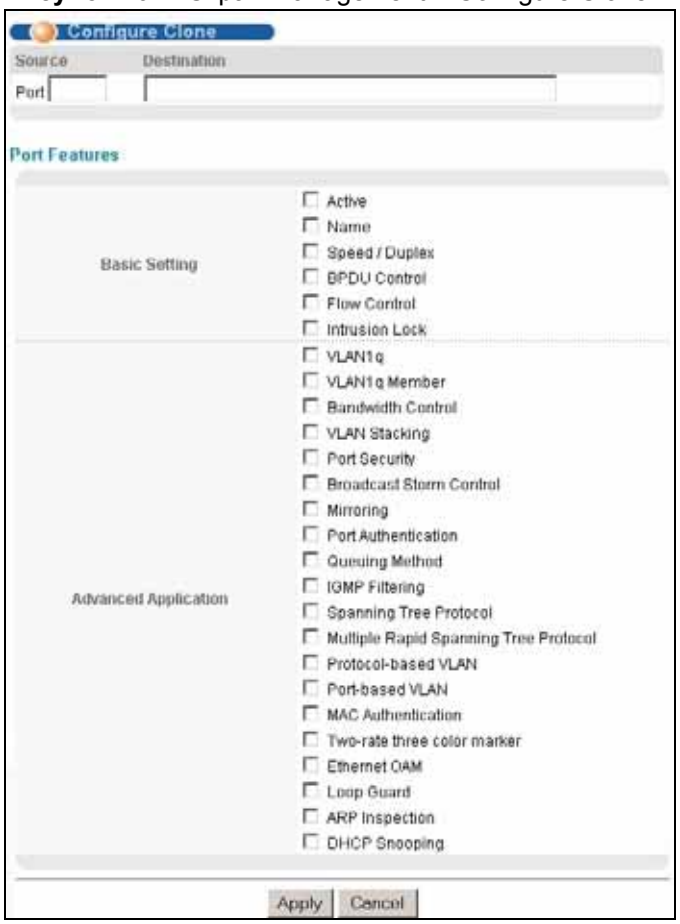
Настройка клонирования

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

44.1 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 202 Экран Management > Configure Clone



Поля экрана описаны в следующей таблице.

Таблица 137 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
Интерфейс командной строки и устранение неполадок

45

Знакомство с командами

В данной главе перечислены имеющиеся команды и приводится их краткое описание.

45.1 Обзор

В дополнение к Web-конфигуратору коммутатор можно настраивать и с помощью интерфейса командной строки. Интерфейс командной строки используется для расширенной диагностики и устранения неполадок коммутатора. При возникновении каких-либо проблем с коммутатором служба поддержки пользователей может попросить ввести некоторые команды, которые могут помочь в поиске неисправности.

Более подробную информацию по функциям, настраиваемым с помощью Web-конфигуратора, можно найти в соответствующей главе руководства пользователя.

45.2 Доступ к интерфейсу командной строки

Для получения доступа к интерпретатору команд коммутатора потребуется либо прямое консольное подключение, либо подключение через Telnet.

Данный коммутатор автоматически разрывает подключение к интерфейсу управления при отсутствии активности в течение пяти минут. Если это случилось, просто введите заново имя пользователя и пароль.

- По умолчанию допускается несколько сессий интерпретатора командной строки, либо через консольный порт, либо через Telnet. Однако при этом допускается не более девяти одновременных подключений.
- Чтобы разрешить вход в систему только одному пользователю в каждый момент времени, воспользуйтесь командой `configure multi-login` в режиме настройки. Наивысший приоритет имеет доступ через консольный порт.

45.2.1 Консольный порт

Подключение к консольному порту коммутатора производится с помощью программы-эмулятора терминала со следующими параметрами:

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

45.2.1.1 Начальный экран

После включения коммутатора он производит несколько внутренних операций по самодиагностике, а также инициализацию линии. Информацию об инициализации можно просмотреть через консольный порт. После инициализации появится экран входа в систему, то есть ввода имени пользователя и пароля (см. разд. 45.3 на стр. 370).

```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:13:49:00:00:01
initialize switch, ethernet address: 00:13:49:00:00:02
Initializing switch unit 0...
Initializing MSTP.............
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Press ENTER to continue...
```

Для подключения к коммутатору через Telnet выполните следующие действия.

1. Чтобы воспользоваться локальным управлением, подключите компьютер к порту управления RJ-45 (обозначенный как **MGMT**) на коммутаторе.
2. Убедитесь, что IP-адрес компьютера и IP-адрес коммутатора принадлежат к одной подсети. В ОС Windows нажмите кнопку **Start** («Пуск», обычно находится в левом нижнем углу), выберите пункт **Run** («Выполнить»), затем введите `telnet 192.168.0.1` (IP-адрес управления по умолчанию) и нажмите **OK**.
3. Появится экран входа в систему (см. разд. 45.3 на стр. 370).

45.3 Экран входа в систему

После успешного подключения к коммутатору напрямую через консольный порт или через Telnet появится экран входа в систему (ввода имени пользователя и пароля), показанный ниже. При первом подключении введите имя пользователя и пароль администратора по умолчанию – «admin»и «1234».

```
Enter User Name : admin
Enter Password : XXXX
```

45.4 Соглашения в отношении синтаксиса команд

Правила ввода команд описаны ниже.

- Для ключевых слов команд используется `шрифт courier new`.
- Обязательные поля команды, в которые необходимо внести какие-либо данные, обозначены угловыми скобками <>, например, строка `ping <ip-адрес>` означает, что для этой команды необходимо указать IP-адрес.
- Необязательные для заполнения поля команды обозначены квадратными скобками, [], например, строка

```
configure snmp-server [contact <системный контакт>] [location <расположение системы>]
```

  означает, что поля contact и location заполнять не обязательно.
- «Команда» – это команда, введенная в интерфейсе командной строки.
- Символ | означает «или».
- Элемент <cr> в командной строке означает возврат каретки. Для выполнения команды нажмите [ENTER] или возврат каретки после ввода команды.
- Для прокрутки истории команд используйте стрелки «вверх» и «вниз».
- Можно ввести уникальную часть команды и нажать [TAB] – тогда коммутатор сам подставит оставшуюся часть. Например, если ввести «`config`»и нажать [TAB], то автоматически появится полная команда «configure».
- Интерфейс – это отдельный Ethernet-порт коммутатора. Команды, настроенные после команды интерфейса, относятся к этим портам.
- Можно ввести несколько портов или диапазонов портов, разделенных запятыми. Диапазоны номеров портов разделяются тире.

45.5 Изменение пароля

Данная команда используется для изменения пароля привилегированного режима (Enable). По умолчанию для доступа к интерфейсу командной строки (CLI), привилегированному режиму (Enable) и режиму настройки (Config) интерфейса CLI используется один и тот же пароль.

С помощью данной команды изменяется пароль, необходимый для входа в привилегированный режим (Enable) и режим настройки (Config).

Синтаксис:

```
password <пароль>
```

Где

`password <пароль>`	=	новый пароль (до 32 алфавитно-цифровых символов) для доступа к привилегированному режиму и режиму настройки.

45.6 Создание нового IP-интерфейса

Чтобы создать новый IP-интерфейс (подходящий для вашей сети) для VLAN 1, воспользуйтесь командой `ip address`. После создания IP-интерфейса данный IP-адрес можно использовать для управления коммутатором. В следующем примере показано создание IP-интерфейса для IP-адреса 172.23.0.1 с маской подсети 255.255.255.0:

```
sysname# config
sysname(config)# vlan 1
sysname(config-vlan)# ip address 172.23.0.1 255.255.255.0
```

45.7 Уровни привилегий

Пользователь имеет доступ только к тем командам, у которых уровень привилегий меньше или равен уровню привилегий учетной записи пользователя. Например, если для учетной записи установлен уровень привилегий 12, пользователь с этой учетной записью может использовать все команды с уровнями привилегий от 0 до 12. Команды с уровнем привилегий 0 доступны для всех учетных записей.

Если для аутентификации пользователей задействован внешний сервер RADIUS, для определения уровня привилегий учетной записи на сервере RADIUS можно использовать специальный атрибут производителя VSA (Vendor Specific Attribute). Дополнительную информацию можно найти в разд. 23.2.4 на стр. 215.

Для присвоения уровней привилегий учетным записям служат следующие команды.

Синтаксис:

```
logins username <имя-пользователя> password <пароль>
logins username <имя-пользователя> privilege <0-14>
```

Где

`username <имя-пользователя>`	=	Определяет имя нового пользователя (до 32 алфавитно-цифровых символов). Для изменения существующей учетной записи введите соответствующее имя пользователя.
`password <пароль>`	=	Определяет новый пароль (до 32 алфавитно-цифровых символов) для данного пользователя.
`privilege <0-14>`	=	Определяет уровень привилегий для пользователя.

45.8 Командные режимы

Существует три командных режима: пользовательский (**User**), привилегированный (**Enable**) и режим настройки (**Configure**). Доступные пользователю режимы (и команды) зависят от уровня привилегий учетной записи. Более подробную информацию о настройке уровней привилегий можно найти в разд. 45.7 на стр. 372.

При первом входе в интерпретатор командной строки с использованием учетной записи, имеющий права только на чтение (с уровнем привилегий 0-12), первоначально устанавливается пользовательский (User) режим. Команды пользовательского режима являются подмножеством команд привилегированного режима (Enable). Приглашение ввести команду в пользовательском режиме заканчивается угловой скобкой (>).

Для входа в привилегированный (Enable) режим введите `enable` и после запроса – пароль администратора (по умолчанию – 1234). При входе в привилегированный режим приглашение меняется на знак решетки (`#`). Если вход в интерпретатор командной строки осуществляется в качестве администратора, привилегированный командный режим (Enable) устанавливается автоматически.

Режимы интерпретатора командной строки и доступ к режимам описаны в следующей таблице.

Таблица 138 Сводка по режимам интерпретатора командной строки

РЕЖИМ	ОПИСАНИЕ	ВХОД/ДОСТУП	ПРИГЛАШЕНИЕ
User	Доступные в этом режиме команды являются подмножеством команд привилегированного режима (Enable). С помощью этих команд можно выполнить базовые тесты и получить общую информацию о системе.	Для учетной записи, имеющей права только на чтение, этот режим используется по умолчанию.	`sysname>` Первая часть приглашения представляет собой имя системы. В данном Руководстве пользователя в примерах работы с интерфейсом командной строки в качестве имени системы везде используется «sysname».
Enable	Команды данного режима позволяют сохранять настройки конфигурации, сбрасывать настройки конфигурации, а также отображать более детальную информацию о системе. В этом режиме имеется также команда `configure`, с помощью которой осуществляется переключение в режим настройки.	Этот режим используется по умолчанию учетных записей с уровнем привилегий 13 или 14. Пользователям с учетными записями, имеющими права только на чтение (с уровнем привилегий 0 -12), для входа в привилегированный режим необходимо ввести команду `enable` и пароль привилегированного режима.	`sysname#`
Config	Команды этого режима позволяют изменять глобальные настройки коммутатора.	В привилегированном режиме необходимо ввести команду `config`.	`sysname(config)#`

Таблица 138 Сводка по режимам интерпретатора командной строки (продолжение)

РЕЖИМ	ОПИСАНИЕ	ВХОД/ДОСТУП	ПРИГЛАШЕНИЕ
Перечисленные ниже командные режимы представляют собой подрежимы режима настройки и доступны только из режима настройки.			
Config-vlan	Данный подрежим режима настройки позволяет изменять параметры виртуальных локальных сетей VLAN.	Введите `vlan` и номер (от 1 до 4094). Например, `vlan 10` для редактирования настроек виртуальной локальной сети VLAN 10.	`sysname(config-vlan)#`
Config-interface	Данный подрежим режима настройки позволяет изменять параметры портов.	Введите `interface port-channel` и номер порта. Например, `interface port-channel 8` для редактирования настроек порта 8 коммутатора.	`sysname(config-interface)#`
Config-mvr	Данный подрежим режима настройки позволяет изменять параметрыVLANмультивещания.	Чтобы войти в режиме `MVR`, введите `mvr` и идентификатор сети VLAN (от 1 до 4094). Например, введите `mvr 2` для редактирования настроек мультивещания VLAN 2.	`sysname(config-mvr)#`

Чтобы выйти из текущего режима, введите `exit`; для выхода из интерпретатора командной строки введите `logout`.

45.9 Получение помощи

Система включает в себя справку, в которой содержится следующая информация о командах:

- Список доступных команд, разделенных на группы.
- Подробное описание каждой команды.

45.9.1 Список доступных команд

Чтобы отобразить список имеющихся команд и соответствующих им подкоманд, введите «help».

```
sysname> help
  Commands available:
  help
  logout
  exit
  history
  enable
  show ip <cr>
  show hardware-monitor <C|F>
  show system-information
  show alarm-status
  show cpu-utilization
  show version flash
  show version <cr>
  ping <ip|host-name> <cr>
  ping <ip|host-name> [vlan <vlan-id>][..]
  ping help
  traceroute <ip|host-name> <cr>
  traceroute <ip|host-name> [vlan <vlan-id>][..]
  traceroute help
  ssh <1|2> <[user@]dest-ip> <cr>
  ssh <1|2> <[user@]dest-ip> [command </>]
sysname>
```

Введите «?», чтобы отобразить список команд, которые можно использовать.

```
sysname> ?
    enable                    Turn on privileged commands
    exit                      Exit from the EXEC
    help                      Description of the interactive help system
    history                   Show a list of previously run commands
    logout                    Exit from the EXEC
    ping                      Exec ping
    show                      Show system information
    ssh                       SSH client
    traceroute                Exec traceroute
sysname>
```

Чтобы отобразить подробную информацию о подкомандах и параметрах команды, введите `<команда> help`.

```
sysname> ping help
  Commands available:

  ping <ip|host-name>
    <
      [ in-band|out-of-band|vlan <vlan-id> ]
      [ size <0-1472> ]
      [ -t ]
    >
sysname>
```

Введите `<команда> ?`, чтобы отобразить подробную справку по команде, ее подкомандах и параметрах.

```
sysname> ping ?
    <ip|host-name>       destination ip address
    help                      Description of ping help

sysname>
```

45.10 Использование истории команд

Данный коммутатор хранит в своей памяти последние использовавшиеся команды. Любые команды, хранящиеся в истории, можно использовать повторно, прокрутив экран стрелками вверх (↑) или вниз (↓) и нажав [ENTER]. Для отображения списка использовавшихся команд введите команду history.

```
sysname> history
  enable
  exit
  show ip
  history
sysname>
```

45.11 Сохранение конфигурации

После изменения настроек коммутатора с помощью соответствующих команд можно сохранить эти изменения, набрав команду `write memory`.

Команда `write memory` недоступна в пользовательском режиме.

После окончания каждой сессии работы с интерфейсом командной строки необходимо сохранять изменения. Все несохраненные настройки будут сброшены после перезагрузки коммутатора.

```
sysname# write memory
```

45.11.1 Файл конфигурации коммутатора

При настройке коммутатора с помощью интерфейса командной строки или Web-конфигуратора эти настройки сохраняются в виде серии команд в специальном файле на коммутаторе. С файлом конфигурации можно выполнить следующие действия:

- Сохранить резервную копию конфигурации коммутатора после настройки коммутатора для работы в сети.
- Восстановить конфигурацию коммутатора.
- Использовать один файл для установки одинаковых настроек на всех коммутаторах (одной модели) в сети.

Кроме того, в файл конфигурации можно вносить изменения с помощью текстового редактора.

Добавляемые команды должны быть корректными. Данный коммутатор не будет работать с файлом конфигурации, содержащим неверные или неполные команды.

45.11.2 Отключение

Чтобы покинуть интерфейс командной строки, наберите в пользовательском или привилегированном режиме команду `exit` или `logout`. В режиме настройки команда `exit` осуществляет выход из режима настройки в привилегированный режим, а команда `logout` – выход из интерфейса командной строки.

45.12 Обзор команд

В последующих разделах приводятся доступные команды коммутатора с кратким описанием каждой команды. Команды, перечисленные в таблице, располагаются в том же порядке, что и в интерфейсе командной строки. Более подробную информацию можно найти в соответствующих разделах руководства пользователя.

45.12.1 Пользовательский режим

Команды, доступные в пользовательском режиме, описаны в следующей таблице.

Таблица 139 Обзор команд: пользовательский режим

КОМАНДА		ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
`help`		Отображает справку по командам.	0
`logout`		Осуществляет выход пользователя из интерфейса командной строки.	0
`exit`		Осуществляет выход из интерфейса командной строки.	0
`history`		Отображает список ранее введенных команд. Данный коммутатор может хранить в своей памяти до 256 команд.	0
`enable`		Осуществляет вход в привилегированный режим. См. разд. 45.12.2 на стр. 379. Включает наивысший уровень привилегий при исполнении команд.	0
	`<0-14>`	Доступ к командам привилегированного режима с уровнем привилегий не выше указанного. См. разд. 45.12.2 на стр. 379.	0
`show`	`ip`	Отображает информацию по протоколу IP.	0
	`hardware-monitor <C|F>`	Отображает текущую информацию аппаратного мониторинга в указанных единицах измерения температуры (в градусах по Цельсию **C** или по Фаренгейту **F**).	0
	`system-information`	Отображает общую информацию о системе.	0
	`alarm-status`	Отображает, какие сигналы тревоги включены на коммутаторе, а также состояние светодиодов для сигналов тревоги.	0
	`cpu-utilization`	Отображает статистику по загрузке CPU на коммутаторе.	0
	`version flash`	Отображает версию установленного на данный момент встроенного программного обеспечения во flash-памяти.	0
	`version <cr>`	Отображает версию встроенного программного обеспечения, работающего на коммутаторе на данный момент.	0
`ping`	`<ip-адрес|имя-хоста>`	Отправляет ping-запрос на Ethernet-устройство.	0

Таблица 139 Обзор команд: пользовательский режим (продолжение)

КОМАНДА		ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	<IP-адрес|имя-хоста> [vlan <идентификатор-vlan>] [size <0-1472>] [-t]	Отправляет ping-запрос на Ethernet-устройство в указанной VLAN и с заданными параметрами.	0
	help	Отображает справку по командам.	0
traceroute	<ip-адрес|имя-хоста>	Определяет путь, который проходит пакет до указанного устройства.	0
	<ip-адрес|имя-хоста> [vlan <идентификатор-vlan>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Определяет путь, который проходит пакет до устройства в указанной VLAN.	0
	help	Отображает справку по командам.	0
ssh	<1|2> <[user@]ip-адрес-назначения>	Осуществляет подключение к серверу SSH с указанной версией протокола SSH.	0

45.12.2 Привилегированный режим

Команды, доступные в привилегированном режиме, описаны в следующей таблице.

Таблица 140 Обзор команд: привилегированный режим

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
baudrate <1|2|3|4|5>			Изменяет скорость консольного порта. Доступные параметры: 1 (9600 бод), 2 (19 200), 3(38 400), 4 (57 600) и 5 (115 200).	13
boot	config <номер>		Перезапуск системы с использованием указанного файла конфигурации.	13
cable-diagnostics	<список-портов>		Запускает тестирование физических пар проводников в соединениях Ethernet на указанных портах.	13
clear	arp inspection	filter	Удаляет все фильтры инспекции ARP-пакетов на коммутаторе.	13
	arp inspection	log	Удаляет все записи контрольного журнала инспекции ARP-пакетов на коммутаторе.	13
	arp inspection	statistics	Удаляет все записи статистики ARP-пакетов, проходящих через коммутатор.	13

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	arp inspection	statistics vlan <список-vlan>	Удаляет все записи статистики ARP-пакетов, проходящих через коммутатор, для указанных VLAN.	13
	dhcp snooping database	statistics	Удаляет все записи статистики DHCP-пакетов, проходящих через коммутатор.	13
	loopguard		Сбрасывает счетчики защиты от образования петель.	13
configure			Доступ в режим настройки. См. разд. 45.12.3 на стр. 393.	13
copy	running-config tftp <ip-адрес> <удаленный-файл>		Осуществляет резервное копирование текущей конфигурации на указанный сервер TFTP в файл с указанным именем.	13
	running-config interface port-channel <порт> <список-портов>		Клонирует (копирует) атрибуты указанного порта на другие порты.	13
	running-config interface port-channel <порт> <список-портов>	[bandwidth-limit ....]	Копирует указанные атрибуты с одного порта на другие.	13
	tftp	config <номер> <ip-адрес> <удаленный-файл>	Восстанавливает конфигурацию из указанного файла, расположенного на указанном сервере TFTP, в файл конфигурации на маршрутизаторе с указанным номером.	13
		flash <ip-адрес> <удаленный-файл>	Восстанавливает встроенное программное обеспечение с сервера TFTP.	13
disable			Осуществляет выход из привилегированного режима.	13
enable			Осуществляет вход в привилегированный режим. См. разд. 45.12.2 на стр. 379. Включает наивысший уровень привилегий при исполнении команд.	0

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	<0-14>		Доступ к командам привилегированного режима с уровнем привилегий не выше указанного. См. разд. 45.12.2 на стр. 379.	0
erase	running-config		Возврат к заводским настройкам по умолчанию.	13
		help	Отображает справку по данной команде.	13
		interface port-channel <список-портов>	Возврат к заводским настройкам по умолчанию на уровне отдельных портов.	13
		interface port-channel <список-портов> [bandwidth-limit...]	Возврат к заводским настройкам по умолчанию на уровне отдельных портов, а также опционально лишь для указанных функций настройки.	13
ethernet oam	remote-loopback test <порт>	[<количество пакетов> [<размер пакета>]]	Осуществляет тестирование указанного порта с использованием обратной петли, опционально можно указать количество пакетов и размер пакетов, отправляемых при тестировании обратной петли.	13
exit			Осуществляет выход из привилегированного режима.	0
help			Отображает справку по командам.	0
history			Отображает список ранее введенных команд.	0
igmp-flush			Удаление всей информации IGMP.	13
kick	tcp <идентификатор сессии>		Разъединяет указанную сессию TCP.	13
logout			Осуществляет выход из привилегированного режима.	0
mac-flush			Очистка таблицы MAC-адресов.	13

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	<номер-порта>		Удаляет все запомненные MAC-адреса на указанном порту (портах).	13
no	arp		Стирает записи в таблице ARP.	13
	arp	inspection filter <mac-адрес> vlan <идентификатор-vlan>	Укажите запись функции инспекции ARP-пакетов, которую необходимо удалить с коммутатора. Запись функции инспекции ARP-пакетов идентифицируется по MAC-адресу и идентификатору VLAN.	13
	interface	<номер-порта>	Сбрасывает все счетчики статистики для указанного порта.	13
	logging		Отключает ведение системного журнала.	13
ping <IP-адрес|имя-хоста>			Отправляет ping-запрос на Ethernet-устройство.	0
	[vlan <идентификатор-vlan>][..]		Отправляет ping-запрос на Ethernet-устройство в указанной VLAN.	13
reload	config <номер>		Перезапуск системы и использование указанного файла конфигурации.	13
renew dhcp snooping database			Загружает динамические привязки из базы данных отслеживания DHCP, используемой по умолчанию.	13
renew dhcp snooping database	<tftp://хост/имя-файла>		Загружает динамические привязки из указанной базы данных отслеживания DHCP.	13
show	aaa	authentication	Отображает, включены ли на коммутаторе аутентификация и проверка уровня привилегий, а также используемые для аутентификации методы.	3
		authentication enable	Отображает метод(ы) аутентификации для проверки уровня привилегий администраторов.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`authentication login`	Отображает методы аутентификации для учетных записей администраторов.	3
		`accounting`	Отображает настройки учета на коммутаторе.	3
		`accounting commands`	Отображает настройки учета для регистрации событий по командам.	3
		`accounting dot1x`	Отображает настройки учета для регистрации событий IEEE 802.1x.	3
		`accounting exec`	Отображает настройки учета для регистрации сеансов администрирования через SSH, Telnet или консольный порт.	3
		`accounting system`	Отображает настройки учета для регистрации системных событий, например, отключения, запуска, включения или отключения учета.	3
		`accounting update`	Отображает период обновления, настроенный на коммутаторе для сеансов учета.	3
	`alarm-status`		Отображает состояние и настройки сигналов тревоги.	0
	`arp inspection`		Отображает детали настройки инспекции ARP-пакетов.	3
		`filter`	В данном поле отображается текущий список фильтров MAC-адресов, созданных коммутатором в связи с обнаружением несанкционированных пакетов ARP.	3
		`filter [<mac-адрес>] [vlan <идентификатор-vlan>]`	Отображает текущий список фильтров MAC-адресов, содержащих указанный MAC-адрес или идентификатор VLAN.	3
		`interface port-channel <список-портов>`	Отображает настройки инспекции ARP-пакетов на указанном порту (портах).	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		log	Отображает настройки контрольного журнала на коммутаторе. Также отображает записи контрольного журнала, записанные на коммутаторе.	3
		statistics	Отображает статистику по общему количеству ARP-пакетов, полученных коммутатором.	3
		statistics vlan <список-vlan>	Отображает статистику по общему количеству ARP-пакетов, полученных коммутатором для указанных VLAN.	3
		vlan <список-vlan>	Отображает настройки инспекции ARP-пакетов для указанных VLAN.	3
	classifier		Отображает всю информацию, относящуюся к классификации.	3
		[имя]	Отображает информацию по указанному правилу классификации.	3
	cluster		Отображает состояние управления кластерами.	3
		candidates	Отображает информацию по кандидатам в члены кластера.	3
		member	Отображает MAC-адреса членов кластера.	3
		members config	Отображает настройки членов кластера.	3
		member mac <mac-адрес>	Отображает состояние членов кластера.	3
	cpu-utilization		Отображает статистику загрузки CPU на коммутаторе.	0
	dhcp	relay <идентификатор-vlan>	Отображает настройки агента ретрансляции DHCP.	3
		server	Отображает настройки сервера DHCP.	3
		server <идентификатор-vlan>	Отображает настройки сервера DHCP в указанной VLAN.	3
		smart-relay	Отображает глобальные настройки агента ретрансляции DHCP.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`snooping`	Отображает настройки отслеживания DHCP на коммутаторе.	3
		`snooping binding`	Отображает таблицу привязок DHCP.	3
		`snooping database`	Отображает статистику обновлений и настройки базы данных отслеживания DHCP.	3
		`snooping database detail`	Отображает статистику обновлений базы данных отслеживания DHCP в подробном виде.	3
	`diffserv`		Отображает общие настройки DiffServ.	3
	`ethernet oam`	`discovery <список-портов>`	Отображает детали настройки OAM и операционный статус указанных портов.	3
	`ethernet oam`	`statistics <список-портов>`	Отображает количество пакетов OAM, переданных для указанных портов.	3
	`ethernet oam`	`summary`	Отображает детали настройки каждого из портов с активированным OAM.	3
	`garp`		Отображает информацию по протоколу GARP.	3
	`hardware-monitor`	`<C|F>`	Отображает текущую информацию аппаратного мониторинга в указанных единицах измерения температуры (в градусах по Цельсию C или по Фаренгейту F).	0
	`https`		Отображает информацию по протоколу HTTPS.	3
		`certificate`	Показывает сертификаты HTTPS.	3
		`key <rsa|dsa>`	Показывает ключ HTTPS.	3
		`session`	Отображает текущие HTTPS-сессии.	3
		`timeout`	Отображает значение тайм-аута HTTPS-сессии.	3
	`igmp-filtering`	`profile`	Отображает настройки профиля фильтрации IGMP.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	igmp-snooping		Отображает глобальные настройки отслеживания многоадресного трафика IGMP.	3
		vlan	Отображает сети VLAN, в которых активировано отслеживание многоадресного трафика IGMP.	3
		querier	Отображает настройки Query-режима IGMP для каждого порта.	3
	interfaces <номер-порта>		Отображает текущее состояние интерфейса.	3
	interfaces config <список-портов>		Отображает текущие настройки интерфейса.	3
		bandwidth-control	Отображает настройки управления пропускной способностью.	3
		bstorm-control	Отображает настройки контроля широковещательных штормов.	3
		egress	Отображает информацию по исходящему порту.	3
		igmp-filtering	Отображает настройки фильтрации многоадресного трафика IGMP.	3
		igmp-group-limited	Отображает лимит числа групп IGMP.	3
		igmp-immediate-leave	Отображает настройки режима немедленного отключения IGMP для порта.	3
		igmp-query-mode	Отображает настройки Query-режима IGMP на указанном порту (портах).	3
		protocol-based-vlan	Отображает настройки VLAN на основе протоколов для указанного порта (портов).	3
	ip		Отображает информацию по протоколу IP.	0
		arp	Отображает таблицу протокола ARP.	3
		dvmrp group	Отображает информацию о группе DVMRP.	3
		dvmrp interface	Отображает информацию об интерфейсе DVMRP.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`dvmrp neighbor`	Отображает информацию о соседних устройствах DVMRP.	3
		`dvmrp prune`	Отображает информацию об отсечении для DVMRP.	3
		`dvmrp route`	Отображает маршруты DVMRP.	3
		`igmp group`	Отображает подробные сведения о группах мультивещания по каждому порту.	3
		`igmp interface`	Отображает настройки IGMP для каждого IP-интерфейса.	3
		`igmp multicast`	Отображает подробную информацию об известных и неизвестных кадрах мультивещания, проходящих через указанные порты коммутатора.	3
		`igmp timer`	Отображает настройки счетчиков и таймеров IGMP для каждого IP-интерфейса.	3
		`iptable all [IP|VID|PORT]`	Отображает таблицу IP-адресов. Таблицу можно отсортировать по IP-адресу, идентификатору VLAN ID или номеру порта.	3
		`iptable count`	Отображает количество IP-интерфейсов, настроенных на коммутаторе.	3
		`iptable static`	Отображает таблицу статических IP-адресов.	3
		`ospf database`	Отображает информацию из базы данных состояний каналов OSPF.	3
		`ospf interface`	Отображает настройки интерфейсов OSPF.	3
		`ospf neighbor`	Отображает информацию о соседних устройствах OSPF.	3
		`protocol-based-vlan`	Отображает настройки VLAN на основе протоколов по портам.	3
		`route`	Отображает информацию по IP-маршрутизации.	3
		`route static`	Отображает информацию по статическому IP-маршруту.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`source binding`	Отображает статические привязки (IP-адреса к MAC-адресу), настроенные на коммутаторе.	3
		`source binding [<mac-адрес>] [...]`	Отображает настроенные на коммутаторе статические привязки для указанных MAC-адресов или идентификаторов VLAN ID.	3
		`source binding help`	Отображает справочную информацию о команде `source binding` command.	3
		`tcp`	Отображает информацию TCP для IP.	3
		`udp`	Отображает информацию UDP для IP.	3
	`lacp`		Отображает настройки протокола LACP.	3
	`logging`		Отображает системные журналы.	3
	`logins`		Отображает информацию по учетным записям пользователей.	3
	`loopguard`		Отображает порты, для которых включена защита от образования петель, а также состояние этих портов.	3
	`mac`	`address-table <all [mac|vid|port]>`	Отображает таблицу MAC-адресов. Информацию можно отсортировать по MAC-адресу, идентификатору VLAN или порту.	3
		`address-table count`	Отображает общее количество MAC-адресов в таблице MAC-адресов.	3
		`address-table static`	Отображает таблицу статических MAC-адресов.	3
		`address-table vlan <идентификатор-vlan>`	Отображает таблицу статических MAC-адресов для указанной VLAN.	3
		`address-table vlan <идентификатор-vlan> <сортировка>`	Отображает таблицу статических MAC-адресов для указанной VLAN. Таблица может быть отсортирована по MAC-адресу, порту или типу.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		address-table port <список-портов>	Отображает таблицу статических MAC-адресов для указанных портов.	3
		address-table port <список-портов> <сортировка>	Отображает таблицу статических MAC-адресов для указанных портов. Таблица может быть отсортирована по MAC-адресу, порту или типу.	3
	mac-aging-time		Отображает срок устаревания запомненных MAC-адресов.	3
	mac-authentication		Отображает настройки аутентификации по MAC-адресам на коммутатора.	3
	mac-authentication	config	Отображает настройки аутентификации по MAC-адресам для различных портов, с указанием статистики аутентификации для каждого порта.	3
	mac-count		Отображает количество запомненных MAC-адресов.	3
	mrstp <номер-дерева>		Отображает настройки быстрого протокола нескольких экземпляров покрывающего дерева для указанного дерева.	3
	mstp		Отображает настройки MSTP на коммутаторе.	3
		instance <0-16>	Отображает настройки указанного экземпляра MSTP.	3
	multicast		Отображает состояние мультивещания, включая номер порта, идентификатор VLAN ID и номер группы мультивещания для участников группы на коммутаторе.	3
		vlan	Отображает состояние VLAN мультивещания.	3
	multi-login		Отображает информацию по нескольким одновременным подключениям.	3
	mvr		Отображает все настройки MVR.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		<идентификатор-vlan>	Отображает настройки указанной группы MVR.	3
	policy		Отображает всю информацию, относящуюся к политикам.	3
		[имя]	Отображает информацию по указанному правилу политики.	3
	port-access-authenticator		Отображает настройки аутентификации на всех портах.	3
		[список-портов]	Отображает настройки аутентификации на указанном порту (портах).	3
	port-security		Отображает настройки безопасности на всех портах.	3
		[список-портов]	Отображает настройки безопасности на указанном порту (портах).	3
	radius-accounting		Отображает настройки сервера учета RADIUS.	3
	radius-server		Отображает настройки сервера RADIUS.	3
	remote-management		Отображает информацию по всем защищенным клиентам.	3
		[номер]	Отображает информацию по указанному защищенному клиенту.	3
	router	dvmrp	Отображает настройки протокола DVMRP.	3
		igmp	Отображает глобальные настройки IGMP.	3
		ospf	Отображает настройки протокола OSPF.	3
		ospf area	Отображает настройки области OSPF.	3
		ospf network	Отображает настройки сети (или интерфейса) OSPF.	3
		ospf redistribute	Отображает настройки перераспределения маршрутов OSPF.	3
		ospf virtual-link	Отображает настройки виртуальных каналов OSPF.	3
		rip	Отображает глобальные настройки RIP.	3

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		vrrp	Отображает настройки протокола VRRP.	3
	running-config		Отображает текущую рабочую конфигурацию.	3
		interface port-channel <список-портов> [bandwidth-limit...]	Отображает текущую действующую конфигурацию по каждому порту. Опционально можно выбрать отображаемые параметры.	3
		help	Отображает справку по данной команде.	3
	service-control		Отображает настройки управления службами.	3
	snmp-server		Отображает настройки протокола SNMP.	3
	spanning-tree	config	Отображает настройки протокола покрывающего дерева (STP).	3
	ssh		Отображает общие настройки SSH.	3
		known-hosts	Отображает информацию по известным SSH-хостам.	3
		key <rsa1|rsa|dsa>	Отображает информацию по внутренним открытым и секретным ключам SSH.	3
		session	Отображает текущие SSH-сессии.	3
	subnet-vlan		Отображает настройки VLAN на основе подсетей на коммутаторе.	3
	system-information		Отображает общую информацию о системе.	0
	tacacs-server		Отображает настройки сервера TACACS+.	3
	tacacs-accounting		Отображает настройки сервера учета TACACS+.	3
	time		Отображает текущее системное время и дату.	3
	timesync		Отображает информацию от сервера времени.	3
	trunk		Отображает информацию по агрегации каналов.	3
	version		Отображает версию встроенного программного обеспечения, работающего на коммутаторе.	0

Таблица 140 Обзор команд: привилегированный режим (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		flash	Отображает версию встроенного программного обеспечения, записанного во Flash-память коммутатора.	0
	vlan		Отображает состояние всех VLAN.	3
		<идентификатор-vlan>	Отображает состояние указанной VLAN.	3
	vlan-stacking		Отображает настройки стекирования VLAN.	3
	vlan1q	gvrp	Отображает настройки протокола GVRP.	3
		port-isolation	Отображает настройки изоляции порта.	3
ssh	<1|2> <[user@]ip-адрес-назначения>		Осуществляет подключение к серверу SSH с указанной версией протокола SSH.	0
		[command </>]	Осуществляет подключение к серверу SSH с указанной версией SSH. Дополнительно вводится список команд, которые необходимо выполнить на сервере.	0
test	interface port-channel <список-портов>		Осуществляет тест внутренней обратной петли на указанных портах.	13
traceroute	<ip-адрес|имя-хоста> [in-band|out-of-band|vlan <идентификатор-vlan>][ttl <1-255>] [wait <1-60>] [queries <1-10>]		Определяет путь, который проходит пакет до указанного устройства.	0
	help		Отображает справку по данной команде.	0
write	memory		Сохраняет текущие настройки в текущий файл конфигурации коммутатора.	13
		<номер>	Сохраняет текущие настройки в указанный файл конфигурации коммутатора.	13

45.12.3 Общий режим настройки

Команды, доступные в режиме настройки, описаны в следующей таблице.

Таблица 141 Обзор команд: режим настройки

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
aaa	accounting	commands <уровень-привилегий> stop-only tacacs+	Включает учет для сессий управления через командную строку и определяет минимальный уровень привилегий для команд, подлежащих учету.	13
		commands <уровень-привилегий> stop-only tacacs+ [broadcast]	Включает отправку учетной информации по сеансам управления через командную строку одновременно на все настроенные серверы учета.	13
		dot1x <start-stop|stop-only> <radius|tacacs+>	Включает учет сеансов аутентификации IEEE 802.1x и определяет используемые режим и протокол.	13
		dot1x <start-stop|stop-only> <radius|tacacs+> [broadcast]	Включает отправку учетной информации по сеансам аутентификации IEEE 802.1x одновременно на все настроенные серверы учета.	13
		exec <start-stop|stop-only> <radius|tacacs+>	Включает учет сеансов администрирования через SSH, Telnet и консольный порт и определяет используемые режим и протокол.	13
		exec <start-stop|stop-only> <radius|tacacs+> [broadcast]	Включает отправку учетной информации по сеансам администрирования через SSH, Telnet и консольный порт одновременно на все настроенные серверы учета.	13
		system <radius|tacacs+>	Включает учет системных событий и определяет используемый протокол.	13
		system <radius|tacacs+> [broadcast]	Включает отправку учетной информации по системным событиям одновременно на все настроенные серверы учета.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`update periodic <1-2147483647>`	Определяет период обновления для учета. Это период времени, в течение которого коммутатор выжидает перед отправкой обновленной информации на сервер учета с момента начала сеанса.	13
	`authentication`	`enable <метод1> [<метод2> [<метод3>]]`	Включает на коммутаторе авторизацию для выполнения команд и определяет методы, используемые в первую, вторую и третью очередь. В качестве методов может быть указано «enable», «radius» или «tacacs+»	14
		`login <метод1> [<метод2> [<метод3>]]`	Включает на коммутаторе авторизацию для сеансов администрирования и определяет методы, используемые в первую, вторую и третью очередь. В качестве методов может быть указано «local», «radius» или «tacacs+»	14
`admin-password`	`<пароль> <подтверждение-пароля>`		Изменяет пароль администратора.	14
`arp inspection`			Включает инспекцию ARP-пакетов на коммутаторе. После этого необходимо включить функцию инспекции ARP-пакетов в конкретной сети VLAN и указать доверенные порты.	13
	`filter-aging-time`	`<1-2147483647>`	Определяет 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.	13
		`none`	Делает фильтр MAC-адресов постоянным.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`log buffer`	`entries <0-1024>`	Определяет максимальное количество сообщений контрольного журнала (1-1024), которые могут быть сгенерированы пакетами ARP до отправки на сервер syslog. 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.	13
		`logs <0-1024> interval <0-86400>`	Определяет максимальное количество сообщений контрольного журнала, которое может быть отправлено на сервер syslog в одной партии, а также периодичность (1-86400 секунд) отправки коммутатором партий сообщений контрольного журнала на сервер syslog.	13
	`vlan <список-vlan>`		Включает инспекцию ARP-пакетов для указанных VLAN.	13
		`logging [all|none|permit|deny]`	Включает регистрацию в системном журнале событий инспекции ARP-пакетов для указанных VLAN. Опционально можно выбрать типы регистрируемых событий.	13
`bandwidth-control`			Включает управление пропускной способностью.	13
`bcp-transparency`			Включает режим прозрачности мостового протокола BCP.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
classifier	<имя> <[packet-format <802.3untag|802.3tag| EtherIIuntag| EtherIItag>] [priority <0-7>] [vlan <идентификатор-vlan>][ethernet-type <ether-num|ip|ipx| arp|rarp| appletalk|decnet| sna|netbios|dlc>] [source-mac <mac-адрес-источника>] [source-port <номер-порта>] [destination-mac <mac-адрес-назначения>] [dscp <0-63>] [ip-protocol <protocol-num|tcp|udp|icmp|egp| ospf|rsvp|igmp| igp|pim|ipsec> [establish-only]] [source-ip <ip-адрес-источника> [mask-bits <битов-маски>]] [source-socket <номер-сокета>] [destination-ip <ip-адрес-назначения> [mask-bits <битов-маски>]] [destination-socket <номер-сокета>] [inactive]>		Настраивает правило классификации. При классификации трафик группируется на потоки данных по определенным критериям, таким как адрес источника, адрес назначения, номер порта источника, номер порта назначения и номер входящего порта.	13
	help		Отображает справку по данной команде.	13
cluster	<идентификатор-vlan>		Включает поддержку кластеров в указанной группе VLAN.	13
	member <mac-адрес> password <пароль>		Определяет члена кластера.	13
	name <имя кластера>		Определяет имя-описание для кластера.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	rcommand <mac-адрес>		Осуществляет вход в интерфейс командной строки указанного члена кластера.	13
default-management	<in-band|out-of-band>		Определяет, каким образом коммутатор должен отправлять пакеты.	13
dhcp	dhcp-vlan <идентификатор-vlan>		Определяет идентификатор VLAN ID для сети VLAN DHCP.	13
dhcp	relay <идентификатор-vlan>	helper-address <удаленный-dhcp-сервер1>	Включает ретрансляцию DHCP для указанной VLAN и определяет IP-адрес 1 сервера DHCP.	13
		helper-address <удаленный-dhcp-сервер1> [<удаленный-dhcp-сервер2>] [<удаленный-dhcp-сервер3>] [option] [information]	Включает ретрансляцию DHCP для указанной VLAN и определяет IP-адреса не более 3 серверов DHCP. Опционально можно настроить на коммутаторе добавление информации агента ретрансляции и имени системы.	13
	server <идентификатор-vlan>	starting-address <ip-адрес> <маска-подсети> size-of-client-ip-pool <1-253>	Включает сервер DHCP для указанной VLAN и определяет параметры настройки TCP/IP, отправляемые клиентам DHCP.	13
		starting-address <ip-адрес> <маска-подсети> size-of-client-ip-pool <1-253> [default-gateway <ip-адрес>] [primary-dns <ip-адрес>] [secondary-dns <ip-адрес>]	Включает сервер DHCP для указанной VLAN и определяет параметры настройки TCP/IP, отправляемые клиентам DHCP. В том числе определяются передаваемые IP-адрес шлюза и адреса серверов DNS.	13
	smart-relay		Включает ретрансляцию DHCP для всех широковещательных доменов на коммутаторе.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`helper-address <удаленный-dhcp-сервер1> [<удаленный-dhcp-сервер2>] [<удаленный-dhcp-сервер3>]`	Определяет IP-адреса не более 3 серверов DHCP.	13
		`information`	Разрешает коммутатору добавлять к информации агента имя системы.	13
		`option`	Разрешает коммутатору добавлять к информацию агента ретрансляции DHCP.	13
`dhcp`	`snooping`		Включает функцию отслеживания DHCP на коммутаторе.	13
		`database <tftp://хост/имя-файла>`	Определяет расположение базы данных отслеживания DHCP. Расположение должно быть указано в следующем виде: tftp://{имя домена или IP-адрес}/каталог, если необходимо/имя файла; например, tftp://192.168.10.1/database.txt.	13
		`database timeout <секунд>`	Определяет, как долго (от 10 до 65535 секунд) коммутатор будет пытаться выполнить конкретное обновление базы данных отслеживания DHCP перед отказом от дальнейших попыток.	13
		`database write-delay <секунд>`	Определяет, как долго (от 10 до 65535 секунд) коммутатор будет выжидать перед обновлением базы данных отслеживания DHCP после первого изменения текущих привязок с момента обновления.	13
		`vlan <список-vlan>`	Определяет идентификаторы VLAN ID для сетей VLAN, на которых необходимо включить отслеживание DHCP.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`vlan <список-vlan> information`	Определяет режим добавления коммутатором имени системы к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN.	13
		`vlan <список-vlan> option`	Определяет режим добавления коммутатором номера слота, номера порта и идентификатора VLAN ID к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN.	13
`diffserv`			Включает службы DiffServ.	13
	`dscp <0-63> priority <0-7>`		Определяет отображение маркеров DSCP на приоритеты IEEE 802.1q.	13
`ethernet oam`			Включает функцию Ethernet OAM на коммутаторе.	13
`exit`			Осуществляет выход из интерфейса командной строки.	13
`fe-spq <q0|q1|..|q7>`			Определяет на коммутаторе использование алгоритма SPQ для обслуживания очередей с номерами, большими или равными указанному, для портов Ethernet на 10/100 Мбит/с.	13
`garp`	`join <100-65535> leave <мсек> leaveall <мсек>`		Определяет настройки таймера GARP.	13
`help`			Отображает справку по командам.	0
`history`			Отображает список ранее введенных команд.	0
`hostname`	`<имя-коммутатора>`		Определяет имя коммутатора для идентификации.	13
`https`	`cert-regeneration <rsa|dsa>`		Заново генерирует сертификат.	13
	`timeout <0-65535>`		Определяет значение тайм-аута для HTTPS.	13
`igmp-filtering`			Включает фильтрацию IGMP на коммутаторе.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`profile <имя> start-address <ip-адрес> end-address <ip-адрес>`		Устанавливает диапазон адресов мультивещания в профиле.	13
`igmp-snooping`			Включает отслеживание многоадресного трафика IGMP.	13
	`8021p-priority`	`<0-7>`	Определяет значение приоритета 802.1p для исходящих пакетов отслеживания IGMP.	13
	`host-timeout`	`<1-16711450>`	Определяет значение тайм-аута для хоста.	13
	`leave-timeout`	`<1-16711450>`	Определяет значение тайм-аута для таймера Leave.	13
	`unknown-multicast-frame <drop|flooding>`		Определяет порядок обработки трафика от неизвестной группы мультивещания (отбрасывание или передача на все порты).	13
	`reserved-multicast-group <drop|flooding>`		Определяет порядок обработки трафика, принадлежащего зарезервированным группам мультивещания (отбрасывание или передача на все порты).	13
	`vlan`	`<идентификатор-vlan>`	Определяет сети VLAN, для которых выполняется отслеживание многоадресного трафика IGMP.	13
		`<идентификатор-vlan> [name <имя>]`	Позволяет определить имя для сети VLAN мультивещания.	13
		`mode <auto|fixed>`	Определяет, должен ли коммутатор автоматически запомнить первые 16 сетей VLAN, отправляющих трафик мультивещания через коммутатор (auto), или отслеживание многоадресного трафика IGMP должно осуществляться коммутатором только для VLAN, настроенных на коммутаторе.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
interface	port-channel <список-портов>		Включает один порт или список портов для настройки. Более подробно см. разд. 45.12.4 на стр. 428.	13
	route-domain <ip-адрес>/<битов-маски>		Активирует домен маршрутизации для настройки. Более подробно см. разд. 45.12.5 на стр. 436.	13
ip	адреса	<ip-адрес> <маска>	Определяет IP-адрес и маску подсети для порта внеполосного управления.	13
		default-gateway <ip-адрес>	Определяет IP-адрес шлюза по умолчанию для порта внеполосного управления.	13
	name-server	<ip-адрес>	Определяет IP-адрес сервера доменных имен (DNS).	13
	route	<ip-адрес> <маска> <адрес-следующего-перехода>	Определяет статический маршрут.	13
		<ip-адрес> <маска><адрес-следующего-перехода> [metric <метрика>] [name <имя>] [inactive]	Определяет метрику статического маршрута или отключает статический маршрут.	13
	source binding <mac-адрес> vlan <идентификатор-vlan> <ip-адрес>		Создает статическую привязку для отслеживания DHCP и инспекции ARP-пакетов.	13
		interface port-channel <идентификатор-интерфейса>	Определяет порты для статической привязки.	13
lacp			Включает протокол LACP.	13
	system-priority	<1-65535>	Определяет приоритет активного порта, использующего LACP.	13
logins	username <имя> password <пароль>		Определяет до четырех пользовательских учетных записей, имеющих доступ только на чтение.	14
	username <имя>	privilege <0-14>	Определяет уровень привилегий для учетной записи пользователя.	14

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
logout			Осуществляет выход пользователя из интерфейса командной строки.	0
loopguard			Включает защиту от образования петель на коммутаторе.	13
mac-authentication			Включает аутентификацию по MAC-адресам на коммутаторе.	13
	nameprefix <строка-имени>		Определяет префикс имени, который будет добавляться ко всем MAC-адресам перед отправкой на сервер RADIUS для аутентификации.	13
	password <строка-имени>		Определяет пароль, отправляемый на сервер RADIUS для клиентов, использующих аутентификацию по MAC-адресу.	13
	timeout <1-3000>		Определяет период времени, по прошествии которого коммутатор разрешит пользователю с MAC-адресом, отвергнутым при аутентификации, повторить попытку аутентификации. Команда mac-aging-time имеет приоритет перед данной настройкой.	13
mac-aging-time	<10-3000>		Определяет срок устаревания запомненных MAC-адресов.	13
mac-filter	name <имя> mac <mac-адрес> vlan <идентификатор-vlan> drop <src/dst/both>		Определяет правило фильтрации для порта со статическим MAC-адресом.	13
		inactive	Отключает правило фильтрации для порта со статическим MAC-адресом.	13
mac-forward	name <имя> mac <mac-адрес> vlan <идентификатор-vlan> interface <идентификатор-интерфейса>		Определяет правило пересылки статического MAC-адреса.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		inactive	Отключает правило пересылки статического MAC-адреса.	13
mirror-port			Включает зеркальное копирование.	13
	<номер-порта>		Включает зеркальное копирование на указанном порту.	13
mode	zynos		Меняет режим интерфейса командной строки на формат ОС ZyNOS.	13
mrstp	<номер-дерева>		Активирует указанную конфигурацию STP.	13
	interface <список-портов>		Активирует протокол STP на указанных портах.	13
		path-cost <1-65535>	Определяет стоимость пути для указанных портов.	13
		priority <0-255>	Определяет значение приоритета указанных портов для протокола STP.	13
		treeIndex <1-4>	Назначает портам указанную конфигурацию STP.	13
	help		Отображает подробную справку по команде mrstp.	13
mstp			Включает протокол MSTP на коммутаторе.	13
	configuration name		Определяет имя для региона MSTP.	13
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Определяет параметры Hello Time, Maximum Age и Forward Delay.	13
	instance <0-16>		Определяет настраиваемый экземпляр MST.	13
		interface port-channel <список-портов>	Определяет порты, которые должны быть включены в указанный экземпляр MST.	13
		interface port-channel <список-портов> path-cost <1-65535>	Назначает стоимость пути для указанных портов.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`interface port-channel <список-портов> priority <1-255>`	Назначает приоритет для указанных портов.	13
	`max-hop <1-255>`		Определяет максимальное число переходов в регионе MST, после которого блок данных BPDU отбрасывается.	13
	`revision <0-65535>`		Определяет номер версии для конфигурации данного региона MST.	13
`multi-login`			Включает функцию нескольких одновременных подключений (multi-login).	14
`mvr`	`<идентификатор-vlan>`		Осуществляет вход в режим настройки MVR (регистрации VLAN-сети мультивещания). Дополнительную информацию можно найти в разд. 45.13 на стр. 440.	13
`no`	`aaa accounting`	`команды`	Отключает учет сессий управления через командную строку на коммутаторе.	13
		`dot1x`	Отключает учет сессий аутентификации IEEE 802.1x на коммутаторе.	13
		`exec`	Отключает учет сеансов администрирования через SSH, Telnet или консольный порт на коммутаторе.	13
		`system`	Отключает учет системных событий на коммутаторе.	13
		`update`	Сбрасывает интервал обновления учетной информации на «0».	13
	`aaa authentication`	`enable`	Отключает авторизацию при выполнении команд на коммутаторе.	13
		`login`	Отключает аутентификацию для сеансов администрирования на коммутаторе.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`arp inspection`		Отключает инспекцию ARP-пакетов на коммутаторе.	13
		`filter-aging-time`	Сбрасывает период времени (1-2147483647 секунд), в течение которого фильтр MAC-адресов будет действовать на коммутаторе с момента обнаружения коммутатором несанкционированного пакета ARP, на значение по умолчанию (300 секунд).	13
		`log-buffer entries`	Сбрасывает максимальное количество сообщений контрольного журнала (1-1024), которые могут быть сгенерированы пакетами ARP до отправки на сервер syslog, на значение по умолчанию (3).	13
		`log-buffer logs`	Сбрасывает максимальное количество сообщений syslog, которые коммутатор может передать на сервер syslog в одной партии, на значение по умолчанию (4).	13
		`vlan <список-vlan>`	Отключает инспекцию ARP-пакетов для указанных VLAN.	13
		`vlan <список-vlan> logging`	Отключает регистрацию в системном журнале событий инспекции ARP-пакетов для указанных VLAN.	13
	`bandwidth-control`		Отключает управление пропускной способностью на коммутаторе.	13
	`bcp-transparency`		Отключает режим прозрачности мостового протокола BCP.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`classifier`	`<имя>`	Отключает правило классификации. Каждая запись включает в себя одно правило. В случае отключения правила классификации невозможно использовать информацию, относящуюся к политике.	13
		`<имя> inactive`	Включает правило классификации.	13
	`cluster`		Отключает управление кластерами на коммутаторе.	13
		`member <mac-адрес>`	Удаляет члена кластера.	13
	`dhcp relay <идентификатор-vlan>`		Отключает ретрансляцию DHCP.	13
		`information`	Отключает добавление информации агента ретрансляции в поле Option 82.	13
		`option`	Отключает добавление имени системы в поле информации Option 82.	13
	`dhcp server <идентификатор-vlan>`		Отключает настройки сервера DHCP.	13
		`default-gateway`	Отключает настройки шлюза по умолчанию для сервера DHCP.	13
		`primary-dns`	Отключает настройки адреса основного сервера DNS для сервера DHCP.	13
		`secondary-dns`	Отключает настройки адреса вспомогательного сервера DNS для сервера DHCP.	13
	`dhcp smart relay`		Отключает глобальные настройки агента ретрансляции DHCP.	13
		`information`	Отключает добавление информации агента ретрансляции в поле Option 82 на уровне глобальных настроек DHCP.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`option`	Отключает добавление имени системы в поле информации Option 82 на уровне глобальных настроек DHCP.	13
	`dhcp snooping`		Отключает функцию отслеживания DHCP на коммутаторе.	13
		`vlan <список-vlan>`	Определяет идентификаторы VLAN ID для сетей VLAN, на которых необходимо отключить отслеживание DHCP.	13
		`vlan <список-vlan> information`	Отключает режим добавления коммутатором имени системы к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN.	13
		`vlan <список-vlan> option`	Отключает режим добавления коммутатором номера слота, номера порта и идентификатора VLAN ID к запросам DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN.	13
		`database`	Удаляет информацию о расположении базы данных отслеживания DHCP.	13
		`database timeout`	Сбрасывает на значение по умолчанию (300) период, в течение которого (10-65535 секунд) коммутатор будет пытаться выполнить конкретное обновление базы данных отслеживания DHCP перед отказом от дальнейших попыток.	13
		`database write-delay`	Сбрасывает на значение по умолчанию (65535) период, в течение которого (10-65535 секунд) коммутатор будет выжидать перед обновлением базы данных отслеживания DHCP после первого изменения текущих привязок с момента обновления.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	dhcp dhcp-vlan		Отключает сеть VLAN DHCP на коммутаторе.	13
	diffserv		Отключает службы DiffServ на коммутаторе.	13
	ethernet oam		Отключает функцию Ethernet OAM на коммутаторе.	13
	fe-spq		Отключает на портах Fast Ethernet (10/100 Мбит/с) использование строгой очереди приоритетов.	13
	igmp-filtering		Отключает фильтрацию IGMP на коммутаторе.	13
		profile <имя>	Отключает указанный профиль фильтрации IGMP.	13
		profile <имя> start-address <ip-адрес> end-address <ip-адрес>	Сбрасывает настройки указанного профиля фильтрации IGMP.	13
	igmp-snooping		Отключает отслеживание многоадресного трафика IGMP.	13
		8021p-priority	Отключает изменение приоритета для исходящих управляющих пакетов IGMP.	13
		vlan <идентификатор-vlan>	Удаляет настройки отслеживания многоадресного трафика IGMP на указанной VLAN.	13
	ip		Возвращает IP-адрес управления к значению по умолчанию.	13
		route <ip-адрес> <маска>	Удаляет указанный статический IP-маршрут.	13
		route <ip-адрес> <маска> inactive	Включает указанный статический IP-маршрут.	13
		source binding <mac-адрес> vlan <идентификатор-vlan>		13
	lacp		Отключает протокол управления агрегацией каналов (динамическое группирование) на коммутаторе.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	logins username <имя>		Отключает доступ для указанного пользователя.	14
	loopguard		Отключает защиту от образования петель на коммутаторе.	13
	mac-authentication		Отключает аутентификацию по MAC-адресам на коммутаторе.	13
	mac-authentication timeout		Сбрасывает значение тайм-аута для аутентификации по MAC-адресам на коммутаторе в «0».	13
	mac-filter	name <имя> mac <mac-адрес> vlan <идентификатор-vlan> drop <src|dst|both> inactive	Включает указанное правило фильтрации по MAC-адресу.	13
		name <имя> mac <mac-адрес> vlan <идентификатор-vlan> drop <src|dst|both>	Отключает указанное правило фильтрации по MAC-адресу.	13
	mac-forward	name <имя> mac <mac-адрес> vlan <идентификатор-vlan> interface <идентификатор-интерфейса>	Отключает указанную запись о пересылке MAC-адреса, принадлежащего к указанной группе VLAN (если таковая есть) и пересылаемого через указанный интерфейс.	13
		name <имя> mac <mac-адрес> vlan <идентификатор-vlan> interface <идентификатор-интерфейса> inactive	Включает указанный MAC-адрес, принадлежащий к указанной группе VLAN (если таковая есть) и пересылаемый через указанный интерфейс.	13
	mirror-port		Отключает зеркальное копирование портов на коммутаторе.	13
	mrstp	<номер-дерева>	Отключает указанную конфигурацию STP (дерево 1-4).	13
	mrstp	interface <список-портов>	Отключает назначение STP для указанных портов.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	mstp		Отключает протокол MSTP на коммутаторе.	13
		<экземпляр> <0-16>	Отключает указанный экземпляр MST на коммутаторе.	13
		<экземпляр> <0-16> vlan <1-4094>	Отключает назначение указанных сетей VLAN указанному экземпляру MST.	13
		instance <0-16> interface port-channel <список-портов>	Отключает назначение указанных портов указанному экземпляру MST.	13
	multi-login		Отключает другому администратору доступ через Telnet или интерфейс командной строки.	14
	mvr <идентификатор-vlan>		Удаляет конфигурацию MVR с коммутатора.	13
	password privilege <0-14>		Отключает пароль на исполнение команд с указанным уровнем привилегий.	14
	policy <имя>		Удаляет политику. Политика определяет действия, выполняемые над трафиком после классификации.	13
		inactive	Включает политику.	13
	port-access-authenticator		Отключает аутентификацию портов на коммутаторе.	13
		<список-портов>	Отключает аутентификацию на указанных портах.	13
		<список-портов> reauthenticate	Отключает механизм повторной аутентификации на указанном порту (портах).	13
	port-security		Отключает средства безопасности портов на устройстве.	13
		<список-портов>	Отключает средства безопасности указанных портов.	13
		<список-портов> learn inactive	Включает получение MAC-адресов на указанных портах.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`radius-accounting`	`<номер>`	Отключает учет с использованием указанного сервера RADIUS.	13
	`radius-server`	`<номер>`	Отключает аутентификацию через указанный сервер RADIUS.	13
	`remote-management`	`<номер>`	Удаляет клиентский набор из списка защищенных клиентов.	13
		`<номер> service <telnet| ftp| http| icmp| snmp| ssh| https>`	Отключает для клиентского набора с указанным номером использование выбранной службы удаленного управления.	13
	`router`	`dvmrp`	Отключает протокол DVMRP на коммутаторе.	13
		`igmp`	Отключает протокол IGMP на коммутаторе.	13
		`ospf`	Отключает протокол OSPF на коммутаторе.	13
		`rip`	Отключает протокол RIP на коммутаторе.	13
		`vrrp network <ip-адрес>/ <битов-маски> vr-id <1-7>`	Удаляет настройки VRRP.	13
	`service-control`	`ftp`	Отключает доступ к коммутатору по FTP.	13
		`http`	Отключает управление коммутатором через Web-конфигуратор.	13
		`https`	Отключает защищенный доступ к коммутатору через Web-браузер.	13
		`icmp`	Отключает доступ к коммутатору по протоколу ICMP – например, пинги и трассировку маршрута.	13
		`snmp`	Отключает управление по протоколу SNMP.	13
		`ssh`	Отключает доступ к коммутатору через SSH (Secure Shell).	13
		`telnet`	Отключает доступ к коммутатору через Telnet.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`snmp-server trap-destination <ip-адрес>`		Отключает отправку менеджеру Trap-команд протокола SNMP.	13
		`enable traps`	Отключает отправку менеджеру всех Trap-команд протокола SNMP.	13
		`enable traps aaa`	Отключает отправку менеджеру всех Trap-команд типа AAA.	13
		`enable traps aaa <опции>`	Отключает отправку менеджеру определенных Trap-команд типа AAA. Возможные опции: «authentication» (аутентификация) или «accounting» (учет).	13
		`enable traps interface`	Отключает отправку менеджеру всех Trap-команд типа Interface.	13
		`enable traps interface <опции>`	Отключает отправку менеджеру определенных Trap-команд типа Interface. Возможные опции: «linkup» (установление соединение), «linkdown» (разрыв соединения) и «autonegotiation» (автосогласование).	13
		`enable traps ip`	Отключает отправку менеджеру всех Trap-команд типа IP.	13
		`enable traps ip <опции>`	Отключает отправку менеджеру определенных Trap-команд типа IP. Возможные опции: «ping» или «traceroute».	13
		`enable traps switch`	Отключает отправку менеджеру всех Trap-команд типа коммутатор.	13
		`enable traps switch <опции>`	Отключает отправку менеджеру определенных Trap-команд типа коммутатор. Возможные опции: «stp», «mactable» или «rmon».	13
		`enable traps system`	Отключает отправку менеджеру всех Trap-команд типа System.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`enable traps system <опции>`	Отключает отправку менеджеру определенных Trap-команд типа System. Возможные опции: «coldstart» («холодный» запуск), «warmstart» («теплый» запуск), «fanspeed» (скорость вентиляторов), «temperature» (температура), «voltage» (напряжение), «reset» (сброс), «timesync» (синхронизация времени), «intrusionlock» (защита от вторжений) или «loopguard» (защита от образования петель).	13
	`spanning-tree`		Отключает протокол STP.	13
		`<список-портов>`	Отключает протокол STP на указанных портах.	13
	`ssh`	`key <rsa1|rsa|dsa>`	Отключает серверный ключ шифрования SSH. Данный коммутатор поддерживает протокол SSH версий 1 и 2, работающий с методами аутентификации RSA и DSA.	13
		`known-hosts <ip-адрес-хоста>`	Удаляет указанные удаленные хосты из списка всех известных хостов.	13
		`known-hosts <ip-адрес-хоста> [1024|ssh-rsa|ssh-dsa]`	Исключает удаленные хосты с указанным открытым ключом (1024-битный RSA1, RSA или DSA).	13
	`storm-control`		Отключает контроль широковещательных штормов.	13
	`subnet-based-vlan`		Отключает настройки VLAN на основе подсетей на коммутаторе.	13
		`source-ip <ip-адрес> mask-bits <битов-маски>`	Удаляет указанную подсеть из конфигурации VLAN на основе подсетей.	13
		`dhcp-vlan-override`	Отключает настройки игнорирования DHCP VLAN для VLAN на основе подсетей.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	syslog		Отключает ведение системного журнала.	13
		server <ip-адрес>	Отключает передачу записей syslog на указанный сервер syslog.	13
		server <ip-адрес> inactive	Включает передачу записей syslog на указанный сервер syslog.	13
		type [тип]	Отключает передачу записей syslog указанного типа (sys, link, config, error или report).	13
	tacacs-accounting	<номер>	Отключает учет с использованием указанного сервера TACACS+.	13
	tacacs-server	<номер>	Отключает аутентификацию с использованием указанного сервера TACACS+.	13
	time	daylight-saving-time	Отключает на коммутаторе переход на летнее время.	13
	timesync		Отключает настройки сервера времени.	13
	trtcm		Отключает функцию маркировки TRTCM на коммутаторе.	13
	trunk	<T1|T2|T3|T4|T5|T6>	Отключает указанную группу портов.	13
		<T1|T2|T3|T4|T5|T6> interface <список-портов>	Удаляет порты из указанной группы портов.	13
		<T1|T2|T3|T4|T5|T6> lacp	Отключает протокол LACP в указанной группе портов.	13
	vlan	<идентификатор-vlan>	Удаляет указанную статическую VLAN.	13
	vlan1q	gvrp	Отключает протокол GVRP на коммутаторе.	13
		port-isolation	Отключает изоляцию портов.	13
	vlan-stacking		Отключает стекирование VLAN.	13
password	<пароль>		Изменяет пароль для наивысшего уровня привилегий.	14

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
password	<пароль>	privilege <0-14>	Изменяет пароль для указанного уровня привилегий.	14
policy	<имя> classifier <список-правил-классификации> < [vlan<идентификатор-vlan>] [egress-port <номер-порта>] [priority <0-7>] [dscp <0-63>] [tos <0-7>] [bandwidth <пропускная-способность>] [outgoing-packet-format <tagged|untagged>] [out-of-profile-dscp <0-63>] [forward-action <drop|forward>] [queue-action <prio-set|prio-queue|prio-replace-tos>] [diffserv-action <diff-set-tos|diff-replace-priority|diff-set-dscp>] [outgoing-mirror] [outgoing-eport] [outgoing-non-unicast-eport] [outgoing-set-vlan] [metering] [out-of-profile-action <[change-dscp][drop][forward] [set-drop-precedence]>] [inactive]>		Настраивает политику. С помощью классификации трафик делится на потоки в соответствии с установленными критериями. Правила политики обеспечивают надлежащую обработку потоков трафика в сети.	13
port-access-authenticator			Включает на коммутаторе аутентификацию по стандарту 802.1x.	13
	<список-портов>		Включает аутентификацию по стандарту 802.1x на указанных портах.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		reauthenticate	Включает режим, когда от клиента требуется периодически заново вводить свои имя пользователя и пароль, чтобы оставаться подключенным к указанному порту.	13
		reauth-period <период-повторной-аутентификации>	Указывает, как часто клиенту требуется вводить заново свое имя пользователя и пароль, чтобы оставаться подключенным к порту.	13
port-security			Включает средства безопасности портов на устройстве.	13
	<список-портов>		Включает средства безопасности на указанном порту (портах).	13
		address-limit <количество>	Ограничивает количество (динамических) MAC-адресов, которые может запомнить порт.	13
		learn inactive	Отключает получение MAC-адресов на указанном порту (портах).	13
		MAC-freeze	Прекращает получение MAC-адресов на порту (портах).	13
queue	priority <0-7> level <0-7>		Определяет соответствие уровня приоритета физической очереди.	13
radius-accounting	host <номер><ip-адрес>		Определяет IP-адрес RADIUS-сервера учета 1 или RADIUS-сервера учета 2 (номер=1 или номер=2).	13
		[acct-port <номер-сокета>] [key <ключ>]	Определяет номер порта и ключ для внешнего сервера учета RADIUS.	13
	timeout <1-1000>		Определяет значение тайм-аута сервера учета RADIUS.	13
radius-server	host <номер> <ip-адрес>		Определяет IP-адрес RADIUS-сервера 1 или RADIUS-сервера 2 (номер=1 или номер=2).	13
		[auth-port <номер-сокета>] [key <ключ>]	Определяет номер порта и ключ для внешнего сервера RADIUS.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`timeout <1-1000>`		Определяет значение тайм-аута сервера RADIUS.	13
	`mode`	`<index-priority|round-robin>`	Определяет режим выбора сервера RADIUS.	13
`remote-management`	`<номер> start-addr <ip-адрес> end-addr <ip-адрес> service <telnet|ftp|http|icmp|snmp>`		Определяет группу доверенных компьютеров, с которых администратор может получить доступ к управлению коммутатором через соответствующую службу.	13
`router`	`dvmrp`		Включает протокол DVMRP и входит в режим настройки DVMRP.	13
		`exit`	Осуществляет выход из режима настройки DVMRP.	13
		`threshold <значение-ttl>`	Определяет пороговое значение для DVMRP.	13
	`igmp`		Включает протокол IGMP и входит в режим настройки IGMP.	13
		`exit`	Осуществляет выход из режима настройки IGMP.	13
		`non-querier`	Переводит коммутатор в режим Non-Querier. (Если маршрутизатор мультивещания имеет меньший IP-адрес, он прекращает отправлять сообщения Query в эту сеть).	13
		`no non-querier`	Отключает на коммутаторе режим Non-Querier (маршрутизатор мультивещания всегда отправляет сообщения Query).	13
		`unknown-multicast-frame <drop|flooding>`	Определяет действия, выполняемые коммутатором при получении неизвестного кадра мультивещания.	13
	`ospf <идентификатор-маршрутизатора>`		Включает протокол OSPF и входит в режим настройки OSPF.	13
		`area <идентификатор-области>`	Включает и устанавливает идентификатор области.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		area <идентификатор-области> authentication	Включает простую аутентификацию для области.	13
		area <идентификатор-области> authentication message-digest	Включает для области аутентификацию MD5.	13
		area <идентификатор-области> default-cost <0-16777214>	Определяет стоимость для области.	13
		area <идентификатор-области> name <имя>	Определяет имя-описание области для идентификации.	13
		area <идентификатор-области> stub	Включает и определяет тупиковую область.	13
		area <идентификатор-области> stub no-summary	Отключает для тупиковой области отправку любых объявлений LSA.	13
		area <идентификатор-области> virtual-link <идентификатор-маршрутизатора>	Определяет идентификационную информацию виртуального канала для области.	13
		area <идентификатор-области> virtual-link <идентификатор-маршрутизатора> authentication-key <ключ>	Включает простую аутентификацию и определяет ключ аутентификации для указанного виртуального канала в области.	13
		area <идентификатор-области> virtual-link <идентификатор-маршрутизатора> authentication-same-as-area	Определяет для виртуального канала использование того же режима аутентификации, что и в области.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		area <идентификатор-области> virtual-link <идентификатор-маршрутизатора> message-digest-key <идентификатор-ключа> md5 <ключ>	Включает аутентификацию по MD5 и определяет идентификатор ключа и ключ для виртуального канала в области.	13
		area <идентификатор-области> virtual-link <идентификатор-маршрутизатора> name <имя>	Определяет имя-описание виртуального канала для идентификации.	13
		exit	Осуществляет выход из режима настройки маршрутизатора OSPF.	13
		network <ip-адрес/битов-маски> area <идентификатор-области>	Создает область OSPF.	13
		no area <идентификатор-области>	Удаляет указанную область.	13
		no area <идентификатор-области> authentication	Отключает аутентификацию для указанной области (режим None).	13
		no area <идентификатор-области> default-cost	Определяет для области использование стоимости по умолчанию (15).	13
		no area <идентификатор-области> stub	Отключает настройки тупиковой сети в области.	13
		no area <идентификатор-области> stub no-summary	Включает для области отправку объявлений LSA.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		no area <идентификатор-области> virtual-link <идентификатор-маршрутизатора> authentication-key	Сбрасывает настройки аутентификации для данного виртуального канала.	13
		no area <идентификатор-области> virtual-link <идентификатор-маршрутизатора> message-digest-key	Сбрасывает настройки аутентификации для данного виртуального канала.	13
		no area <идентификатор-области> virtual-link <идентификатор-маршрутизатора> authentication-same-as-area	Сбрасывает настройки аутентификации для данной виртуальной области.	13
		no area <идентификатор-области> virtual-link <идентификатор-маршрутизатора>	Удаляет виртуальный канал из области.	13
		no network <ip-адрес/битов-маски>	Удаляет сеть OSPF.	13
		no redistribute rip	Отключает на коммутаторе получение информации о маршрутах RIP.	13
		no redistribute static	Отключает на коммутаторе получение информации о статических маршрутах.	13
		redistribute rip metric-type <1|2> metric <0-65535>	Включает на коммутаторе получение информации о маршрутах RIP с использованием указанных метрик.	13
		redistribute static metric-type <1|2> metric <0-65535>	Включает на коммутаторе получение информации о статических маршрутах с использованием указанных метрик.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		passive-iface <ip-адрес/ битов-маски>	Определяет пассивный режим для интерфейса. Пассивный интерфейс не осуществляет отправку и получение трафика OSPF.	13
	rip		Включает протокол RIP и входит в режим настройки RIP.	13
		exit	Осуществляет выход из режима настройки RIP.	13
	vrrp network <ip-адрес>/<битов-маски> vr-id <1-7> uplink-gateway <ip-адрес>		Добавляет новую сеть VRRP и осуществляет переход в режим настройки VRRP.	13
		exit	Осуществляет выход из командного режима VRRP.	13
		inactive	Отключает настройки VRRP.	13
		interval <1..255>	Определяет интервал времени (в секундах) между передачей сообщений Hello.	13
		name <строка-имени>	Определяет имя-описание настроек VRRP для идентификации.	13
		no inactive	Активирует данный VRRP.	13
		no preempt	Отключает режим вытеснения VRRP.	13
		no primary-virtual-ip	Переводит сеть на использование основного виртуального шлюза по умолчанию (IP-адреса интерфейса).	13
		no secondary-virtual-ip	Определяет для сети использование вспомогательного виртуального шлюза по умолчанию (0.0.0.0).	13
		preempt	Включает режим вытеснения.	13
		primary-virtual-ip <ip-адрес>	Определяет IP-адрес основного виртуального шлюза VRRP.	13
		priority <1-254>	Определяет приоритет шлюза.	13
		secondary-virtual-ip <ip-адрес>	Определяет IP-адрес вспомогательного виртуального шлюза VRRP.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
service-control	ftp <номер-сокета>		Открывает FTP-доступ на указанном порту службы.	13
	http <номер-сокета> <тайм-аут>		Открывает HTTP-доступ на указанном порту службы и определяет период тайм-аута.	13
	https <номер-сокета>		Открывает HTTP-доступ на указанном порту службы.	13
	icmp		Разрешает прохождение управляющих пакетов ICMP.	13
	snmp		Разрешает управление по протоколу SNMP.	13
	ssh <номер-сокета>		Открывает SSH-доступ на указанном порту службы.	13
	telnet <номер-сокета>		Открывает Telnet-доступ на указанном порту службы.	13
snmp-server	[contact <контакт-владельца-системы>] [location <расположение-системы>]		Определяет географическое положение и имя лица, ответственного за коммутатор.	13
	get-community <собственность>		Определяет параметр get community.	13
	set-community <собственность>		Определяет параметр set community.	13
	trap-community <собственность>		Определяет параметр trap community.	13
	trap-destination <ip-адрес>		Определяет до 4-х IP-адресов станций, на которые будут рассылаться Trap-команды протокола SNMP.	13
	trap-destination <ip-адрес>	[udp-port <номер-сокета>] [version <v1v2cv3][username<имя>]	Определяет IP-адрес менеджера SNMP. Всего можно настроить максимум четырех менеджеров, на которые будут отправляться Trap-команды («ловушки») SNMP.	13
	trap-destination <ip-адрес> enable traps		Включает отправку Trap-команд SNMP менеджеру.	13
		aaa	Отключает отправку менеджеру всех Trap-команд типа AAA.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`aaa <опции>`	Включает отправку менеджеру конкретных Trap-команд типа AAA. Возможные опции: «authentication» (аутентификация) или «accounting» (учет).	13
		`help`	Отображает справку по командам SNMP.	13
		`interface`	Включает отправку менеджеру всех Trap-команд типа Interface.	13
		`interface <опции>`	Включает отправку менеджеру определенных Trap-команд типа Interface. Возможные опции: «linkup» (установление соединение), «linkdown» (разрыв соединения) и «autonegotiation» (автосогласование).	13
		`ip`	Включает отправку менеджеру всех Trap-команд типа IP.	13
		`ip <опции>`	Включает отправку менеджеру определенных Trap-команд типа IP. Возможные опции: «ping» или «traceroute».	13
		`коммутатор`	Включает отправку менеджеру всех Trap-команд типа коммутатор.	13
		`switch <опции>`	Включает отправку менеджеру определенных Trap-команд типа коммутатор. Возможные опции: «stp», «mactable» или «rmon».	13
		`system`	Включает отправку менеджеру всех Trap-команд типа System.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`system <опции>`	Включает отправку менеджеру определенных Trap-команд типа System. Возможные опции: «coldstart» («холодный» запуск), «warmstart» («теплый» запуск), «fanspeed» (скорость вентиляторов), «temperature» (температура), «voltage» (напряжение), «reset» (сброс), «timesync» (синхронизация времени), «intrusionlock» (защита от вторжений) или «loopguard» (защита от образования петель).	13
	`username <имя>`	`sec-level <noauth|auth|priv>`	Определяет режим аутентификации пользователей SNMP v3.	13
		`sec-level <noauth|auth|priv> [auth <md5sha>][priv <des|aes>]`	Определяет режимы аутентификации и методы шифрования при обмене данными с менеджером SNMP.	13
	`version <v2c|v3|v3v2c>`		Определяет версию SNMP, которая будет использоваться для обмена данными с менеджером SNMP.	13
`spanning-tree`			Включает STP на коммутаторе.	13
	`mode <RSTP|MRSTP|MSTP>`		Определяет режим STP, который должен быть реализован на коммутаторе.	13
	`<список-портов>`		Включает протокол STP на заданном порту.	13
	`<список-портов> path-cost <1-65535>`		Определяет стоимость пути по протоколу STP для указанного порта.	13
	`<список-портов> priority <0-255>`		Определяет приоритет для указанного порта.	13
	`hello-time <1-10> maximum-age <6-40> forward-delay <4-30>`		Определяет параметры Hello Time, Maximum Age и Forward Delay.	13
	`help`		Отображает справку по командам.	13
	`priority <0-61440>`		Определяет приоритет моста для коммутатора.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
spq			Определяет на коммутаторе использование строгой очереди приоритетов (SPQ).	13
ssh	known-hosts <ip-адрес-хоста> <1024|ssh-rsa|ssh-dsa> <ключ>		Добавляет удаленный хост, к которому коммутатор может получить доступ с помощью службы SSH.	13
storm-control			Включает на порту коммутатора контроль широковещательных штормов.	13
subnet-based-vlan			Включает настройки VLAN на основе подсетей на коммутаторе.	13
	dhcp-vlan-override		Определяет на коммутаторе режим принудительного получения клиентами DHCP своих IP-адресов через VLAN DHCP.	13
	name <имя> source-ip <ip-адрес> mask-bits <битов-маски> vlan <vid> priority <0-7>		Определяет имя, IP-адрес, маску подсети, идентификатор VLAN ID для VLAN на основе подсети, которую необходимо настроить, а также приоритет, назначаемый исходящим в эту VLAN кадрам.	13
		inactive	Отключает настройки VLAN на основе подсетей.	13
syslog			Включает ведение системного журнала.	13
	server <ip-адрес>	inactive	Отключает передачу записей syslog на указанный сервер syslog.	13
		level [0 ~ 7]	Определяет IP-адрес сервера syslog и уровень серьезности.	13
	type <тип> facility [local 1 ..7]		Определяет тип журнала и расположение файла на сервере syslog.	13
tacacs-accounting	host <номер><ip-адрес>		Определяет IP-адрес сервера учета 1 TACACS+ или сервера учета 2 TACACS+ (номер=1 или номер=2).	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		[acct-port <номер-сокета>] [key <ключ>]	Определяет номер порта и ключ для внешнего сервера учета TACACS+.	13
	timeout <1-1000>		Определяет значение тайм-аута сервера учета TACACS+.	13
tacacs-server	host <номер> <ip-адрес>		Определяет IP-адрес сервера 1 TACACS+ или сервера 2 TACACS+ (номер=1 или номер=2).	13
		[auth-port <номер-сокета>] [key <ключ>]	Определяет номер порта и ключ для внешнего сервера TACACS+.	13
	timeout <1-1000>		Определяет значение тайм-аута сервера TACACS+.	13
	mode	<index-priority|round-robin>	Определяет режим выбора сервера TACACS+.	13
time	<Час:Мин:Сек>		Определяет время в формате «час-минута-секунда».	13
	date <месяц/день/год>		Определяет дату в формате «год, месяц, день».	13
	daylight-saving-time		Включает переход на летнее время.	13
		end-date <неделя> <день> <месяц> <час>	Определяет день и время окончания действия летнего времени.	13
		help	Отображает справку по команде daylight-saving-time.	13
		start-date <неделя> <день> <месяц> <час>	Определяет день и время начала действия летнего времени.	13
	help		Отображает справку по командам.	13
	timezone <-1200|...|1200>		Определяет разницу между всеобщим скоординированным временем UTC (ранее – время по Гринвичу, GMT) и вашим часовым поясом.	13
timesync	<daytime|time|ntp>		Определяет протокол службы времени.	13
	server <ip-адрес>		Определяет IP-адрес сервера времени.	13

Таблица 141 Обзор команд: режим настройки (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
trtcm			Включает функцию маркировки TRTCM на коммутаторе.	13
	mode <color-aware|color-blind>		Определяет режим работы маркировки TRTCM на коммутаторе.	13
trunk	<T1|T2|T3|T4|T5|T6>		Активирует группу портов.	13
	<T1|T2|T3|T4|T5|T6> lacp		Включает протокол LACP для группы портов.	13
	<T1|T2|T3|T4|T5|T6> interface <список-портов>		Добавляет порт (порты) к указанной группе портов.	13
	interface <список-портов> timeout <тайм-аут-lacp>		Определяет номер порта и период тайм-аута для протокола LACP.	13
vlan	<1-4094>		Осуществляет вход в режим настройки VLAN. Дополнительную информацию можно найти в разд. 45.12.6 на стр. 438.	13
vlan1q	gvrp		Включает протокол GVRP.	13
	port-isolation		Включает изоляцию портов.	13
vlan-stacking			Включает стекирование VLAN на коммутаторе.	13
	<SPTPID>		Определяет идентификатор протокола тега (провайдера услуг) (SP TPID).	13
vlan-type	<802.1q|port-based>		Указывает тип VLAN.	13
wfq			Определяет использование метода организации очередей WFQ (взвешенной справедливой постановки в очередь).	13
wrr			Определяет использование метода организации очередей WRR (взвешенного циклического обслуживания).	13

45.12.4 Команды interface port-channel

Команды типа `interface port-channel` в режиме настройки перечислены в следующей таблице. Эти команды используются для настройки портов.

Таблица 142 Команды interface port-channel

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
`interface port-channel <список-портов>`			Включает один порт или список портов для настройки.	13
	`arp inspection`	`trust`	Определяет порт как доверенный для функции инспекции ARP-пакетов. Пакеты ARP, приходящие через доверенные порты, коммутатором не отбрасываются ни по какой причине.	13
		`limit rate <пакетов-в-секунду>`	Определяет максимальную скорость (1-2048 пакетов в секунду), с которой коммутатор будет принимать ARP-пакеты через каждый из портов. Все пакеты ARP сверх указанного лимита коммутатором отбрасываются. Значение 0 позволяет отключить данный лимит.	13
		`limit rate <пакетов-в-секунду> burst interval <секунд>`	Определяет продолжительность интервала оценки (1-15 секунд). Под этим значением понимается период времени, в течение которого контролируется скорость поступления ARP-пакетов через каждый порт.	13
	`bandwidth-limit`		Включает лимиты скорости для входящего трафика (PIR), CIR и исходящего трафика через порты.	13
		`cir`	Включает лимиты гарантированной пропускной способности для входящего трафика через порт (порты).	13
		`cir <кбит/с>`	Определяет гарантированную пропускную способность для входящего трафика через порт (порты).	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		pir	Включает лимиты пропускной способности для входящего трафика через порт (порты).	13
		pir <кбит/с>	Определяет максимальное значение пропускной способности для входящего трафика через порт (порты).	13
		egress	Включает лимиты пропускной способности для исходящего трафика через порт (порты).	13
		egress <кбит/с>	Определяет максимальное значение пропускной способности для исходящего трафика через порт (порты).	13
	bpdu-control <peer|tunnel|discard|network>		Определяет порядок использования блоков данных мостового протокола (BPDU) в различных состояниях портов STP.	13
	broadcast-limit		Включает лимит контроля широковещательных штормов на коммутаторе.	13
		<пакетов/с>	Определяет максимальное количество широковещательных пакетов за секунду, которое может проходить через данный порт. Широковещательные пакеты сверх этого лимита коммутатором отбрасываются.	13
	dhcp snooping trust		Определяет данный порт как доверенный для функции отслеживания DHCP. Доверенные порты подключаются к серверам DHCP или другим коммутаторам, поэтому коммутатор отбрасывает пакеты DHCP от доверенных портов лишь в том случае, если скорость их поступления слишком высока.	13
	dhcp snooping limit rate <пакетов-в-секунду>		Определяет максимальную скорость поступления пакетов DHCP через доверенный порт функции отслеживания DHCP.	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	`diffserv`		Включает на порту (портах) службы DiffServ.	13
	`dlf-limit`		Включает лимит DLF-пакетов.	13
		`<пакетов/с>`	Определяет лимит прохождения DLF-пакетов через интерфейс в пакетах за секунду.	13
	`egress set <список-портов>`		Определяет список исходящих портов для VLAN на основе портов.	13
	`ethernet oam`		Включает функцию Ethernet OAM на порту (портах).	13
		`mode <active|passive>`	Определяет для портов активный или пассивный режим OAM. В активном режиме порт может передавать команды на удаленное тестирование обратной петли и обнаружение устройств. В пассивном режиме порт может только реагировать на команды Ethernet OAM.	13
		`remote-loopback supported`	Включает на портах поддержку теста удаленной обратной петли Ethernet OAM.	13
	`exit`		Осуществляет выход из командного режима interface port-channel.	13
	`flow-control`		Включает управление потоком на интерфейсе. Управление потоком помогает настроить скорость передачи в соответствии с пропускной способностью принимающего порта.	13
	`frame-type <all|tagged>`		Выбор режима – принимать ли на порт входящие кадры как с тегами, так и без тегов (all), или принимать только кадры с тегами (tagged).	13
	`ge-spq`	`<q0|q1|...|q7>`	Включает на гигабитных портах механизм строгой очереди приоритетов, начиная с указанной очереди и далее.	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	gvrp		Включает функцию, которая разрешает создание групп VLAN за пределами локального коммутатора.	13
	help		Отображает описание команд interface port-channel.	13
	igmp-filtering	profile <имя>	Применяется к указанному профилю фильтрации IGMP.	13
	igmp-group-limited		Включает лимит числа групп IGMP.	13
		number <число>	Определяет максимально допустимое число групп IGMP.	13
	igmp-immediate-leave		Включает режим немедленного отключения IGMP.	13
	igmp-querier-mode <auto|fixed|edge>		Назначает Query-режим IGMP для порта.	13
	inactive		Отключает указанный порт (порты) коммутатора.	13
	ingress-check		Включает режим, когда коммутатор отбрасывает входящие кадры для VLAN, членом которых не является данный порт.	13
	intrusion-lock		Включает функцию блокировки вторжений для порта (портов), в результате чего после отключения кабеля повторное подключение к порту оказывается невозможным.	13
	ipmc egress-untag-vlan <1-4094>		Включает на порту (портах) режим удаления тегов указанной VLAN из пакетов IP-мультивещания перед пересылкой.	13
	loopguard		Включает функцию защиты от образования петель на порту (портах).	13
	mac-authentication		Включает аутентификацию по MAC-адресам через сервер RADIUS на порту (портах).	13
	mirror		Включает зеркальное копирование порта на интерфейсе.	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		dir <ingress|egress|both>	Включает зеркальное копирование порта для входящего (ingress), исходящего (egress) или всего (both) трафика. С помощью функции зеркального копирования можно копировать трафик, идущий от одного или всех портов на другой порт или все порты, для внешнего анализа.	13
	multicast-limit		Включает лимит мультивещания на порту (портах).	13
		<пакетов/с>	Определяет количество получаемых через порт (порты) пакетов мультивещания в секунду.	13
	name <имя-порта>		Определяет имя порта (портов). Введите имя-описание (до девяти отображаемых ASCII-символов).	13
	no	arp inspection trust	Исключает данный порт из числа доверенных портов для функции инспекции ARP-пакетов.	13
		arp inspection limit	Сбрасывает лимит для функции инспекции ARP-пакетов на значение по умолчанию (0).	13
		bandwidth-limit	Отключает ограничение пропускной способности на порту (портах).	13
		bandwidth-limit cir	Отключает ограничение пропускной способности по CIR на порту (портах).	13
		bandwidth-limit pir	Отключает ограничение пропускной способности по PIR на порту (портах).	13
		bandwidth-limit egress	Отключает ограничение пропускной способности для исходящего трафика на порту (портах).	13
		broadcast-limit	Отключает лимит контроля широковещательных штормов на порту (портах).	13
		dhcp snooping trust	Исключает данный порт из числа доверенных портов для функции отслеживания DHCP.	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`dhcp snooping limit rate`	Сбрасывает лимит для функции отслеживания DHCP на значение по умолчанию (0).	13
		`diffserv`	Отключает на порту (портах) службы DiffServ.	13
		`dlf-limit`	Отключает лимит DLF-пакетов на коммутаторе.	13
		`egress-set <список-портов>`	Отключает настройки исходящего трафика для портов.	13
		`ethernet oam`	Отключает функцию Ethernet OAM на порту (портах).	13
		`ethernet oam mode`	Устанавливает на портах режим Ethernet OAM по умолчанию (активирован).	13
		`ethernet oam remote-loopback supported`	Отключает на портах поддержку теста удаленной обратной петли Ethernet OAM.	13
		`flow-control`	Включает управление потоком на порту (портах).	13
		`ge-spq`	Отключает строгую очередь приоритетов на гигабитных портах.	13
		`gvrp`	Отключает протокол GVRP на порту (портах).	13
		`igmp-filtering profile`	Отключает фильтрацию многоадресного трафика IGMP.	13
		`igmp-group-limit`	Отключение ограничения числа групп IGMP.	13
		`igmp-immediate-leave`	Отключает режим немедленного отключения IGMP.	13
		`ipmc egress-untag-vlan <идентификатор-vlan>`	Отключает на порту (портах) режим удаления тегов VLAN из исходящих кадров мультивещания перед пересылкой.	13
		`inactive`	Включает порты на коммутаторе.	13
		`ingress-check`	Отключает проверку входящих кадров на порту (портах).	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		`intrusion-lock`	Отключение функции блокировки вторжений для порта, в результате чего после отключения кабеля возможно повторное подключение к порту.	13
		`loopguard`	Отключает функцию защиты от образования петель на порту (портах).	13
		`mac-authentication`	Отключает аутентификацию по MAC-адресам через сервер RADIUS на порту (портах).	13
		`mirror`	Отключает зеркальное копирование порта (портов).	13
		`multicast-limit`	Отключает лимит трафика мультивещания на порту (портах).	13
		`protocol-based-vlan ethernet-type <тип-ethernet>`	Отключает для порта VLAN на основе указанного протокола.	13
		`trtcm`	Отключает TRTCM-маркировку на порту (портах).	13
		`vlan-trunking`	Отключает функцию магистральных соединений VLAN на порту (портах).	13
	`protocol-based-vlan name <имя> ethernet-type <тип-ethernet> vlan <идентификатор-vlan> priority <0-7>`		Создает VLAN на основе протокола с указанными параметрами.	13
		`inactive`	Отключает VLAN на основе протокола.	13
	`pvid <1-4094>`		Идентификатор VLAN (PVID) для всех портов по умолчанию – VLAN 1. Команда устанавливает PVID в диапазоне от 1 до 4094 для указанного интерфейса.	13
	`qos`	`priority <0 .. 7>`	Определяет приоритет управления качеством обслуживания для интерфейса.	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	speed-duplex	<auto|10-half|10-full|100-half|100-full|1000-full>	Определяет режим дуплекса (half – полудуплекс или full – дуплекс) и скорость (10, 100 или 1000 Мбит/с) для соединения на интерфейсе. По выбору auto (автосогласование) порт автоматически согласовывает с портом-партнером ту скорость и режим дуплекса, которые поддерживают они оба.	13
	trtcm		Включает TRTCM-маркировку на порту (портах).	13
		cir <кбит/с>	Определяет гарантированную скорость передачи информации (CIR) для порта (портов).	13
		pir <кбит/с>	Определяет пиковую скорость передачи информации (PIR) для порта (портов).	13
		dscp green <0-63>	Определяет значение DSCP, которое назначается пакетам с низким приоритетом отбрасывания.	13
		dscp yellow <0-63>	Определяет значение DSCP, которое назначается пакетам со средним приоритетом отбрасывания.	13
		dscp red <0-63>	Определяет значение DSCP, которое назначается пакетам с высоким приоритетом отбрасывания.	13
	vlan-stacking	priority <0-7>	Определяет приоритеты указанных портов при стекировании VLAN.	13
		role <access | tunnel>	Определяет роли указанных портов при стекировании VLAN.	13
		SPVID <1-4094>	Определяет VID провайдера услуг для указанных портов.	13

Таблица 142 Команды interface port-channel (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	vlan-trunking		Включает функцию магистральных соединений VLAN на портах, подключенных к другим коммутаторам или маршрутизаторам (но не портах, напрямую подключенных к конечным пользователям), что позволяет пропускать через коммутатор кадры, принадлежащие к неизвестным группам VLAN.	13
	weight <вес1> <вес2> ... <вес8>		Значение веса от 1 до 8 устанавливается для каждой переменной от вес1 до вес8.	13

45.12.5 Команды interface route-domain

Команды типа `interface route-domain` в режиме настройки перечислены в следующей таблице.

Эти команды используются для настройки доменов IP-маршрутизации.

Таблица 143 Команды interface route-domain

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
interface route-domain <ip-адрес>/ <битов-маски>			Активирует домен маршрутизации для настройки.	13
	exit		Осуществляет выход из командного режима interface routing-domain.	13
	ip	dvmrp	Включает функцию, которая разрешает создание групп VLAN за пределами локального коммутатора.	13
		igmp <v1|v2|v3>	Включает IGMP в данном домене маршрутизации и определяет версию для пакетов IGMP, которая будет использоваться коммутатором.	13
		igmp robustness-variable <2-255>	Определяет параметр робастности IGMP на коммутаторе. Данный параметр определяет степень восприимчивости подсети к потерям пакетов.	13

Таблица 143 Команды interface route-domain (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
		igmp query-interval	Определяет интервал запроса IGMP на коммутаторе. Данный параметр определяет период времени в секундах между общими сообщениями типа Query, рассылаемыми маршрутизаторами.	13
		igmp query-max-response-time <1-25>	Определяет максимальный период ожидания маршрутизатором ответа на общие сообщения типа Query.	13
		igmp last-member-query-interval <1-25>	Определяет период ожидания маршрутизатором ответа на сообщение Query для определенной группы (в секундах).	13
		ospf authentication-key <ключ>	Включает аутентификацию OSPF в данном домене маршрутизации.	13
		ospf authentication-same-aa	Определяет использование для аутентификации OSPF тех же настроек, что и в соответствующей области.	13
		ospf cost <1-65535>	Определяет стоимость OSPF в данном домене маршрутизации.	13
		ospf message-digest-key <ключ>	Определяет ключ аутентификации OSPF в данном домене маршрутизации.	13
		ospf priority <0-255>	Определяет приоритет OSPF для указанного интерфейса. Установка приоритета равным 0 исключает данный маршрутизатор из участия в выборах маршрутизатора.	13
		rip direction <Outgoing|In>	Определяет направление работы RIP в данном домене маршрутизации.	13
		vrrp authentication-key <ключ>	Определяет ключ аутентификации VRRP в данном домене маршрутизации.	13

Таблица 143 Команды interface route-domain (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	no	ip dvmrp	Отключает DVMRP в данном домене маршрутизации.	13
		ip igmp	Отключает IP IGMP в данном домене маршрутизации.	13
		ip ospf authentication-key	Определяет настройки ключа аутентификации OSPF в данном домене маршрутизации.	13
		ip ospf authentication-sama	Определяет отказ от использования для аутентификации OSPF тех же настроек, что и в соответствующей области.	13
		ip ospf cost	Отключает настройку стоимости OSPF в данном домене маршрутизации.	13
		ip ospf message-digest-key	Отключает использование ключа безопасности OSPF в данном домене маршрутизации.	13
		ip ospf priority	Сбрасывает настройку приоритета OSPF для указанного интерфейса.	13
		ip vrrp authentication-key	Сбрасывает настройки аутентификации VRRP.	13

45.12.6 Команды config-vlan

Команды типа `vlan` в режиме настройки перечислены в следующей таблице.

Таблица 144 Обзор команд: команды config-vlan

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
vlan <1-4094>			Создает новую группу VLAN.	13
	exit		Осуществляет выход из режима настройки VLAN.	13
	fixed <список-портов>		Закрепляет указанный порт (порты) за данной группой VLAN.	13
	forbidden <список-портов>		Указывает, какому порту (портам) запрещено присоединяться к данной группе VLAN.	13
	help		Отображает список доступных команд VLAN.	13

Таблица 144 Обзор команд: команды config-vlan (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	inactive		Отключает указанную группу VLAN.	13
	ip address	<ip-адрес> <маска>	Определяет IP-адрес коммутатора в данной VLAN.	13
		<ip-адрес> <маска> manageable	Определяет IP-адрес коммутатора в данной VLAN и разрешает удаленное управление для данного IP-адреса.	13
		default-gateway <ip-адрес>	Определяет IP-адрес шлюза по умолчанию для данной VLAN.	13
	name <имя>		Указывает имя, которое будет использоваться в целях идентификации.	13
	no	fixed <список-портов>	Делает фиксированный порт (порты) обычным портом (портами).	13
		forbidden <список-портов>	Делает запрещенный порт (порты) обычным портом (портами).	13
		inactive	Включает указанную VLAN.	13
		ip address <ip-адрес> <маска>	Удаляет указанный IP-адрес и маску подсети для данной VLAN.	13
		ip address default-gateway	Удаляет шлюз по умолчанию для данной VLAN.	13
		untagged <список-портов>	Указывает порт (порты), для которых необходимо включить добавление тегов ко всем исходящим кадрам, передаваемым с идентификатором данной группы VLAN.	13
	normal <список-портов>		Указывает порт (порты), которые могут динамически присоединяться к данной группе VLAN по протоколу GVRP.	13
	untagged <список-портов>		Указывает порт (порты), для которых необходимо отключить добавление тегов ко всем исходящим кадрам, передаваемым с идентификатором данной группы VLAN.	13

45.13 Команды mvr

Команды типа `mvr` в режиме настройки перечислены в следующей таблице.

Таблица 145 Обзор команд: Команды mvr

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
`mvr <1-4094>`			Осуществляет вход в режим настройки MVR (регистрации VLAN-сети мультивещания).	13
	`8021p-priority <0-7>`		Осуществляет выход из режима настройки MVR.	13
	`exit`		Осуществляет выход из режима настройки MVR.	13
	`group <имя> start-address <ip-адрес> end-address <ip-адрес>`		Определяет диапазон адресов группы мультивещания для MVR.	13
	`inactive`		Включает настройки MVR.	13
	`mode <dynamic|compatible>`		Назначает режим MVR (dynamic – динамический или compatible – режим совместимости).	13
	`name <имя>`		Определяет имя MVR для идентификации.	13
	`no`	`group`	Отключение всех настроек групп MVR.	13
		`group <имя>`	Отключение настроек указанной группы MVR.	13
		`inactive`	Включение MVR.	13
		`receiver-port <список-портов>`	Отключает порты-приемники. Порт-приемник MVR способен только принимать трафик мультивещания во VLAN-сети мультивещания.	13
		`source-port <список-портов>`	Отключает порты-источники. Порт-источник MVR способен передавать и принимать трафик мультивещания во VLAN-сети мультивещания.	13
		`tagged <список-портов>`	Определяет для портов режим удаления тегов VLAN.	13

Таблица 145 Обзор команд: Команды mvr (продолжение)

КОМАНДА			ОПИСАНИЕ	УРОВЕНЬ ПРИВИЛЕГИЙ
	receiver-port <список-портов>		Определяет порты-приемники. Порт-приемник MVR способен только принимать трафик мультивещания во VLAN-сети мультивещания.	13
	source-port <список-портов>		Определяет порты-источники. Порт-источник MVR способен передавать и принимать трафик мультивещания во VLAN-сети мультивещания.	13
	tagged <список-портов>		Определяет для портов режим добавления тегов VLAN.	13

46

Команды пользовательского и привилегированного режимов

В данной главе описаны некоторые команды, которые можно использовать в пользовательском и привилегированном режимах.

46.1 Обзор

Приведенные ниже примеры команд демонстрируют возможности диагностики и управления коммутатором из пользовательского и привилегированного режимов.

46.2 Команды show

Чаще всего используются команды `show`.

46.2.1 show system-information

Синтаксис:

```
show system-information
```

Эта команда отображает общую информацию о системе (например, номер версии встроенного программного обеспечения и время работы системы).

Ниже показан пример.

```
sysname# show system-info
System Name              : ES-4124
System Contact           :
System Location          :
Ethernet Address         : 00:19:cb:00:00:02
ZyNOS F/W Version        : V3.80(AIC.0)b4 | 03/30/2007
RomRasSize               : 3617086
System up Time           :   307:31:34 (6994a9d ticks)
Bootbase Version         : V0.8 | 03/13/2007
ZyNOS CODE               : RAS Mar 21 2007 20:48:38
Product Model            : ES-4124
```

46.2.2 show ip

Синтаксис:

```
show ip
```

Эта команда отображает информацию о протоколе IP (например, IP-адрес и маска подсети) на всех интерфейсах коммутатора.

Ниже показан пример настроек интерфейса по умолчанию.

```
sysname> show ip
Management IP Address
     IP[192.168.0.1], Netmask[255.255.255.0], VID[0]
IP Interface
     IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
sysname>
```

46.2.3 show logging

Синтаксис:

```
show logging
```

Данная команда отображает системные журналы. Пример показан на следующем рисунке.

```
sysname# show logging
   1 Thu Jan  1 00:02:08 1970 PP05 -WARN  SNMP TRAP 3: link up
   2 Thu Jan  1 00:03:14 1970       INFO  adjtime task pause 1 day
   3 Thu Jan  1 00:03:16 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
   4 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 1: warm start
   5 Thu Jan  1 00:03:16 1970 PINI -WARN  SNMP TRAP 3: link up
   6 Thu Jan  1 00:03:16 1970 PINI  INFO  main: init completed
   7 Thu Jan  1 00:00:13 1970 PP26  INFO  adjtime task pause 1 day
   8 Thu Jan  1 00:00:14 1970 PP0f -WARN  SNMP TRAP 26: Event On Trap
   9 Thu Jan  1 00:00:14 1970 PINI -WARN  SNMP TRAP 0: cold start
  10 Thu Jan  1 00:00:14 1970 PINI  INFO  main: init completed
  11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
  11 Thu Jan  1 00:00:04 1970 PP05 -WARN  SNMP TRAP 3: link up
Clear Error Log (y/n):
```

После очистки журнала (нажатием на `y` в ответ на вопрос `Clear Error Log (y/n):`), просмотреть его еще раз уже невозможно.

46.2.4 show interface

Синтаксис:

```
show interface [номер-порта]
```

Эта команда отображает статистику порта. На показанном ниже примере видно, что порт 2 работает, и показана его сопутствующая информация.

```
sysname# show interface 2
  Port Info     Port NO.                :2
                Link                    :100M/F
                Status                  :FORWARDING
                LACP                    :Disabled
                TxPkts                  :0
                RxPkts                  :63
                Errors                  :0
                Tx KBs/s                :0.0
                Rx KBs/s                :0.0
                Up Time                 :0:02:33
  TX Packet     Tx Packets              :0
                Multicast               :0
                Broadcast               :0
                Pause                   :0
                Tagged                  :0
  RX Packet     Rx Packets              :63
                Multicast               :0
                Broadcast               :63
                Pause                   :0
                Control                 :0
  TX Collison   Single                  :0
                Multiple                :0
                Excessive               :0
                Late                    :0
  Error Packet  RX CRC                  :0
                Length                  :0
                Runt                    :0
  Distribution  64                      :3
                65 to 127               :44
                128 to 255              :14
                256 to 511              :2
                512 to 1023             :0
                1024 to 1518            :0
                Giant                   :0
sysname#
```

46.2.5 show mac address-table

Синтаксис:

```
show mac address-table <all <сортировка>|static>
```

Где

<сортировка> = обозначает критерий сортировки (MAC-адрес, идентификатор VLAN или порт).

Эта команда отображает MAC-адреса, хранящиеся в коммутаторе. На приведенном ниже примере показана таблица статических MAC-адресов.

```
sysname# show mac address-table static
Port      VLAN ID        MAC Address         Type
CPU       1              00:a0:c5:01:23:46   Static
sysname#
```

46.3 ping

Синтаксис:

```
ping <ip-адрес|имя-хоста> < [in-band|out-of-band|vlan <идентификатор-vlan> ]
[ size
-> <0-1472> ] [ -t ]>
```

Где

`<ip-адрес|имя-хоста>`	=	IP-адрес или имя хоста Ethernet-устройства.
`[ in-band|out-of-band|vlan <vlan-id> ]`	=	Определяет сетевой интерфейс или идентификатор VLAN ID, к которой относится устройство Ethernet. `out-of-band` означает порт управления, тогда как `in-band` – все остальные порты коммутатора.
`[ size <0-1472> ]`	=	Определяет размер отправляемого пакета.
`[ -t ]`	=	Отправляет ping-пакеты на Ethernet-устройство бесконечным потоком. Чтобы прервать этот процесс, нажмите `[CTRL]+ C`.

Эта команда отправляет ping-пакеты на Ethernet-устройство. На приведенном ниже примере показаны ping-запросы и ответ на них от Ethernet-устройства с IP-адресом `192.168.1.100`.

```
sysname# ping 192.168.1.100
 sent  rcvd  rate    rtt     avg    mdev     max     min  reply from
    1     1  100       0       0       0       0       0  192.168.1.100
    2     2  100       0       0       0       0       0  192.168.1.100
    3     3  100       0       0       0       0       0  192.168.1.100
sysname#
```

46.4 traceroute

Синтаксис:

```
traceroute <ip-адрес|имя-хоста> [in-band|out-of-band|vlan <идентификатор-
vlan>][ttl
-> <1-255>] [wait <1-60>] [queries <1-10>]
```

Где

`<ip-адрес|имя-хоста>`	=	IP-адрес или имя хоста Ethernet-устройства.
`[ in-band|out-of-band|vlan <vlan-id> ]`	=	Определяет сетевой интерфейс или идентификатор VLAN, к которой принадлежит Ethernet-устройство.
`[ttl <1-255>]`	=	Указывает период времени жизни пакета (TTL).
`[wait <1-60>]`	=	Указывает период ожидания.
`[queries <1-10>]`	=	Указывает, сколько попыток трассировки должен совершить коммутатор.

Эта команда отображает информацию о маршруте к Ethernet-устройству. На приведенном ниже примере показана информация о маршруте к Ethernet-устройству с IP-адресом `192.168.1.100`.

```
sysname> traceroute 192.168.1.100
traceroute to 192.168.1.100, 30 hops max, 40 byte packet
  1:192.168.1.100 (10 ms) (10 ms) (0 ms)
traceroute done:
sysname>
```

46.5 Копирование атрибутов порта

Для копирования атрибутов порта на один или несколько других портов можно использовать команду `copy running-config`.

Синтаксис:

```
copy running-config interface port-channel <порт> <список-портов>
copy running-config interface port-channel <порт> <список-портов>
-> [active] [name] [speed-duplex] [bpdu-control] [flow-control]
-> [intrusion-lock] [vlan1q] [vlan1q-member] [bandwidth-limit]
-> [vlan-stacking] [port-security] [broadcast-storm-control] [mirroring]
-> [port-access-authenticator] [queuing-method] [igmp-filtering]
-> [spanning-tree] [mrstp] [port-based-vlan] [protocol-based-vlan]
-> [mac-authentication] [trtcm] [ethernet-oam] [loopguard] [arp-inspection]
-> [dhcp-snooping]
```

Где

`copy running-config interface port-channel <порт> <список-портов>`	=	Копирование всех доступных атрибутов порта на один или несколько других портов.
`copy running-config interface port-channel <порт> <список-портов> [active ... ]`	=	Копирование только указанных атрибутов порта на один или несколько других портов.

Ниже показан пример.

- Скопировать все атрибуты с порта 1 на порт 2
- Скопировать некоторые атрибуты (настроек активности, ограничения пропускной способности и протокола покрывающего дерева) на порты 5-8

```
sysname# copy running-config interface port-channel 1 2
sysname# copy running-config interface port-channel 1 5-8 active
bandwidth-limit spanning-tree
```

46.6 Обслуживание файла конфигурации

В следующих разделах описано управление файлами конфигурации.

46.6.1 Использование другого файла конфигурации

На коммутаторе можно сохранить не более двух файлов конфигурации. В каждый момент времени может использоваться только один из них. По умолчанию коммутатор использует первый файл конфигурации (с порядковым номером 1). Можно переключить коммутатор на использование другого файла конфигурации. Переключить коммутатор на использование другого файла конфигурации можно двумя способами: с использованием перезапуска коммутатора («холодный» перезапуск) или с использованием перезапуска системы («теплый» перезапуск).

Чтобы перезапустить коммутатор и переключить его на использование другого файла конфигурации (если таковой указан), введите команду `boot config`. Ниже показан пример перезапуска коммутатора с переключением на второй файл конфигурации.

```
sysname# boot config 2
```

Чтобы перезапустить систему и переключить ее на использование другого файла конфигурации (если таковой указан), введите команду `reload config`. Ниже показан пример перезапуска системы с переключением на второй файл конфигурации.

```
sysname# reload config 2
```

При использовании команды `write memory` без указания порядкового номера файла конфигурации коммутатор сохраняет изменения в тот файл конфигурации, который используется коммутатором в настоящий момент.

46.6.2 Возврат к заводским настройкам по умолчанию

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

1. Введите команду `erase running config`, чтобы перезагрузить текущие настройки.
2. Чтобы сохранить изменения в текущем файле конфигурации, введите команду `write memory`. Если необходимо сбросить второй файл конфигурации, воспользуйтесь командой `write memory` еще раз с указанием соответствующего порядкового номера.

На приведенном ниже примере продемонстрирован возврат к заводским настройкам по умолчанию для обоих файлов конфигурации.

```
sysname# erase running-config
sysname# write memory
sysname# write memory 2
```

47

Команды режима настройки

В данной главе описывается включение и настройка функций коммутатора с использованием команд. Дополнительную информацию по этим функциям можно найти в соответствующих главах ранее.

47.1 Включение отслеживания многоадресного трафика IGMP

Чтобы включить отслеживание IGMP на коммутаторе, введите `igmp-snooping` и нажмите [ENTER]. Также имеется возможность настроить порядок обработки трафика от неизвестных групп мультивещания с использованием параметра `unknown-multicast-frame`.

Синтаксис:

```
igmp-snooping
igmp-snooping 8021p-priority <0-7>
igmp-snooping host-timeout <1-16711450>
igmp-snooping leave-timeout <1-16711450>
igmp-snooping unknown-multicast-frame <drop|flooding>
igmp-snooping reserved-multicast-group <drop|flooding>
```

Где

`igmp-snooping`	=	Включает на коммутаторе отслеживание многоадресного трафика IGMP.
`8021p-priority`	=	Определяет приоритет (0-7), который устанавливается коммутатором для исходящих управляющих пакетов IGMP.
`host-timeout <1-16711450>`	=	Определяет период тайм-аута на коммутаторе для запросов IGMP типа Report. Если в течение указанного периода тайм-аута для хоста коммутатор не получает IGMP-пакет типа Report для группы мультивещания от указанного порта, данный порт удаляется из списка участников группы мультивещания.
`leave-timeout <1-16711450>`	=	Определяет время, в течение которого коммутатор ожидает от членов группы мультивещания ответа на запрос Leave. При отсутствии ответа в течение указанного периода тайм-аута коммутатор удаляет порт из группы мультивещания.

`unknown-multicast-frame <drop|flooding>`	=	Позволяет выбрать для пакетов от неизвестных групп мультивещания режим отбрасывания или пересылки на все порты.
`reserved-multicast-group <drop|flooding>`	=	Позволяет выбрать для пакетов от зарезервированных групп мультивещания режим отбрасывания или пересылки на все порты.

Ниже показан пример.

- Включить отслеживание многоадресного трафика IGMP на коммутаторе.
- Назначить `тайм-аут хоста` и `тайм-аут Leave` равными 30 секундам
- Назначить на коммутаторе режим отбрасывания пакетов от неизвестных групп мультивещания.

```
sysname(config)# igmp-snooping
sysname(config)# igmp-snooping host-timeout 30
sysname(config)# igmp-snooping leave-timeout 30
sysname(config)# igmp-snooping unknown-multicast-frame drop
```

47.2 Настройка фильтра IGMP

Для настройки профилей фильтрации IGMP используются следующие команды режима настройки (config).

Синтаксис:

```
igmp-filtering
igmp-filtering profile <имя> start-address <ip-адрес> end-address <ip-адрес>
```

Где

`igmp filtering`	=	Включает фильтрацию IGMP на коммутаторе.
`profile <имя>`	=	Определяет имя (до 32 алфавитно-цифровых символов) для данного профиля IGMP. При необходимости изменить настройки существующего профиля IGMP необходимо ввести его имя и затем параметры начального `start-address` и конечного `end-address` адресов диапазона.
`start-address`	=	Определяет начальный адрес диапазона IP-адресов мультивещания, который необходимо включить в профиль фильтрации IGMP. В качестве IP-адресов мультивещания используются IP-адреса в диапазоне от 224.0.0.0 до 239.255.255.255.
`end-address`	=	Определяет конечный адрес диапазона IP-адресов мультивещания, который необходимо включить в профиль фильтрации IGMP. В качестве IP-адресов мультивещания используются IP-адреса в диапазоне от 224.0.0.0 до 239.255.255.255.

Ниже показан пример.

- Включить фильтрацию IGMP на коммутаторе.
- Создать профиль фильтрации IGMP **filter1** и определить для данного профиля IP-адресов мультивещания в диапазоне от **224.255.255.0** до **225.255.255.255**.

```
sysname(config)# igmp-filtering
sysname(config)# igmp-filtering profile filter1 start-address
224.255.255.0 end-address 225.255.255.255
```

47.3 Включение протокола STP

Для включения и настройки на коммутаторе протокола покрывающего дерева STP используются команды `spanning-tree` и `mrstp`. Различие между командами заключается в том, что с помощью `spanning-tree` можно настроить только одну конфигурацию покрывающего дерева, тогда как `mrstp` позволяет работать с несколькими экземплярами.

Синтаксис:

```
spanning-tree
spanning-tree priority <0-61440>
spanning-tree hello-time <1-10> maximum-age <6-40> forward-delay <4-30>
spanning-tree <список-портов> path-cost <1-65535>
spanning-tree <список-портов> priority <0-255>
```

и

```
mrstp <номер-дерева> <cr>
mrstp <номер-дерева> priority <0-61440>
mrstp <номер-дерева> hello-time <1-10> maximum-age <6-40> forward-delay
-> <4-30>
mrstp interface <список-портов> <cr>
mrstp interface <список-портов> path-cost <1-65535>
mrstp interface <список-портов> priority <0-255>
mrstp interface <список-портов> treeIndex <1-2>
```

Где

`spanning-tree`	=	Включает STP на коммутаторе.
`mrstp <номер-дерева>`		Включает конкретную конфигурацию дерева.

`priority <0-61440>`	=	Определяет приоритет моста для коммутатор. Чем меньшее числовое значение будет выбрано, тем выше будет приоритет у этого моста. 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. Параметр Bridge Priority определяет корневой мост, который, в свою очередь, определяет параметры Hello Time, Max Age и Forwarding Delay.
`hello-time <1-10>`	=	Определяет временной интервал в секундах между конфигурационными сообщениями BPDU (блоки данных мостового протокола), генерируемыми корневым коммутатором.
`maximum-age <6-40>`	=	Определяет 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.
`forward-delay <4-30>`	=	Определяет временной интервал (в секундах), в течение которого коммутатор 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.
`<список-портов>`	=	Включает протокол STP на указанных портах.
`path-cost <1-65535>`		Определяет стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Она назначается в зависимости от скорости моста.

<список-портов> priority <0-255>	=	Определяет 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.
<список-портов> treeIndex <1-2>	=	Определяет, к какому дереву STP должны принадлежать данные порты. (только для команды mrstp).

Пример использования команды spanning-tree приводится ниже.

- Включить протокол STP коммутаторе.
- Назначить приоритет моста для коммутатора равным 0.
- Назначить на коммутаторе параметры Hello Time = 4, Maximum Age = 20 и Forward Delay = 15.
- Включить STP на порту 5 со стоимостью пути, равной 150.
- Назначить приоритет для порта 5 равным 20.

```
sysname(config)# spanning-tree priority 0
sysname(config)# spanning-tree hello-time 4 maximum-age 20 forward-delay
15
sysname(config)# spanning-tree 5 path-cost 150
sysname(config)# spanning-tree 5 priority 20
```

47.4 Примеры работы команды no

Существует несколько часто используемых команд из группы команд no. Группой команд no называют команды, перед которыми ставится ключевое слово no. Это ключевое слово изменяет действие команды на противоположное. В большинстве случаев команда no отключает, сбрасывает или очищает настройки. В некоторых случаях, однако, команда no может активировать функции. В данном разделе приводится ряд примеров использования данных команд.

47.4.1 Команды отключения

Команда no позволяет отключать функции коммутатора.

Синтаксис:

```
no spanning-tree
no mirror-port
```

Отключает STP на коммутаторе.

Отключает зеркальное копирование портов на коммутаторе.

47.4.2 Команды сброса

Команда no позволяет сбрасывать настройки коммутатора в значения по умолчанию.

Синтаксис:

```
no https timeout
```

Возвращает значение тайм-аута для HTTPS-сессии к значению по умолчанию.

Ниже показан пример. Вернуть для тайм-аута сессии значение по умолчанию – 300 секунд.

```
sysname(config)# no https timeout
  Cache timeout 300
```

47.4.3 Команды повторного включения

Команда no позволяет также повторно включить ранее отключенные функции.

Синтаксис:

```
no ip route <ip-адрес> <маска> inactive
```

Где

`<ip-адрес> <маска> inactive`	=	Повторное включение IP-маршрута с указанным IP-адресом и маской подсети.

Ниже показан пример.

- Включить IP-маршрут с IP-адресом 192.168.11.1 и маской подсети 255.255.255.0. Данный IP-маршрут уже должен быть создан ранее и отключен до выполнения команды повторного включен.

```
sysname(config)# no ip route 192.168.11.1 255.255.255.0 inactive
```

47.4.4 Другие примеры использования команды no

В некоторых случаях команда `no` позволяет отключить функцию, отключить определенную опцию в функции или отключить функцию на уровне отдельного порта.

47.4.4.1 no trunk

Синтаксис:

```
no trunk <T1|T2|T3|T4|T5|T6>
no trunk <T1|T2|T3|T4|T5|T6> lacp
no trunk <T1|T2|T3|T4|T5|T6> interface <список-портов>
```

Где

`<T1|T2|T3|T4|T5|T6>`	=	Отключает указанную группу портов.

<T1|T2|T3|T4|T5|T6> lacp	=	Отключает протокол LACP в указанной группе портов.
<T1|T2|T3|T4|T5|T6> interface <список-портов>	=	Удаляет порты из указанной группы портов.

Ниже показан пример.

- Отключить группу портов 1 (T1).
- Отключить протокол LACP для группы портов 3 (T3).
- Удалить порты 1, 3, 4 и 5 из группы портов 2 (T2).

```
sysname(config)# no trunk T1
sysname(config)# no trunk T3 lacp
sysname(config)# no trunk T2 interface 1,3-5
```

47.4.4.2 no port-access-authenticator

Синтаксис:

```
no port-access-authenticator
no port-access-authenticator <список-портов> reauthenticate
no port-access-authenticator  <список-портов>
```

Где

	=	Отключает аутентификацию портов на коммутаторе.
<список-портов> reauthenticate	=	Отключает механизм повторной аутентификации на указанном порту (портах).
<список-портов>	=	Отключает аутентификацию на указанных портах.

Ниже показан пример.

- Отключить аутентификацию на коммутаторе.
- Отключить повторную аутентификацию на портах 1, 3, 4 и 5.
- Отключение аутентификации на портах 1, 6 и 7.

Рисунок 203 Пример работы команды no port-access-authenticator

```
sysname(config)# no port-access-authenticator
sysname(config)# no port-access-authenticator 1,3-5 reauthenticate
sysname(config)# no port-access-authenticator 1,6-7
```

47.4.4.3 no ssh

Синтаксис:

```
no ssh key <rsa1|rsa|dsa>
no ssh known-hosts <ip-адрес-хоста>
no ssh known-hosts <ip-адрес-хоста> [1024|ssh-rsa|ssh-dsa]
```

Где

`key <rsa1|rsa|dsa>`	=	Отключает серверный ключ шифрования SSH. Данный коммутатор поддерживает протокол SSH версий 1 и 2, работающий с методами аутентификации RSA и DSA.
`known-hosts <ip-адрес-хоста>`	=	Удаляет указанные удаленные хосты из списка всех известных хостов.
`known-hosts <ip-адрес-хоста> [1024|ssh-rsa|ssh-dsa]`	=	Исключает удаленные хосты с указанным типом открытого ключа (1024-битный RSA1, RSA или DSA).

Ниже показан пример.

- Отключить защищенный ключ шифрования SSH по алгоритму RSA1.
- Исключить удаленный хост с IP-адресом 172.165.1.8 из списка всех известных хостов.
- Исключить удаленный хост с IP-адресом 172.165.1.9 и ключом шифрования SSH по алгоритму RSA из списка всех известных хостов.

```
sysname(config)# no ssh key rsa1
sysname(config)# no ssh known-hosts 172.165.1.8
sysname(config)# no ssh known-hosts 172.165.1.9 ssh-rsa
```

47.5 Команды управления методами организации очередей

Команды управления методами организации очередей используются для настройки очередей для исходящего трафика на коммутаторе. Для коммутатора можно выбрать только один метод организации очередей.

Синтаксис:

```
spq

wfq

wrr
```

Где

`spq`	=	Определяет использование метода организации очередей SPQ (строгой очереди приоритетов).
`wfq`	=	Определяет использование метода организации очередей WFQ (взвешенной справедливой постановки в очередь).
`wrr`	=	Определяет использование метода организации очередей WRR (взвешенного циклического обслуживания).

Ниже показан пример.

- Назначить метод организации очередей SPQ.

```
sysname(config)# spq
```

47.6 Команды статических маршрутов

С помощью команды `ip route` можно создавать и настраивать статические маршруты на коммутаторе.

Синтаксис:

```
ip route <ip-адрес> <маска> <адрес-следующего-перехода>
ip route <ip-адрес> <маска> <адрес-следующего-перехода> [metric
<метрика>][name <имя>]
--> [inactive]
```

Где

`<ip-адрес>`	=	Определяет сетевой IP-адрес конечного пункта назначения.
`<маска>`	=	Определяет маску подсети для данного пункта назначения.
`<адрес-следующего-перехода>`	=	Определяет 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>]`	=	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.
`[name <имя>]`	=	Определяет имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать этот маршрут.
`[inactive]`	=	Отключает статический маршрут.

Ниже показан пример.

- Создать статический маршрут с IP-адресом пункта назначения 172.21.1.104, маской подсети 255.255.0.0 и IP-адресом шлюза 192.168.1.2.
- Назначить статическому маршруту значение метрики 2.

- Назначить статическому маршруту имя «route1».

```
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 metric 2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 name route1
```

47.7 Включение фильтрации MAC-адресов

Имеется возможность создать фильтр, который будет отбрасывать пакета в зависимости от MAC-адреса источника или MAC-адреса пункта назначения.

Синтаксис:

```
mac-filter name <имя> mac <mac-адрес> vlan <идентификатор-vlan> drop <src/
dst/both>
```

Где

`name <имя>`	=	Имя правила фильтрации.
`mac <mac-адрес>`	=	Определяет MAC-адрес, который необходимо фильтровать.
`vlan <идентификатор-vlan>`	=	Определяет сеть VLAN, к которой относится данное правило.
`drop <src/dst/both>`	=	Выбирает порядок работы правила. • src – отбрасывать пакеты, поступающие от указанного MAC-адреса • dst – отбрасывать пакеты, направляемые на указанный MAC-адрес • both – отбрасывать пакеты, поступающие от указанного MAC-адреса и направляемые на указанный MAC-адрес

Ниже показан пример.

- Создать правило фильтрации с именем «filter1».
- Отбрасывать пакеты, поступающие от и направляемые на MAC-адрес 00:12:00:12:00:12 в сети VLAN 1.

```
sysname(config)# mac-filter name filter 1
sysname(config)# mac-filter name filter 1 mac 00:12:00:12:00:12 vlan 1 drop
both
```

47.8 Включение группировки портов

Чтобы создать и активировать группу портов, введите `trunk` и номера портов, которые необходимо объединить в группу, после чего нажмите [ENTER].

Синтаксис:

```
trunk <T1|T2|T3|T4|T5|T6>
trunk <T1|T2|T3|T4|T5|T6> interface <список-портов>
trunk <T1|T2|T3|T4|T5|T6> lacp
```

Где

`<T1|T2|T3|T4|T5|T6>`	=	Включение группы портов.
`<T1|T2|T3|T4|T5|T6> interface <список-портов>`	=	Включение портов в группу.
`<T1|T2|T3|T4|T5|T6> lacp`	=	Включение протокола LACP в группе.

Ниже показан пример.

- Создать группу портов 1 на коммутаторе.
- Включить порты 5-8 в группу 1.
- Включить протокол динамической агрегации каналов (LACP) для группы 1.

```
sysname(config)# trunk t1
sysname(config)# trunk t1 interface 5-8
sysname(config)# trunk t1 lacp
```

47.9 Включение аутентификации портов

Чтобы включить аутентификацию портов, необходимо указать сведения о сервере RADIUS и выбрать порты, для которых будет применяться внешняя аутентификация. Имеется возможность настроить несколько серверов RADIUS и определить порядок обработки коммутатором запросов на аутентификацию.

47.9.1 Настройки сервера RADIUS

Для настройки сервера RADIUS используется команда `radius-server`.

Синтаксис:

```
radius-server host <номер> <ip-адрес>
radius-server host <номер> <ip-адрес> [acct-port <номер-сокета>] [key
--> <ключ>]
radius-server timeout <1-1000>
radius-server mode <priority|round-robin>
```

Где

`radius-server host <номер> <ip-адрес>`	=	Определяет IP-адрес сервера RADIUS.
`[acct-port <номер-сокета>]`	=	Изменяет установленный по умолчанию UDP-порт (1812) сервера RADIUS.
`[key <ключ>]`	=	Определяет пароль (до 32 алфавитно-цифровых символов), который будет служить общим ключом для внешнего сервера RADIUS и коммутатора.
`radius-server timeout <1-1000>`	=	Определяет период тайм-аута (в секундах), в течение которого коммутатор будет ожидать ответа от сервера RADIUS. При настройке 2 серверов RADIUS данный тайм-аут представляет собой общее время, в течение которого коммутатор ожидает ответа от любого из серверов.
`mode <priority|round-robin>`	=	Определяет режим обработки коммутатором запросов к серверу RADIUS от клиентов. (Применяется лишь при настройке нескольких серверов RADIUS). `priority` – При отправке клиентом запроса на аутентификацию к серверу RADIUS через коммутатор этот запрос пересылается коммутатором на сервер RADIUS. При отсутствии ответа в течение половины периода тайм-аута коммутатор пересылает запрос на второй сервер RADIUS. `round-robin` – При отправке клиентом запроса на аутентификацию к серверу RADIUS через коммутатор этот запрос пересылается коммутатором на первый сервер RADIUS. При отсутствии ответа в течение установленного периода происходит тайм-аут. Клиент направляет запрос на авторизацию повторно, и этот запрос пересылается коммутатором на второй сервер RADIUS.

Пример можно найти в разд. 47.9.2 на стр. 462.

47.9.2 Настройки аутентификации портов

Для настройки средств безопасности портов на коммутаторе используется команда `port-access-authenticator`.

Синтаксис:

```
port-access-authenticator
port-access-authenticator <список-портов>
port-access-authenticator <список-портов> reauthenticate
port-access-authenticator <список-портов> reauth-period <период-повторной-
аутентификации>
```

Где

`port-access-authenticator`	=	Включает аутентификацию портов на коммутаторе.
`port-access-authenticator <список-портов>`	=	Определяет порты, для которых требуется аутентификация.
`reauthenticate`	=	Включает повторную аутентификацию для порта.
`reauth-period <период-повторной-аутентификации>`	=	Определяет, как часто клиенту требуется вводить заново свое имя пользователя и пароль, чтобы оставаться подключенным к порту.

Ниже показан пример.

- Определить RADIUS-сервер 1 с IP-адресом 10.10.10.1, номером порта 1890 и строкой secretKey в качестве пароля. Дополнительную информацию о командах, связанных с сервером RADIUS, можно найти в разд. 47.9.1 на стр. 461.
- Определить период тайм-аута, в течение которого коммутатор ожидает ответа от сервера RADIUS, равным 30 секундам.
- Включить аутентификацию портов на портах с 4 по 8.
- Активировать повторную аутентификацию на портах.
- Определить интервал повторной аутентификации клиента равным 1800 секундам.

```
sysname(config)# radius-server host 1 10.10.10.1 acct-port 1890 key
--> secretKey
sysname(config)# radius-server timeout 30
sysname(config)# port-access-authenticator
sysname(config)# port-access-authenticator 4-8
sysname(config)# port-access-authenticator 4-8 reauthenticate
sysname(config)# port-access-authenticator 4-8 reauth-period 1800
```

48

Команды interface

Существует несколько часто используемых команд настройки из группы команд `interface`.

48.1 Обзор

С помощью команд interface можно настраивать параметры отдельных портов коммутатора.

48.2 Примеры команд interface

В данном разделе приводятся примеры часто используемых команд interface.

48.2.1 interface port-channel

Эта команда используется для включения указанных портов для настройки. Несколько идущих не подряд портов указываются через запятую. Диапазон портов можно указать через дефис.

Синтаксис:

```
interface port-channel <список-портов>
```

Ниже показан пример.

- Войти в режим настройки.
- Включить для настройки порты 1, 3, 4 и 5.
- Приступить к настройке этих портов.

```
sysname# config
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)#
```

48.2.2 Реализация функций Ethernet OAM уровня канала передачи данных IEEE 802.3ah

Функции Ethernet OAM (эксплуатация, администрирование и обслуживание) уровня канала передачи данных, описанные в IEEE 802.3ah, представляют собой протокол мониторинга состояния канала. В этом протоколе для передачи информации о состоянии канала между непосредственно подключенными устройствами Ethernet используются блоки данных протокола OAM (OAMPDU). Оба устройства должны поддерживать стандарт IEEE 802.3ah. Так как функции Ethernet OAM уровня канала передачи данных работают на втором уровне модели OSI (эталонной модели взаимодействия открытых систем), для мониторинга или устранения неполадок с сетевыми соединениями не требуются ни протокол IP, ни протокол SNMP.

Данный коммутатор поддерживает следующие функции IEEE 802.3ah:

- **Обнаружение (Discovery)** – данная функция позволяет идентифицировать устройства на каждой из сторон канала Ethernet, а также OAM-настройки этих устройств.
- **Удаленная обратная петля (Remote Loopback)** – данная функция запускает на устройствах Ethernet тест удаленной обратной петли.

Синтаксис:

```
ethernet oam
ethernet oam mode <active|passive>
ethernet oam remote-loopback supported
ethernet oam remote-loopback test <список-портов>
show ethernet oam discovery <список-портов>
show ethernet oam statistics <список-портов>
show ethernet oam summary
```

Где

`ethernet oam`	=	Включает функцию Ethernet OAM на указанном порту.
`mode <active|passive>`	=	Значение `active` включает возможность инициирования тестов удаленной обратной петли или команд обнаружения на портах. Значение `passive` отключает возможность инициирования тестов удаленной обратной петли или команд обнаружения на портах. В этом режимы порты могут только реагировать на запросы от портов в режиме «active».
`remote-loopback supported`	=	Включает функцию удаленной обратной петли на порту (портах).
`remote-loopback test <список-портов>`	=	Инициирует тест удаленной обратной петли на указанном порту (портах).
`discovery <список-портов>`	=	Инициирует запрос на обнаружение на указанном порту (портах). При выполнении запроса возвращается состояние функции Ethernet OAM на указанном порту, а также на удаленном подключенном порту.

`statistics <список-портов>`	=	Отображает количество отправленных и полученных блоков данных OAMPDU для указанного порта (портов).
`summary`	=	Отображает состояние всех включенных портов Ethernet OAM на коммутаторе.

Пример настройки показан ниже.

- Включить для настройки порт 7.
- Включить на порту функции Ethernet OAM и перевести порт в активный режим.
- Включить на порту тест удаленной обратной петли.

```
sysname(config)# interface port-channel 7
sysname(config-interface)# ethernet oam
sysname(config-interface)# ethernet oam mode active
sysname(config-interface)# ethernet oam remote-loopback supported
```

Ниже приводится несколько примеров использования функций Ethernet OAM.

- Инициировать функцию обнаружения Ethernet OAM на порту 7.

- Инициировать тест удаленной обратной петли на порту 7.

```
sysname# show ethernet oam discovery 7
Port 7
Local client
------------
  OAM configurations:
    Mode              : Active
    Unidirectional    : Not supported
    Remote loopback   : Supported
    Link events       : Not supported
    Variable retrieval: Not supported
    Max. OAMPDU size  : 1518

  Operational status:
    Link status       : Up
    Info. revision    : 10
    Parser state      : Forward
    Discovery state   : Send Any

Remote client
-------------
  MAC address: 00:a0:c5:dd:e8:f4
  Vendor(oui): 0x00 0xa0 0xc5

  OAM configurations:
    Mode              : Active
    Unidirectional    : Not supported
    Remote loopback   : Supported
    Link events       : Not supported
    Variable retrieval: Not supported
    Max. OAMPDU size  : 1518

  Operational status:
    Info. revision    : 6

sysname# ethernet oam remote-loopback test 7
Port 7: Transmitting packets ...
OAM Remote Loopback Test: 1000 transmitted, 1000 received correctly
```

48.2.3 bpdu-control

Синтаксис:

```
bpdu-control <peer|tunnel|discard|network>
```

Где

<peer|tunnel|discard| network>	=	В случае ввода peer любые блоки BPDU, принимаемые через данные порты, будут обрабатываться. В случае ввода tunnel все блоки BPDU, принимаемые через данные порты, будут пересылаться. В случае ввода discard все блоки BPDU, принимаемые через данные порты, будут отбрасываться. В случае ввода network блоки BPDU, не имеющие тега VLAN, будут обрабатываться, а блоки BPDU с тегами – пересылаться.

Ниже показан пример.

- Включить для настройки порты 1, 3, 4 и 5.
- Выбрать для управления блоками BPDU режим tunnel, чтобы принимаемые через порты один, четыре и пять блоки BPDU пересылались.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# bpdu-control tunnel
sysname(config-interface)#
```

48.2.4 broadcast-limit

Синтаксис:

```
broadcast-limit
broadcast-limit <пакетов/с>
```

Где

broadcast-limit	=	Включает лимит контроля широковещательных штормов на коммутаторе.
<пакетов/с>	=	Определяет лимит широковещательных пакетов, принимаемых через интерфейс за секунду.

Ниже показан пример.

- Включить для настройки порт 1.
- Включить контроль широковещательных штормов.
- Определить количество получаемых интерфейсом широковещательных пакетов в секунду.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# broadcast-limit
sysname(config-interface)# broadcast-limit 21
```

48.2.5 bandwidth-limit

Команда `bandwidth-limit` включает на коммутаторе управление пропускной способностью.

Синтаксис:

```
bandwidth-limit
bandwidth-limit pir <кбит/с>
bandwidth-limit cir <кбит/с>
bandwidth-limit egress <кбит/с>
```

Где

`pir <кбит/с>`	=	Определяет максимальное значение пропускной способности для входящего трафика.
`cir <кбит/с>`	=	Определяет гарантированную пропускную способность для входящего трафика.
`egress <кбит/с>`	=	Определяет максимальное значение пропускной способности для исходящего трафика на коммутаторе.

Ниже показан пример.

- Включить для настройки порт 1.
- Установить лимит пропускной способности для исходящего трафика равным 5000 кбит/с.
- Установить гарантированную пропускную способность для входящего трафика равной 4000 кбит/с.
- Установить максимальную пропускную способность для входящего трафика равной 8000 кбит/с.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit egress 5000
sysname(config-interface)# bandwidth-limit cir 4000
sysname(config-interface)# bandwidth-limit pir 8000
```

48.2.6 mirror

Команда `mirror` включает зеркальное копирование портов на интерфейсе.

Синтаксис:

```
mirror
mirror dir <ingress|egress|both>
```

Где

`dir <ingress|egress|both>`	=	Включает зеркальное копирование порта для входящего (ingress), исходящего (egress) или всего (both) трафика. С помощью функции зеркального копирования можно копировать трафик, идущий от одного или всех портов на другой порт или все порты, для внешнего анализа.

Ниже показан пример.

- Включить зеркальное копирование.
- Включить порт мониторинга 3.
- Включить для настройки порты 1, 4, 5 и 6.
- Включить на портах зеркальное копирование.
- Включить на портах зеркальное копирование для исходящего трафика. Трафик копируется с портов 1, 4, 5 и 6 на порт 3 для его подробного изучения без вмешательства в поток данных через исходные порты.

```
sysname(config)# mirror-port
sysname(config)# mirror-port 3
sysname(config)# interface port-channel 1,4-6
sysname(config-interface)# mirror
sysname(config-interface)# mirror dir egress
```

48.2.7 gvrp

Синтаксис:

`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.

Ниже показан пример.

- Включить команды VLAN на основе тегов по стандарту IEEE 802.1Q для настройки на коммутаторе VLAN на основе тегов.
- Включить для настройки порты 1, 3, 4 и 5.
- Включить протокол GVRP на интерфейсе.

```
sysname(config)# vlan1q gvrp
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# gvrp
```

48.2.8 ingress-check

Команда `ingress-check` включает режим, когда устройство отбрасывает входящие кадры для VLAN, членом которых не является данный порт.

Синтаксис:

`ingress-check`

Ниже показан пример.

- Включить для настройки порты 1, 3, 4 и 5.
- Включить проверку входящих кадров на интерфейсе.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
```

48.2.9 frame-type

Синтаксис:

```
frame-type <all|tagged>
```

Где

`<all|tagged>`	=	Выбор режима – принимать ли на порт входящие кадры как с тегами, так и без тегов (all), или принимать только кадры с тегами (tagged).

Ниже показан пример.

- Включить для настройки порты 1, 3, 4 и 5.
- Включить проверку входящих кадров на портах.
- Включить на интерфейсе поддержку кадров с тегами.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# ingress-check
sysname(config-interface)# frame-type tagged
```

48.2.10 weight

Синтаксис:

```
weight <вес1> <вес2> ... <вес8>
```

Где

`<вес1> <вес2> ... <вес8>`	=	Определяет веса интерфейсов для механизма взвешенной справедливой постановки в очередь (WFQ). Значение веса от `1` до `8` устанавливается для каждой переменной от вес1 до вес8.

Ниже показан пример.

- Включить на коммутаторе метод организации очередей WFQ.
- Включить для настройки порт 2 и порты 6-8.
- Назначить веса очередей Q0-Q7.

```
sysname# configure
sysname(config)# wfq
sysname (config)# interface port-channel 2,6-8
sysname(config-interface)# weight 8 7 6 5 4 3 2 1
```

48.2.11 egress set

Синтаксис:

```
egress set <список-портов>
```

Где

`<список-портов>`	=	Определяет список исходящих портов для VLAN на основе портов.

Ниже показан пример.

- Включить VLAN на основе портов на коммутаторе.
- Включить для настройки порты 1, 3, 4 и 5.
- Определить исходящие порты как порт CPU (0), седьмой (7) и восьмой (8).

```
sysname(config)# vlan-type port-based
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# egress set 0,7,8
```

48.2.12 qos priority

Синтаксис:

```
qos priority <0 .. 7>
```

Где

<0 .. 7>	=	Определяет приоритет управления качеством обслуживания для порта.

Ниже показан пример.

- Включить для настройки порты 1, 3, 4 и 5.
- Установить приоритет качества обслуживания по стандарту IEEE 802.1p, равный четырем (4).

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# qos priority 4
```

48.2.13 name

Синтаксис:

```
name <имя-порта>
```

Где

<имя-порта>	=	Определяет имя для интерфейса порта.

Ниже показан пример.

- Включить для настройки порты 1, 3, 4 и 5.
- Присвоить имя портам.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# name Test
```

48.2.14 speed-duplex

Синтаксис:

```
speed-duplex <auto|10-half|10-full|100-half|100-full|1000-full>
```

Где

`<auto|10-half|10-full|100-half|100-full|1000-full>`	=	Определяет режим дуплекса (half – полудуплекс или full – дуплекс) и скорость (10, 100 или 1000 Мбит/с) для соединения через порт. По выбору auto (автосогласование) порт автоматически согласовывает с портом-партнером ту скорость и режим дуплекса, которые поддерживают они оба.

Ниже показан пример.

- Включить для настройки порты 1, 3, 4 и 5.
- Установить скорость 100 Мбит/с и полудуплексный режим.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# speed-duplex 100-half
```

48.2.15 test

Имеется возможность выполнить для указанных портов тест обратной петли. В результате теста выдается `Passed!` (пройден) или `Failed!` (ошибка).

Ниже показан пример.

- Выбрать для теста внутренней обратной петли порты 3-6.
- Выполнить команду test.
- Просмотреть результаты.

```
sysname(config)# interface port-channel 3-6
sysname(config-interface)# test 3-6
Testing internal loopback on port  3 :Passed!
  Ethernet Port 3 Test ok.
Testing internal loopback on port  4 :Passed!
  Ethernet Port 4 Test ok.
Testing internal loopback on port  5 :Passed!
  Ethernet Port 5 Test ok.
Testing internal loopback on port  6 :Passed!
  Ethernet Port 6 Test ok.
```

48.3 Примеры использования команд no для интерфейсов

Аналогично командам no в привилегированном режиме и режиме настройки, с помощью команд no при работе с интерфейсами также можно отключать некоторые функции. В этом режиме, однако, команды действуют на уровне отдельных портов.

48.3.1 no bandwidth-limit

Просто добавив `no` перед командой `bandwidth-limit`, можно отключить ограничение пропускной способности на порту 1.

Синтаксис:

```
no bandwidth-limit
```

Ниже показан пример.

- Отключить ограничение пропускной способности на порту 1.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# no bandwidth-limit cir
```

49

Команды для VLAN на основе тегов (согласно IEEE 802.1Q)

В данной главе описана работа с виртуальными локальными сетями (VLAN) на основе тегов (согласно IEEE 802.1Q) и соответствующие команды.

49.1 Настройка VLAN на основе тегов

Ниже описана процедура настройки VLAN на основе тегов.

1 Для настройки на коммутаторе VLAN на основе тегов используются команды VLAN на основе тегов (согласно IEEE 802.1Q).

- Для создания или настройки VLAN на коммутаторе используется команда `vlan <идентификатор-vlan>`. При этом коммутатор автоматически войдет в режим `config-vlan`. Для отключения VLAN используется команда `inactive`.
- Для входа в режим config-interface и редактирования настроек VLAN для порта используется команда `interface port-channel <список-портов>`, затем с помощью команды `pvid <идентификатор-vlan>` определяется созданный идентификатор VLAN для указанного порта в таблице идентификаторов VLAN.
- После окончания настройки VLAN введите команду `exit`.

```
sysname(config)# vlan 2000
sysname(config-vlan)# name up1
sysname (config-vlan)# fixed 5-8
sysname (config-vlan)# no untagged 5-8
sysname(config-vlan)# exit
sysname (config)# interface port-channel 5-8
sysname(config-interface)# pvid 2000
sysname(config-interface)# exit
```

2 Настройка VLAN управления.

- Для создания VLAN управления коммутатором (в данном примере – VLAN 3) используется команда `vlan <идентификатор-vlan>`. При этом коммутатор активирует новую VLAN управления.

- Для отключения новой VLAN управления используется команда `inactive`.

```
sysname(config)# vlan 3
sysname(config-vlan)# inactive
```

49.2 Глобальные команды настройки VLAN на основе тегов

В данном разделе описана настройка и мониторинг VLAN на основе тегов (согласно IEEE 802.1Q).

49.2.1 Состояние протокола GARP

Синтаксис:

```
show garp
```

Эта команда отображает настройки таймера GARP на коммутаторе, в том числе таймеры join, leave и leave all.

Ниже показан пример.

```
sysname# show garp
GARP Timer
------------------------
Join Timer = 200
Leave Timer = 600
Leave All Timer = 10000
sysname#
```

49.2.2 Таймеры GARP

Синтаксис:

```
garp join <мсек> leave <мсек> leaveall <мсек>
```

Где

`join <мсек>` = Определяет длительность таймера Join Period для GVRP в миллисекундах. У каждого порта имеется таймер Join Period. Допустимый диапазон значений параметра Join Period для GVRP – от 100 до 32 767 миллисекунд; по умолчанию это значение равно 200 миллисекундам.

`leave <мсек>`	=	Определяет длительность таймера Leave Period для GVRP в миллисекундах. У каждого порта имеется отдельный таймер Leave Period. Значение параметра Leave Period должно быть в два раза больше параметра Join Period; по умолчанию оно равно 600 миллисекундам.
`leaveall <мсек>`	=	Определяет длительность таймера Leave All Period для GVRP в миллисекундах. У каждого порта имеется отдельный таймер Leave All Period. Значение параметра Leave All Period должно больше параметра Leave Period; по умолчанию это значение равно 10 000 миллисекунд.

Эта команда определяет настройки таймера GARP на коммутаторе, в том числе таймеры join, leave и leave all.

Коммутаторы присоединяются к виртуальным локальным сетям VLAN путем передачи декларации. Декларация издается путем передачи 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.

В следующем примере таймер Join Timer выставляется на 300 миллисекунд, таймер Leave Timer – на 800 миллисекунд, а Leave All Timer – на 11 000 миллисекунд.

```
sysname(config)# garp join 300 leave 800 leaveall 11000
```

49.2.3 Таймеры GVRP

Синтаксис:

```
show vlan1q gvrp
```

Эта команда отображает состояние настроек протокола GVRP на коммутаторе.

Ниже показан пример.

```
sysname# show vlan1q gvrp
GVRP Support
--------------------
gvrpEnable = YES
sysname#
```

49.2.4 Включение протокола GVRP

Синтаксис:

```
vlan1q gvrp
```

Эта команда включает обращение к протоколу GVRP для распространения информации о VLAN за пределами коммутатора.

49.2.5 Отключение GVRP

Синтаксис:

```
no vlan1q gvrp
```

Эта команда отключает протокол GVRP, чтобы информация о VLAN не распространялась за пределами коммутатора.

49.3 Команды настройки порта VLAN

Редактировать настройки VLAN портов коммутатора необходимо в режиме config-interface.

49.3.1 Назначение идентификатора виртуальной локальной сети VID для порта

Синтаксис:

```
pvid <идентификатор-vlan-порта>
```

Где

`<идентификатор-vlan-порта>`	= Номер VLAN в диапазоне от 1 до 4094.

Эта команда определяет идентификатор VLAN по умолчанию на порту (портах).

В данном примере на портах с первого по пятый установлен идентификатор VLAN по умолчанию, равный 200.

```
sysname(config)# interface port-channel 1-5
sysname(config-interface)# pvid 200
```

49.3.2 Установка допустимого типа кадра

Синтаксис:

```
frame-type <all|tagged|untagged>
```

Где

`<all|tagged|untagged>`	= Указывает, Ethernet-кадры какого типа будут приниматься – все, с тегами и без тегов (all), только Ethernet-кадры с тегами (tagged) или только Ethernet-кадры без тегов (untagged).

Эта команда приказывает указанному порту принимать все Ethernet-кадры или только маркированные тегом VLAN согласно IEEE 802.1Q.

В данном примере портам 1 и 5 приказано принимать только кадры с тегами.

```
sysname(config)# interface port-channel 1-5
sysname(config-interface)# frame-type tagged
```

49.3.3 Включение и отключение протокола GVRP на порту

Для включения протокола GVRP на порту (портах) используется команда `gvrp`. Для отключения GVRP используется команда `no gvrp`.

В данном примере протокол GVRP отключается на портах 1 и 5.

```
sysname(config)# interface port-channel 1-5
sysname(config-interface)# no gvrp
```

49.3.4 Изменение статической VLAN

Для настройки таблицы статических VLAN в режиме config-vlan используются следующие команды.

Синтаксис:

```
vlan <идентификатор-vlan>
fixed <список-портов>
forbidden <список-портов>
name <имя>
normal <список-портов>
untagged <список-портов>
no fixed <список-портов>
no forbidden <список-портов>
no untagged <список-портов>
```

Где

`<идентификатор-vlan>`	=	Идентификатор VLAN [1 – 4094].
`<имя>`	=	Идентификационное имя записи SVLAN.
`<список-портов>`	=	Список портов коммутатора.

- Введите команду `fixed` для регистрации списка портов `<список-портов>` в таблице статических VLAN с идентификатором `<идентификатор-vlan>`.
- Введите `normal` для подтверждения регистрации списка портов `<список-портов>` в таблице статических VLAN с идентификатором `<идентификатор-vlan>`.
- Введите `forbidden` для блокировки списка портов `<список-портов>` от записи в таблицу статических VLAN с идентификатором `<идентификатор-vlan>`.
- Введите `no fixed` или `no forbidden` для возврата состояния списка портов `<список-портов>` к нормальному.
- Введите `untagged`, чтобы исходящие кадры отправлялись без тега.
- Введите `no untagged`, чтобы маркировать тегами исходящие кадры.

49.3.4.1 Пример изменения таблицы статических VLAN

В приведенном примере порты с первого по пятый настраиваются для VLAN 2000 как фиксированные без тегов.

```
sysname(config)# vlan 2000
sysname(config-vlan)# fixed 1-5
sysname(config-vlan)# untagged 1-5
```

49.3.4.2 Пример процесса пересылки

49.3.4.2.1 Кадры с тегами

1. Прежде всего коммутатор проверяет идентификаторы VLAN входящих кадров с тегами или назначает временные идентификаторы для немаркированных кадров.
2. Затем коммутатор сверяет идентификатор VLAN в теге кадра с таблицей SVLAN.
3. Далее коммутатор получает информацию из таблицы SVLAN (из таблица статических VLAN коммутатор узнает, требуется ли пересылать кадр и должны ли пересылаемые кадры иметь теги).
4. Затем коммутатор применяет фильтр порта для завершения принятия решения о пересылке. Это означает, что кадр может быть отброшен, даже если таблица статических VLAN определила его на пересылку. Кадры также могут быть отброшены, если они направляются на пользовательское DSL-устройство, не поддерживающее кадры с тегами.

49.3.4.2.2 Кадры без тегов

1. Из локальной сети поступает кадр без тега.
2. В этот момент коммутатор сверяется с таблицей идентификаторов VLAN и назначает для этого кадра временный идентификатор 1.
3. Данный коммутатор игнорирует порт, с которого поступил кадр, поскольку коммутатор не будет пересылать кадр на тот порт, с которого он поступил. Кроме того, коммутатор также не будет пересылать кадр на «запрещенные» порты.
4. Если после сверки с таблицей статических VLAN коммутатор не нашел портов, на которые можно переслать кадр, то фильтр порта не запускается.

49.3.5 Удаление идентификатора VLAN

Синтаксис:

```
no vlan <идентификатор-vlan>
```

Где

`<идентификатор-vlan>`	=	Идентификатор VLAN [1 – 4094].

Эта команда удаляет идентификатор VLAN с указанным номером из таблицы статических VLAN. В данном примере из таблицы статических VLAN удаляется идентификатор 2.

```
sysname(config)# no vlan 2
```

49.4 Включение VLAN

Синтаксис:

```
vlan <идентификатор-vlan>
```

Эта команда включает VLAN с указанным идентификатором в таблице статических VLAN.

49.5 Отключение VLAN

Синтаксис:

```
vlan <идентификатор-vlan> inactive
```

Эта команда отключает VLAN с указанным идентификатором в таблице статических VLAN.

49.6 Отображение настроек VLAN

Синтаксис:

```
show vlan
```

Эта команда отображает таблицу статических VLAN на основе тегов (согласно IEEE 802.1Q).

Ниже показан пример.

- Идентификатор VLAN (VID) представляет собой идентификационный номер сети VLAN.
- В поле Status показывается, является ли данная VLAN статической (Static) или активной (Active).
- Elap-Time – время с момента создания сети VLAN на коммутаторе.

- В разделе `TagCtl` последнего столбца указывается, какие порты работают с тегами и какие – без тегов.

```
sysname# show vlan
  The Number of VLAN:    3
  Idx. VID   Status    Elap-Time    TagCtl
  ---- ----  -------- ------------ ------------------------
  1   1    Static     0:12:13    Untagged :1-2
                                    Tagged   :

  1   100    Static     0:00:17  Untagged :
                                    Tagged   :1-4

  1   200    Static     0:00:07    Untagged :1-2
                                    Tagged   :3-8
```

50

Команды регистрации VLAN-сети мультивещания

В данной главе описано использование команд регистрации VLAN-сети мультивещания (mvr).

50.1 Обзор

Команды mvr в режиме настройки используются для создания и настройки VLAN-сетей мультивещания.

Включение механизма отслеживания многоадресного трафика IGMP описано в разд. 47.1 на стр. 451.

50.2 Создание VLAN-сети мультивещания

Для настройки VLAN-группы мультивещания используются следующие команды в режиме config-mvr.

Синтаксис:

```
mvr <идентификатор-vlan>
mvr <идентификатор-vlan> source-port <список-портов>
mvr <идентификатор-vlan> receiver-port <список-портов>
mvr <идентификатор-vlan> inactive
mvr <идентификатор-vlan> mode <dynamic|compatible>
mvr <идентификатор-vlan> name <имя>
mvr <идентификатор-vlan> tagged <список-портов>
mvr <идентификатор-vlan> group <имя> start-address <ip-адрес> end-address
<ip-адрес>
mvr <идентификатор-vlan> exit
```

Где

`<идентификатор-vlan>`	=	Идентификатор VLAN [1 – 4094].
`source-port <список-портов>`	=	Определяет порты-источники MVR, которые способны передавать и принимать трафик мультивещания.
`receiver-port <список-портов>`	=	Определяет порты-приемники MVR, которые способны только принимать трафик мультивещания.
`name <имя>`	=	Имя для идентификации VLAN-группы мультивещания.
`mode <dynamic|compatible>`	=	Определяет динамический (dynamic) режим – сообщения IGMP отправляются на все порты источников во VLAN-сети мультивещания, или режим совместимости (compatible) – сообщения IGMP коммутатором не отправляются.
`group name <имя>`	=	Имя для идентификации группы мультивещания MVR.
`start-address <ip-адрес>`	=	Определяет начальный IP-адрес группы мультивещания в виде десятичных чисел, разделенных точками.
`end-address <ip-адрес>`	=	Определяет конечный IP-адрес группы мультивещания в виде десятичных чисел, разделенных точками. Если в группу мультивещания необходимо внести только один адрес, в это поле вводится тот же IP-адрес, что и в поле start-address.

- Войти в режим MVR. Создать VLAN мультивещания с именем `multiVlan` и идентификатором VLAN 3.
- Определить в качестве портов-источников порты 2, 3, 5, и в качестве портов-приемников – порты 6-8.
- Выбрать динамический режим для группы мультивещания.
- Настроить адреса группы мультивещания MVR с именем `ipgroup`.
- Выйти из режима MVR.

Пример приводится ниже.

```
sysname(config)# mvr 3
sysname(config-mvr)# name multivlan
sysname(config-mvr)# source-port 2,3,5
sysname(config-mvr)# receiver-port 6-8
sysname(config-mvr)# mode dynamic
sysname(config-mvr)# group ipgroup start-address 224.0.0.1 end-address
--> 224.0.0.255
sysname(config-mvr)# exit
```

51

Примеры использования команд route-domain

51.0.1 interface route-domain

Синтаксис:

```
interface route-domain <ip-адрес>/<битов-маски>
```

Где

`<ip-адрес>`	=	IP-адрес коммутатора в домене маршрутизации. IP-адрес должен вводиться в виде десятичных чисел, разделенных точками. Например, 192.168.1.1.
`<битов-маски>`	=	Количество единичных битов в маске подсети. Перед количеством битов в маске подсети ставится «/». Чтобы определить количество битов, переведите маску подсети в двоичную форму и подсчитайте число единичных битов. Возьмем, к примеру, маску «255.255.255.0». 255 в двоичной форме – это восемь единиц. Всего в маске 3 байта со значением «255», поэтому количество единичных битов будет три на восемь (24).

Эта команда используется для включения/создания указанного домена маршрутизации для настройки.

Ниже показан пример.

- Войти в режим настройки.
- Включить для настройки домен маршрутизации по умолчанию (подсеть 192.168.1.1).
- Приступить к настройке данного домена.

```
sysname# config
sysname(config)# interface route-domain 192.168.1.1/24
cmd interface route domain
 192.168.1.1 255.255.255.0
sysname(config-if)#
```

52

Устранение неполадок

В данной главе описаны возможные проблемы и способы их устранения.

52.1 Проблемы с запуском коммутатора

Таблица 146 Устранение неполадок при запуске коммутатора

ПРОБЛЕМА	УСТРАНЕНИЕ
При включении питания коммутатора не загорается ни один из индикаторов.	Проверьте, правильно ли подключен шнур питания и включен ли источник питания.
	Если ошибка не исчезла, возможно, имеет место проблема с аппаратным обеспечением. В этом случае следует связаться с поставщиком оборудования.

52.2 Проблемы с доступом к коммутатору

Таблица 147 Устранение неполадок при доступе к коммутатору

ПРОБЛЕМА	УСТРАНЕНИЕ
Невозможно получить доступ к коммутатору через Telnet.	Убедитесь, что порты должным образом подключены. Вероятно, превышено допустимое количество одновременных Telnet-сессий. Завершите остальные Telnet-сессии или попробуйте подключиться еще раз. Убедитесь, что доступ через службу Telnet включен. Если был сконфигурирован IP-адрес защищенного клиента, то IP-адрес компьютера должен совпадать с ним. Более подробную информацию можно найти в главе о контроле доступа.
Невозможно получить доступ к Web-конфигуратору.	Имя пользователя администратора – «admin». Пароль администратора по умолчанию – «1234». Имя пользователя и пароль чувствительны к регистру. Убедитесь, что вводятся правильные имя пользователя и пароль в нужном регистре. Если вы изменили пароль и забыли его, необходимо загрузить файл настроек по умолчанию. При этом все настройки, включая пароль, возвращаются к заводским значениям по умолчанию. В случае настройки нескольких IP-интерфейсов убедитесь, что другой администратор НЕ вошел в Web-конфигуратор через другой интерфейс с использованием той же самой учетной записи. Убедитесь, что доступ через службу Web включен. Если был сконфигурирован IP-адрес защищенного клиента, то IP-адрес компьютера должен совпадать с ним. Более подробную информацию можно найти в главе о контроле доступа. IP-адрес компьютера и IP-адрес коммутатора должны принадлежать к одной подсети. Чтобы убедиться, что всплывающие окна, JavaScript и разрешения Java включены, обратитесь к следующему разделу.

52.2.1 Всплывающие окна, JavaScript и разрешения Java

Для использования Web-конфигуратора нужно разрешить:

- Всплывающие окна браузера на устройстве.
- JavaScript (по умолчанию включен).
- Разрешения Java (по умолчанию включены).

Ниже описаны экраны браузера Internet Explorer 6. Экраны других версий Internet Explorer могут отличаться.

52.2.1.1 Блокировщики всплывающих окон Internet Explorer

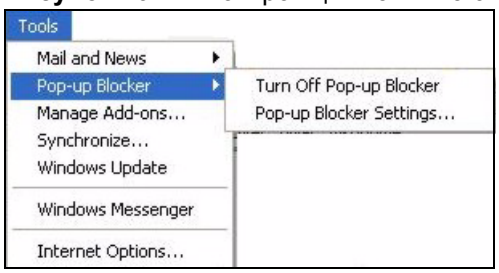
Для подключения к устройству нужно отключить блокировку всплывающих окон.

Необходимо либо отключить блокировку всплывающих окон (она включена по умолчанию в ОС Windows XP с установленным пакетом обновлений Service Pack 2), либо включить блокировку и создать исключение для IP-адреса устройства.

52.2.1.1.1 Отключение блокировки всплывающих окон

1 В Internet Explorer выберите пункт **Tools**, **Pop-up Blocker** и затем **Turn Off Pop-up Blocker**.

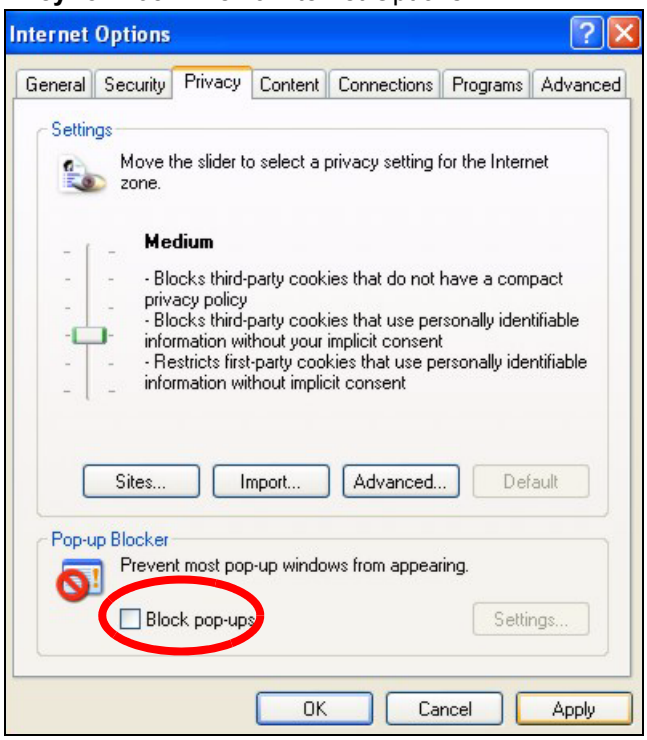
Рисунок 204 Блокировщик всплывающих окон



Проверить, включена ли блокировка всплывающих окон, можно также в разделе **Pop-up Blocker** на вкладке **Privacy**.

1 В браузере Internet Explorer выберите пункты **Tools**, **Internet Options**, **Privacy**.
2 Снимите выделение с переключателя **Block pop-ups** в разделе **Pop-up Blocker** на этом экране. В результате будет отключены все блокировщики окон, которые были включены.

Рисунок 205 Меню Internet Options



3 Нажмите **Apply**, чтобы сохранить эти настройки.

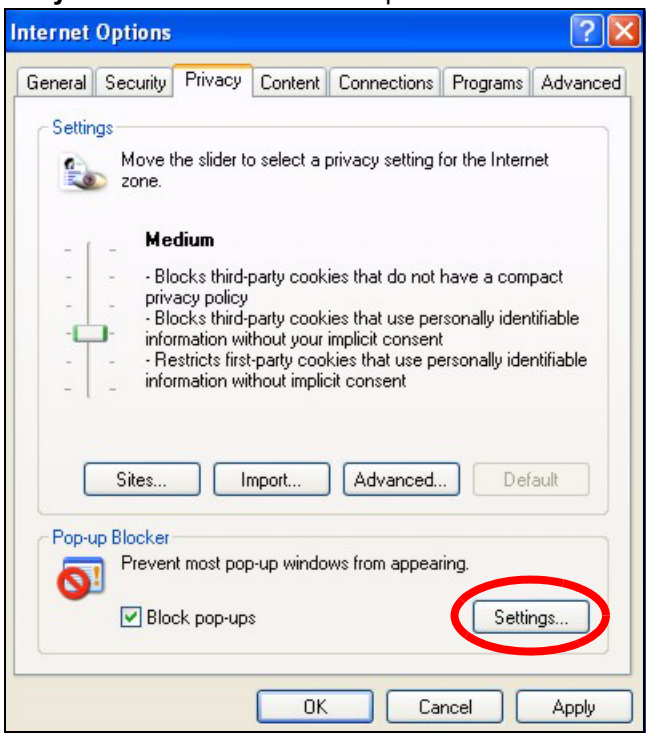
52.2.1.1.2 Включение блокировки всплывающих окон и создание исключений

Как вариант, если необходимо разрешить всплывающие окна только от устройства, выполните следующие действия.

1 В браузере Internet Explorer выберите пункты меню **Tools**, **Internet Options**, **Privacy**.

2 Выберите **Settings…**, чтобы открыть экран **Pop-up Blocker Settings**.

Рисунок 206 Меню Internet Options



3 Введите IP-адрес устройства (Web-страницы, которую не требуется блокировать) с префиксом «http://». Например, http://192.168.1.1.

4 Нажмите **Add**, чтобы этот IP-адрес попал в список разрешенных сайтов **Allowed sites**.

Рисунок 207 Экран Pop-up Blocker Settings

5 Нажмите **Close**, чтобы вернуться к экрану **Privacy**.

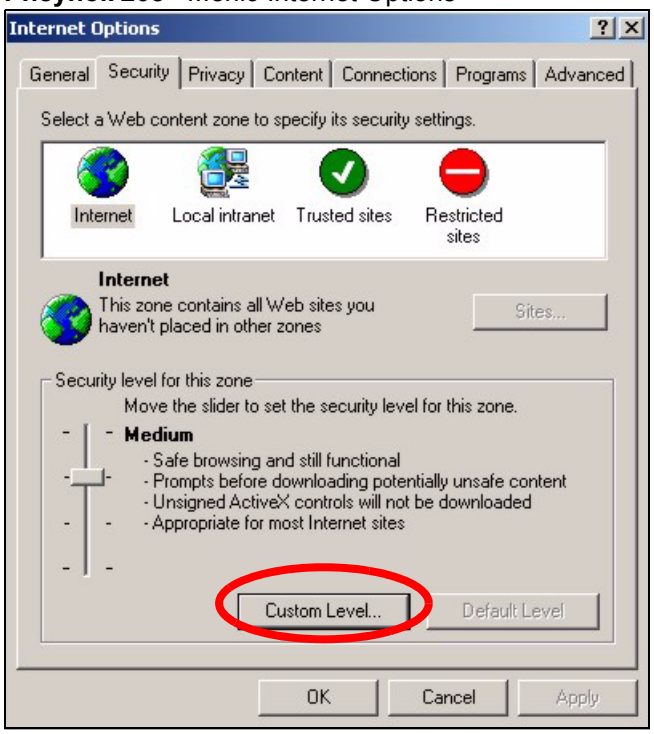
6 Нажмите **Apply**, чтобы сохранить эти настройки.

52.2.1.2 JavaScript

Если страницы Web-конфигуратора отображаются в Internet Explorer неправильно, проверьте, включен ли JavaScript.

1 В браузере Internet Explorer выберите пункты меню **Tools**, **Internet Options**, **Privacy**.

Рисунок 208 Меню Internet Options



2 Нажмите кнопку **Custom Level...**.

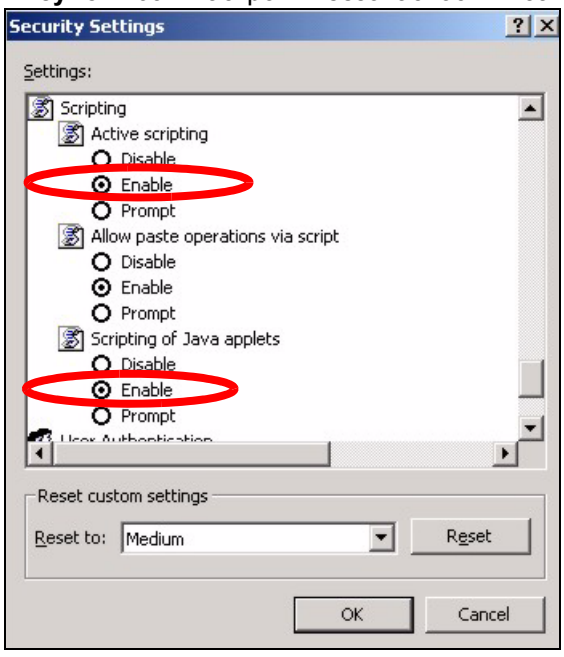
3 Прокрутите экран до пункта **Scripting**.

4 Убедитесь, что в разделе **Active scripting** выбран параметр **Enable** (по умолчанию).

5 Убедитесь, что в разделе **Scripting of Java applets** выбран параметр **Enable** (по умолчанию).

6 Нажмите **OK**, чтобы закрыть это окно.

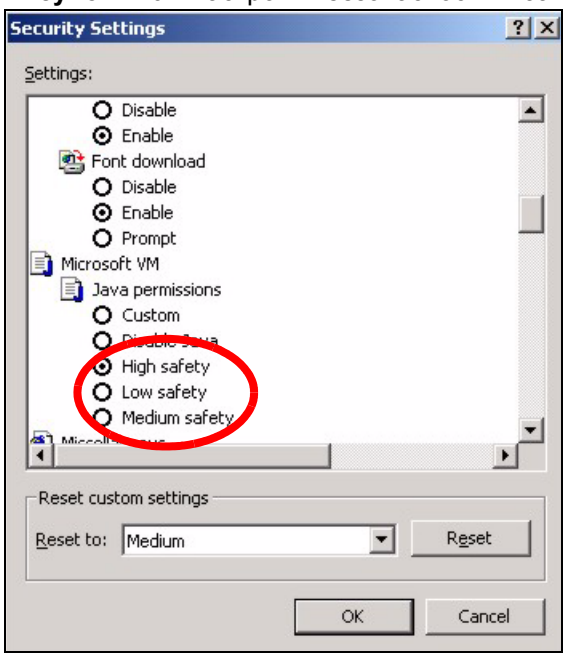
Рисунок 209 Настройки безопасности – JavaScript



52.2.1.3 Разрешения Java

1. В браузере Internet Explorer выберите пункты меню **Tools**, **Internet Options**, затем **Security**.
2. Нажмите кнопку **Custom Level...**.
3. Прокрутите экран до пункта **Microsoft VM**.
4. Убедитесь, что в разделе **Java permissions** выбран нужный уровень безопасности.
5. Нажмите **OK**, чтобы закрыть это окно.

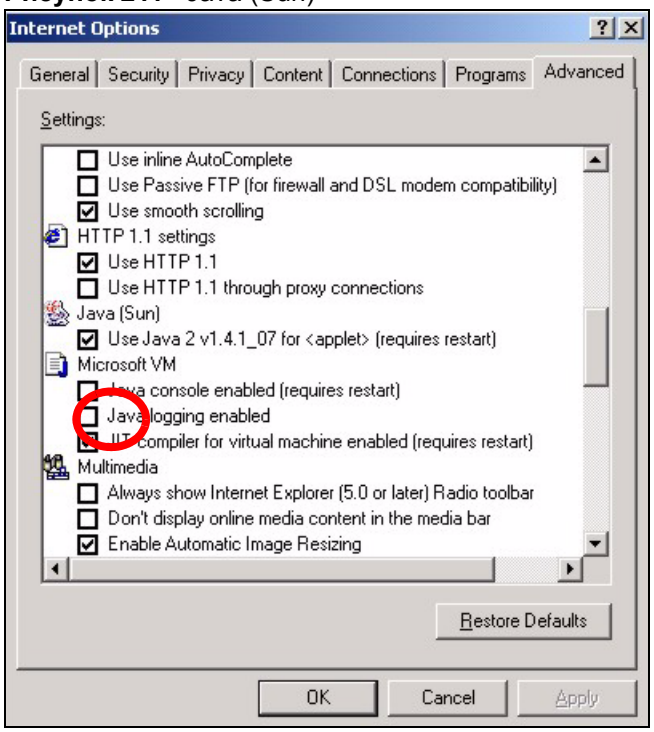
Рисунок 210 Настройки безопасности – Java



52.2.1.3.1 JAVA (Sun)

1. В браузере Internet Explorer выберите пункты меню **Tools**, **Internet Options**, затем **Advanced**.
2. Убедитесь, в разделе **Java (Sun)** установлен переключатель **Use Java 2 for <applet>**.
3. Нажмите **OK**, чтобы закрыть это окно.

Рисунок 211 Java (Sun)



52.3 Проблемы с паролем

Таблица 148 Устранение неполадок с паролем

ПРОБЛЕМА	УСТРАНЕНИЕ
Невозможно получить доступ к коммутатору.	Поле для ввода пароля чувствительно к регистру. Убедитесь, что вводится правильный пароль в нужном регистре.
	Имя пользователя администратора – «admin». Пароль администратора по умолчанию – «1234». Имя пользователя и пароль чувствительны к регистру. Убедитесь, что вводятся правильные имя пользователя и пароль в нужном регистре. Если вы изменили пароль и забыли его, необходимо загрузить файл настроек по умолчанию. При этом все настройки, включая пароль, возвращаются к заводским значениям по умолчанию.

Часть VII Приложения и индекс

A

Характеристики продукта

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

Таблица 149 Характеристики аппаратного обеспечения

СПЕЦИФИКАЦИЯ	ОПИСАНИЕ
Габариты	Возможность установки в стандартную 19-дюймовую стойку 438 мм (ширина) x 270 мм (глубина) x 44,45 мм (высота)
Вес	3,6 кг
Характеристики питания	Один разъем для резервного источника питания (BPS) С питанием от переменного тока: Встроенный универсальный источник питания на 100-240 В перем. тока, 50/60 Гц, 1,5 А макс. С питанием от постоянного тока: -48 ~ -60 В пост. тока, 1,5 А, макс. потребляемая мощность 48 Вт Примечание: Допусков на входное напряжение постоянного тока не предусмотрено
Интерфейсы	24 порта 10/100 Base-Tx 2 совмещенных интерфейса GbE (каждый из интерфейсов включает в себя один порт для витой пары 1000Base-T и один оптоволоконный порт SFP, из которых только один может быть активен в каждый момент времени) Два порта Gigabit Ethernet для стекирования Один Ethernet-порт локального управления Автосогласование Автоматическое определение типа кабеля (MDI/MDIX) Один консольный порт Соответствие стандартам IEEE 802.3ad/u/x Управление потоком методом обратного давления для полудуплексного режима Управление потоком для дуплексного режима согласно IEEE 802.3x
Индикаторы	Для коммутатора в целом: BPS, PWR, SYS, ALM, LNK/ACT, FDX На каждый порт Gigabit Ethernet: LNK/ACT, FDX На порт mini-GBIC: LNK, ACT На порт управления: 10, 100
Условия эксплуатации	Температура: 0є C ~ 45є C (32є F ~ 113є F) Влажность: 10 ~ 90% (без конденсации)
Условия хранения	Температура: -10є C ~ 70є C (13є F ~ 158є F) Влажность: 10 ~ 90% (без конденсации)
Сечение заземляющего провода	18 AWG или больше

Таблица 149 Характеристики аппаратного обеспечения

Сечение силового провода	18 AWG или больше
Номинал предохранителя	250 В перем. тока, T2A

Таблица 150 Характеристики встроенного программного обеспечения

ХАРАКТЕРИСТИКИ	ОПИСАНИЕ
IP-адрес по умолчанию	Внутриполосное управление: 192.168.1.1 Внеполосное управление (порт управления): 192.168.0.1
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+.
Домен IP-маршрутизации	IP-интерфейс (также называемый доменом IP-маршрутизации) не привязан к физическому порту. Настройка домена IP-маршрутизации позволяет коммутатору маршрутизировать трафик между различными сетями.
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.
Стекирование VLAN	С помощью стекирования VLAN можно добавить внешний тег VLAN к кадрам с внутренними тегами IEEE 802.1Q при их поступлении в сеть. Посредством добавления тегов к уже имеющим теги кадрам (использования «двух тегов») провайдер услуг может управлять максимум 4 094 группами VLAN, каждая из которых может содержать до 4 094 клиентских сетей VLAN. Благодаря этому провайдер услуг может предоставлять дифференцированные услуги в зависимости от конкретной VLAN многим различным клиентам.
Фильтр MAC-адресов	Фильтрация трафика на основе MAC-адреса источника и/или назначения и группы VLAN (идентификатора).
DHCP (протокол динамической конфигурации хоста)	Благодаря поддержке данного протокола коммутатор может назначать компьютерам в сети IP-адреса, адреса шлюза по умолчанию и адреса серверов DNS.
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.

Таблица 150 Характеристики встроенного программного обеспечения

ХАРАКТЕРИСТИКИ	ОПИСАНИЕ
Классификация и политики	С помощью созданных политик можно определить действия, выполняемые с потоками трафика после классификации трафика по определенным критериям, таким как IP-адрес, номер порта, тип протокола и т.д.
Организация очередей	Организация очередей помогает решить проблему снижения производительности в случаях перегрузки сети. Поддерживаются три алгоритма организации очередей: строгая очередь приоритетов (SPQ), взвешенное циклическое обслуживание (WRR) и взвешенная справедливая постановка в очередь (WFQ). 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.
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.
IP-мультивещание	При использовании IP-мультивещания (или групповой передачи) коммутатор доставляет IP-пакеты определенной группе хостов в сети – но не всем. Кроме того, коммутатор может отправлять пакеты на устройства Ethernet, не поддерживающие сети VLAN, посредством удаления тегов VLAN из пакетов IP-мультивещания.
RIP	Протокол маршрутной информации RIP позволяет маршрутизирующим устройствам обмениваться информацией о маршрутах с другими маршрутизаторами.
OSPF	Протокол «предпочтения кратчайшего пути» OSPF представляет собой протокол маршрутизации по состоянию канала, предназначенный для распространения информации о маршрутах в пределах автономной системы (AS). Под автономной системой понимается группа сетей, использующих общий протокол маршрутизации для обмена информацией о маршрутах. OSPF лучше всего подходит для крупных сетей.
DVMRP	Протокол маршрутизации мультивещания «вектор-длина» DVMRP (Distance Vector Multicast Routing Protocol) представляет собой протокол, используемый для маршрутизации данных мультивещания в пределах автономной системы (AS). DVMRP обеспечивает поддержку передачи мультивещательного трафика на коммутаторах уровня 3, использующих протокол IPv4 (с поддержкой IP-мультивещания) и протокол IGMP.
VRRP	Протокол резервирования виртуального маршрутизатора (VRRP), определенный в RFC 2338, позволяет создать резервные шлюзы, чтобы шлюз по умолчанию был всегда доступен для хостов.

Таблица 150 Характеристики встроенного программного обеспечения

ХАРАКТЕРИСТИКИ	ОПИСАНИЕ
Протокол покрывающего дерева (STP) / быстрый протокол покрывающего дерева (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.
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 DHCP и 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!
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 151 Характеристики коммутации

Функции уровня 2	Мостовая конфигурация	Таблица MAC-адресов на 16 тыс. записей Фильтрация на основе статических MAC-адресов источника/пункта назначения Контроль широковещательных штормов Пересылка на основе статических MAC-адресов
	Коммутация	Коммутирующая матрица: 12,8 Гбит/с, без блокирования Максимальный размер кадра: 1522 байта Пересылка кадров: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Предотвращение пересылки поврежденных пакетов
	STP	IEEE 802.1w – быстрый протокол покрывающего дерева (RSTP) Поддержка быстрого протокола нескольких экземпляров покрывающего дерева (4 настраиваемых дерева) IEEE 802.1s – протокол нескольких экземпляров покрывающего дерева
	QoS	IEEE 802.1p Восемь очередей приоритетов на порт Ограничение исходящего трафика на уровне порта Зеркальное копирование трафика на основе правил Поддержка отслеживания многоадресного трафика IGMP
	VLAN	Виртуальные локальные сети на основе портов Виртуальные локальные сети на основе тегов (IEEE 802.1Q) Количество сетей VLAN: максимум 4 тыс., 1000 статических Поддержка GVRP Двойные теги для стекирования VLAN VLAN на основе протоколов VLAN на основе подсетей
	Агрегация портов	Поддержка стандарта IEEE 802.3ad; статическое и динамическое (по протоколу LACP) группирование портов Шесть групп (до 8 портов в каждой)
	Зеркальное копирование портов	Поддержка зеркального копирования на всех портах Поддержка зеркального копирования порта по IP/TCP/UDP
	Управление пропускной способностью	Поддержка ограничения скорости с шагом 64 кбит/с
Функции уровня 3	Функции IP	Поддержка IPV4 64 домена IP-маршрутизации Таблица IP-адресов на 4 тыс. записей Пересылка IP-пакетов на скорости среды передачи
	Протоколы маршрутизации	Одноадресной передачи: RIP-V1/V2, OSPF V2 Мультивещания: DVMRP, IGMP V1/V2/V3 Статические маршруты VRRP
	IP-службы	Ретрансляция DHCP; Сервер/агент ретрансляции DHCP на уровне отдельной VLAN Отслеживание DHCP
Безопасность		Аутентификация порта по стандарту IEEE 802.1x Фильтрация на основе статических MAC-адресов Ограничение количества динамических адресов на порт

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

Таблица 152 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 1058	RIP-1 (протокол маршрутной информации)
RFC 1112	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 1723	RIP-2 (протокол маршрутной информации)
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
RFC 2338	Протокол резервирования виртуального маршрутизатора (VRRP)
RFC 2698	Маркеры TRTCM (Two Rate Three Color Marker)
RFC 2865	RADIUS – специальный атрибут производителя
RFC 2674	P-BRIDGE-MIB, Q-BRIDGE-MIB
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

Таблица 152 Поддерживаемые стандарты (продолжение)

СТАНДАРТ	ОПИСАНИЕ
IEEE 802.3ad	Агрегация каналов
IEEE 802.3ah	Ethernet OAM (эксплуатация, администрирование и обслуживание)
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.

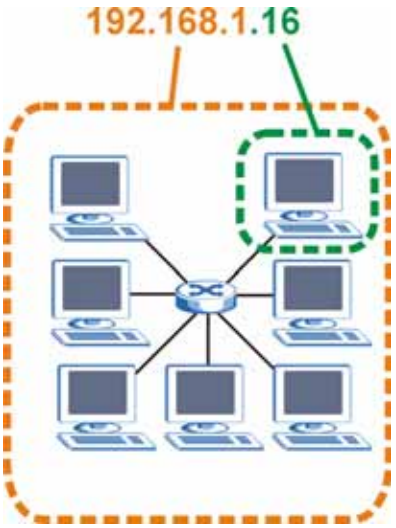
Структура

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 212 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 153 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 154 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 155 Максимально возможное число хостов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИ-ФИКАТОРА 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 156 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

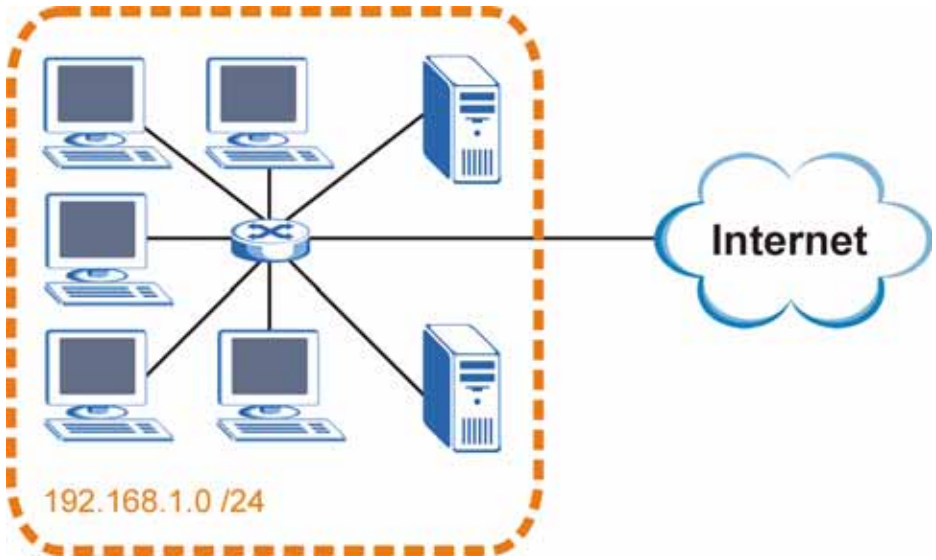
Формирование подсетей

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 213 Пример формирования подсетей: до разделения на подсети

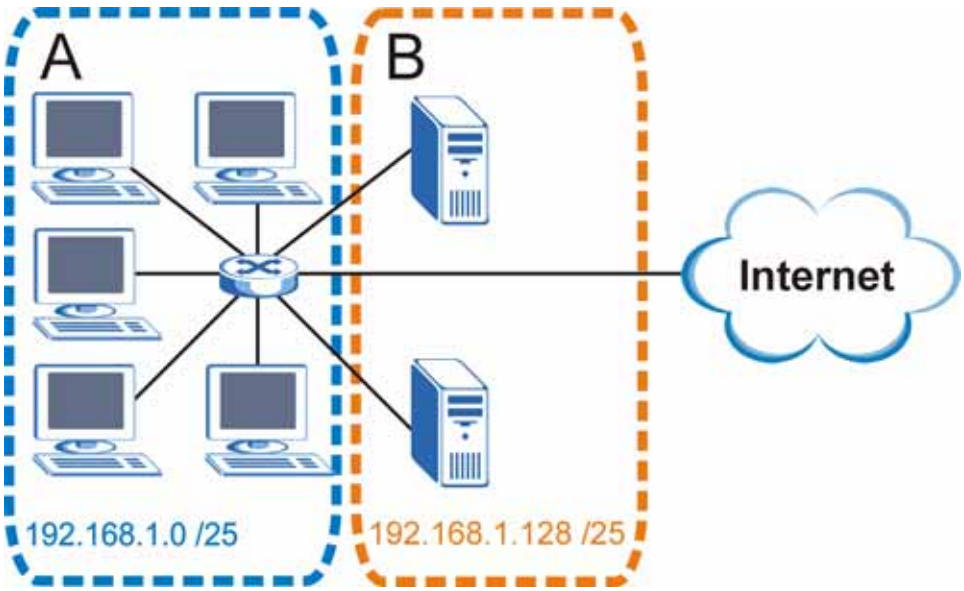


Чтобы разделить сеть 192.168.1.0 на две отдельные подсети, можно «позаимствовать» один бит из идентификатора хоста. В этом случае маска подсети станет 25-битной (255.255.255.128 или /25).

«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 214 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 157 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 158 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 159 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 160 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
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 161 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 162 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 163 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

Таблица 163 Планирование подсетей для сети с 16-битным номером (продолжение)

КОЛИЧЕСТВО «ОДОЛЖЕННЫХ» БИТОВ ИДЕНТИФИКАТОРА ХОСТА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ПОДСЕТИ
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 коммутаторекоммутатор 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

Коммутатор ZyXEL ES-4124 одобрен для применения государственными органами по сертификации средств связи.

Система сертификации ГОСТ Р, Госстандарт России

Сертификат соответствия № РОСС TW.АЯ46.B55031. Срок действия с 29.03.2007 по 28.03.2010.

Соответствие 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.

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.

Соответствие требованиям: СанПиН 2.2.2./2.4.1340-03,СанПиН 2.1.8./2.2.4.1190-03.

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.

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: SYxWWxxxxx, 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.

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

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

Индекс

Символы

A

Б

B (C)

Г (D)

Д

E (F)

Ж (G)

З (H)

И (I)

K

Л (L)

M

Н (N)

О

П (P)

Q

P (R)

C (S)

T

У

Ф (V)

X (W)

Ч

Ш

Э