Серия MGS3520

Управляемый Metro коммутатор GbE уровня 2

Версия 4.10
Издание 3-е, 05/2014

Руководство пользователя

Параметры входа по умолчанию	
IP-адрес интерфейса LAN	http://192.168.1.1
Имя пользователя	admin
Пароль	1234

ВАЖНО!

ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ ПЕРЕД ИСПОЛЬЗОВАНИЕМ.

СОХРАНИТЕ ЭТО РУКОВОДСТВО ДЛЯ БУДУЩИХ СПРАВОК.

Настоящий документ является руководством пользователя для серии продуктов. Не все продукты из этой серии поддерживают все функциональные возможности встроенного программного обеспечения. Снимки экрана и графические изображения в этом руководстве могут отличаться от реального вида продукта из-за различий во встроенном программном обеспечении или в операционной системе, установленной на компьютере пользователя. Нами сделано все возможное для того, чтобы информация, приведенная в настоящем руководстве, была точной.

Дополнительная документация

- Справочное руководство по интерфейсу командной строки

  В справочном руководстве по интерфейсу командной строки описана настройка коммутатор с использованием этого интерфейса.

Примечание: Для настройки коммутатор предпочтительнее использовать Web-конфигуратор.

Обзорное оглавление

Оглавление

Часть I
Руководство пользователя

1

Знакомство с коммутатором

1.1 Введение

В этой главе описаны основные характеристики и способы применения коммутатора. Серия MGS3520 включает в себя следующие три модели:

- MGS3520-28
- MGS3520-28F
- MGS3520-50

Данные устройства представляют собой автономные коммутаторы Ethernet уровня 2 с дополнительными функциями второго, третьего и четвертого уровня, которые можно использовать в сетях Ethernet.

Встроенный Web-конфигуратор облегчает просмотр, управление и настройку параметров коммутатора и подключенных к нему устройств. 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.

В таблице, приведенной ниже, описаны порты коммутатора для каждой из моделей.

Таблица 1 Модели и доступные порты

МОДЕЛЬ КОММУТАТОРА	ПОРТЫ
MGS3520-28	• 24 порта Ethernet на 10/100/1000 Мбит/с • 4 совмещенных интерфейса GbE
MGS3520-28F	• 24 порта open SFP Ethernet • 4 совмещенных интерфейса GbE
MGS3520-50	• 44 порта Ethernet на 100/1000 Мбит/с • 4 совмещенных интерфейса GbE • 2 интерфейса SFP

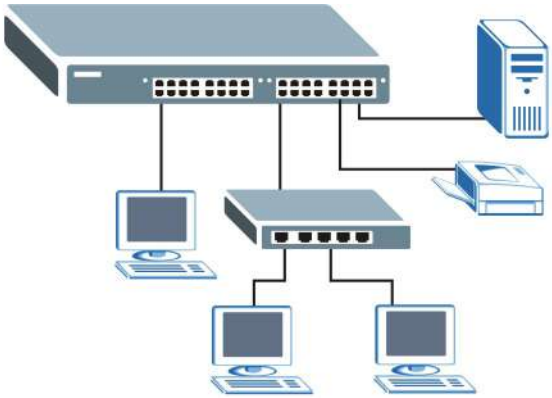
ОВ данном разделе приводится несколько примеров использования коммутатора в различных сетевых конфигурациях.

1.1.1 Применение в магистральной сети

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

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

Рисунок 1 Применение в магистральной сети

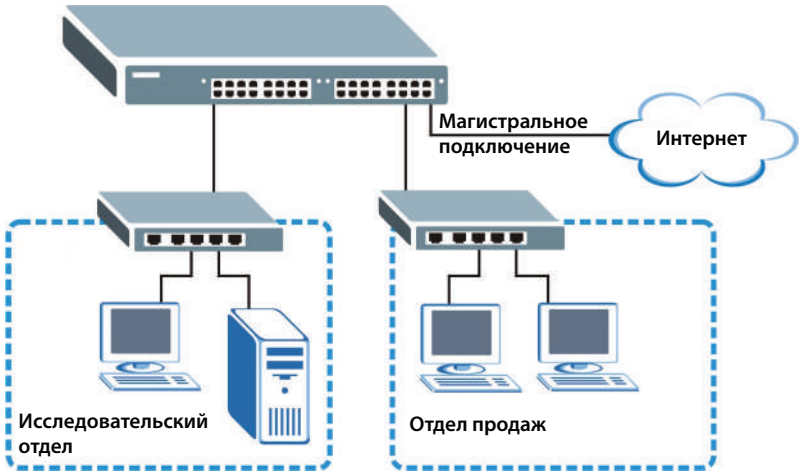


1.1.2 Пример мостовой конфигурации

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

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

Рисунок 2 Применение в мостовой конфигурации

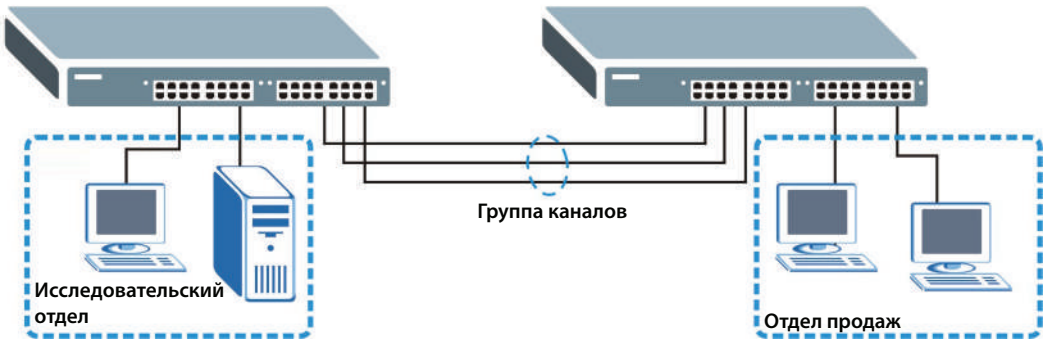


1.1.3 Пример высокоскоростной коммутации

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

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

Рисунок 3 Пример высокоскоростной коммутации в рабочей группе



1.1.4 Примеры применения в сетях VLAN на базе IEEE 802.1Q

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

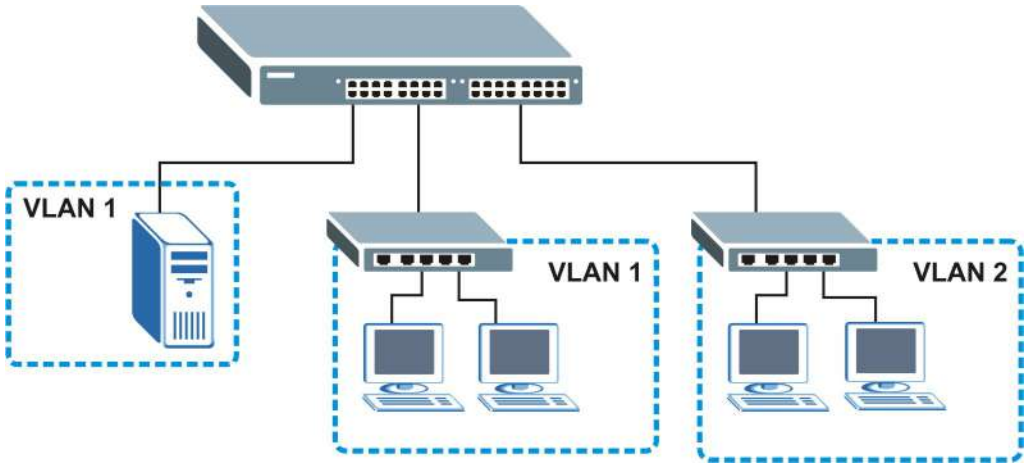
Дополнительную информацию о виртуальных локальных сетях можно найти в гл. 9 на стр. 86.

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. 32.
- Интерфейс командной строки. Интерфейс командной строки является альтернативой Web-конфигуратору и может потребоваться в некоторых случаях для настройки расширенных функций. См. Справочное руководство по интерфейсу командной строки.
- FTP. Протокол передачи файлов FTP можно использовать для обновления встроенного программного обеспечения и резервного копирования/восстановления конфигурации. См. разд. 37.7.1 на стр. 329.
- SNMP. Данный коммутатор поддерживает мониторинг с использованием менеджера SNMP. См. разд. 37.5 на стр. 327.
- Управление кластерами. Управление кластерами позволяет управлять несколькими коммутаторами через один, называемый менеджером кластера. См. гл. 40 на стр. 361.

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 забыт пароль, можно восстановить на коммутаторе заводские настройки по умолчанию. При наличии резервной копии более ранней версии файла конфигурации не придется повторно настраивать коммутатор от начала и до конца. Можно будет просто восстановить последнюю конфигурацию.

2

Установка и подключение устройства

2.1 Сценарии установки

В данной главе описаны процедуры установки и подключения коммутатора.

Данный коммутатор может быть установлен на столе или смонтирован в стандартную стойку. При установке на столе используются резиновые ножки, а в случае установки в стойку – монтажные кронштейны.

Примечание: 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 Процедура установки 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.

2.3 Установка коммутатора в стойку

Возможна установка коммутатора в стандартную 19-дюймовую стойку или в шкаф вместе с другим оборудованием. Для установки коммутатора в стандартную стойку с использованием комплекта для монтажа в стойку выполните следующие действия.

2.3.1 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.

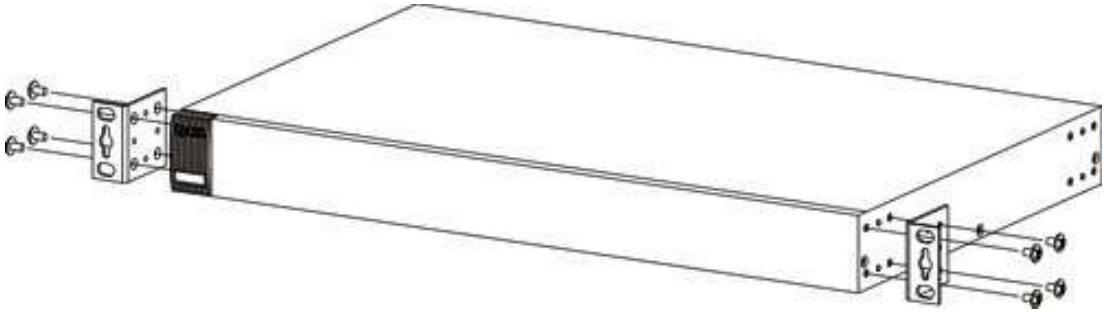
2.3.1.1 Меры предосторожности

- 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.

2.3.2 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 5 Закрепление кронштейнов



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

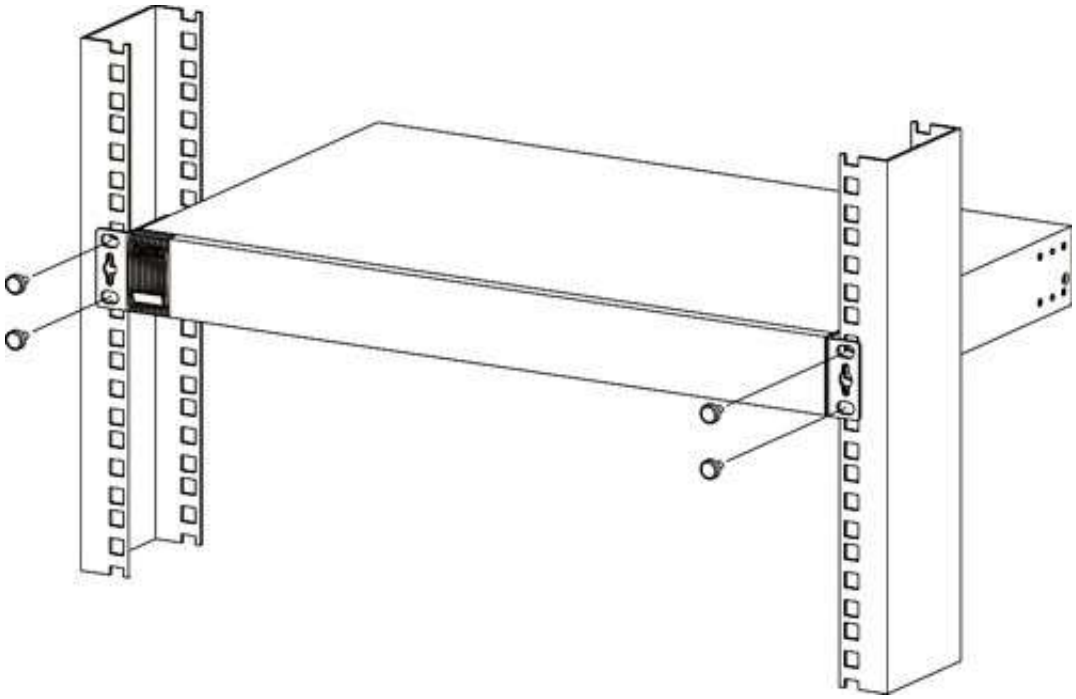
3 Повторите шаги 1 и 2, чтобы закрепить кронштейн на другой стороне коммутатора.

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

2.3.3 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 6 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

Панели устройства

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

3.1 Передняя панель

На рисунках ниже изображены передние панели различных моделей коммутатора.

Рисунок 7 Передняя панель: MGS3520-28

Рисунок 8 Передняя панель: MGS3520-28F

Рисунок 9 Передняя панель: MGS3520-50

3.1.1 Порты Gigabit Ethernet

Данный коммутатор оснащен портами Ethernet 1000Base-T с функциями автосогласования и автоматического определения типа кабеля. Порты Gigabit Ethernet на 10/100/1000 Мбит/с могут работать на скорости 10 Мбит/с, 100 Мбит/с или 1000 Мбит/с в полудуплексном или дуплексном режиме.

Порт с функцией автосогласования может определять и настраивать оптимальную скорость (10/100/1000 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.

Четыре порта Ethernet 1000Base-T, совмещенные со слотами mini-GBIC, образуют совмещенные интерфейсы. Данный коммутатор использует только одно соединение из каждой пары mini-GBIC и 1000Base-T Ethernet. Слоты mini-GBIC имеют приоритет перед портами Gigabit Ethernet. Это означает, что если слот mini-GBIC и соответствующий ему порт GbE подключены одновременно, то порт GbE работать не будет.

Примечание: При установке оптического модуля совмещенные порты переходят в оптический режим.

Когда автосогласование включено, Ethernet-порт автоматически обменивается данными с портом на другой стороне и сам выбирает скорость соединения и режим дуплекса. Если порт Ethernet 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 Ethernet-порт использует заранее определенную скорость и режим дуплекса. Таким образом, чтобы соединение произошло, у Ethernet-порта на другой стороне должны быть точно такие же параметры, что и у порта коммутатора.

3.1.1.1 Настройки Ethernet по умолчанию

По умолчанию для портов Gigabit Ethernet коммутатора установлены следующие заводские настройки автосогласования:

- Скорость: Автосогласование
- Режим дуплекса: Автосогласование
- Управление потоком: Нет
- Агрегация каналов: Отключено

3.1.1.2 Автоматическое определение типа кабеля

Все порты поддерживают автоматическое определение типа кабеля, то есть автоматический выбор режима MDI/MDI-X, поэтому для подключения к любым портам Gigabit Ethernet можно использовать как стандартный (прямой), так и кроссоверный (перекрещенный) кабели Ethernet. Порты с автоматическим определением типа кабеля автоматически переключаются в нужный режим, поэтому с помощью кроссоверных кабелей можно подключать как компьютеры, так и другие коммутаторы/концентраторы.

3.1.2 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.

Трансиверы можно менять во время работы коммутатора. Для подключения к Ethernet-коммутаторам с различными типами оптоволоконных интерфейсов или даже интерфейсов для витой пары можно пользоваться различными типами трансиверов.

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

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

3.1.2.1 Установка трансивера

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

1 Вставьте трансивер в слот открытой секцией печатной платы вниз.

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.

4 Закройте защелку трансивера (их вид может различаться).

5 Подключите оптоволоконные кабели к трансиверу.

Рисунок 10 Пример установки трансивера

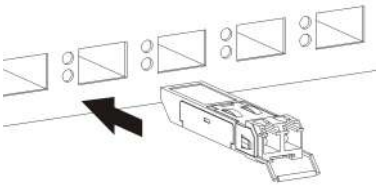
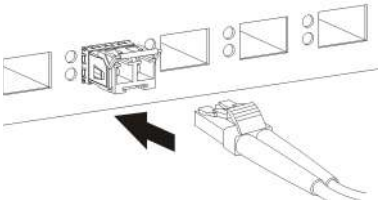


Рисунок 11 Подключение оптоволоконных кабелей



3.1.2.2 Удаление трансивера

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

1 Отключите оптоволоконные кабели от трансивера.

2 Откройте защелку трансивера (их вид может различаться).

3 Выньте трансивер из слота.

Рисунок 12 Отключение оптоволоконных кабелей

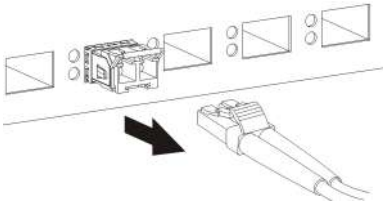


Рисунок 13 Пример открытия защелки трансивера

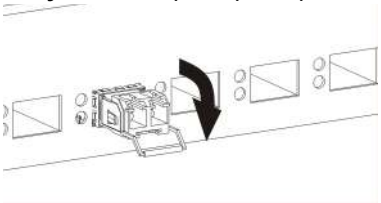
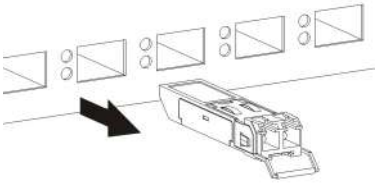


Рисунок 14 Пример удаления трансивера



3.2 Задняя панель

На рисунках ниже изображены передние панели различных моделей коммутатора.

Рисунок 15 Задняя панель: MGS3520-28

Рисунок 16 Задняя панель: MGS3520-28F

Рисунок 17 Задняя панель: MGS3520-50

3.2.1 Консольный порт

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

- VT100
- Эмуляция терминала
- Скорость 9600 бит/с
- 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.

3.2.2 Разъем питания

Примечание: Убедитесь, что параметры питающей сети соответствуют указанным на панели.

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

источнику питания. Убедитесь, что потокам воздуха от вентиляторов (на боковых стенках) ничего не мешает.

Более подробную информацию о требованиях коммутатора к электропитанию можно найти в гл. 47 на стр. 381.

3.3 Индикаторы

После подключения питания к коммутатору с помощью индикаторов можно убедиться в надлежащей работе коммутатора, а также использовать их в процессе устранения неполадок.

Таблица 2 Описание индикаторов

ИНДИКАТОР	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
PWR	Зеленый	Горит	Система работает.
		Не горит	Система выключена или неисправна.
SYS	Зеленый	Горит	Система включена и функционирует нормально.
		Мигает	Система перезагружается и выполняет самодиагностику.
		Не горит	Питание отключено или система не готова / работает с ошибками.
ALM	Красный	Горит	Обнаружен сбой оборудования.
		Не горит	Система работает нормально.
Порты Ethernet			
1-24 и 1-48 LNK/ACT	Зеленый	Мигает	Осуществляется прием или передача данных в сети Ethernet со скоростью 10 Мбит/с или 1000 Мбит/с.
		Горит	Установлено соединение с сетью Ethernet на скорости 10 Мбит/с или 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.
Слоты mini-GBIC			
25-28 45-50 SFP	Зеленый	Горит	На порту каскадирования установлено соединение на скорости 1000 Мбит/с.
		Мигает	Система осуществляет передачу/прием данных на скорости 1000 Мбит/с.
	Желтый	Горит	На порту каскадирования установлено соединение на скорости 100 Мбит/с.
		Мигает	Система осуществляет передачу/прием данных на скорости 100 Мбит/с.
		Не горит	Отсутствует соединение или порт, порт каскадирования отключен.

Часть II
Техническое справочное руководство

4

Web-конфигуратор

4.1 Обзор

В данном разделе описаны настройки и функции Web-конфигуратора.

Web-конфигуратор – это интерфейс управления на основе HTML, который позволяет легко настраивать и управлять коммутатором через Интернет-браузер. Используйте Internet Explorer 6.0, Netscape Navigator 7.0 и Mozilla Firefox 3.0 или более поздние версии указанных браузеров. Рекомендованное разрешение экрана – 1024 на 768 пикселей.

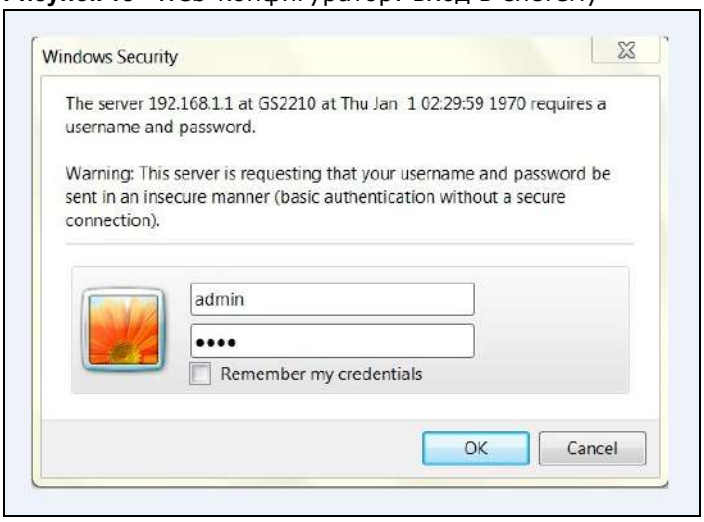
Для использования Web-конфигуратора нужно разрешить:

- 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, IP-адрес для управления по умолчанию – 192.168.1.1) в поле **Location** или поле **Address**. 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 не был настроен сервер времени или дата и время не были настроены в меню **General Setup**.

Рисунок 18 Web-конфигуратор: вход в систему



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

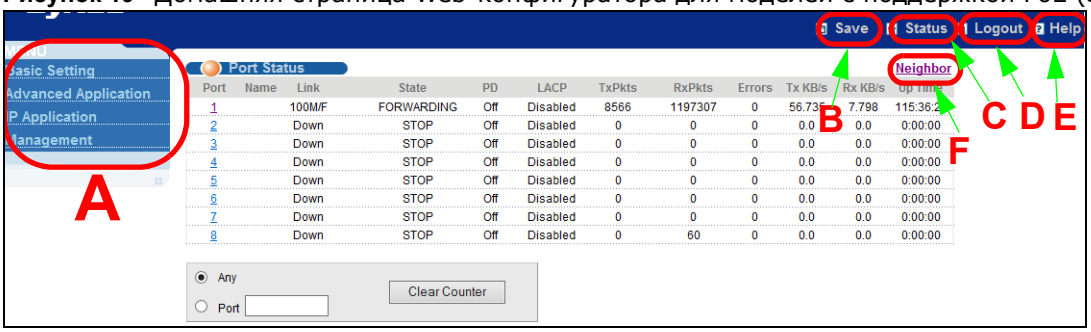
4.3 Окно состояния (Status)

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

В этом руководстве для примера использованы экраны с изображением моделей, поддерживающих питание устройств по витой паре (PoE). Для других моделей экраны могут немного отличаться.

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

Рисунок 19 Домашняя страница Web-конфигуратора для моделей с поддержкой PoE (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. После сохранения в энергонезависимой памяти конфигурация коммутатора остается неизменной даже в случае выключения питания коммутатора.

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

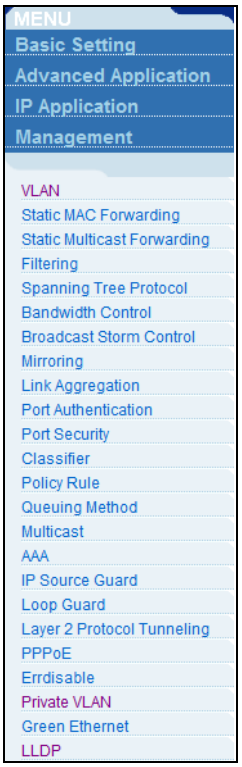
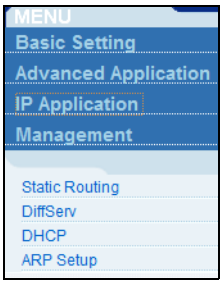
D – Нажатие на данную ссылку вызывает выход из Web-конфигуратора.

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

F – Щелкните по этой ссылке, чтобы перейти к экрану Neighbor Management, с помощью которого можно просматривать информацию о соседних устройствах, собранную коммутатором, и управлять ими.

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)
			

Пункты меню навигационной панели описаны в следующей таблице.

Таблица 4 Пункты меню навигационной панели

ПУНКТ	ОПИСАНИЕ
Basic setting (Основные настройки)	
System Info (Информация о системе)	Этот пункт открывает экран общей информации о системе.

Таблица 4 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
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, 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 экран, позволяющий настроить отдельные порты коммутатора.
PoE Setup (Настройки PoE)	Для моделей с поддержкой PoE Этот пункт открывает экран, с помощью которого на коммутаторе можно установить приоритеты резервирования и выделения мощности для определенных питаемых устройств.
Interface Setup (Настройка интерфейса)	Этот пункт открывает экран, с помощью которого можно задать параметры для определенных типов интерфейсов или интерфейсов с определенными идентификаторами.
IPv6	Этот пункт открывает экран, с помощью которого можно просмотреть статус и настроить параметры протокола IPv6.
Advanced Application (Расширенные приложения)	
VLAN	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 экран, позволяющий настроить статические MAC-адреса для каждого из портов. Такие статические MAC-адреса не имеют срока действия.
Static Multicast Forwarding (Многоадресная рассылка на основе статических MAC-адресов)	Этот пункт открывает экран, позволяющий настроить статические MAC-адреса многоадресной рассылки для портов. Такие статические MAC-адреса многоадресной рассылки 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 экран, позволяющий настроить ограничения пропускной способности на коммутаторе.

Таблица 4 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
Broadcast Storm Control (Контроль широковеща-тельных штормов)	Этот пункт открывает экран, позволяющий настроить фильтры широковещательной передачи.
Mirroring (Зеркальное дублирование)	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 (Аутентифика-ция портов)	Этот пункт открывает экран, позволяющий настроить аутентификацию портов на основе IEEE 802.1x для клиентов, подключающихся к коммутатору.
Port Security (Безопасность портов)	Этот пункт открывает экран, позволяющий включить получение таблицы MAC-адресов и установить максимальное количество MAC-адресов, которые может запомнить порт.
Classifier (Классифика-ция)	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.
Multicast (Многоадресная рассылка)	Этот пункт открывает экраны, позволяющие настроить различные функции многоадресной рассылки и отслеживания многоадресного трафика IGMP, а также создавать VLAN-сети многоадресной рассылки.
AAA (Аутенти-фикация, авторизация и учет)	Этот пункт открывает экран, позволяющий настроить различные функции аутентификации и авторизации 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 экраны, позволяющие настроить фильтрацию несанкционированных DHCP и ARP-пакетов в сети.
Loop Guard (Защита от образования петель)	Этот пункт открывает экран, позволяющий настроить защиту от образования сетевых петель на границе сети.
Layer 2 Protocol Tunneling (Протокол туннелирования уровня 2)	Этот пункт открывает экран, позволяющий настроить параметры протокола L2PT (Layer 2 Protocol Tunneling, протокол туннелирования уровня 2) на коммутаторе.
PPPoE	Этот пункт открывает экран, позволяющий настроить параметры промежуточного агента для портов, VLAN и PPPoE.
Errdisable (Отключение ошибок)	Этот пункт открывает экран, позволяющий настроить параметры отключения ошибок для функций защиты процессора, обнаружения сбоев и восстановления после них.

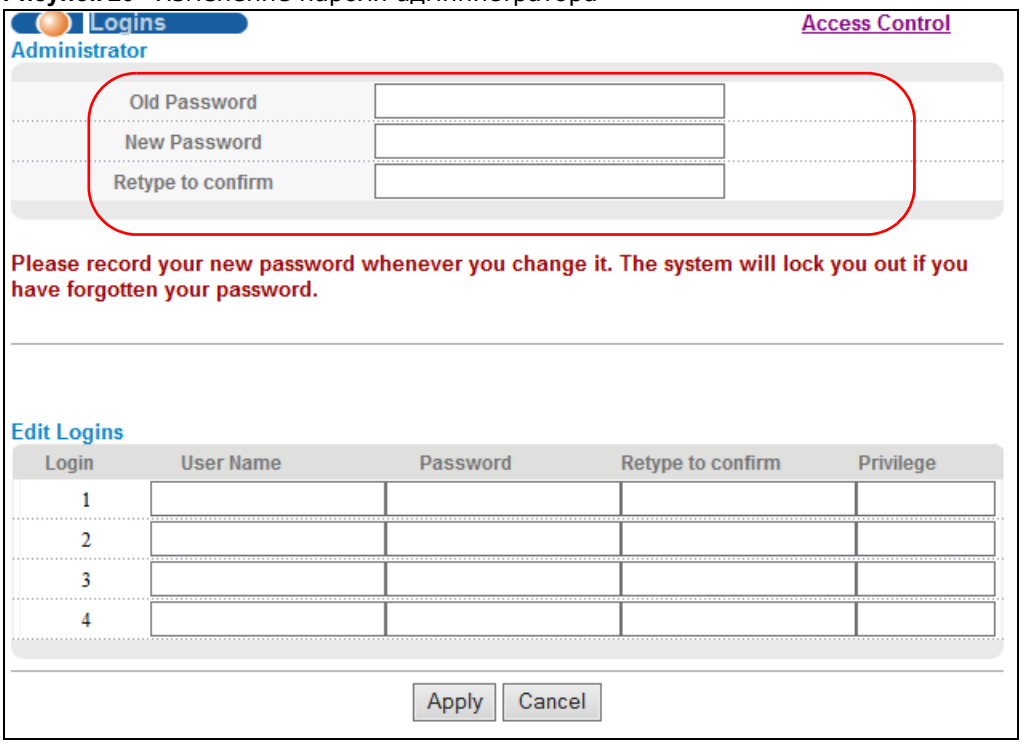
Таблица 4 Пункты меню навигационной панели (продолжение)

ПУНКТ	ОПИСАНИЕ
Private VLAN (Частная VLAN)	Этот пункт открывает экран, позволяющий настроить параметры частных виртуальных локальных сетей (VLAN).
Green Ethernet («Зеленый» Ethernet)	Этот пункт открывает экран, позволяющий настроить экологические параметры Ethernet, такие, как EEE (энергоэффективный Ethernet), автоматическое отключение питания и уменьшение протяженности соединений до каждого порта.
LLDP	Этот пункт открывает экран, позволяющий настроить параметры протокола LLDP.
IP Application (IP-приложения)	
Static Routing (Статические маршруты)	Этот пункт открывает экран, позволяющий настроить статические маршруты. Статический маршрут указывает коммутатору, куда следует направлять IP-трафик, посредством ручной настройки параметров протокола TCP/IP.
DiffServ	Этот пункт открывает экраны, позволяющие включить DiffServ, настроить правила маркировки и определить отображения между битами DSCP и IEEE802.1p.
DHCP	Этот пункт открывает экраны, позволяющие настроить протокол DHCP.
ARP Setup (Настройка ARP)	Этот пункт открывает экраны, позволяющие настроить параметры запоминания ARP для каждого порта.
Management (Управление)	
Maintenance (Обслужива-ние)	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 экран, позволяющий просматривать системные журналы и тестировать порты.
Syslog	Этот пункт открывает экраны, позволяющие настраивать системные журналы и сервер системного журнала.
Cluster Management (Управление кластерами)	Этот пункт открывает экраны, позволяющие настроить управление кластерами и просмотреть его состояние.
MAC Table (Таблица MAC-адресов)	Этот пункт открывает экран, позволяющий просматривать MAC-адреса (и типы) устройств, подключенных к каким-либо портам, а также идентификаторы виртуальных локальных сетей VLAN ID.
ARP Table (Таблица ARP)	Этот пункт открывает экран, позволяющий просмотреть таблицу соответствия MAC-адресов и IP-адресов.
Path MTU Table (Таблица MTU путей)	Этот пункт открывает экран, позволяющий просмотреть такие параметры, как время устаревания MTU пути, порядковый номер, адрес назначения, MTU и срок действия.
Configure Clone (Настройка клонирования)	Данный пункт открывает экран, позволяющий скопировать настройки одного из портов на другие порты.
Neighbor Table (Таблица соседних устройств)	Этот пункт открывает экран, позволяющий просмотреть таблицу соседей IPv6, которая включает в себя порядковый номер, интерфейс, адрес соседнего устройства, MAC-адрес, статус и тип.

4.3.1 Изменение пароля

После первого входа в систему рекомендуется изменить пароль администратора по умолчанию. Чтобы отобразить показанный ниже экран, нажмите **Management** > **Access Control** > **Logins**.

Рисунок 20 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.

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

4.5 Блокировка коммутатора

Выполнение любого из действий приводит к блокированию доступа к коммутатору:

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.

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

4.6 Сброс коммутатора

Если доступ к коммутатору был заблокирован (для текущего и остальных пользователей) или забыт пароль администратора, необходимо будет загрузить файл конфигурации с заводскими настройками по умолчанию или сбросить коммутатор до заводских настроек 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 бит/с, 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.

2 Отключите и включите снова питание коммутатора, чтобы начать сеанс. 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.

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 21 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

5.1 Обзор

В данной главе описаны настройки коммутатора на примере конкретной сети.

Первичная настройка включает в себя следующие шаги:

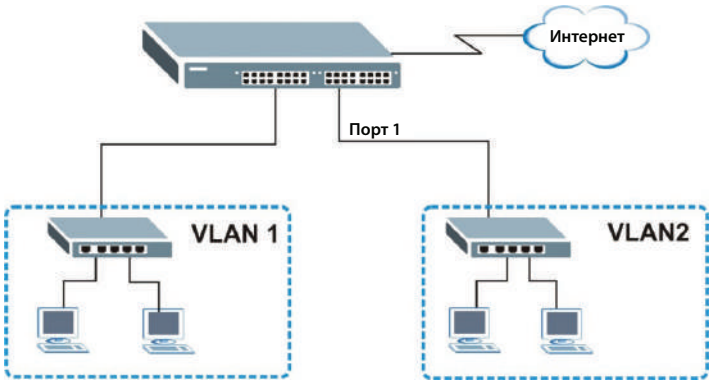
- Создание виртуальной локальной сети VLAN
- Определение идентификаторов VLAN для портов
- Настройка IP-адреса управления коммутатором

5.1.1 Создание виртуальной локальной сети VLAN

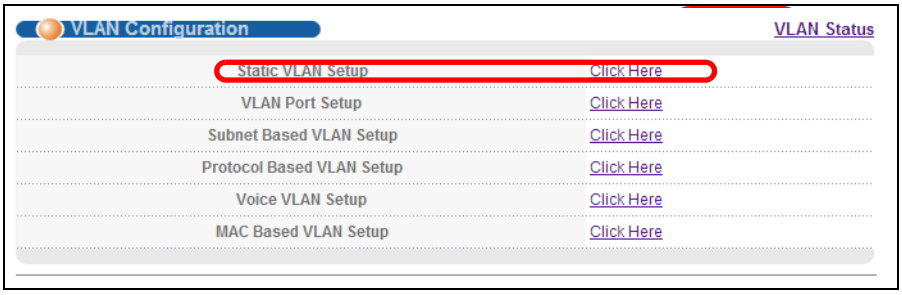
Виртуальные локальные сети ограничивают широковещательные кадры той группой VLAN, которой принадлежит порт (порты). Для этого можно использовать виртуальные локальные сети на основе портов или статические виртуальные локальные сети на основе тегов с фиксированными портами-членами.

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

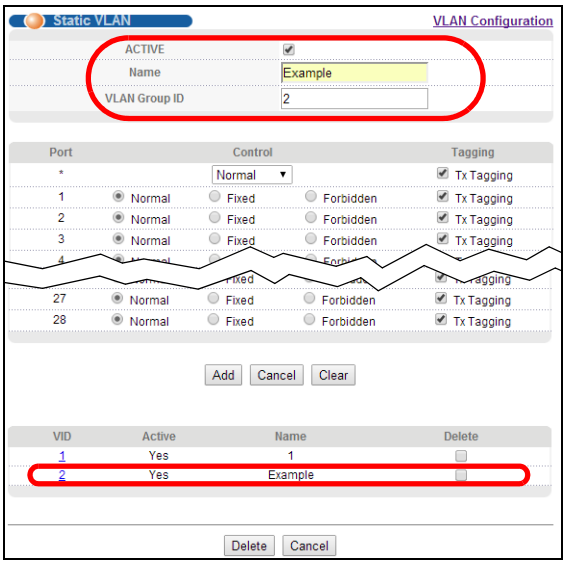
Рисунок 22 Пример первичной настройки сети: виртуальная локальная сеть



1 Выберите в навигационной панели **Advanced Application** > **VLAN > VLAN Configuration** и перейдите по ссылке **Static VLAN Setup**.



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



Примечание: 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.

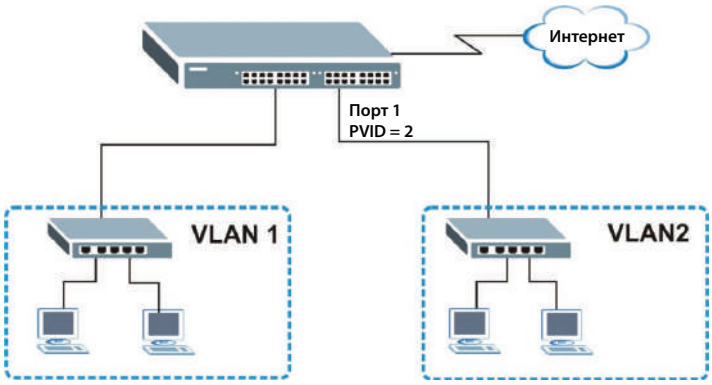
5 Нажмите **Add**, чтобы сохранить настройки в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

5.1.2 Назначение идентификатора виртуальной локальной сети VID для порта

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

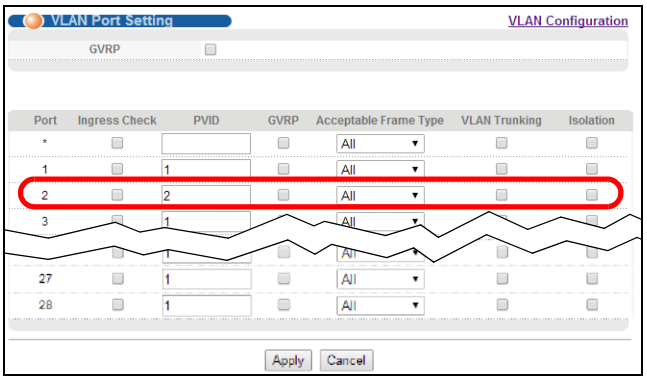
В данном примере необходимо установить 2 в качестве идентификатора VID для порта 1, чтобы все непомеченные тегами кадры, принятые через этот порт, отправлялись в виртуальную локальную сеть VLAN 2.

Рисунок 23 Пример первичной настройки сети: идентификатор виртуальной локальной сети для порта



1 Выберите в навигационной панели **Advanced Applications** > **VLAN > VLAN Configuration**. Затем перейдите по ссылке **VLAN Port Setup**.

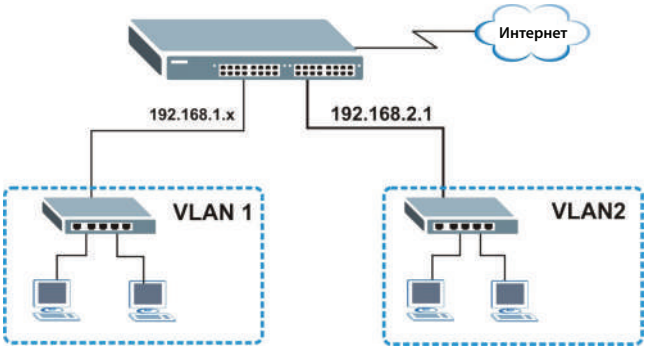
2 Введите 2 в поле **PVID** для порта 2 и нажмите **Apply**, чтобы сохранить изменения в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.



5.2 Настройка IP-адреса управления коммутатором

По умолчанию в качестве IP-адреса управления на коммутаторе используется адрес 192.168.1.1. Для управления устройством можно настроить другой IP-адрес из отличной подсети. Пример показан на следующем рисунке.

Рисунок 24 Пример первичной настройки: IP-адрес управления



1 Подключите компьютер к любому из портов Ethernet на коммутаторе. Убедитесь, что компьютер находится в той же подсети, что и коммутатор.

2 Откройте Web-браузер и введите в строке адреса 192.168.1.1 (IP-адрес по умолчанию), чтобы получить доступ к Web-конфигуратору. Дополнительную информацию можно найти в разд. 4.2 на стр. 32.

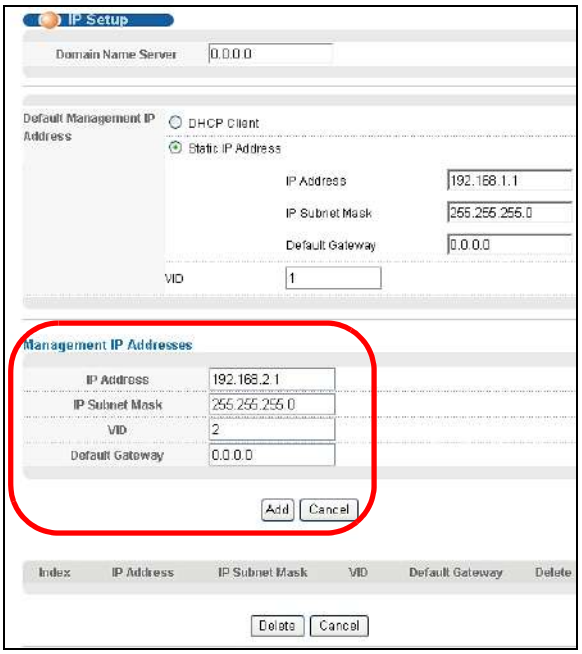
3 Выберите в навигационной панели **Basic Setting** > **IP Setup**.

4 Введите нужную информацию на экране **IP Setup**.

5 Для сети **VLAN2** введите в качестве IP-адреса 192.168.2.1 и маску подсети 255.255.255.0.

6 В поле **VID** введите идентификатор группы VLAN, которой должен принадлежать этот IP-адрес управления. Это должно быть то же значение, которое было введено в поле VLAN ID на экране меню **Static VLAN**.

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



6

Пошаговые указания

6.1 Обзор

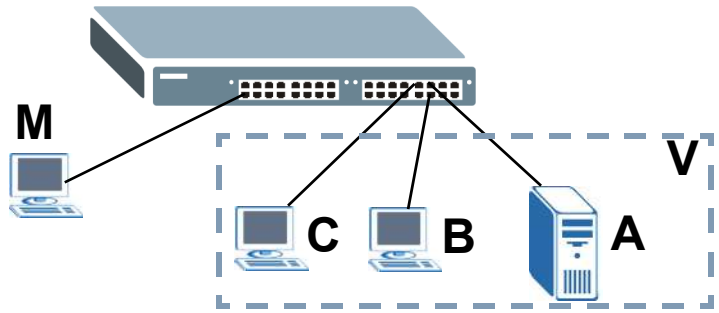
Эта глава содержит некоторые примеры использования Web-конфигуратора для настройки коммутатора и работы с ним. Пошаговые указания описывают выполнение следующих задач:

- Работа с функцией отслеживания DHCP на коммутаторе
- Использование ретрансляции DHCP на коммутаторе

6.2 Работа с функцией отслеживания DHCP на коммутаторе

Требуется, чтобы DHCP-сервер **A**, подключенный к порту 5, осуществлял раздачу IP-адресов всем устройствам в сети VLAN (**V**). Создайте сеть VLAN, включающую в себя порты 5, 6 и 7. Подключите компьютер **M** к коммутатору для управления.

Рисунок 25 Пошаговые указания: Обзор пошаговых указаний по работе с функцией отслеживания DHCP



Примечание: Дополнительную информацию о функции отслеживания DHCP можно найти в разд. 25.1 на стр. 217.

В этом примере используются следующие настройки.

Таблица 5 Пошаговые указания: Настройки в данном примере

ХОСТ	ПОДКЛЮЧЕННЫЙ ПОРТ	VLAN	PVID	ДОВЕРЕННЫЙ ПОРТ ОТСЛЕЖИВАНИЯ DHCP
DHCP-сервер (**A**)	5	1 и 100	100	Да
DHCP-клиент (**B**)	6	1 и 100	100	Нет
DHCP-клиент (**C**)	7	1 и 100	100	Нет

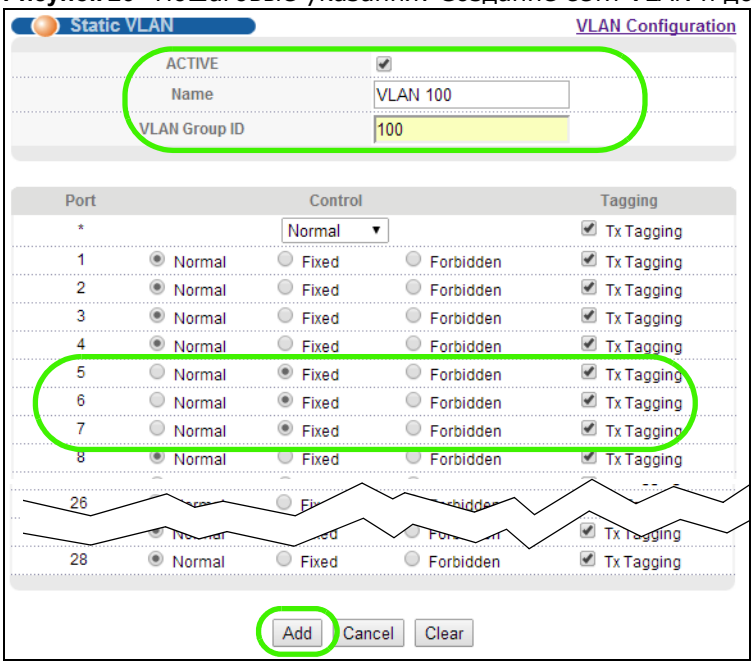
1 Откройте интерфейс управления коммутатором, набрав в строке браузера адрес по умолчанию **http://192.168.1.1**. Выполните вход на коммутатор, указав имя пользователя (по умолчанию **admin**) и пароль (по умолчанию **1234**).

2 Выберите в меню **Advanced Application** > **VLAN** > **VLAN Configuration** > **Static VLAN Setup** и создайте сеть VLAN с ID=100. Добавьте порты 5, 6 и 7 в сеть VLAN, выбрав опцию **Fixed** в поле **Control**.

Снимите выделение с переключателя **Tx Tagging**, поскольку исходящий трафик не должен содержать тег этой сети VLAN.

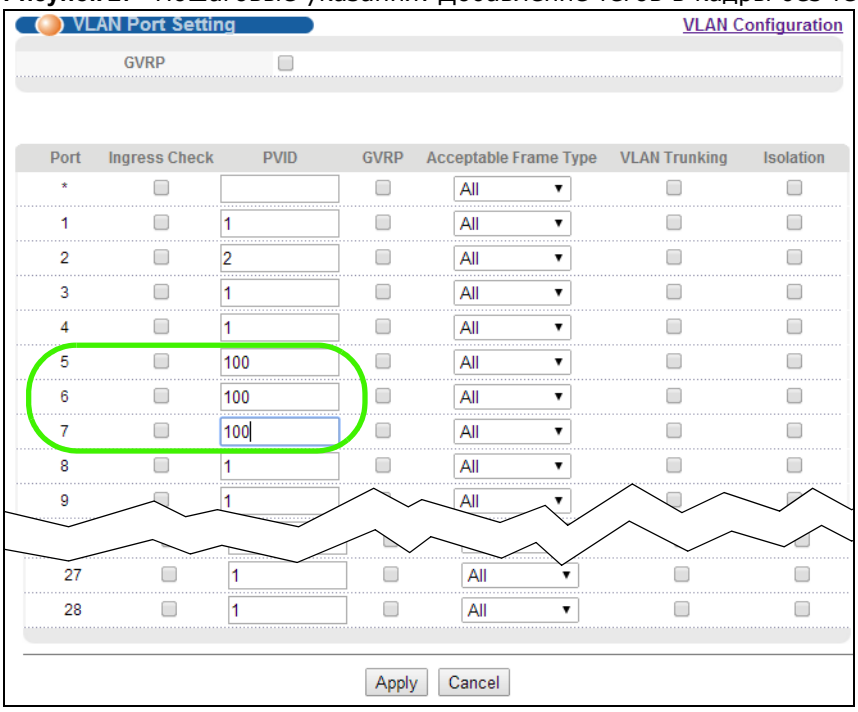
Нажмите кнопку **Add**.

Рисунок 26 Пошаговые указания: Создание сети VLAN и добавление портов в нее



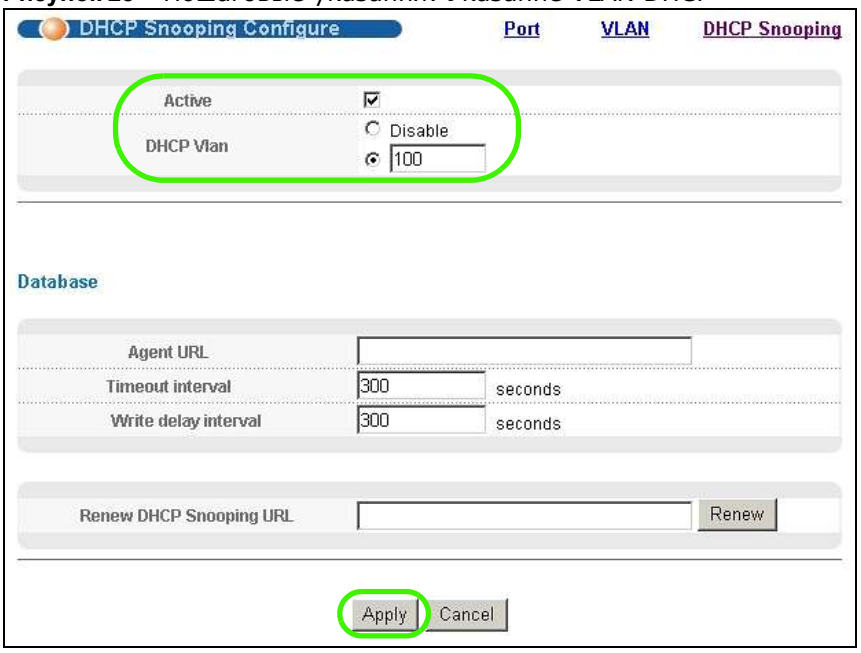
3 Выберите в меню **Advanced Application** > **VLAN** > **VLAN Configuration** > **VLAN Port Setup** и установите идентификатор PVID портов 5, 6 и 7 равным 100. Теперь входящим кадрам без тегов, принимаемым через порты 5, 6 и 7, будет присваиваться тег 100.

Рисунок 27 Пошаговые указания: Добавление тегов в кадры без тегов



4 Выберите в меню **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure**, затем активируйте и укажите VLAN 100 в качестве VLAN DHCP, как показано на рисунке. Нажмите на **Apply**.

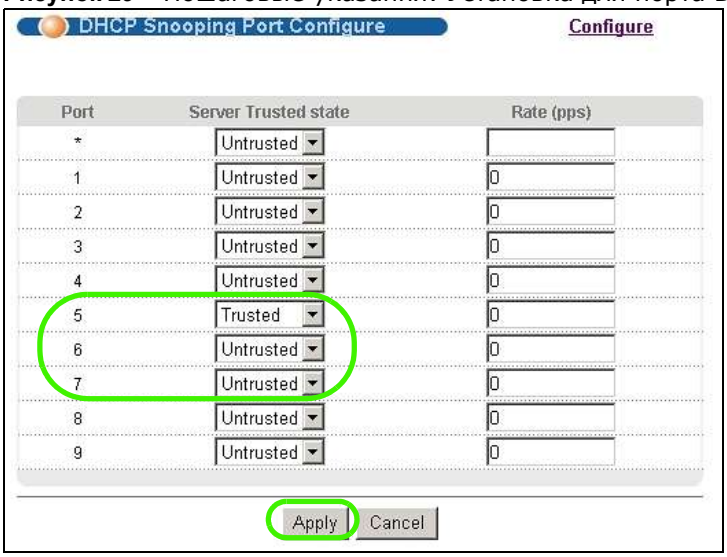
Рисунок 28 Пошаговые указания: Указание VLAN DHCP



5 Перейдите по ссылке **Port** в верхнем правом углу.

6 Откроется экран **DHCP Snooping Port Configure**. Выберите опцию **Trusted** в поле **Server Trusted state** для порта 5, поскольку к этому порту подключен DHCP-сервер. Для портов 6 и 7 выберите опцию **Untrusted**, поскольку к ним подключены DHCP-клиенты. Нажмите на **Apply**.

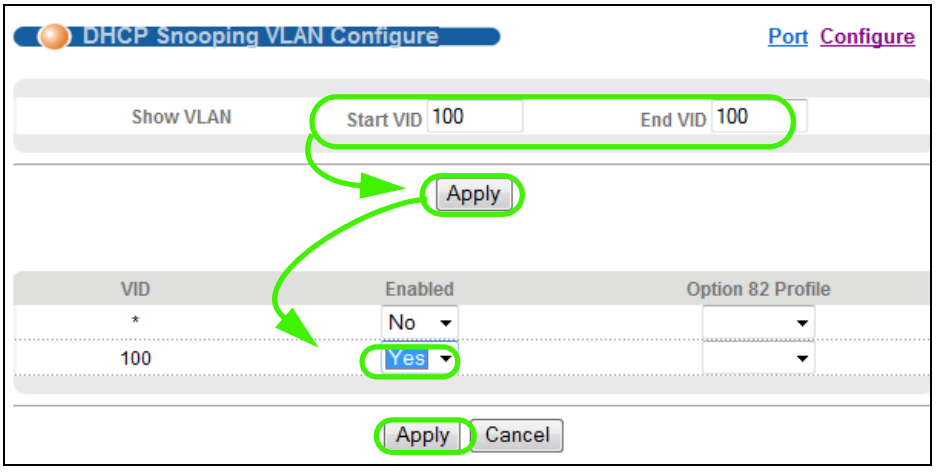
Рисунок 29 Пошаговые указания: Установка для порта DHCP-сервера опции Trusted



7 Выберите в меню **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure** > **VLAN**, выберите запись, соответствующую VLAN 100, указав значение 100 в полях **Start VID** и **End VID**, и нажмите **Apply**. Затем выберите опцию **Yes** в поле **Enabled** для записи, соответствующей VLAN 100, которая показана в нижней части экрана.

Чтобы включить в пакеты DHCP-запросов дополнительную информацию, такую, как идентификатор VLAN источника или имя системы, выберите опцию **Option82 Profile** для данной записи. См. разд. 25.10.1.3 на стр. 240.

Рисунок 30 Пошаговые указания: Включение функции отслеживания DHCP для данной сети VLAN



8 Нажмите **Save** в правом верхнем углу Web-конфигуратора, чтобы сохранить конфигурацию на постоянной основе.

9 Подключите DHCP-сервер к порту 5, а компьютер, выступающий в качестве DHCP-клиента, к порту 6 или 7. Компьютер должен иметь возможность получения IP-адреса от данного DHCP-сервера. В случае подключения DHCP-сервера к порту 6 или 7 такой возможности у компьютера не будет.

10 Чтобы проверить работу функции отслеживания DHCP, выберите в меню **Advanced Application** > **IP Source Guard**. Должен появиться назначенный IP-адрес с типом **DHCP-Snooping**, как показано на рисунке.

Рисунок 31 Пошаговые указания: Проверка работы привязки при включенной функции отслеживания DHCP

Подключиться к коммутатору можно также через telnet или консольный порт коммутатора. Чтобы просмотреть таблицу привязок функции отслеживания DHCP, как это показано ниже, воспользуйтесь командой «`show dhcp snooping binding`».

```
sysname# show dhcp snooping binding
         MacAddress        IpAddress         Lease           Type  VLAN   Port
  -----------------  ---------------  ------------  -------------  ----  -----
  00:02:00:00:00:1c       10.10.1.16   6d23h59m20s  dhcp-snooping   100      7
  Total number of bindings: 1
```

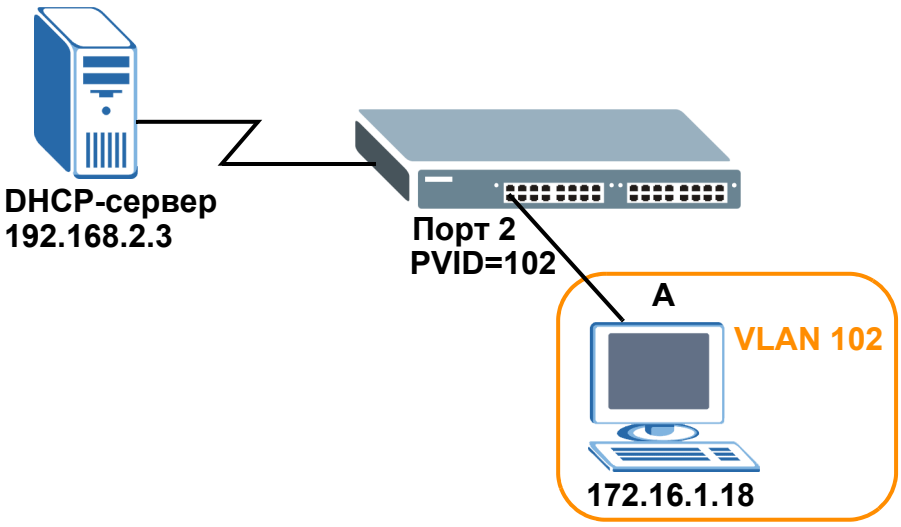
6.3 Использование ретрансляции DHCP на коммутаторе

В этих пошаговых указаниях показывается, как настроить коммутатор таким образом, чтобы он осуществлял пересылку запросов DHCP-клиента определенному DHCP-серверу. Указанный DHCP-сервер выделяет соответствующий IP-адрес исходя из информации, содержащейся в DHCP-запросах.

6.3.1 Условия для пошаговых указаний по работе с ретрансляцией DHCP

В этом примере имеется DHCP-сервер (192.168.2.3), который должен назначить определенный IP-адрес (например, 172.16.1.18) DHCP-клиенту **A**, выбрав его исходя из сведений об имени системы, идентификаторе VLAN и номере порта, содержащихся в DHCP-запросе. Клиент **A** подключается к порту 2 коммутатора в сети VLAN 102.

Рисунок 32 Пошаговые указания: Сценарий ретрансляции DHCP



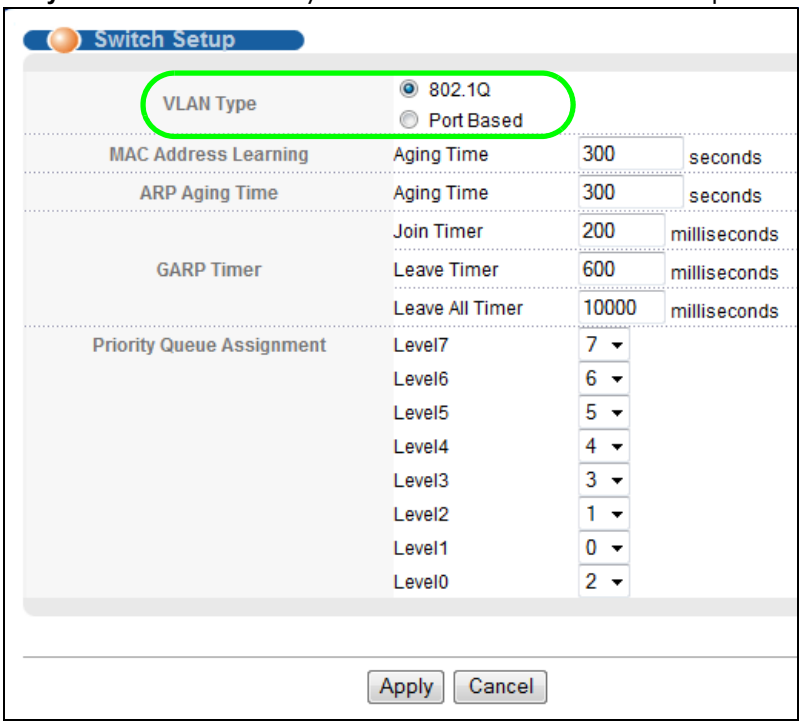
6.3.2 Создание виртуальной локальной сети VLAN

Чтобы сделать порт 2 членом сети VLAN 102, проделайте следующее.

1 Выполните вход в Web-конфигуратор через порт управления коммутатора.

2 Выберите в меню **Basic Setting** > **Switch Setup** и установите тип VLAN равным **802.1Q**. Нажмите **Apply**, чтобы сохранить настройки в оперативной памяти.

Рисунок 33 Пошаговые указания: Установка типа VLAN равным 802.1Q



3 Выберите в меню **Advanced Application** > **VLAN** > **VLAN Configuration** > **Static VLAN Setup**.

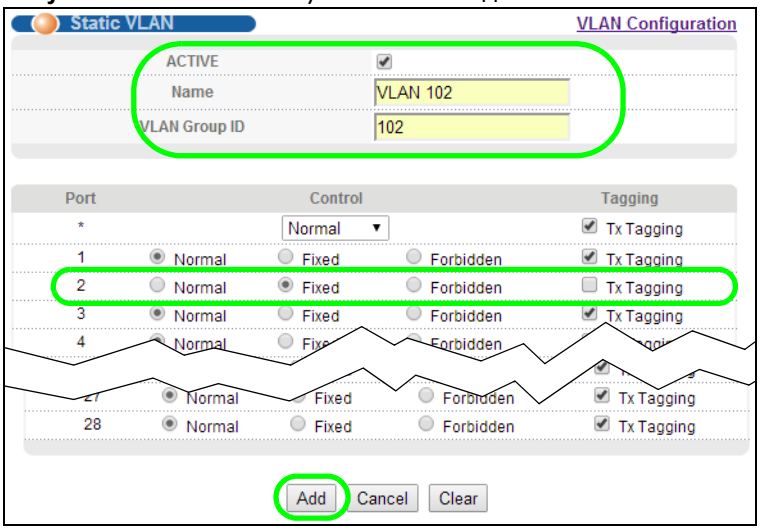
4 На экране **Static VLAN** выберите опцию **ACTIVE**, введите имя-описание (например, VLAN 102) в поле **Name** и номер 102 в поле **VLAN Group ID**.

5 Выберите опцию **Fixed**, чтобы сделать порт 2 постоянным членом данной сети VLAN.

6 Снимите выделение с переключателя **TX Tagging**, чтобы коммутатор выполнял удаление тегов VLAN перед отправкой пакетов.

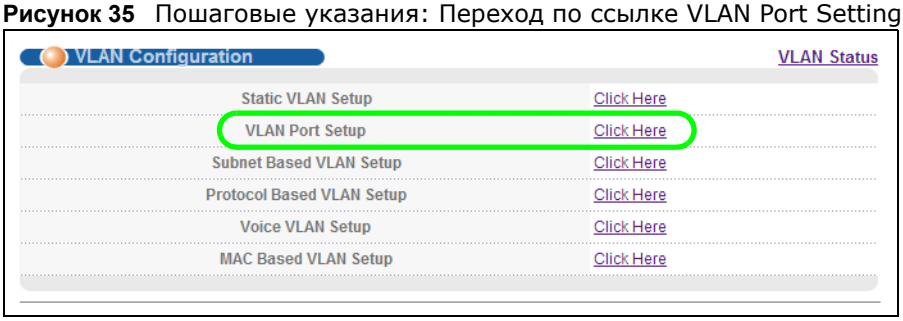
7 Нажмите **Add**, чтобы сохранить настройки в оперативной памяти. Настройки в оперативной памяти теряются при отключении питания коммутатора.

Рисунок 34 Пошаговые указания: Создание статической сети VLAN



8 Перейдите по ссылке **VLAN Configuration** на экране **Static VLAN Setup**, а затем по ссылке **VLAN Port Setup** на экране **VLAN Configuration**.

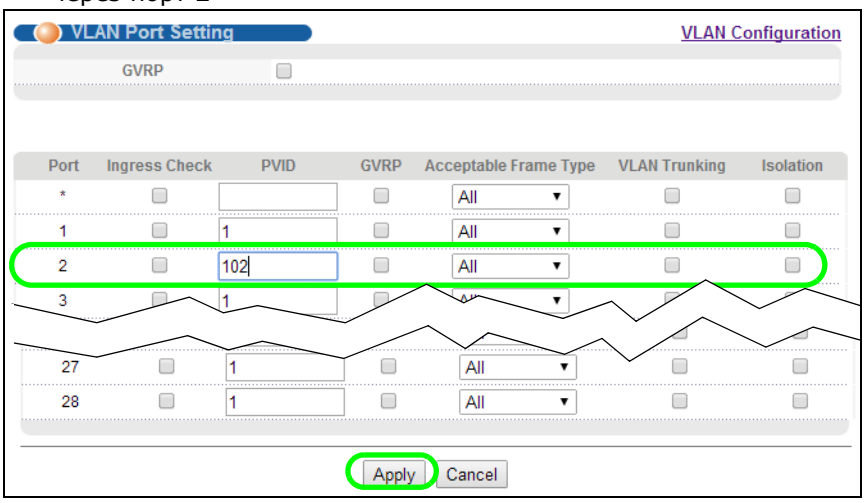
Рисунок 35 Пошаговые указания: Переход по ссылке VLAN Port Setting



9 Введите номер 102 в поле **PVID** для порта 2. Теперь коммутатор будет добавлять тег к входящим кадрам без тегов, принимаемым через этот порт, с тем, чтобы обеспечить пересылку этих кадров в группу VLAN, которую идентифицирует данный тег.

10 Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти.

Рисунок 36 Пошаговые указания: Включение добавления тегов для кадров, принимаемых через порт 2



11 Перейдите по ссылке **Save** в правом верхнем углу Web-конфигуратора, чтобы сохранить конфигурацию на постоянной основе.

6.3.3 Настройка ретрансляции DHCP

Выполните действия, описанные ниже, чтобы включить ретрансляцию DHCP на коммутаторе и разрешить коммутатору добавлять сведения агента ретрансляции (например, идентификатор сети VLAN) в DHCP-запросы.

1 Выберите в меню **IP Application > DHCP > DHCPv4**, а затем перейдите по ссылке **Global**, чтобы открыть экран **DHCP Relay**.

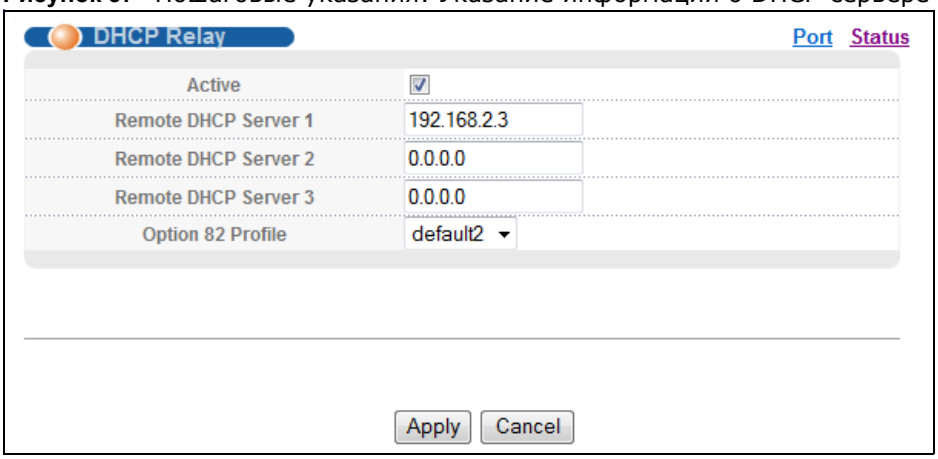
2 Установите переключатель **Active**.

3 Введите IP-адрес DHCP-сервера (в данном примере – 192.168.2.3) в поле **Remote DHCP Server 1**.

4 Выберите одну из опций **default1** или **default2** в поле **Option 82 Profile**.

5 Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти.

Рисунок 37 Пошаговые указания: Указание информации о DHCP-сервере и ретрансляторе



6 Перейдите по ссылке **Save** в правом верхнем углу Web-конфигуратора, чтобы сохранить конфигурацию на постоянной основе.

7 Указанный DHCP-сервер выделяет соответствующий IP-адрес исходя из информации, содержащейся в DHCP-запросах.

6.3.4 Устранение неполадок

Проверьте IP-адрес клиента **A**. Если этому клиенту не был назначен IP-адрес 172.16.1.18, удостоверьтесь в следующем:

1 Клиент **A** подключен к порту 2 в сети VLAN 102 коммутатора.

2 Идентификатор VLAN, номер порта и имя системы для DHCP-ретранслятора верно указаны как на DHCP-сервере, так и на коммутаторе.

3 Вы не забыли щелкнуть по ссылке **Save**, чтобы сохранить изменения в настройках коммутатора.

7

Neighbor Management и Port Status

7.1 Обзор

В данной главе описаны настройки экранов Neighbor Management, Port Status, Port Details.

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

7.1.1 О чем рассказывается в этой главе

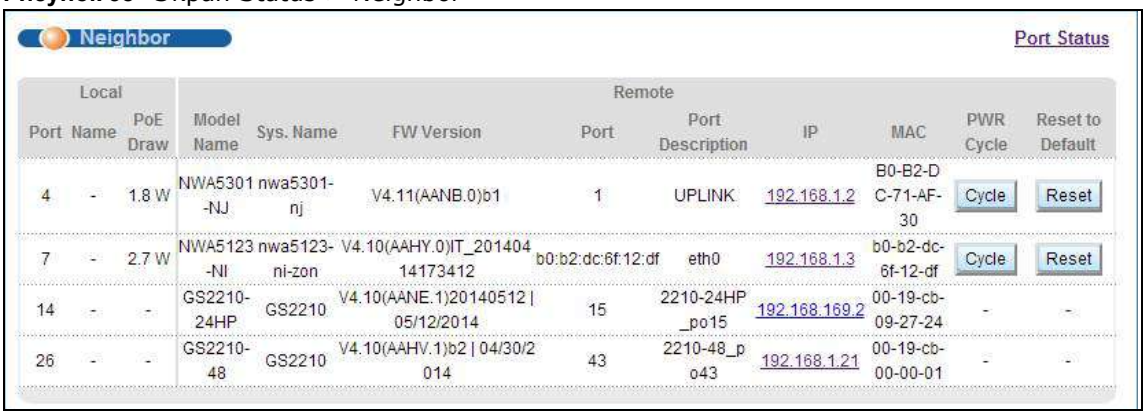
- С помощью экрана **Neighbor** (разд. 7.2 на стр. 54) можно просматривать информацию о соседних устройствах коммутатора и управлять ими.
- С помощью экрана **Port Status Summary** (разд. 7.3 на стр. 56) можно просматривать статистику для портов.
- С помощью экрана **Port Details** (разд. 7.3.1 на стр. 57) можно просматривать статистику для отдельных портов.

7.2 Экран Neighbor Management

Экран Neighbor Management предоставляет удобные средства для просмотра соседних устройств коммутатора и управления ими.Данная утилита использует протокол LLDP (Layer Link Discovery Protocol) для обнаружения всех соседних устройств, подключенных к коммутатору, в том числе устройств других производителей (не ZyXEL). Экран Neighbor Management позволяет выполнять на соседних устройствах такие действия, как вход в систему, перезагрузка (последовательное выключение и включение питания) и возврат к заводским настройкам по умолчанию. Более подробную информацию о протоколе LLDP можно найти в (разд. 32.2 на стр. 271).

Чтобы открыть экран, изображенный ниже, выберите в меню **Status** > **Neighbor**.

Рисунок 38 Экран Status > Neighbor



Поля экрана описаны в следующей таблице.

Таблица 6 Экран Status > Neighbor

ПОЛЕ	ОПИСАНИЕ
Local	
Port	Это поле показывает номер порта локального устройства в сети.
Name	Это поле показывает имя локального устройства в сети.
PoE Draw	Это поле показывает значение мощности, которую локальное устройство в сети потребляет от коммутатора. Наличие такого поля позволяет спланировать и использовать в соответствии с планом бюджет мощности коммутатора.
Remote	
Model Name	Это поле показывает название модели соседнего устройства в удаленной сети. Для устройств других производителей (не Zyxel) это поле содержит символ «-».
Sys. Name	Это поле показывает имя системы соседнего устройства в удаленной сети.
FW Version	Это поле показывает версию встроенного программного обеспечения соседнего устройства в удаленной сети. Для устройств других производителей (не Zyxel) это поле содержит символ «-».
Port	Это поле показывает номер порта соседнего устройства в удаленной сети.
Port Description	Это поле показывает описание порта соседнего устройства в удаленной сети.
IP	Это поле показывает IP-адрес соседнего устройства в удаленной сети. IP-адрес представляет собой **гиперссылку**, по которой можно щелкнуть и выполнить вход на удаленное устройство. Для устройств других производителей (не Zyxel) это поле содержит символ «-».
MAC	Это поле показывает MAC-адреса соседнего устройства в удаленной сети. Для устройств других производителей (не Zyxel) это поле содержит символ «-».

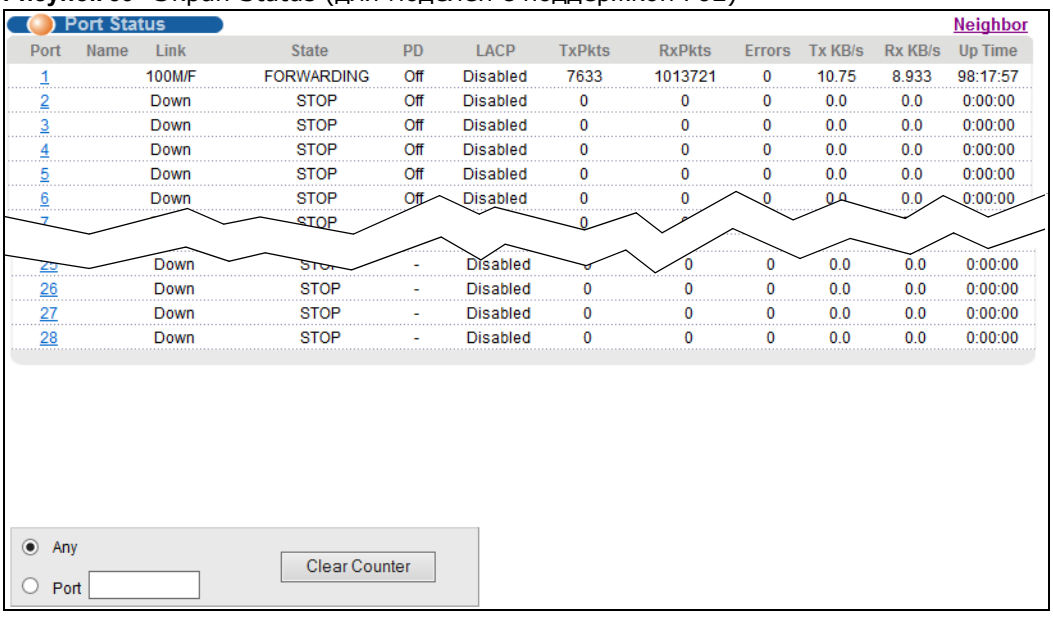
Таблица 6 Экран Status > Neighbor

ПОЛЕ	ОПИСАНИЕ
PWR Cycle	Нажмите кнопку **Cycle**, чтобы отключить питание соседнего устройства в удаленной сети и снова включить его. Начинает действовать кнопка обратного счета (с 5 до 0). Примечание: • Данный коммутатор должен представлять собой питающее устройство, либо сетевое устройство должно быть питаемым устройством. • Если два и более соседних устройств используют один и тот же порт, то кнопка **Cycle** отображается только на первом устройстве, на остальных вместо этого будет показан знак дефиса («**-**»).
Reset to Default	Нажмите кнопку **Reset**, чтобы вернуть для соседнего устройства в удаленной сети заводские настройки по умолчанию. На экране появится предупредительное сообщение «**Are you sure you want to load factory default?**» («Действительно вернуться к настройкам по умолчанию?») с предложением подтвердить выполняемое действие. После подтверждения начинает действовать кнопка обратного отсчета (от 5 до 0). Примечание: • Данный коммутатор должен представлять собой питающее устройство, либо сетевое устройство должно быть питаемым устройством. • Если два и более соседних устройств используют один и тот же порт, то кнопка **Reset** становится недоступной, и вместо нее отображается знак дефиса («**-**»). • Выполнить возврат к заводским настройкам по умолчанию можно только для устройств производства ZyXEL.

7.3 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 39 Экран Status (для моделей с поддержкой PoE)



Поля экрана описаны в следующей таблице.

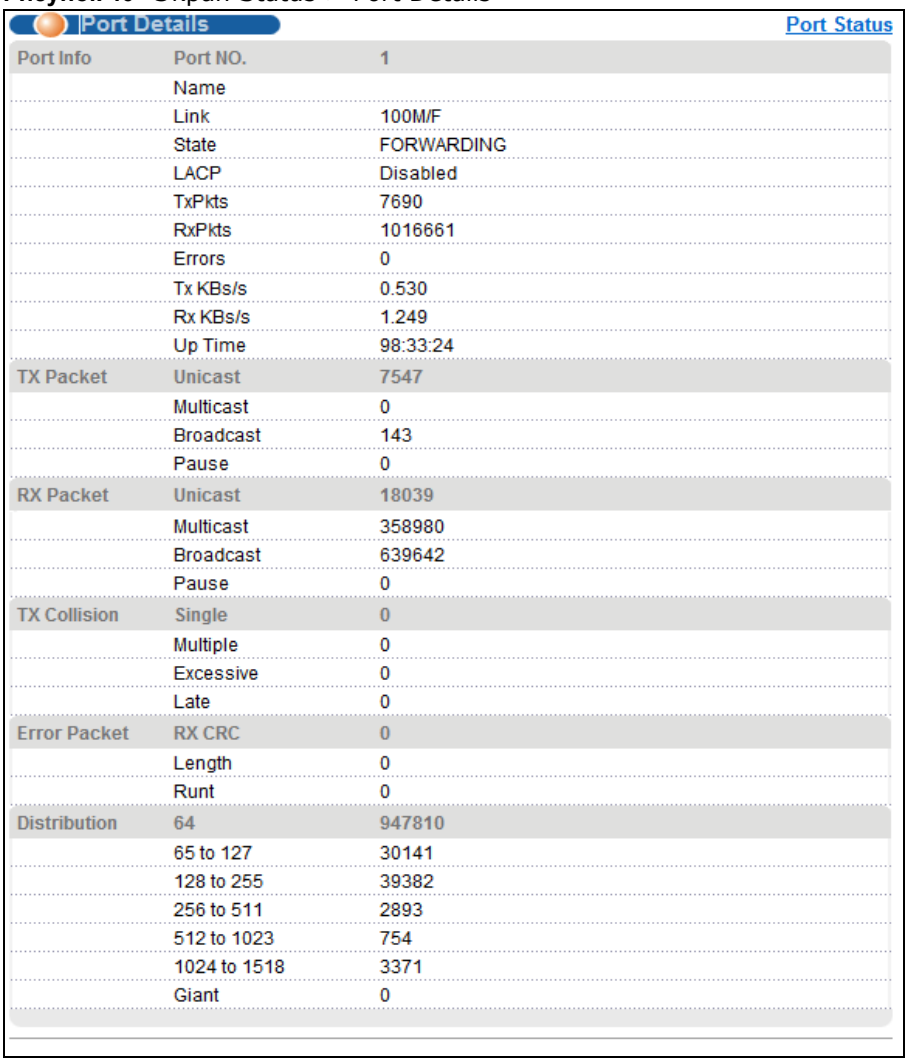
Таблица 7 Экран Status

ПОЛЕ	ОПИСАНИЕ
Port	Номер Ethernet-порта. Нажмите на номер порта, чтобы отобразить экран подробной статистики порта **Port Details** (см. рис. 40 на стр. 58).
Name	Имя, назначенное данному порту на экране **Basic Setting** > **Port Setup**.
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. 13.1 на стр. 118. Если протокол STP отключен, в этом поле отображается **FORWARDING** в случае установленного соединения и **STOP** в противном случае.
PD	Только для моделей с поддержкой PoE Это поле указывает на то, разрешено ли питаемому устройству получать питание от коммутатора через данный порт.
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**.

7.3.1 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 40 Экран Status > Port Details



Поля экрана описаны в следующей таблице.

Таблица 8 Экран Status: Port Details

ПОЛЕ	ОПИСАНИЕ
Port Info	
Port NO.	В этом поле отображается номер порта.
Name	В этом поле отображается имя порта.
Link	В этом поле отображается скорость (**10M** для 10 Мбит/с, **100M** для 100 Мбит/с или **1000M** для 1000 Мбит/с) и режим дуплекса (**F** для дуплекса или **H** для полудуплекса). Кроме того, в поле отображается тип кабеля (**Copper** для витой пары или **Fiber** для оптоволокна).
Status	Если активирован протокол покрывающего дерева STP, в этом поле отображается состояние порта по протоколу STP. Дополнительную информацию можно найти в разд. 13.1 на стр. 118. 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.

Таблица 8 Экран Status: Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
RxPkts	В этом поле отображается количество принятых этим портом кадров.
Errors	В этом поле отображается количество принятых этим портом кадров с ошибками.
Tx KB/s	В этом поле отображается количество переданных этим портом килобайт в секунду.
Rx KB/s	В этом поле отображается количество принятых этим портом килобайт в секунду.
Up Time	В этом поле отображается полное время, в течение которого поддерживалось соединение.
Tx Packet В следующих полях отображается подробная информация о переданных пакетах.	
Unicast	В этом поле отображается количество переданных цельных одноадресных пакетов.
Multicast	В этом поле отображается количество переданных цельных многоадресных пакетов.
Broadcast	В этом поле отображается количество переданных цельных широковещательных пакетов.
Pause	В этом поле отображается количество переданных пакетов 802.3x типа Pause.
Rx Packet В следующих полях отображается подробная информация о принятых пакетах.	
Unicast	В этом поле отображается количество принятых цельных одноадресных пакетов.
Multicast	В этом поле отображается количество принятых цельных многоадресных пакетов.
Broadcast	В этом поле отображается количество принятых цельных широковещательных пакетов.
Pause	В этом поле отображается количество принятых пакетов 802.3x типа Pause.
TX Collision В следующих полях отображается информация о коллизиях в процессе передачи.	
Single	Количество успешно переданных пакетов, передача которых была запрещена в точности одиночной коллизией.
Multiple	Количество успешно переданных пакетов, передача которых была запрещена несколькими коллизиями.
Excessive	Количество пакетов, передача которых оказалась невозможна из-за избыточного количества коллизий. Под избыточным количеством коллизий понимается максимальное количество коллизий, после которого сбрасывается счетчик попыток повторной передачи.
Late	Количество зафиксированных с опозданием коллизий, то есть коллизий, обнаруженных после передачи как минимум 512 бит пакета.
Error Packet	В следующих полях отображается подробная информация о принятых пакетах с ошибками.
RX CRC	В этом поле отображается количество пакетов, принятых с ошибкой (ошибками) циклического избыточного кода CRC.
Runt	В этом поле отображается количество принятых пакетов, оказавшихся слишком короткими (менее 64 октетов), включая пакеты с ошибками CRC.
Distribution	
64	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет 64 октета.
65-127	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 65 до 127 октетов.
128-255	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 128 до 255 октетов.
256-511	В этом поле отображается количество принятых пакетов (включая ошибочные), длина которых составляет от 256 до 511 октетов.

Таблица 8 Экран Status: Port Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
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 принятых пакетов (включая ошибочные), длина которых составляет от 1519 октетов до максимального размера кадра. Максимальный размер кадра зависит от модели коммутатора.

Основные настройки

8.1 Обзор

В данной главе описаны настройки экранов **System Info, General Setup**, **Switch Setup**, **IP Setup**, **Port Setup**, **Interface Setup** и **IPv6**.

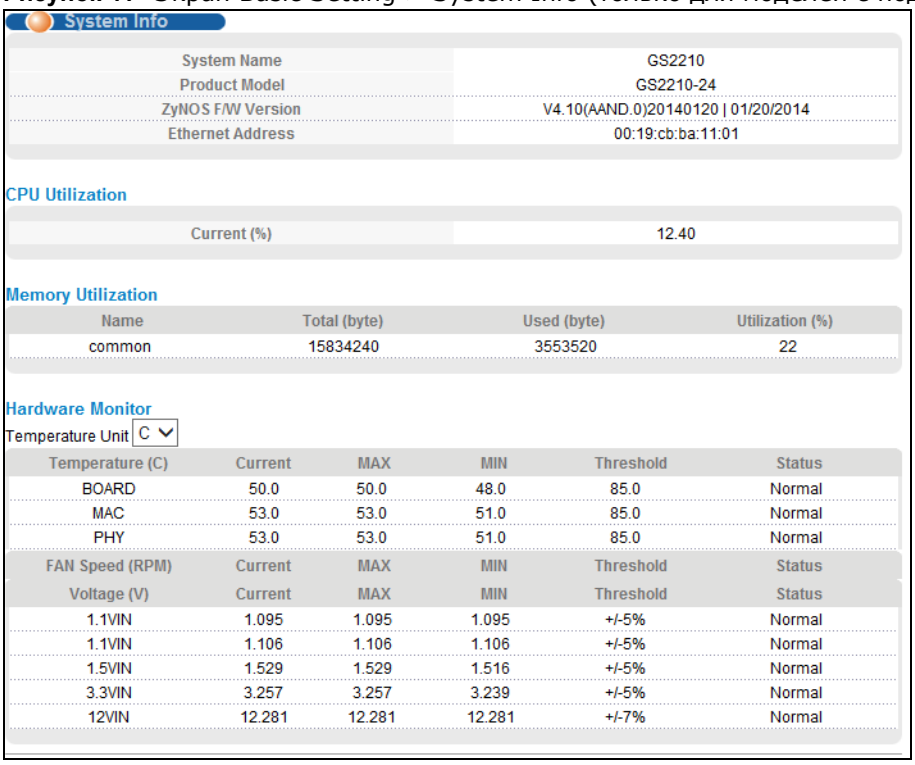
8.1.1 О чем рассказывается в этой главе

- С помощью экрана **System Info** (разд. 8.8 на стр. 72) можно узнать версию встроенного программного обеспечения.
- С помощью экрана **General Setup** (разд. 8.3 на стр. 63) можно настроить общесистемные параметры, например, указать имя системы или задать время.
- С помощью экрана **Switch Setup** (разд. 8.5 на стр. 66) можно выбрать тип сети VLAN, установить таймеры GARP и назначить приоритеты очередям.
- С помощью экрана **IP Setup** (разд. 8.6.1 на стр. 68) можно задать IP-адрес коммутатора, указать основной шлюз, основной сервер доменных имен и идентификатор управляющей сети VLAN.
- С помощью экрана **Port Setup** (разд. 8.7 на стр. 70) можно задать параметры портов коммутатора.
- С помощью экранов **Interface Setup** (разд. 8.8 на стр. 72) можно выбрать тип интерфейса для коммутатора и задать параметры его идентификатора.
- С помощью экранов **IPv6** (разд. 8.8 на стр. 72) можно просмотреть сведения о статусе протокола IPv6 и его настройках.

8.2 Информация о системе

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting** > **System Info**. Этот экран отображает версию встроенного программного обеспечения.

Рисунок 41 Экран Basic Setting > System Info (только для моделей с поддержкой PoE)



Поля экрана описаны в следующей таблице.

Таблица 9 Экран Basic Setting > System Info

ПОЛЕ	ОПИСАНИЕ
System Name	В этом поле отображается имя-описание коммутатора, с помощью которого его можно идентифицировать.
Product Model	Это поле показывает модель коммутатора. Эту информацию следует использовать при поиске свежей версии встроенного программного обеспечения или других сведений, касающихся поддержки, на веб-сайте.
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.
CPU Utilization	Утилизация процессорных ресурсов представляет собой количественную оценку загруженности системы. Поле **Current (%)** показывает текущую процентную долю утилизации процессорных ресурсов.
Memory Utilization	Поле Memory Utilization показывает доступный и задействованный объемы динамической оперативной памяти (DRAM). Кроме того, оно показывает текущую процентную долю утилизации оперативной памяти.
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	**BOARD**, **MAC** и **PHY** указывают на размещение температурных датчиков 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.

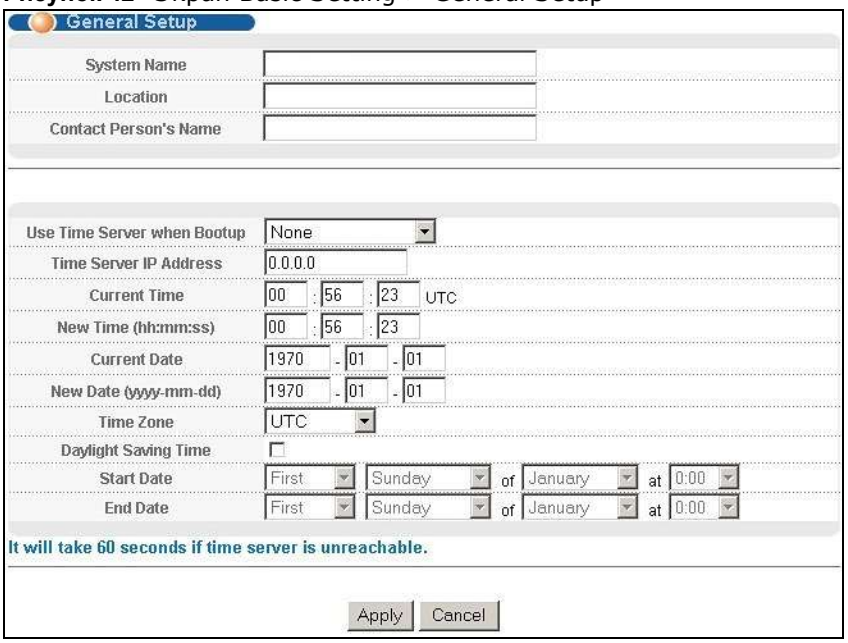
Таблица 9 Экран Basic Setting > System Info (продолжение)

ПОЛЕ	ОПИСАНИЕ
Threshold	В этом поле отображается верхний лимит температуры для данного датчика.
Status	Если температура не превышает порогового значения, в этом поле указывается **Normal**, в противном случае – **Error**.
Fan Speed (RPM)	Для соблюдения надлежащего теплового режима устройства огромное значение имеет правильная работа вентиляторов (наряду с хорошо вентилируемым, охлаждаемым помещением). В каждом из вентиляторов имеется датчик, который обнаруживает и сообщает о понижении скорости работы вентилятора ниже указанного порогового значения.
Current	В этом поле отображается текущая скорость вентилятора в оборотах в минуту (RPM).
MAX	В этом поле отображается максимальная измеренная скорость вентилятора в оборотах в минуту (RPM).
MIN	В этом поле отображается минимальная измеренная скорость вентилятора в оборотах в минуту (RPM). Если скорость слишком низкая и не поддается измерению (меньше 2000 об/мин), в этом поле указывается «<41».
Threshold	В этом поле отображается минимальная допустимая скорость работы вентилятора.
Status	Значение **Normal** указывает на то, что скорость вращения вентилятора выше минимальной. Значение **Error** указывает на то, что скорость вращения вентилятора ниже минимальной.
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	Значение **Normal** указывает на то, что напряжение в данной точке находится в пределах допустимого рабочего диапазона; в противном случае в этом поле отображается значение **Error**.

8.3 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** > **General Setup**.

Рисунок 42 Экран Basic Setting > General Setup



Поля экрана описаны в следующей таблице.

Таблица 10 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 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)** схож с форматом **Time (RFC-868)**. По умолчанию установлено значение **None**. Время вводится вручную. Каждый раз при включении коммутатора время и дата сбрасываются на 1970-1-1 0:0:0.
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.

Таблица 10 Экран Basic Setting > General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Current Date	В этом поле отображается дата, соответствующая моменту открытия этого меню.
New Date (yyyy-mm-dd)	Введите новую дату в формате «год, месяц, день». После нажатия на **Apply** в поле **Current Date** появится новая дата.
Time Zone	Выберите в ниспадающем списке разницу во времени между поясом UTC (всеобщее скоординированное время, ранее известное как GMT или время по Гринвичу) и вашим часовым поясом.
Daylight Saving Time	Период летнего времени – период с поздней весны до начала осени, когда во многих странах принято переводить часы на один час вперед в целях более рационального использования светлого времени суток по вечерам. При использовании летнего времени необходимо установить данный переключатель.
Start Date	Укажите день и час, когда начинается действие летнего времени (в случае выбора переключателя **Daylight Saving Time**). Время отображается в 24-часовом формате. Ниже приводится несколько примеров: Действие летнего времени на большей части 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 вступает в силу одномоментно (1 A.M. GMT или UTC). 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 прекращает действовать одномоментно (1 A.M. GMT или UTC). 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.

8.4 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.

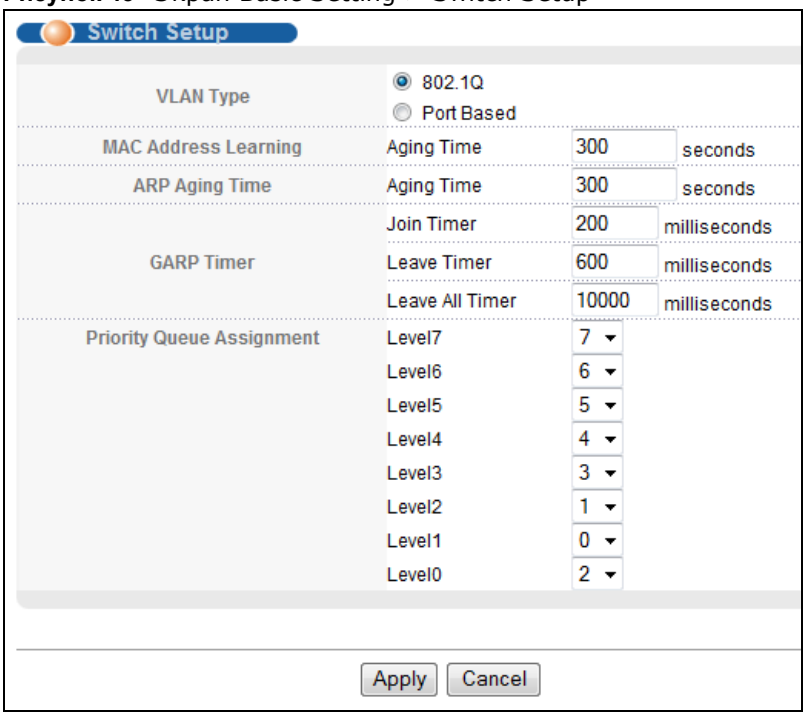
Примечание: Механизм поддержки виртуальных локальных сетей VLAN работает только в одном направлении; им контролируется только исходящий трафик.

Информацию о виртуальных локальных сетях на основе портов и на основе тегов 802.1Q можно найти в гл. 9 на стр. 86.

8.5 Экран Switch Setup

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Basic Setting** > **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**. Более подробную информацию о сетях VLAN можно найти в гл. 9 на стр. 86.

Рисунок 43 Экран Basic Setting > Switch Setup



Поля экрана описаны в следующей таблице.

Таблица 11 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. 9 на стр. 86.
MAC Address Learning: Функция получения (запоминания) MAC-адресов снижает объем исходящего широковещательного трафика.	
Aging Time	Устанавливает продолжительность временного интервала в секундах (от 30 до 65536); продолжительность интервала по умолчанию – 300 секунд.
ARP Aging Time	
Aging Time	Устанавливает продолжительность временного интервала в секундах (от 30 до 65536); продолжительность интервала по умолчанию – 300 секунд.
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.
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.

Таблица 11 Экран Basic Setting > Switch Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Priority Queue Assignment Стандарт IEEE 802.1p различает до 8 отдельных типов трафика путем добавления в кадр MAC-уровня тега, содержащего биты определения класса обслуживания. Кадры без явного тега приоритета получают на входящем порту приоритет по умолчанию. Следующие поля используются для определения соответствия между уровнями приоритетов и физическими очередями. У коммутатора имеется 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 сбросить все поля.

8.6 Настройки протокола IP

Экран **IP Setup** используется для настройки IP-адреса коммутатора, шлюза по умолчанию, сервера DNS по умолчанию и идентификатора VLAN управления. Адрес шлюза по умолчанию представляет собой IP-адрес следующего перехода для исходящего трафика.

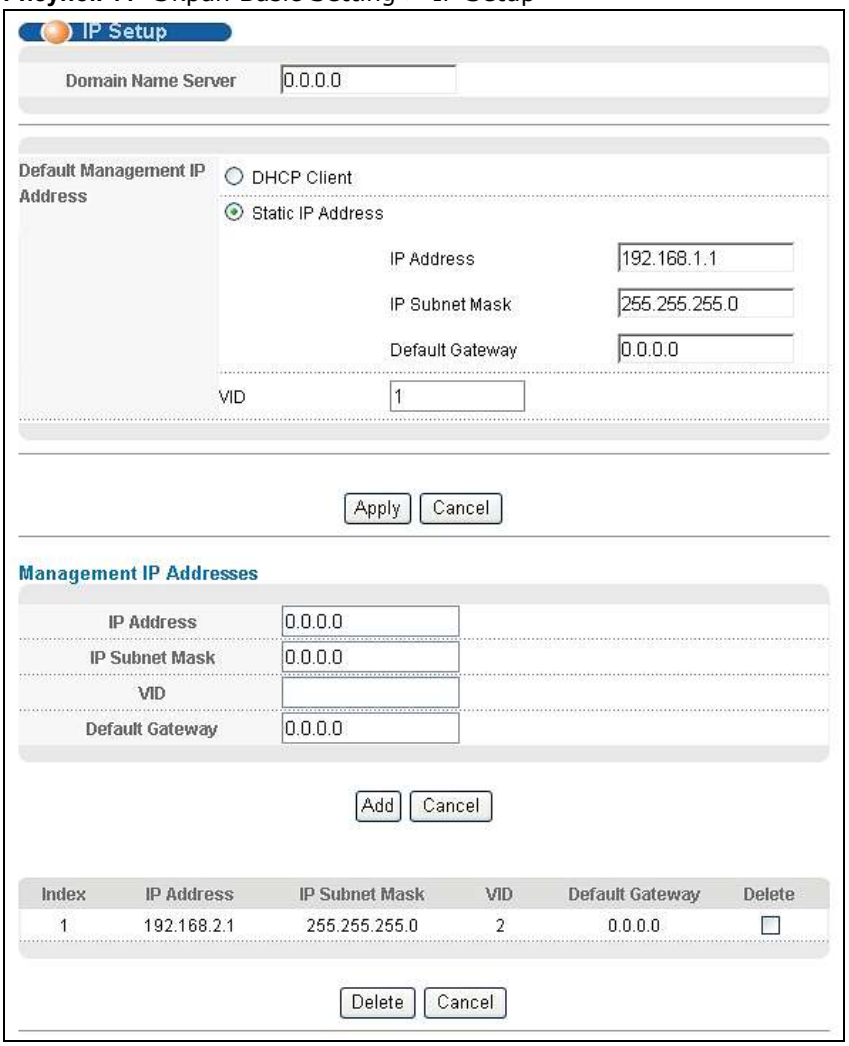
8.6.1 IP-адреса управления

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.

В общей сложности для получения доступа и управления коммутатором с портов, принадлежащих определенным сетям VLAN, можно настроить до 64 IP-адресов.

Примечание: Предварительно необходимо настроить сети VLAN.

Рисунок 44 Экран Basic Setting > IP Setup



Поля экрана описаны в следующей таблице.

Таблица 12 Экран Basic Setting > IP Setup

ПОЛЕ	ОПИСАНИЕ
Domain Name Server	Сервер DNS (системы доменных имен) определяет соответствие между доменным именем и IP-адресом, и наоборот. Введите IP-адрес сервера DNS, чтобы вместо IP-адресов можно было использовать доменные имена.
Default Management IP Address	
DHCP Client	Выберите данную опцию, если коммутатор должен автоматически получать IP-адрес, маску подсети, IP-адрес шлюза по умолчанию и IP-адрес сервера DNS через сервер DHCP.
Static IP Address	Выберите данную опцию, если сервер DHCP не используется или коммутатору необходимо присвоить статический IP-адрес. В этом случае потребуется заполнить следующие поля.

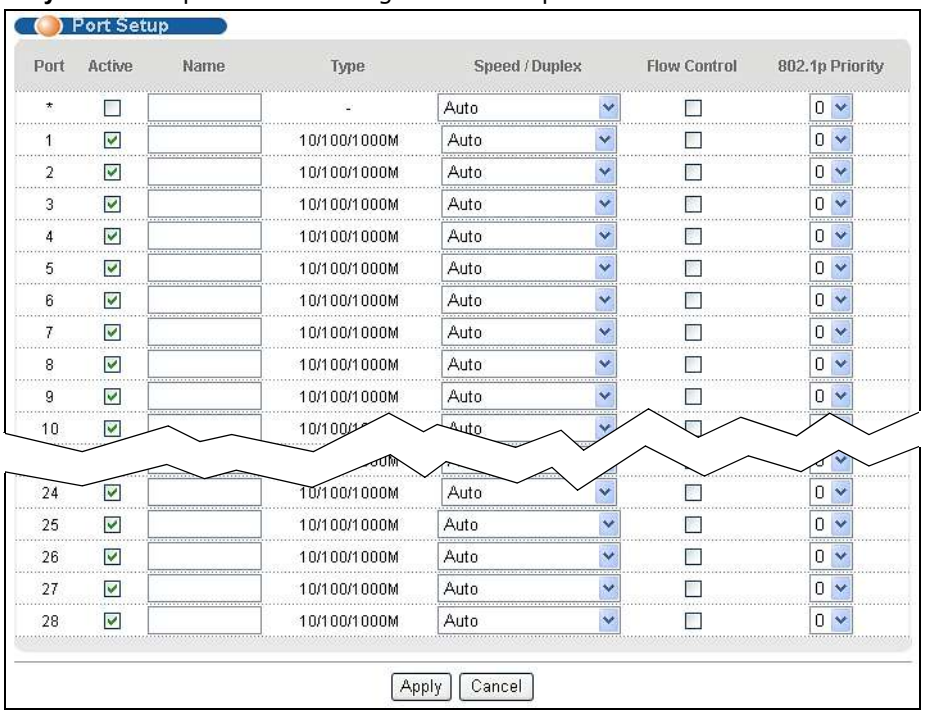
Таблица 12 Экран Basic Setting > IP Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес коммутатора в виде десятичных чисел, разделенных точками, например 192.168.1.1.
IP Subnet Mask	Введите IP-маску подсети коммутатора в виде десятичных чисел, разделенных точками, например 255.255.255.0.
Default Gateway	Введите IP-адрес исходящего шлюза по умолчанию в виде десятичных чисел, разделенных точками, например 192.168.1.254.
VID	Введите идентификационный номер сети VLAN, связанной с IP-адресом коммутатора. Этот идентификатор VLAN ID соответствует CPU и используется только для управления. По умолчанию используется значение «1». По умолчанию все порты являются членами данной «VLAN управления», благодаря чему устройством можно управлять через любой порт. Если порт не входит в состав данной VLAN, то пользователи на этому порту не смогут получить доступа к устройству. Чтобы получить доступ к коммутатору, к нему необходимо подключиться через порт, являющийся членом VLAN управления.
Management IP Addresses В общей сложности для получения доступа и управления коммутатором с портов, принадлежащих определенным сетям VLAN, можно настроить до 64 IP-адресов. Предварительно необходимо настроить сети VLAN.	
IP Address	Введите IP-адрес для управления коммутатором с членов сети VLAN, указанной в поле **VID** ниже.
IP Subnet Mask	Введите маску подсети в виде десятичных чисел, разделенных точками.
VID	Введите идентификационный номер группы VLAN.
Default Gateway	Введите IP-адрес шлюза по умолчанию в виде десятичных чисел, разделенных точками.
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.
Index	В этом поле отображается порядковый номер правила. Нажмите на этот номер, чтобы отредактировать правило.
IP Address	В этом поле отображается IP-адрес.
IP Subnet Mask	В этом поле отображается маска подсети.
VID	В этом поле отображается идентификационный номер группы VLAN.
Default Gateway	В этом поле отображается IP-адрес шлюза по умолчанию.
Delete	В столбце **Delete** установите переключатели IP-адресов управления, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей в столбце **Delete**.

8.7 Настройки портов

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

Рисунок 45 Экран Basic Setting > Port Setup



Поля экрана описаны в следующей таблице.

Таблица 13 Экран Basic Setting > Port Setup

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

Таблица 13 Экран Basic Setting > Port Setup (продолжение)

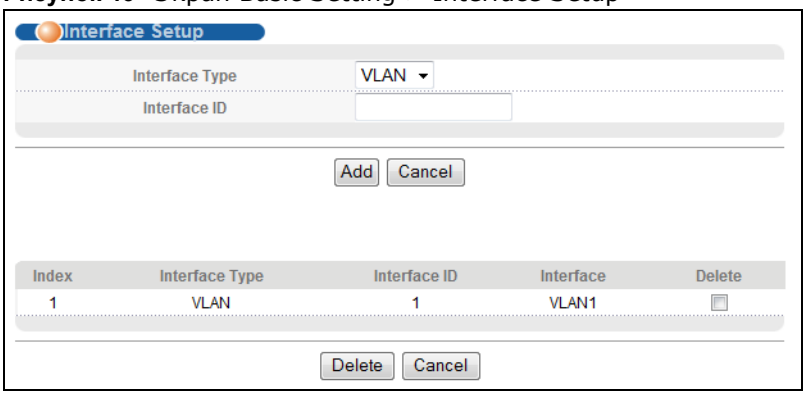
ПОЛЕ	ОПИСАНИЕ
Speed/Duplex	Выберите скорость и режим дуплекса для Ethernet-соединения на этом порту. Возможные значения: **Auto** (Автосогласование), **10M/Half Duplex** (10 Мбит/с, полудуплекс), **10M/Full Duplex** (10 Мбит/с, дуплекс), **100M/Half Duplex** (100 Мбит/с, полудуплекс), **100M/Full Duplex** (100 Мбит/с, дуплекс) и **1000M/Full Duplex** (1000 Мбит/с, дуплекс) (только для гигабитных соединений). 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 IEEE802.3x в дуплексном режиме и управление потоком методом обратного давления (противодавления) в полудуплексном режиме. Управление потоком по стандарту IEEE802.3x 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. 11 на стр. 67.
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.

8.8 Экран Interface Setup

Настройка адресов IPv6 осуществляется в индивидуальном порядке для каждого интерфейса. Интерфейсы могут поддерживать виртуальные интерфейсы (например, интерфейсы VLAN). На момент написания этого документа коммутатор поддерживает тип интерфейса VLAN для протокола IPv6.

Выберите с помощью этого экрана интерфейсы IPv6, для которых можно указать адреса IPv6, по которым будет осуществляться доступ и управление коммутатором. Выберите в навигационной панели **Basic Setting > Interface Setup**, чтобы открыть экран настроек.

Рисунок 46 Экран Basic Setting > Interface Setup



Поля экрана описаны в следующей таблице.

Таблица 14 Экран Basic Setting > Interface Setup

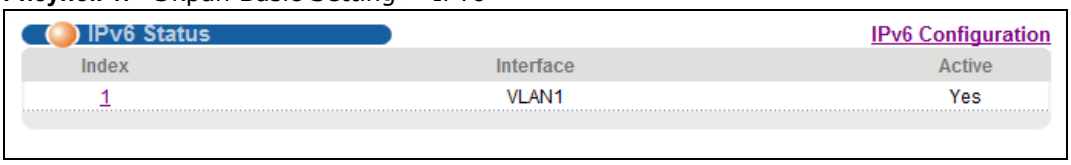
ПОЛЕ	ОПИСАНИЕ
Interface Type	Выберите тип интерфейса IPv6, параметры которого будут настраиваться. На момент написания этого документа коммутатор поддерживает тип интерфейса VLAN для протокола IPv6.
Interface ID	Выберите число, которое будет уникальным образом идентифицировать данный интерфейс (в диапазоне от 1 до 4094). Для нормальной работы протокола IPv6 необходимо создать статическую сеть VLAN с тем же идентификатором, который был указан на экранах **Advanced Application > VLAN**.
Add	Нажатие на этот значок позволяет создать новую запись. Это действие позволяет сохранить изменения настроек 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.
Interface Type	Это поле показывает тип интерфейса.
Interface ID	Это поле показывает идентификатор интерфейса.
Interface	Это поле показывает имя-описание интерфейса, которое коммутатор генерирует автоматически. Оно представляет собой сочетание типа интерфейса и его идентификатора.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

8.9 Экран IPv6

С помощью этого экрана можно просмотреть состояние интерфейсов IPv6 и указать адреса IPv6 для управления коммутатором.

Выберите в навигационной панели **Basic Setting** > **IPv6**, чтобы открыть экран состояния IPv6, изображенный на рисунке ниже.

Рисунок 47 Экран Basic Setting > IPv6



Поля экрана описаны в следующей таблице.

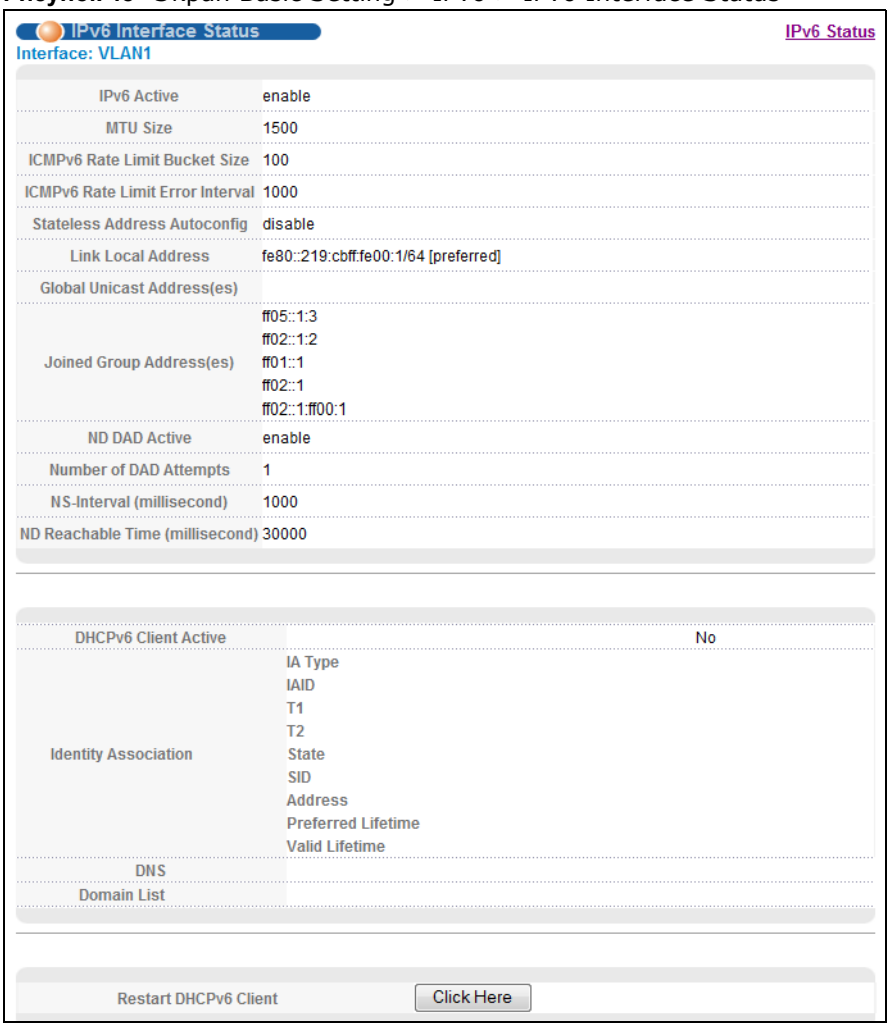
Таблица 15 Экран Basic Setting > IPv6

ПОЛЕ	ОПИСАНИЕ
Index	Это поле показывает порядковый номер интерфейса IPv6. Щелчок на порядковом номере позволяет отобразить более подробную информацию об интерфейсе.
Interface	Это поле отображает имя созданного интерфейса IPv6.
Active	Это поле указывает на то, активирован ли данный интерфейс IPv6.
Index	Это поле показывает порядковый номер интерфейса IPv6. Щелчок на порядковом номере позволяет отобразить более подробную информацию об интерфейсе.

8.9.1 Экран IPv6 Interface Status

С помощью этого экрана можно узнать статус определенного интерфейса IPv6 и просмотреть детальную информацию о нем. Щелкните на порядковом номере интерфейса на экране **Basic Setting** > **IPv6**. Откроется следующий экран.

Рисунок 48 Экран Basic Setting > IPv6 > IPv6 Interface Status



Поля экрана описаны в следующей таблице.

Таблица 16 Экран Basic Setting > IPv6 > IPv6 Interface Status

ПОЛЕ	ОПИСАНИЕ
IPv6 Active	Это поле указывает на то, активирован ли данный интерфейс IPv6.
MTU Size	Это поле показывает размер блока MTU (Maximum Transmission Unit) для пакетов IPv6 на данном интерфейсе.
ICMPv6 Rate Limit Bucket Size	Это поле показывает максимально допустимое количество сообщений об ошибках ICMPv6, передаваемых за указанный временной интервал. При достижении указанного порогового значения происходит подавление всех последующих сообщений об ошибках.
ICMPv6 Rate Limit Error Interval	Это поле показывает период времени в миллисекундах, на протяжении которого осуществляется передача сообщений об ошибках ICMPv6 до тех пор, пока не будет достигнуто пороговое значение переполнения. 0 означает отсутствие ограничений.
Stateless Address Autoconfig	Это поле указывает на то, может ли интерфейс коммутатора автоматически генерировать адрес типа link-local посредством механизма автоматической настройки без сохранения состояния.
Link Local Address	Это поле отображает IP-адрес link local коммутатора и префикс, сгенерированный интерфейсом. Кроме того, оно указывает на то, является ли этот IP-адрес предпочтительным, то есть является ли он допустимым, и можно ли его использовать в качестве адреса отправителя или получателя.

Таблица 16 Экран Basic Setting > IPv6 > IPv6 Interface Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
Global Unicast Address(es)	Это поле показывает глобальный одноадресный адрес коммутатора, используемый для идентификации данного интерфейса.
Joined Group Address(es)	Это поле показывает адреса многоадресной рассылки IPv6 групп, с которыми соединяется интерфейс коммутатора.
ND DAD Active	Это поле указывает на то, включена ли на данном интерфейсе функция Neighbor Discovery (ND) Duplicate Address Detection (DAD) [Выявление дублированных адресов при обнаружении соседей].
Number of DAD Attempts	Это поле показывает количество последовательных сообщений типа «Запрос доступных соседей», рассылаемых коммутатором через данный интерфейс.
NS-Interval (millisecond)	Это поле показывает временной интервал в миллисекундах между сообщениями типа «Запрос доступных соседей».
ND Reachable Time (millisecond)	Это поле показывает, на протяжении какого времени, измеряемого в миллисекундах, соседнее устройство считается доступным для данного интерфейса.
DHCPv6 Client Active	Это поле указывает на то, выступает ли коммутатор в качестве клиента DHCPv6, получающего адрес IPv6 от сервера DHCPv6.
Identity Association	Ассоциация идентификаторов (Identity Association, IA) – это коллекция адресов, назначенных DHCP-клиенту, посредством которой сервер и клиент могут управлять группой связанных IP-адресов. Каждая ассоциация IA должна быть ассоциирована только с одним интерфейсом.
IA Type	Тип IA – это тип адреса в IA. Каждая ассоциация IA хранит адреса одного типа. **IA_NA** представляет собой ассоциацию идентификаторов для постоянных адресов, а **IA_TA** – для временных адресов.
IAID	Каждая ассоциация IA включает в себя уникальный идентификатор IAID и связанную с ним информацию протокола IP.
T1	Это поле отображает значение таймера DHCPv6 T1. По истечении времени таймера T1 коммутатор посылает сообщение Renew серверу DHCPv6. Опция IA_NA содержит поля T1 и T2, а опция IA_TA – нет. Сервер DHCPv6 использует поля T1 и T2 для управления временем обращения клиента к серверу с целью заблаговременного продления сроков жизни любых адресов, входящих в ассоциацию IA_NA.
T2	Это поле отображает значение таймера DHCPv6 T2. Если по истечении времени таймера T2 сервер не отвечает, коммутатор посылает сообщение Rebind всем доступным серверам.
State	Это поле показывает состояние TA. Возможные варианты **Active**, если коммутатор получает адреса от сервера DHCpv6, и создается TA. **Renew**, если истекает срок жизни адреса TA, и коммутатор посылает сообщение Renew. **Rebind**, если коммутатор не получает отклика от исходного сервера DHCPv6 и посылает сообщение Rebind другому серверу DHCPv6.
SID	Это поле показывает уникальный идентификатор сервера DHCPv6.
Address	Это поле отображает глобальный адрес коммутатора, назначенный ему сервером DHCPv6.
Preferred Lifetime	Это поле показывает, в течение какого времени, измеряемого в секундах, этот глобальный адрес остается предпочтительным.
Valid Lifetime	Это поле показывает, в течение какого времени, измеряемого в секундах, этот глобальный адрес остается действующим.
DNS	Это поле отображает адрес DNS-сервера, назначенный сервером DHCPv6.

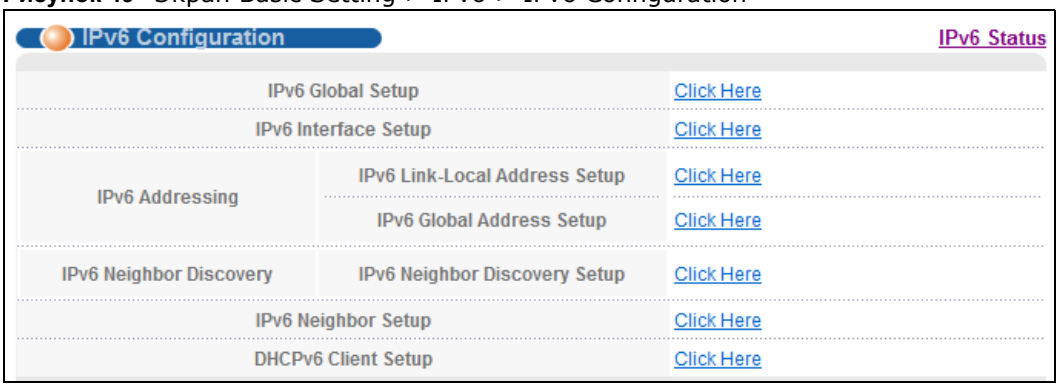
Таблица 16 Экран Basic Setting > IPv6 > IPv6 Interface Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
Domain List	Это поле отображает адресную запись, когда коммутатор отправляет запрос о разрешении доменных имен на DNS-сервер.
Restart DHCPv6 Client	Перейдите по ссылке **Click Here**, чтобы отправить новый DHCP-сервер на сервер DHCPv6 и обновить адрес IPv6 и DNS-информацию для данного интерфейса.

8.9.2 Экран IPv6 Configuration

С помощью этого экрана можно настроить параметры IPv6 коммутатора. Перейдите по ссылке **IPv6 Configuration** на экране **Basic Setting** > **IPv6**. Откроется следующий экран.

Рисунок 49 Экран Basic Setting > IPv6 > IPv6 Configuration



Поля экрана описаны в следующей таблице.

Таблица 17 Экран Basic Setting > IPv6 > IPv6 Configuration

ПОЛЕ	ОПИСАНИЕ
IPv6 Global Setup	Щелкните по этой ссылке, чтобы перейти на экран, с помощью которого можно изменить глобальные настройки IPv6 на коммутаторе.
IPv6 Interface Setup	Щелкните по этой ссылке, чтобы перейти на экран, с помощью которого можно активировать интерфейс IPv6 на коммутаторе.
IPv6 Addressing	
IPv6 Link-Local Address Setup	Щелкните по этой ссылке, чтобы перейти на экран, с помощью которого можно задать адрес IPv6 link-local для определенного интерфейса.
IPv6 Global Address Setup	Щелкните по этой ссылке, чтобы перейти на экран, с помощью которого можно задать глобальный адрес IPv6 для определенного интерфейса.
IPv6 Neighbor Discovery	
IPv6 Neighbor Discovery Setup	Щелкните по этой ссылке, чтобы перейти на экран, с помощью которого можно настроить параметры обнаружения соседних устройств IPv6.
IPv6 Neighbor Setup	Щелкните по этой ссылке, чтобы перейти на экран, с помощью которого можно создать статическую запись IPv6 о соседнем устройстве в таблице соседних устройств IPv6 коммутатора.
DHCPv6 Client Setup	Щелкните по этой ссылке, чтобы перейти на экран, с помощью которого можно настроить параметры DHCP коммутатор.

8.9.3 Экран IPv6 Global Setup

С помощью этого экрана можно настроить глобальные параметры IPv6. Перейдите по ссылке, расположенной рядом с надписью **IPv6 Global Setup** на экране **IPv6 Configuration**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 50 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

Поля экрана описаны в следующей таблице.

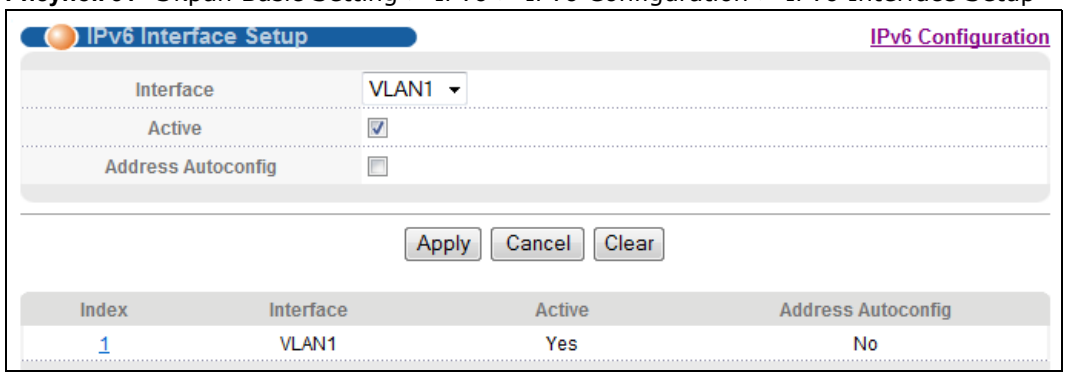
Таблица 18 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

ПОЛЕ	ОПИСАНИЕ
IPv6 Hop Limit	Укажите максимальное число переходов (в диапазоне от 1 до 255) в анонсах маршрутизатора. Значение этого поля определяет максимальное число переходов, которое может преодолеть пакет IPv6, прежде чем его отбросит маршрутизатор IPv6. Роль этого параметра аналогична роли поля TTL в протоколе IPv4.
ICMPv6 Rate Limit Bucket Size	Укажите максимальное количество сообщений об ошибках ICMPv6 (в диапазоне от 1 до 200), передача которых разрешена в заданном временном интервале. При достижении указанного порогового значения происходит подавление всех последующих сообщений об ошибках.
ICMPv6 Rate Limit Error Interval	Укажите период времени (в диапазоне от 0 до 2147483647 миллисекунд), в течение которого может осуществляться передача сообщений об ошибках ICMPv6 до достижения порогового значения переполнения. 0 означает отсутствие ограничений.
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 щелкнуть по ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы заново начать настройку на этом экране.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.

8.9.4 Экран IPv6 Interface Setup

С помощью этого экрана можно включить или отключить интерфейс IPv6 и активировать для него функцию автоматической настройки без сохранения состояния. Перейдите по ссылке, расположенной рядом с надписью **IPv6 Interface Setup** на экране **IPv6 Configuration**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 51 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup



Поля экрана описаны в следующей таблице.

Таблица 19 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

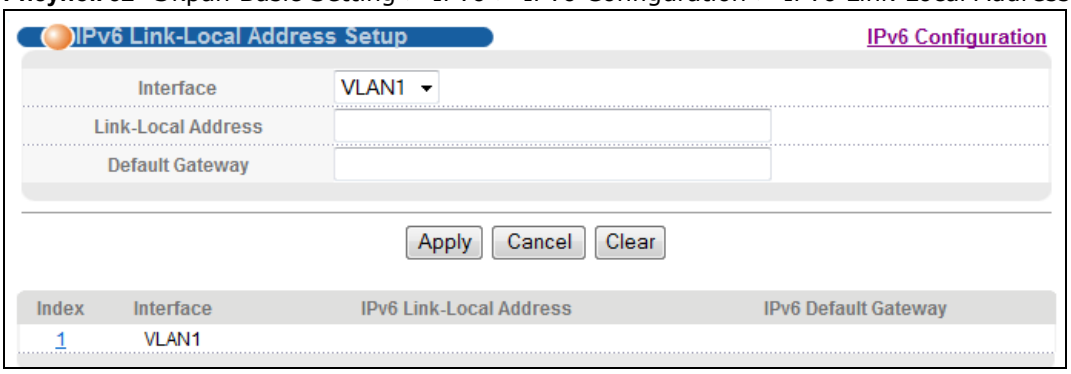
ПОЛЕ	ОПИСАНИЕ
Interface	Выберите интерфейс IPv6, параметры которого будут настраиваться.
Active	Выберите эту опцию, чтобы включить данный интерфейс.
Address Autoconfig	Выберите эту опцию, чтобы разрешить интерфейсу автоматически генерировать адрес link-local с использованием автонастройки без сохранения состояния.
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 щелкнуть по ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы заново начать настройку на этом экране.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это поле содержит порядковый номер интерфейса. Щелкните на порядковом номере, чтобы изменить настройки.
Interface	Это поле отображает имя созданного интерфейса IPv6.
Active	Это поле указывает на то, активирован ли данный интерфейс IPv6.
Address Autoconfig	Это поле указывает на то, включена ли для данного интерфейса функция автоматической настройки без сохранения состояния.

8.9.5 Экран IPv6 Link-Local Address Setup

Адрес link-local уникальным образом идентифицирует устройство в локальной сети. Он аналогичен «частному IP-адресу» протокола IPv4. Один и тот же адрес link-local может быть назначен двум и более интерфейсам одного устройства. Однонаправленный адрес link-local имеет предопределенный префикс fe80::/10.

С помощью этого экрана можно указать для данного интерфейса адрес link-local и основной шлюз. Перейдите по ссылке, расположенной рядом с надписью **IPv6 Link-Local Address Setup** на экране **IPv6 Configuration**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 52 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup



Поля экрана описаны в следующей таблице.

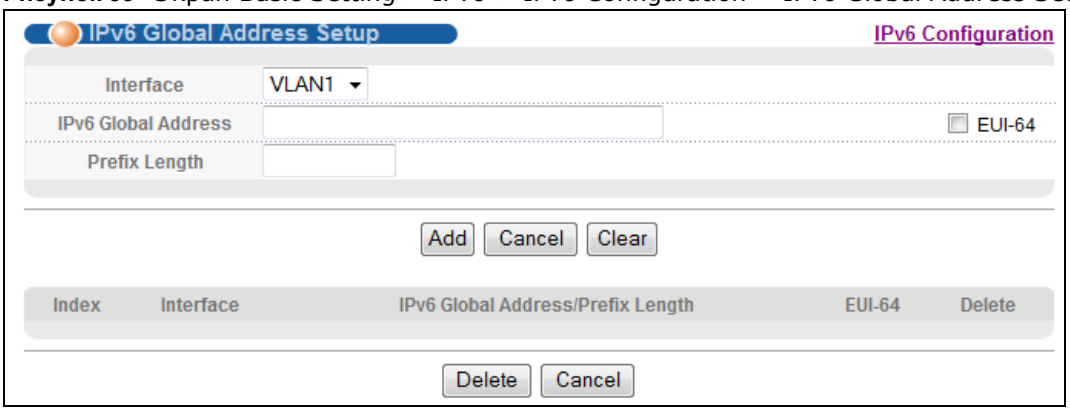
Таблица 20 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

ПОЛЕ	ОПИСАНИЕ
Interface	Выберите интерфейс IPv6, параметры которого будут настраиваться.
Link-Local Address	Укажите статический адрес link-local IPv6 для данного интерфейса.
Default Gateway	Укажите адрес IPv6 основного шлюза для данного интерфейса. Если шлюз не может найти маршрутную информацию для указанного в кадре адреса назначения, он пересылает пакет на основной шлюз.
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 щелкнуть по ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы заново начать настройку на этом экране.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это поле содержит порядковый номер интерфейса. Щелкните на порядковом номере, чтобы изменить настройки.
Interface	Это поле отображает имя созданного интерфейса IPv6.
IPv6 Link-Local Address	Это поле отображает статический адрес link-local IPv6 для данного интерфейса.
IPv6 Default Gateway	Это поле отображает адрес IPv6 основного шлюза для данного интерфейса.

8.9.6 Экран IPv6 Global Address Setup

С помощью этого экрана можно указать глобальный адрес IPv6 для данного интерфейса. Перейдите по ссылке, расположенной рядом с надписью **IPv6 Global Address Setup** на экране **IPv6 Configuration**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 53 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup



Поля экрана описаны в следующей таблице.

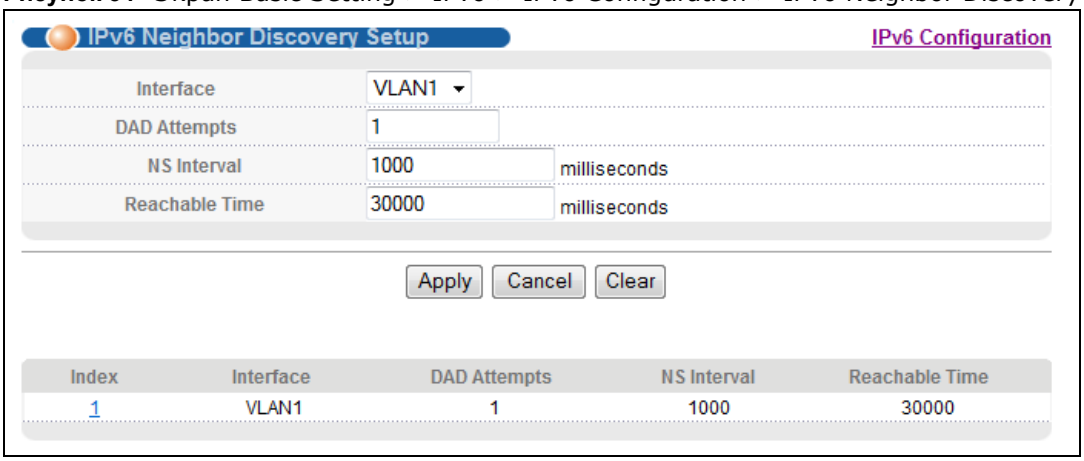
Таблица 21 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

ПОЛЕ	ОПИСАНИЕ
Interface	Выберите интерфейс IPv6, параметры которого будут настраиваться.
IPv6 Global Address	Укажите статический глобальный адрес IPv6 для данного интерфейса.
Prefix Length	Укажите префикс IPv6, который говорит о том, сколько наиболее значимых битов адреса, если отсчитывать слева, составляют адрес сети.
EUI-64	Выберите эту опцию, чтобы автоматически сгенерировать идентификатор интерфейса в формате EUI-64.
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 щелкнуть по ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы заново начать настройку на этом экране.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это поле содержит порядковый номер интерфейса. Щелкните на порядковом номере, чтобы изменить настройки.
Interface	Это поле отображает имя созданного интерфейса IPv6.
IPv6 Global Address/Prefix Length	Это поле показывает глобальный адрес IPv6 и длину префикса для данного интерфейса.
EUI-64	Это поле указывает на то, был ли идентификатор интерфейса глобального адреса сгенерирован с использованием формата EUI-64.
Delete	Пометьте записи, которые нужно удалить, в столбце **Delete** и нажмите кнопку **Delete**, чтобы удалить выбранные записи из сводной таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

8.9.7 Экран IPv6 Neighbor Discovery Setup

С помощью этого экрана можно настроить параметры обнаружения соседних устройств для каждого интерфейса. Перейдите по ссылке, расположенной рядом с надписью **IPv6 Neighbor Discovery Setup** на экране **IPv6 Configuration**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 54 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup



Поля экрана описаны в следующей таблице.

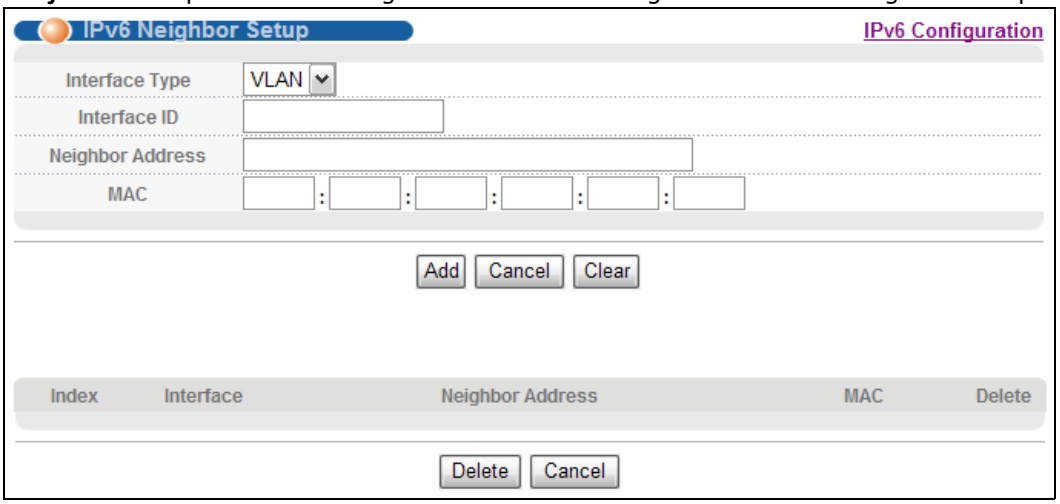
Таблица 22 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

ПОЛЕ	ОПИСАНИЕ
Interface	Выберите интерфейс IPv6, параметры которого будут настраиваться.
DAD Attempts	коммутатор использует механизм DAD (Duplicate Address Detection, выявление дублей адресов) в сочетании с сообщениями типа «Запрос доступных соседей» и сообщениями-анонсами, чтобы проверить, не занят ли уже определенный адрес IPv6 перед тем, как назначить его какому-либо интерфейсу, например, адрес link-local, созданный в процессе автоматической настройки адресов без сохранения состояния. Укажите количество последовательных сообщений типа «Запрос доступных соседей» (из диапазона от 0 до 600), которые коммутатор посылает для данного интерфейса. Укажите число 0, чтобы отключить функцию DAD.
NS Interval	Укажите временной интервал (из диапазона от 1000 до 3600000 миллисекунд) между сообщениями типа «Запрос доступных соседей» для данного интерфейса.
Reachable Time	Укажите, на протяжении какого времени (значение выбирается из диапазона от 1000 до 3600000 миллисекунд) соседнее устройство считается доступным для данного интерфейса.
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 щелкнуть по ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы заново начать настройку на этом экране.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это поле содержит порядковый номер интерфейса. Щелкните на порядковом номере, чтобы изменить настройки.
Interface	Это поле отображает имя созданного интерфейса IPv6.
DAD Attempts	Это поле показывает количество последовательных сообщений типа «Запрос доступных соседей», рассылаемых коммутатором через данный интерфейс.
NS Interval	Это поле показывает временной интервал в миллисекундах между сообщениями типа «Запрос доступных соседей».
Reachable Time	Это поле показывает, на протяжении какого времени, измеряемого в миллисекундах, соседнее устройство считается доступным для данного интерфейса.

8.9.8 Экран IPv6 Neighbor Setup

С помощью этого экрана можно создать статическую запись IPv6 о соседнем устройстве в таблице соседних устройств IPv6 коммутатора для хранения информации о соседнем устройстве на постоянной основе. Перейдите по ссылке, расположенной рядом с надписью **IPv6 Neighbor Setup** на экране **IPv6 Configuration**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 55 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup



Поля экрана описаны в следующей таблице.

Таблица 23 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

ПОЛЕ	ОПИСАНИЕ
Interface Type	Выберите тип интерфейса IPv6, параметры которого будут настраиваться. На момент написания этого документа коммутатор поддерживает тип интерфейса VLAN для протокола IPv6.
Interface ID	Выберите число, которое будет уникальным образом идентифицировать данный интерфейс (в диапазоне от 1 до 4094). Статическая запись IPv6 о соседнем устройстве отображается на экране **Management > Neighbor Table** только в том случае, если идентификатор данного интерфейса был создан с помощью экрана **Basic Setup > Interface Setup**. Для нормальной работы протокола IPv6 необходимо создать статическую сеть VLAN с тем же идентификатором, который был указан на экранах **Advanced Application > VLAN**.
Neighbor Address	Укажите адрес IPv6 соседнего устройства, доступного через данный интерфейс.
MAC	Укажите MAC-адрес соседнего устройства, доступного через данный интерфейс.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо щелкнуть по ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы заново начать настройку на этом экране.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это поле содержит порядковый номер интерфейса. Щелкните на порядковом номере, чтобы изменить настройки.

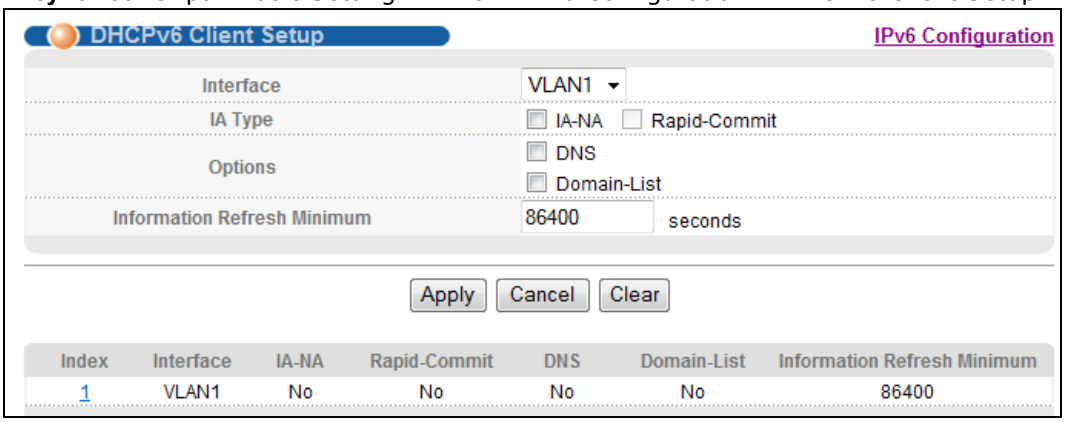
Таблица 23 Экран Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

ПОЛЕ	ОПИСАНИЕ
Interface	Это поле отображает имя созданного интерфейса IPv6.
Neighbor Address	Это поле отображает адрес IPv6 соседнего устройства, доступного через данный интерфейс
MAC	Это поле отображает MAC-адрес соседнего устройства, доступного через данный интерфейс
Delete	Пометьте записи, которые нужно удалить, в столбце **Delete** и нажмите кнопку **Delete**, чтобы удалить выбранные записи из сводной таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

8.9.9 Экран DHCPv6 Client Setup

С помощью этого экрана можно настроить параметры DHCP коммутатора для тех случаев, когда он выступает в качестве клиента DHCPv6.Перейдите по ссылке, расположенной рядом с надписью **IPv6 Neighbor Setup** на экране **IPv6 Configuration**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 56 Экран Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup



Поля экрана описаны в следующей таблице.

Таблица 24 Экран Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

ПОЛЕ	ОПИСАНИЕ
Interface	Выберите интерфейс IPv6, параметры которого будут настраиваться.
IA Type	Опция **IA-NA** означает, что коммутатор будет получать для данного интерфейса постоянный IP-адрес от сервера DHCPv6. Опция **Rapid-Commit** означает, что коммутатор будет посылать сообщения DHCPv6 Solicit с опцией Rapid Commit для получения информации от сервера DHCPv6 посредством быстрого обмена двумя сообщениями. В этом случае коммутатор отбрасывает все сообщения Reply, которые не содержат опции Rapid Commit. Соответственно, для нормальной работы указанного механизма сервер DHCPv6 должен также поддерживать опцию Rapid Commit.
Options	Опция **DNS** означает, что коммутатор будет получать адреса IPv6 сервера DNS, а опция **Domain-List** – что коммутатор будет получать список доменных имен от DHCP-сервера.
Information Refresh Minimum	Укажите периодичность (из диапазона от 600 до 4294967295 секунд), с которой коммутатор обменивается иными сведениями о конфигурации с сервером DHCPv6.

Таблица 24 Экран Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

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 щелкнуть по ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы заново начать настройку на этом экране.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это поле содержит порядковый номер интерфейса. Щелкните на порядковом номере, чтобы изменить настройки.
Interface	Это поле отображает имя созданного интерфейса IPv6.
IA-NA	Это поле указывает на то, получает ли коммутатор постоянный IP-адрес от сервера DHCPv6.
Rapid-Commit	Это поле указывает на то, получает ли коммутатор информацию от сервера DHCPv6 посредством быстрого обмена двумя сообщениями.
DNS	Это поле указывает на то, получает ли коммутатор адреса IPv6 сервера DNS от сервера DHCPv6.
Domain-List	Это поле указывает на то, получает ли коммутатор список доменных имен от DHCP-сервера.
Information Refresh Minimum	Это поле указывает на периодичность (в секундах), с которой коммутатор обменивается иными сведениями о конфигурации с сервером DHCPv6.

9

Виртуальные локальные сети (VLAN)

9.1 Обзор

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

9.1.1 О чем рассказывается в этой главе

- С помощью экрана **VLAN Status** (разд. 9.2 на стр. 90) можно выполнять просмотр и поиск среди всех групп VLAN.
- С помощью экрана **VLAN Detail** (разд. 9.2.1 на стр. 91) можно просмотреть подробную информацию о настройках портов и статусе определенной группы VLAN.
- С помощью экрана **Static VLAN** (разд. 9.4 на стр. 92) можно просмотреть и настроить параметры VLAN 802.1Q для коммутатора.
- С помощью экрана **VLAN Port Setting** (разд. 9.5 на стр. 94) можно настроить параметры статической сети VLAN (IEEE 802.1Q) для определенного порта.
- С помощью экрана **Subnet Based VLAN** (разд. 9.6 на стр. 96) можно создать логические сети VLAN для группировки трафика на основе указанного IP-адреса подсети источника.
- С помощью экрана **Protocol Based VLAN** (разд. 9.7 на стр. 99) можно создать логические сети VLAN для группировки трафика на основе указанного протокола.
- С помощью экрана **Port-Based VLAN** (разд. 9.8 на стр. 101) можно создать сети VLAN, в которых решение о пересылке пакета принимается на основе MAC-адреса назначения и связанного с ним порта.
- С помощью экрана **Voice VLAN** (разд. 9.8 на стр. 101) можно создать сети VLAN, которые позволяют группировать голосовой трафик с заданным приоритетом, и сконфигурировать требуемый порт коммутатора таким образом, чтобы он передавал голосовой трафик отдельно от трафика данных во избежание ухудшения качества передачи голоса.
- С помощью экрана **MAC-based VLAN** (разд. 9.10 на стр. 107) можно создать логические сети VLAN для группировки пакетов без тегов на основе MAC-адреса источника пакета. Это позволяет обойтись без перенастройки коммутатора при смене портов. Коммутатор будет осуществлять пересылку пакетов на основе MAC-адреса источника, указанного ранее.

9.1.2 Что необходимо знать

Ознакомьтесь с этим разделом, чтобы получить дополнительную информацию о сетях VLAN и о настройке экранов.

Сети VLAN с тегами 802.1Q IEEE

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

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

9.1.2.1 Автоматическая регистрация VLAN

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

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.

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.

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 25 Терминология сетей VLAN на основе IEEE 802.1Q

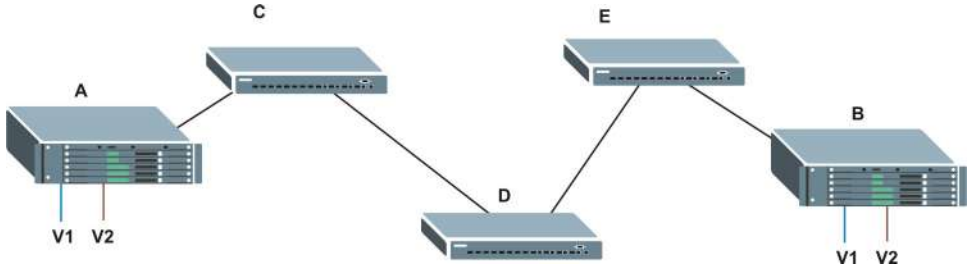
ПАРАМЕТРЫ VLAN	ТЕРМИН	ОПИСАНИЕ
Тип VLAN	Постоянная VLAN	Статическая виртуальная локальная сеть VLAN, созданная вручную.
	Динамическая VLAN	Сеть VLAN, настроенная в процессе регистрации/ дерегистрации протоколом GVRP.
Административный контроль над VLAN	Фиксированная регистрация	Порты с фиксированной регистрацией 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 (Tagged)	Порты, принадлежащие к данной VLAN, добавляют теги ко всем передаваемым исходящим кадрам.
	Без тегов (Untagged)	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.
	Допустимый тип кадра	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.

9.1.2.2 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, требуется создать группы VLAN 1 и 2 (V1 и V2) на устройствах A и B. В отсутствие **магистральных соединений VLAN** придется 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.

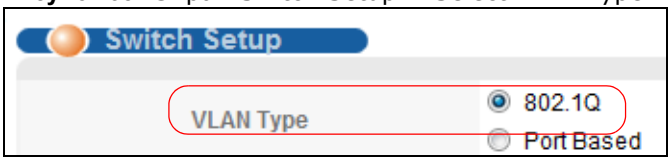
Рисунок 57 Магистральные порты VLAN



9.1.2.3 Выбор типа VLAN

Выберите тип VLAN на экране **Basic Setting** > **Switch Setup**.

Рисунок 58 Экран Switch Setup > Select VLAN Type



Статические VLAN

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

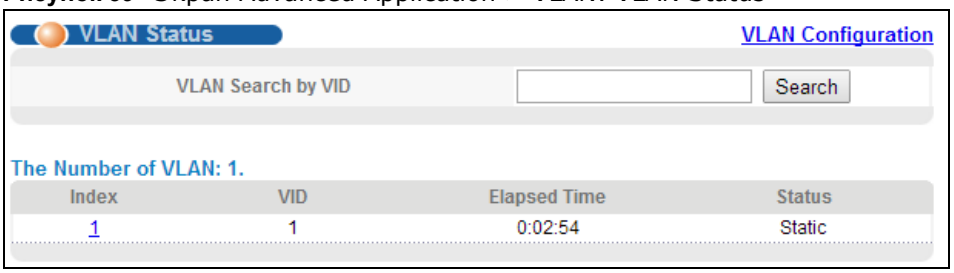
- отправлен в группу VLAN обычным образом, в зависимости от его тега VLAN.
- отправлен в группу независимо от того, имеется у него тег VLAN или нет.
- заблокирован от направления в группу VLAN независимо от его тега VLAN.

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

9.2 Экран VLAN Status

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

Рисунок 59 Экран Advanced Application > VLAN: VLAN Status



Поля экрана описаны в следующей таблице.

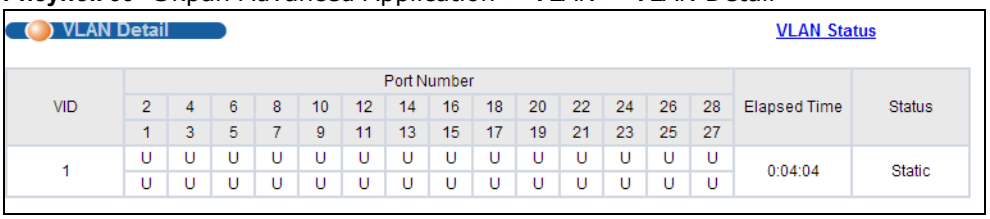
Таблица 26 Экран Advanced Application > VLAN: VLAN Status

ПОЛЕ	ОПИСАНИЕ
VLAN Search by VID	Введите идентификаторы существующих сетей VLAN (разделенные запятыми) и нажмите кнопку **Search**, чтобы отобразить в списке ниже только указанные сети VLAN. Оставьте это поле пустым и нажмите кнопку **Search**, чтобы вывести полный список сетей VLAN, сконфигурированных на коммутаторе.
The Number of VLAN	Количество виртуальных локальных сетей (VLAN), настроенных на коммутаторе.
The Number of Search Results	Это поле показывает количество сетей VLAN, соответствующих критериям поиска и содержащихся в списке ниже. Это поле доступно только в случае использования кнопки **Search** для поиска определенных сетей VLAN.
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	Это поле указывает на способ, при помощи которого данная сеть VLAN была создана на коммутаторе. **dynamic**: с использованием GVRP **static**: добавлена как постоянная запись **Voice**: создана вручную как сеть VLAN голосовой связи **MVR**: добавлена посредством регистрации VLAN многоадресной рассылки **MAC-based**: добавлена вручную в качестве VLAN на основе MAC-адреса
Change Pages	Нажмите **Previous** или **Next**, чтобы отобразить предыдущий/следующий экран, если информация о состоянии не помещается на одном экране.

9.2.1 Подробная информация о VLAN

На этом экране отображается подробные настройки портов и информация о состоянии группы VLAN. Чтобы отобразить экран подробной информации о сети VLAN, нажмите на порядковом номере сети на экране **VLAN Status**.

Рисунок 60 Экран Advanced Application > VLAN > VLAN Detail



Поля экрана описаны в следующей таблице.

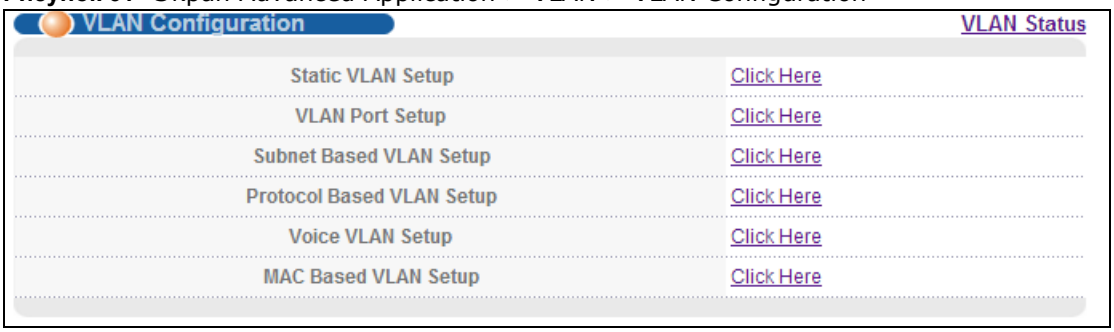
Таблица 27 Экран Advanced Application > VLAN > VLAN Detail

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	Это поле указывает на способ, при помощи которого данная сеть VLAN была создана на коммутаторе. **Dynamic**: с использованием GVRP **Static**: добавлена как постоянная запись **Voice**: создана вручную как сеть VLAN голосовой связи **MVR**: добавлена посредством регистрации VLAN многоадресной рассылки **MAC-based**: добавлена вручную в качестве VLAN на основе MAC-адреса

9.3 Экран VLAN Configuration

С помощью этого экрана можно просмотреть параметры VLAN IEEE 802.1Q для данного коммутатора. Чтобы открыть следующий экран, выберите в меню **Advanced Application** > **VLAN** > **VLAN Configuration**.

Рисунок 61 Экран Advanced Application > VLAN > VLAN Configuration



Поля экрана, приведенного выше, описаны в следующей таблице.

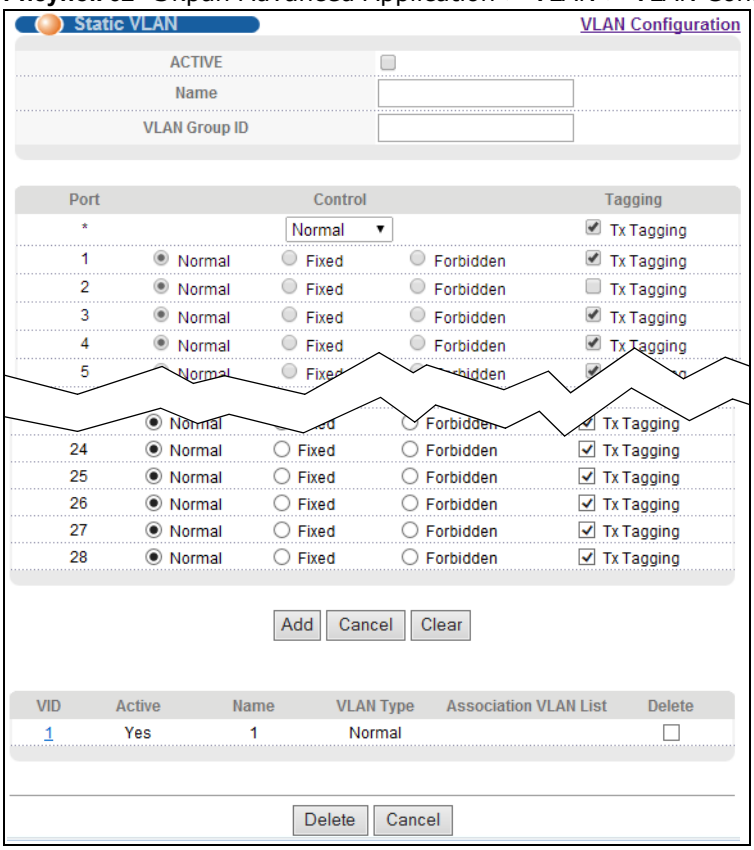
Таблица 28 Экран Advanced Application > VLAN > VLAN Configuration

ПОЛЕ	ОПИСАНИЕ
Static VLAN Setup	Перейдите по ссылке **Click Here**, чтобы создать статическую сеть VLAN для данного коммутатора.
VLAN Port Setup	Перейдите по ссылке **Click Here**, чтобы создать порт сети VLAN для данного коммутатора.
Subnet Based VLAN Setup	Перейдите по ссылке **Click Here**, чтобы создать подсеть на основе сети VLAN для данного коммутатора.
Protocol Based VLAN Setup	Перейдите по ссылке **Click Here**, чтобы создать сеть VLAN на основе протокола для данного коммутатора.
Voice VLAN Setup	Перейдите по ссылке **Click Here**, чтобы создать сеть VLAN голосовой связи для данного коммутатора.
MAC Based VLAN Setup	Перейдите по ссылке **Click Here**, чтобы создать сеть VLAN на основе MAC-адресов для данного коммутатора.

9.4 Настройка статической сети VLAN

С помощью этого экрана можно создать статическую сеть VLAN для данного коммутатора. Перейдите по ссылке **Static VLAN** на экране **VLAN Status**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 62 Экран Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup



Поля экрана описаны в следующей таблице.

Таблица 29 Экран Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

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. В этом поле можно использовать пробелы.
VLAN Group ID	Введите идентификатор VLAN для данной статической записи; допустимое значение находится в диапазоне от 1 до 4094.
Port	Номер порта – определяет настраиваемый порт.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Control	Выберите **Normal**, если порт должен присоединяться к данной группе VLAN динамически с использованием протокола GVRP. Данный параметр выбран по умолчанию. Выберите **Fixed**, если порт должен стать постоянным членом данной группы VLAN. Выберите **Forbidden**, чтобы запретить порту присоединяться к данной группе VLAN.

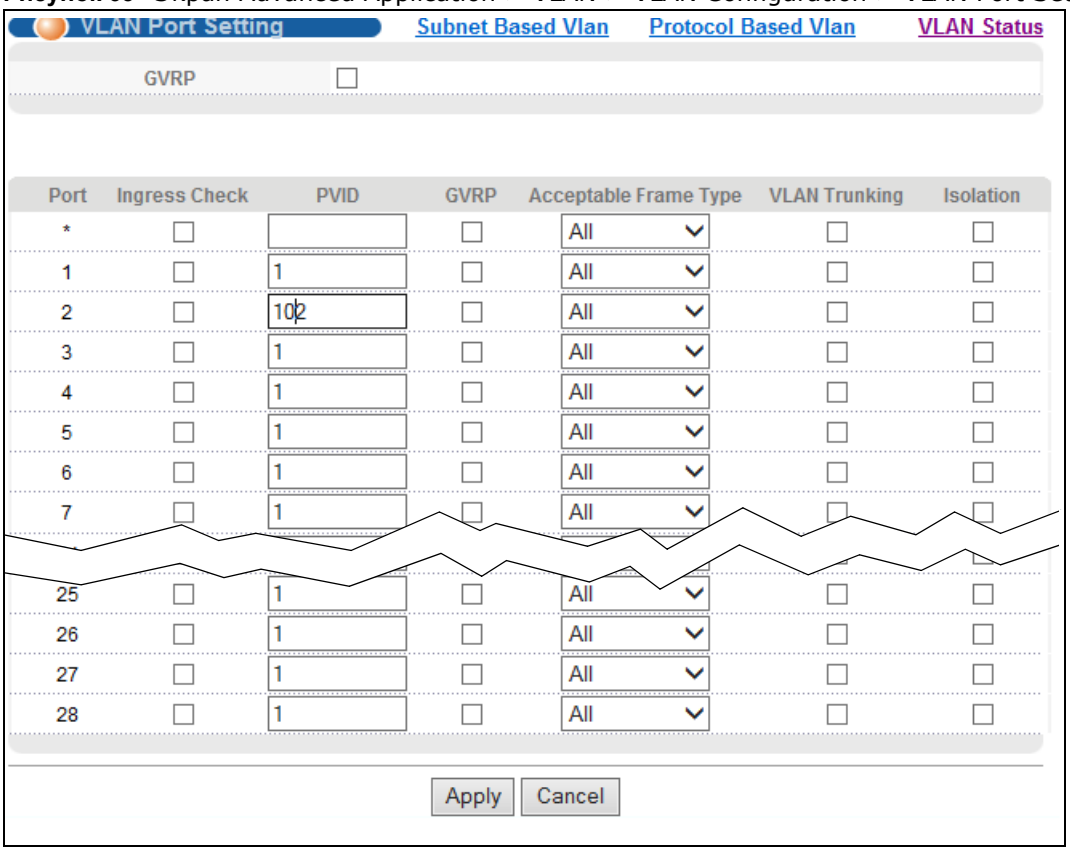
Таблица 29 Экран Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

ПОЛЕ	ОПИСАНИЕ
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 вернуться к сохраненным значениям полей.
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	Установите переключатель **Delete**, чтобы выбрать запись для сети VLAN, подлежащую удалению.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

9.5 Настройка порта VLAN

Для настройки параметров статической VLAN (на основе IEEE 802.1Q) для порта используется экран VLAN Port Setup. Перейдите по ссылке **VLAN Port Setup** на экране **VLAN Configuration**.

Рисунок 63 Экран Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup



Поля экрана описаны в следующей таблице.

Таблица 30 Экран Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup

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	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 сетей VLAN, членом которых данный порт не является. Снимите выделение с переключателя, если требуется отключить фильтрацию входящих кадров.

Таблица 30 Экран Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup

ПОЛЕ	ОПИСАНИЕ
PVID	PVID (идентификатор сети VLAN порта) – это тег, которым помечаются входящие кадры без тегов, принимаемые портом, с тем, чтобы потом перенаправить эти кадры в группу VLAN, которую определяет данный тег. Введите номер от 1 до 4094 в качестве идентификатора VLAN для порта.
GVRP	Установите этот переключатель, чтобы включить на этом порту протокол GVRP.
Acceptable Frame Type	Укажите тип кадров, разрешенных для данного порта. Можно выбрать значения **All**, **Tag Only** и **Untag 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. Выбор **Untag Only** разрешает прием через этот порт только кадров без тегов. Все кадры с тегами 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.
Isolation	Выберите эту опцию, чтобы разрешить каждому из портов обмениваться данными только с портом управления CPU и с портами, для которых не включена функция изоляции.
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.

9.6 VLAN на основе подсетей

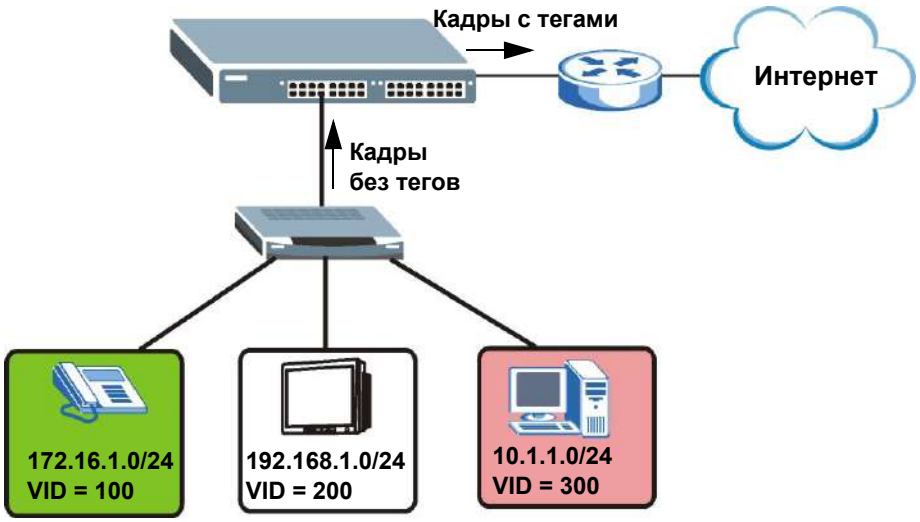
VLAN на основе подсетей позволяют сгруппировать трафик по логическим сетям VLAN на основе указанных IP-подсетей источников пакетов. При поступлении кадра через порт коммутатор проверяет, не был ли добавлен к нему тег и из какой IP-подсети он поступил. Пакеты без тегов от одной и той же IP-подсети помещаются 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 64 Пример использования VLAN на основе подсетей

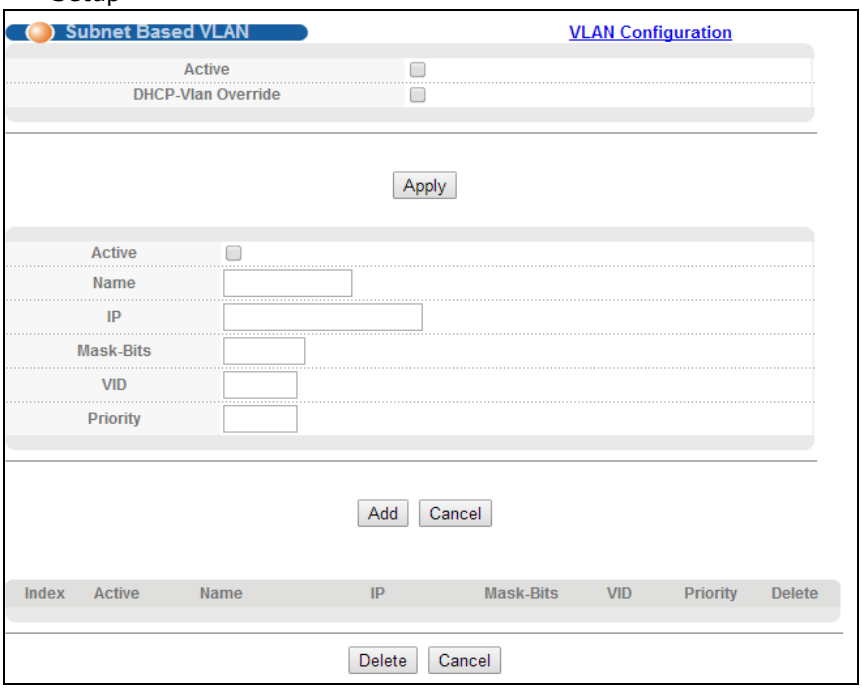


9.6.1 Настройка VLAN на основе подсетей

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

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

Рисунок 65 Экран Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup



Поля экрана описаны в следующей таблице.

Таблица 31 Экран Advanced Application > VLAN > VLAN Configuration > 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 создана на экранах **Advanced Applications**, **VLAN**.
Priority	Выберите уровень приоритета, назначаемый коммутатором кадрам из данной VLAN.

Таблица 31 Экран Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup (продолжение)

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

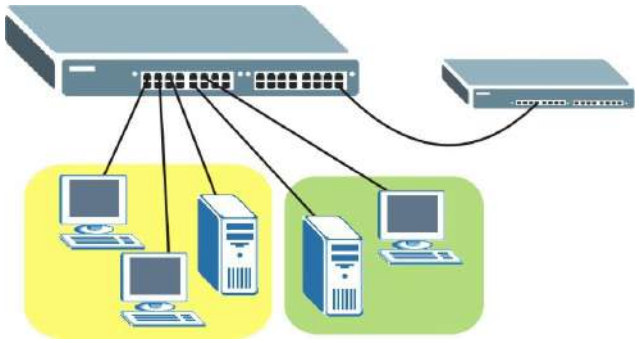
9.7 VLAN на основе протоколов

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.

Примечание: 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 66 Пример использования VLAN на основе протоколов

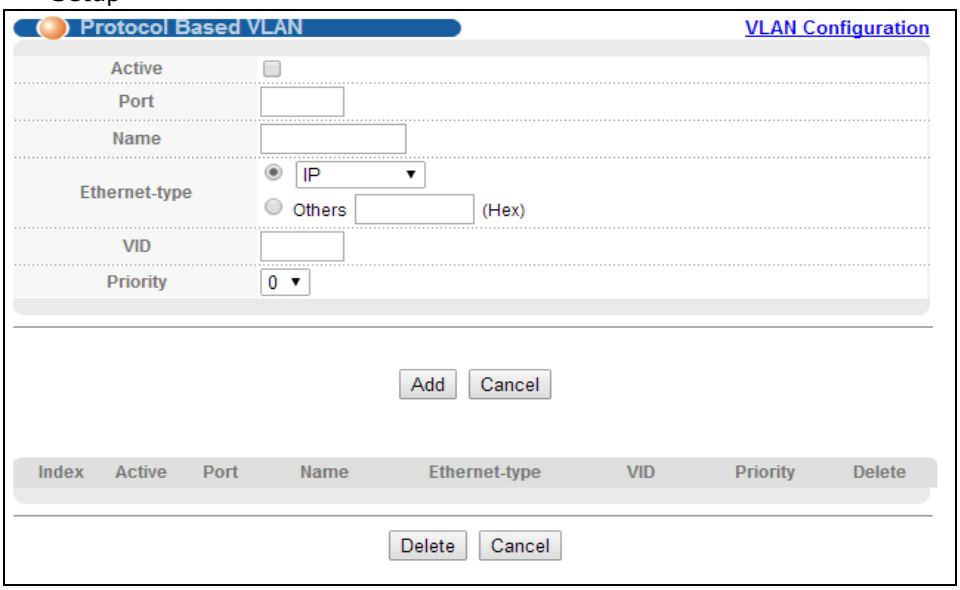


9.7.1 Настройка VLAN на основе протоколов

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

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

Рисунок 67 Экран Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup



Поля экрана описаны в следующей таблице.

Таблица 32 Экран Advanced Application > VLAN > VLAN Configuration > 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. 9 на стр. 86.
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, которой принадлежит порт. Данная VLAN должна быть предварительно создана 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.
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.

9.8 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.

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

Примечание: 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.

9.8.1 Настройка VLAN на основе портов

Выберите **Port Based** в качестве типа VLAN (**VLAN Type**) на экране **Basic Setting** > **Switch Setup**, затем выберите **Advanced Application** > **VLAN** в навигационной панели. Появится следующий экран.

Рисунок 68 Экран Port Based VLAN Setup (All Connected)

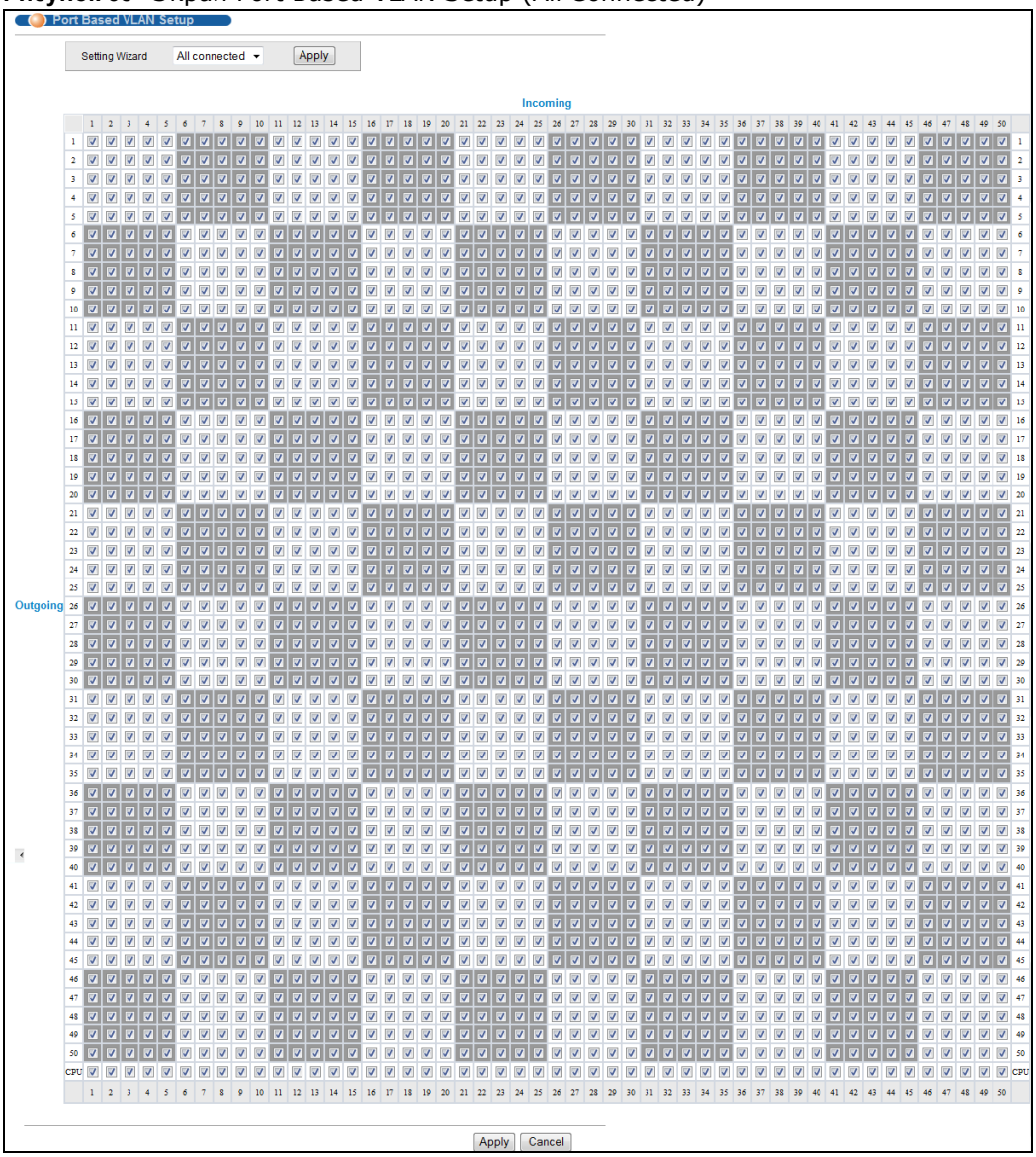
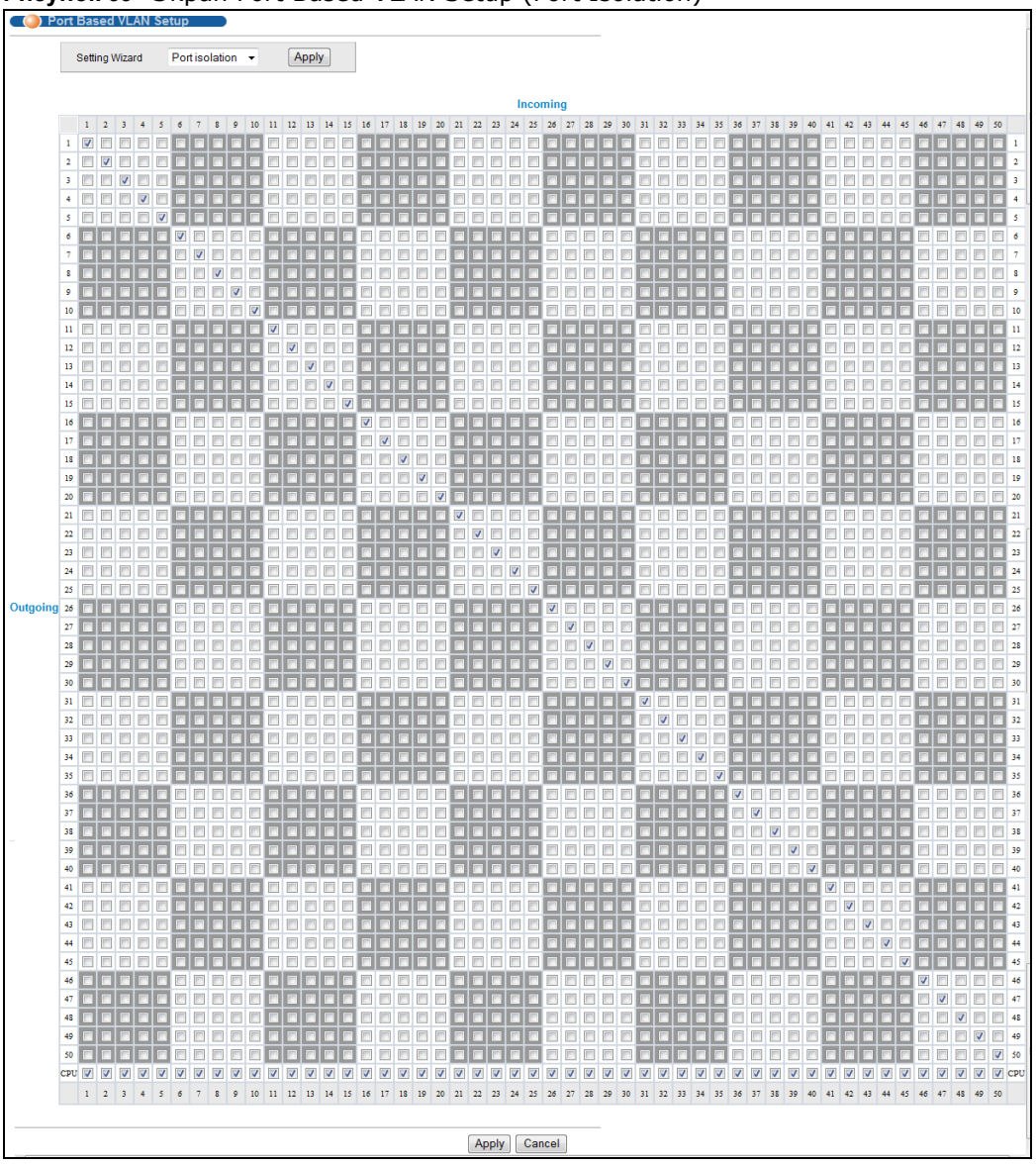


Рисунок 69 Экран Port Based VLAN Setup (Port Isolation)



Поля экрана описаны в следующей таблице.

Таблица 33 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. В эти настройки можно вносить изменения, 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.

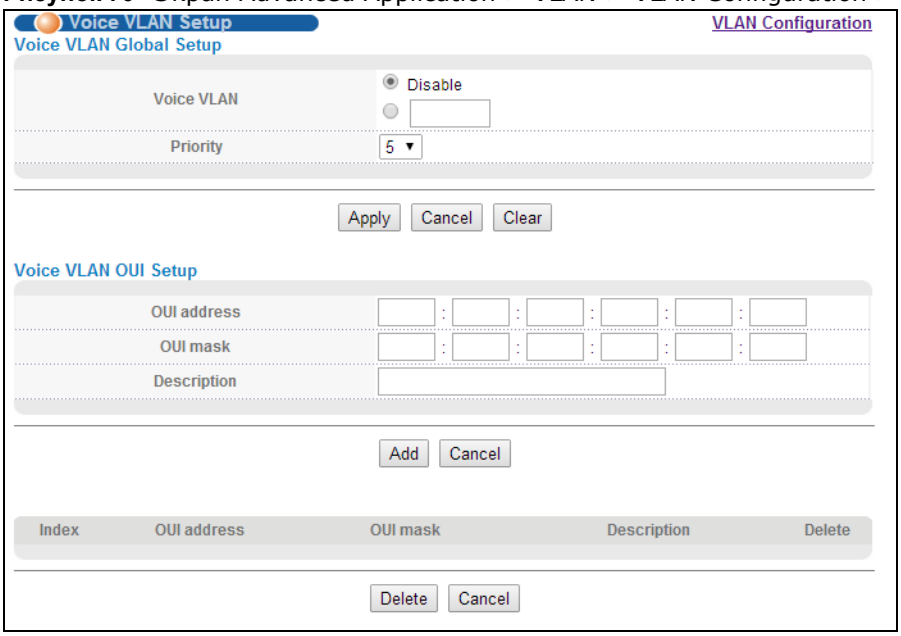
9.9 Сеть VLAN голосовой связи

Сеть VLAN голосовой связи гарантирует сохранение высокого качества передачи голоса на IP-телефоне в момент прохождения через порты коммутатора больших объемов трафика данных. Голосовой трафик с заданным приоритетом передается по специальной сети VLAN, и таким образом осуществляется разделение голосового трафика и трафика данных, проходящего через порт коммутатора.

Существует возможность установить уровень приоритета для сети VLAN голосовой связи и добавить в нее MAC-адреса IP-телефонов от определенных производителей, используя их идентификаторы, уникальные в пределах организации (Organizationally Unique Identifiers, OUI).

Выберите пункт **Voice VLAN** на экране **VLAN Configuration**, чтобы открыть экран настроек, изображенный на рисунке ниже.

Рисунок 70 Экран Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup



Поля экрана описаны в следующей таблице.

Таблица 34 Экран Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Voice VLAN Global Setup	
Voice VLAN	Чтобы включить функцию сети VLAN голосовой связи, установите радиопереключатель Voice VLAN. Введите идентификатор сети VLAN в текстовом поле рядом с радиопереключателем, который ассоциирован с данной сетью VLAN голосовой связи. Если включать функцию сети VLAN голосовой связи не нужно, установите радиопереключатель **Disable**.
Priority	Установите уровень приоритета для сети VLAN голосовой связи, выбрав его из диапазона от 0 до 7. Значение по умолчанию – 5. Чем выше присваиваемое числовое значение, тем выше уровень приоритета для данной сети VLAN голосовой связи.
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.
Clear	Нажмите **Clear**, чтобы вернуть значения полей к настройкам по умолчанию.
Voice VLAN OUI Setup	
OUI address	Укажите MAC-адрес OUI производителя IP-телефона. Первые три байта содержат идентификатор производителя, а последние три байта – уникальный идентификатор станции.
OUI mask	Введите адрес маски OUI производителя IP-телефона.
ОПИСАНИЕ	Введите описание устройства сети VLAN голосовой связи (не более 32 символов). Например: Siemens.

Таблица 34 Экран Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

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.
Index	Это поле содержит порядковый номер сети VLAN голосовой связи.
OUI address	Это поле отображает адрес OUI сети VLAN голосовой связи.
OUI mask	Это поле показывает адрес маски OUI сети VLAN голосовой связи.
ОПИСАНИЕ	Это поле содержит описание сети VLAN голосовой связи с адресом OUI.
Delete	Установите переключатель **Delete**, чтобы выбрать запись OUI для сети VLAN голосовой связи, которую необходимо удалить.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

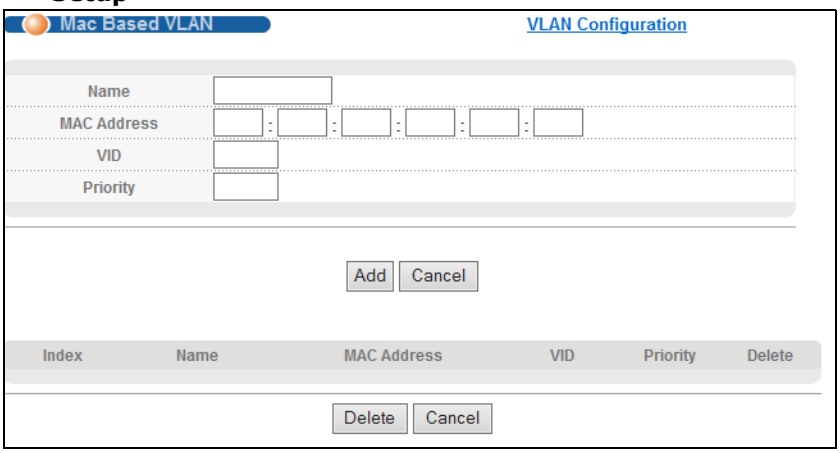
9.10 Сети VLAN на основе MAC-адресов

В сеть VLAN, созданную на основе MAC-адресов, можно включить входящие пакеты без тегов и классифицировать трафик по MAC-адресу источника пакета. При поступлении пакетов без тегов коммутатор ищет MAC-адрес источника пакета в таблице соответствия MAC-адресов и сетей VLAN. Если запись в таблице удалось найти, коммутатор назначает пакету идентификатор соответствующей сети VLAN. Коммутатор проверяет назначенный идентификатор VLAN в таблице сетей VLAN. Если данная сеть VLAN является действующей, то коммутатор продолжает обработку входящего пакета; в противном случае он отбрасывает этот пакет.

Это функция позволяет пользователям менять порты, не прибегая к перенастройке сети VLAN. Сети VLAN, созданной на основе MAC-адресов, можно назначить определенный приоритет, и создать таблицу соответствия между MAC-адресами и сетями, указав определенный MAC-адрес источника на экране настройки параметров сети VLAN на основе MAC-адресов. На том же экране можно удалить запись для сети VLAN на основе MAC-адресов.

Чтобы открыть следующий экран, выберите в меню **MAC-based VLAN** в окне **VLAN Configuration**.

Рисунок 71 Экран Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup



Поля экрана описаны в следующей таблице.

Таблица 35 Экран Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя, состоящее из алфавитно-цифровых символов (не более 32), для данной сети VLAN на основе MAC-адресов.
MAC Address	Укажите MAC-адрес, который необходимо привязать к записи для данной сети VLAN на основе MAC-адресов. Это поле будет содержать MAC-адрес источника пакета данных, который будет искать коммутатор при поступлении входящих пакетов без тегов.
VID	Укажите идентификатор (из диапазона от 1 до 4094) сети VLAN, который необходимо ассоциировать с записью для данной сети VLAN на основе MAC-адресов.
Priority	Укажите приоритет (от 0 до 7) записи для сети VLAN на основе MAC-адресов. Чем больше указанное число, тем более высоким будет приоритет записи для данной сети VLAN на основе MAC-адресов.
Add	Нажмите **Add**, чтобы сохранить новую запись для сети VLAN на основе MAC-адресов.
Cancel	Нажмите **Cancel**, чтобы очистить поля записи для сети VLAN на основе MAC-адресов.
Index	Это поле показывает порядковый номер записи для сети VLAN на основе MAC-адресов.
Name	Это поле показывает имя записи для сети VLAN на основе MAC-адресов.
MAC Address	Это поле показывает MAC-адрес источника, который привязан к записи для сети VLAN на основе MAC-адресов.
VID	Это поле показывает идентификатор сети VLAN на основе MAC-адресов.
Priority	Это поле показывает уровень приоритета сети VLAN на основе MAC-адресов.
Delete	Установите переключатель **Delete**, чтобы выбрать запись для сети VLAN на основе MAC-адресов, подлежащую удалению.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

9.11 Справочная техническая информация

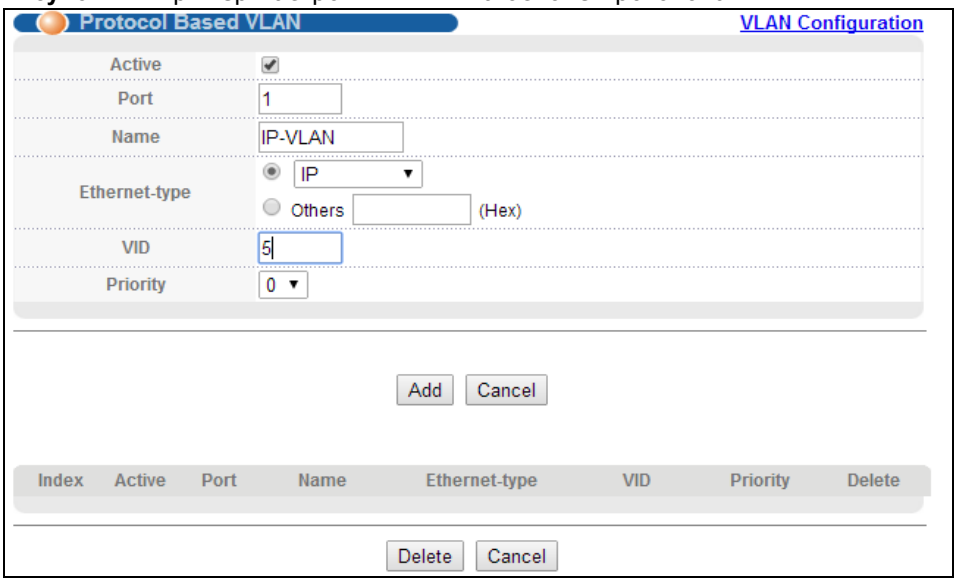
Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

9.11.1 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 72 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**.

10

Настройка пересылки на основе статических MAC-адресов

10.1 Обзор

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

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

10.1.1 О чем рассказывается в этой главе

С помощью экрана **Static MAC Forwarding** (разд. 10.2 на стр. 110) можно назначить статические MAC-адреса для портов.

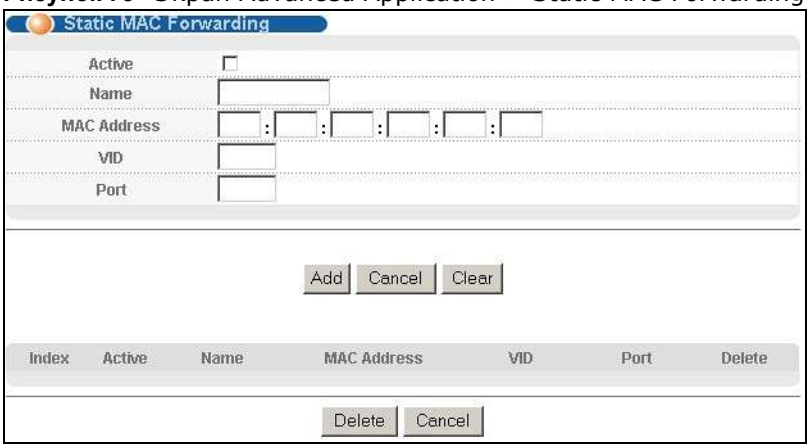
10.2 Настройка пересылки на основе статических MAC-адресов

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. 19 на стр. 161.

Чтобы открыть экран настроек, изображенный ниже, выберите в навигационной панели **Advanced Application** > **Static MAC Forwarding**.

Рисунок 73 Экран Advanced Application > Static MAC Forwarding



Поля экрана описаны в следующей таблице.

Таблица 36 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 вернуться к сохраненным значениям полей.
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, 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**.

11

Многоадресная рассылка на основе статических адресов

11.1 Обзор настройки многоадресной рассылки на основе статических адресов

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

С помощью этих экранов можно настроить параметры многоадресной рассылки на основе статических адресов.

11.1.1 О чем рассказывается в этой главе

С помощью экрана **Static Multicast Forward Setup** (разд. 11.2 на стр. 113) можно настроить правила пересылки определенных кадров многоадресной рассылки, например, кадров потоковой передачи или управляющих кадров, на определенные порты.

11.1.2 Что необходимо знать

MAC-адрес многоадресной рассылки – это MAC-адрес члена группы многоадресной рассылки. Статический адрес многоадресной рассылки – это MAC-адрес многоадресной рассылки, который был добавлен в таблицу многоадресной рассылки вручную. Статические адреса многоадресной рассылки не имеют срока действия. Многоадресная рассылка на основе статических адресов позволяет администратору организовать пересылку кадров многоадресной рассылки на определенные порты, не являющиеся членами группы.

Если в группе многоадресной рассылки нет членов, то коммутатор либо пересылает кадры многоадресной рассылки на все порты, либо отбрасывает их. На рис. 74 показан процесс пересылки неизвестных кадров многоадресной рассылки на все порты. С помощью многоадресной рассылки на основе статических адресов можно организовать пересылку этих кадров многоадресной рассылки на порты, входящие в группу VLAN. На рис. 75 показаны кадры, пересылаемые на устройства, подключенные к порту 3. На рис. 76 показаны кадры, пересылаемые на порты 2 и 3, которые входят в группу VLAN 4.

Рисунок 74 Многоадресная рассылка на основе статических адресов отключена

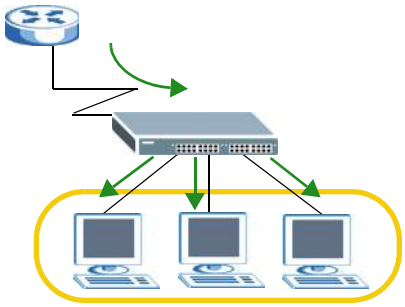


Рисунок 75 Многоадресная рассылка на основе статических адресов на один порт A

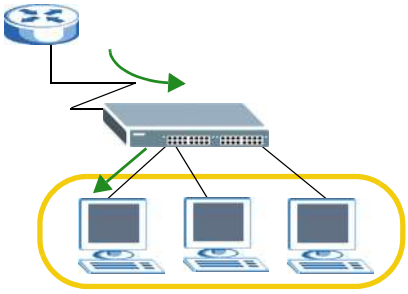
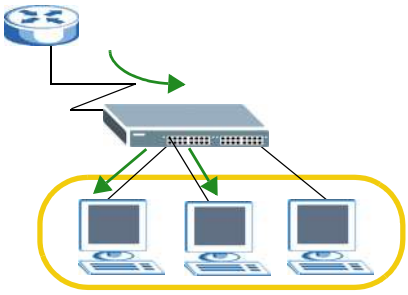


Рисунок 76 Многоадресная рассылка на основе статических адресов на два и более портов

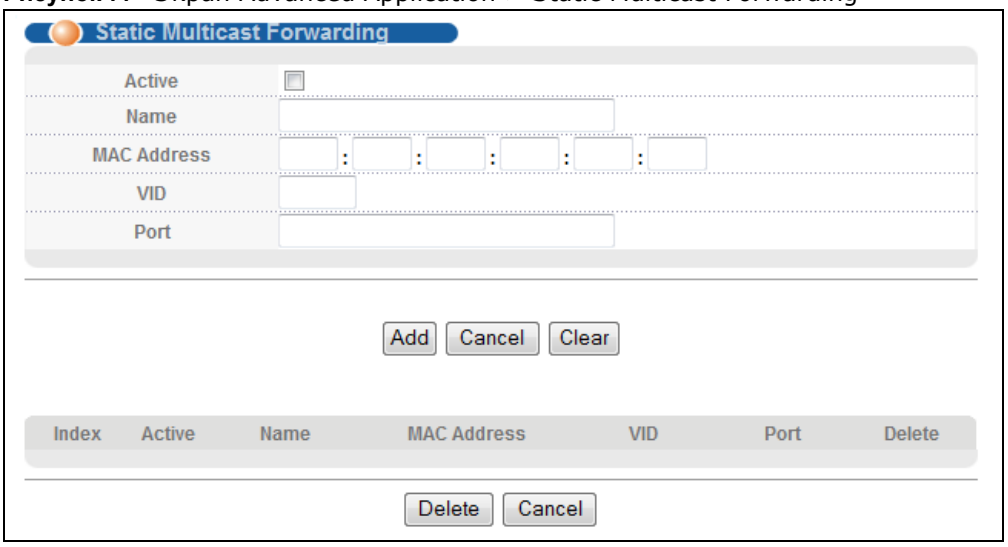


11.2 Настройка многоадресной рассылки на основе статических адресов

С помощью этого экрана можно настроить правила пересылки определенных кадров многоадресной рассылки, например, кадров потоковой передачи или управляющих кадров, на определенные порты.

Чтобы открыть экран настроек, изображенный ниже, выберите в меню **Advanced Application** > **Static Multicast Forwarding**.

Рисунок 77 Экран Advanced Application > Static Multicast Forwarding



Поля экрана описаны в следующей таблице.

Таблица 37 Экран Advanced Application > Static Multicast 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 (до 32 отображаемых ASCII-символов) для данного правила многоадресной рассылки на основе статических MAC-адресов. Оно будет использоваться только для идентификации.
MAC Address	Введите MAC-адрес многоадресной рассылки, который идентифицирует группу многоадресной рассылки. Последний двоичный разряд первой пары октетов MAC-адреса многоадресной рассылки должен быть равен 1. Например, первая пара октетов числа 00000001 равна 01, а в шестнадцатеричной нотации число 00000011 равно 03, соответственно, адреса 01:00:5e:00:00:0A и 03:00:5e:00:00:27 являются действительными MAC-адресами многоадресной рассылки.
VID	Существует возможность организовать пересылку кадров с MAC-адресами назначения, соответствующих критериям отбора, на порты в пределах группы VLAN. Укажите в этом поле число, которое идентифицирует группу VLAN. В отсутствие конкретной целевой сети VLAN в этом поле следует указать число 1.
Port	Укажите порты, на которые должны пересылаться кадры, чем MAC-адрес назначения соответствует критериям отбора, указанным в записи выше. В этом поле можно указать два и более портов, разделенных (без пробелов) символами запятой (,) или дефиса (-). Например, запись «3-5» будет означать порты 3, 4 и 5. Чтобы указать порты 3, 5 и 7, введите в этом поле значение «3,5,7».
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 вернуться к сохраненным значениям полей.
Clear	Нажмите **Clear**, чтобы начать настройку на этом экране заново.
Index	Щелкните по порядковому номеру, чтобы изменить правило многоадресной рассылки на основе статических MAC-адресов для данного порта (или портов).
Active	В этом поле указано, активно данное правило многоадресной рассылки на основе статических MAC-адресов (**Yes**) или нет (**No**). Правило можно временно отключить, не удаляя его.

Таблица 37 Экран Advanced Application > Static Multicast Forwarding (продолжение)

ПОЛЕ	ОПИСАНИЕ
Name	Это поле отображает имя-описание, по которому можно будет идентифицировать это правило многоадресной рассылки на основе статических MAC-адресов.
MAC Address	Это поле отображает MAC-адрес многоадресной рассылки, который идентифицирует группу многоадресной рассылки.
VID	Это поле показывает идентификатор группы VLAN, в которую будут пересылаться кадры, содержащие указанные MAC-адреса многоадресной рассылки.
Port	Это поле показывает порт (или порты), входящие в данную группу VLAN, на которые будут пересылаться кадры, содержащие указанные MAC-адреса многоадресной рассылки.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

12

Фильтрация

12.1 Обзор фильтрации

В этой главе описана фильтрация MAC-адресов на портах.

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

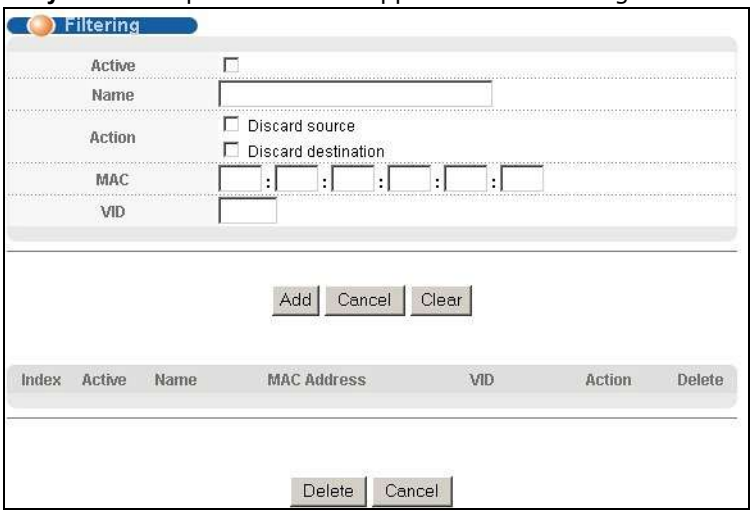
12.1.1 О чем рассказывается в этой главе

С помощью экрана **Filtering** (разд. 12.2 на стр. 116) можно создать правила для трафика, проходящего через коммутатор.

12.2 Настройка правила фильтрации

С помощью этого экрана можно создать правила фильтрации для трафика, проходящего через коммутатор. Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Filtering**.

Рисунок 78 Экран Advanced Application > Filtering



Поля экрана описаны в следующей таблице.

Таблица 38 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.
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 сбросить поля к предыдущим значениям.
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, 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**.

13

Протокол покрывающего дерева

13.1 Обзор протокола покрывающего дерева (Spanning Tree Protocol)

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.

13.1.1 О чем рассказывается в этой главе

- С помощью экрана состояния **Spanning Tree Protocol** (разд. 13.2 на стр. 121) можно просмотреть статус протокола STP в различных режимах STP (RSTP, MRSTP или MSTP), которые можно настроить на коммутаторе.
- С помощью экрана **Spanning Tree Configuration** (разд. 13.3 на стр. 122) можно активировать на коммутаторе один из режимов STP.
- С помощью экрана **Rapid Spanning Tree Protocol** (разд. 13.4 на стр. 123) можно настроить параметры режима RSTP.
- С помощью экрана **Rapid Spanning Tree Protocol Status** (разд. 13.5 на стр. 125) можно открыть экран состояния, изображенный на рисунке ниже.
- С помощью экрана **Multiple Rapid Spanning Tree Protocol** (разд. 13.6 на стр. 126) можно настроить параметры режима MRSTP.
- С помощью экрана **Multiple Rapid Spanning Tree Protocol Status** (разд. 13.7 на стр. 129) можно просмотреть состояние MRSTP.
- С помощью экрана **Multiple Spanning Tree Protocol** (разд. 13.8 на стр. 130) можно настроить параметры MSTP.
- С помощью экрана **Multiple Spanning Tree Protocol Status** (разд. 13.10 на стр. 135) можно просмотреть состояние MSTP.

13.1.2 Что необходимо знать

Ознакомьтесь с приведенной ниже информацией о протоколе STP, которая поможет в работе с экранами, описанными ниже в этой главе.

(Быстрый) протокол покрывающего дерева

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.

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

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 39 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 65535
Стоимость пути	10 Мбит/с	100	От 50 до 600	От 1 до 65535
Стоимость пути	16 Мбит/с	62	От 40 до 400	От 1 до 65535
Стоимость пути	100 Мбит/с	19	От 10 до 60	От 1 до 65535
Стоимость пути	1 Гбит/с	4	От 3 до 10	От 1 до 65535
Стоимость пути	10 Гбит/с	2	От 1 до 5	От 1 до 65535

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.

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.

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 40 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.

Быстрый протокол нескольких экземпляров покрывающего дерева

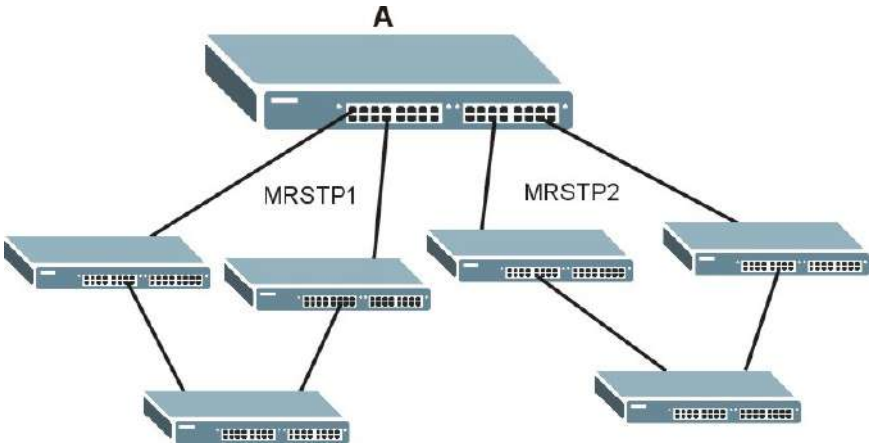
Протокол MRSTP (быстрый протокол нескольких экземпляров покрывающего дерева, Multiple RSTP) представляет собой фирменную функцию ZyXEL, совместимую с протоколами RSTP и STP. Поддержка MRSTP позволяет настроить на коммутаторе несколько экземпляров покрывающего дерева и назначать порты каждому дереву. 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.

Примечание: Каждый порт может принадлежать только к одному дереву STP.

Рисунок 79 Пример сети с поддержкой MRSTP



Протокол MSTP

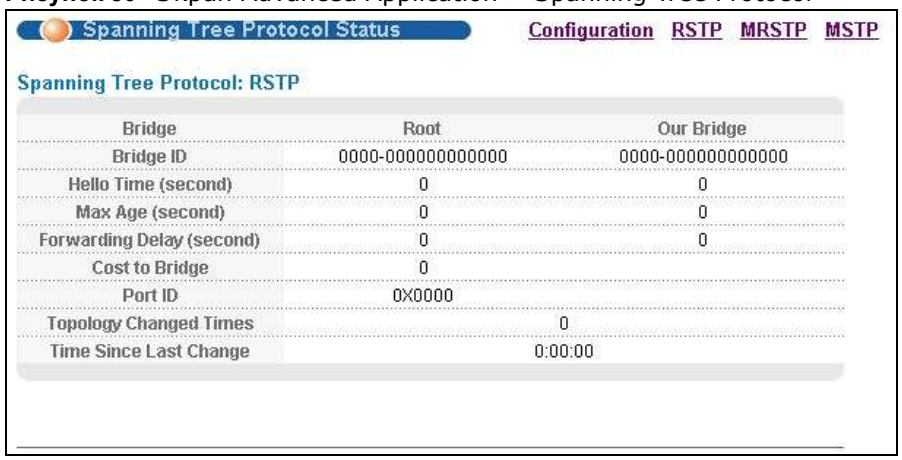
Протокол нескольких экземпляров покрывающего дерева MSTP (IEEE 802.1s) обратно совместим с протоколами STP/RSTP и устраняет ограничения, характерные для существующих протоколов STP и RSTP за счет реализации следующих функций:

- 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.

13.2 Состояние протокола покрывающего дерева

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

Рисунок 80 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**.

13.3 Настройка протокола покрывающего дерева

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

Рисунок 81 Экран Advanced Application > Spanning Tree Protocol > Configuration

Поля экрана описаны в следующей таблице.

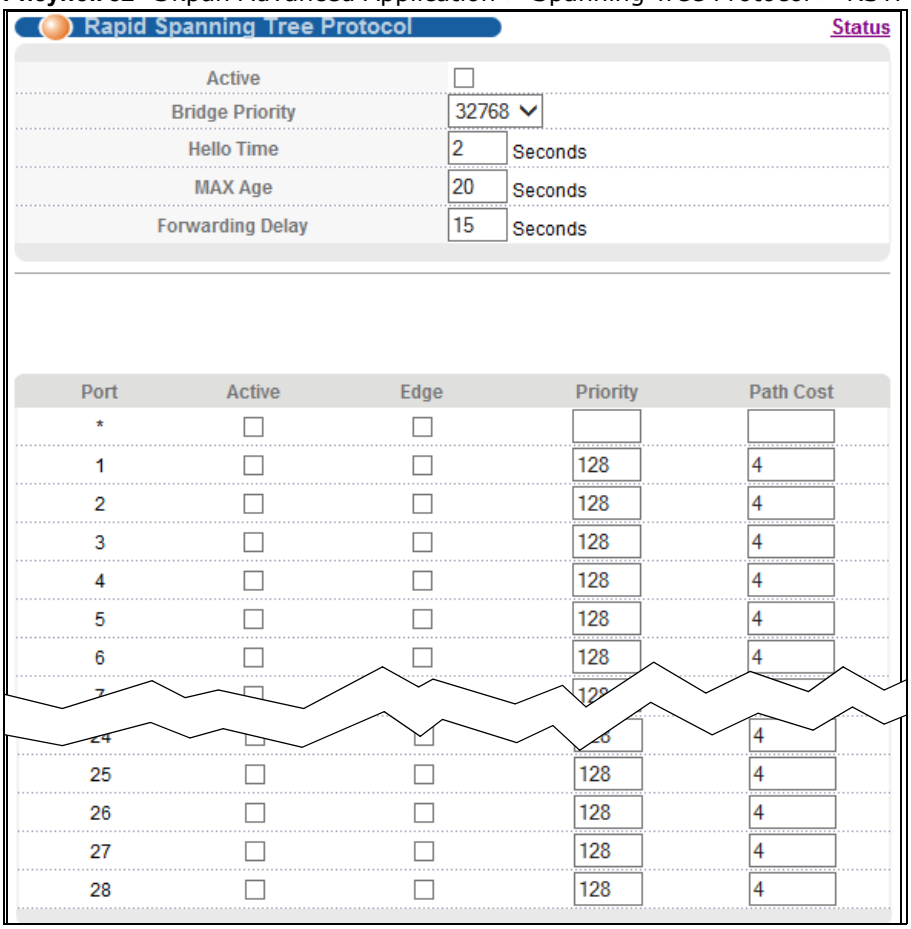
Таблица 41 Экран Advanced Application > Spanning Tree Protocol > Configuration

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. 13.1 на стр. 118.
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.

13.4 Настройка быстрого протокола покрывающего дерева

С помощью этого экрана можно настроить параметры режима RSTP, более подробную информацию о режиме RSTP можно найти в разд. 13.1 на стр. 118. Выберите пункт **RSTP** на экране **Advanced Application** > **Spanning Tree Protocol**.

Рисунок 82 Экран Advanced Application > Spanning Tree Protocol > RSTP



Поля экрана описаны в следующей таблице.

Таблица 42 Экран Advanced Application > Spanning Tree Protocol > RSTP

ПОЛЕ	ОПИСАНИЕ
Status	Выберите **Status**, чтобы отобразить экран состояния **RSTP Status** (см. рис. 83 на стр. 125).
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 42 Экран Advanced Application > Spanning Tree Protocol > RSTP (продолжение)

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 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. 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.
Edge	Установите этот переключатель, чтобы выбрать для порта роль граничного порта, если он напрямую подключен к компьютеру. Граничный порт немедленно меняет свое первоначальное состояние как порта STP с блокирующего на пересылающее, минуя состояния прослушивания и запоминания, сразу после выбора этого порта в качестве граничного или после изменения состояния соединения на этом порту. Примечание: Граничный порт перестает быть таковым, как только он получает блок данных мостового протокола (BPDU).
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 42 Экран Advanced Application > Spanning Tree Protocol > RSTP (продолжение)

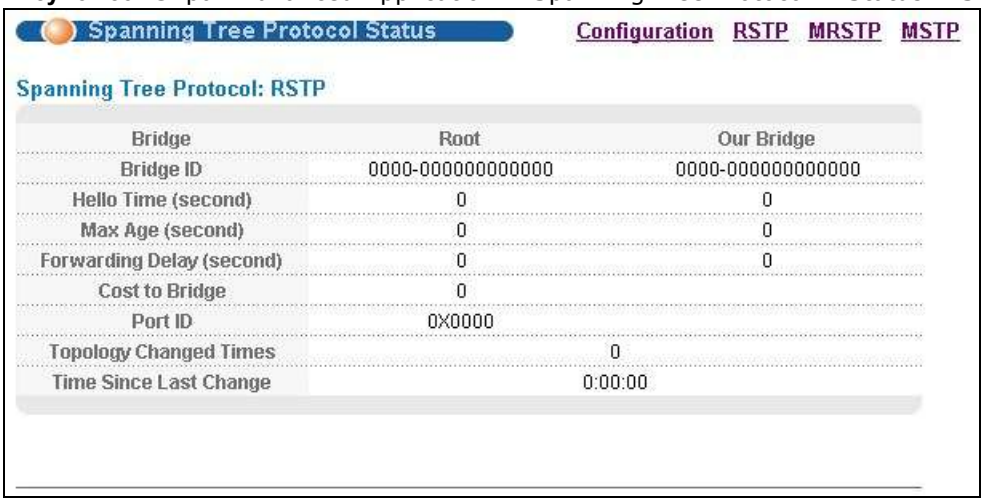
ПОЛЕ	ОПИСАНИЕ
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – для получения дополнительной информации см. табл. 39 на стр. 119.
Apply	Нажмите **Apply**, 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.

13.5 Состояние быстрого протокола покрывающего дерева

Чтобы отобразить следующий экран состояния, выберите пункт **Advanced Application** > **Spanning Tree Protocol** в навигационной панели. Более подробную информацию о RSTP можно найти в разд. 13.1 на стр. 118.

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

Рисунок 83 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP



Поля экрана описаны в следующей таблице.

Таблица 43 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.

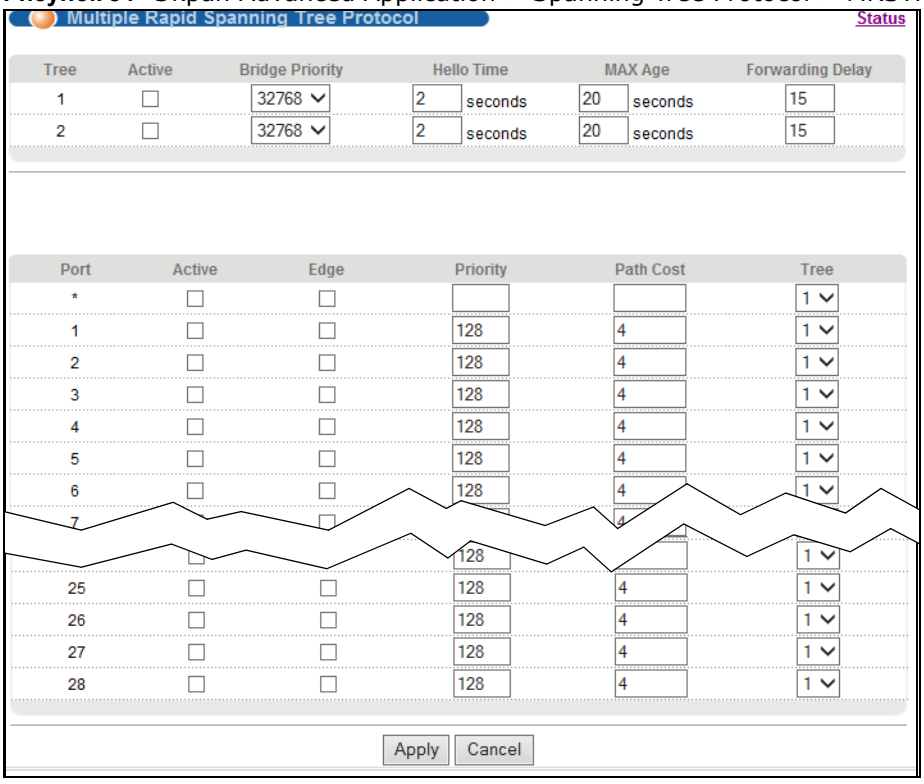
Таблица 43 Экран Advanced Application > Spanning Tree Protocol > Status: RSTP (продолжение)

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.

13.6 Настройка протокола MRSTP

Чтобы настроить протокол MRSTP, выберите пункт **MRSTP** на экране **Advanced Application** > **Spanning Tree Protocol**. Более подробную информацию о MRSTP можно найти в разд. 13.1 на стр. 118.

Рисунок 84 Экран Advanced Application > Spanning Tree Protocol > MRSTP



Поля экрана описаны в следующей таблице.

Таблица 44 Экран Advanced Application > Spanning Tree Protocol > MRSTP

ПОЛЕ	ОПИСАНИЕ
Status	Нажмите **Status**, чтобы отобразить экран состояния **MRSTP Status** (см. рис. 83 на стр. 125).
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**.
Bridge Priority	Приоритет моста используется для определения корневого коммутатора, корневого порта и назначенного порта. Коммутатор с наивысшим приоритетом (наименьшее числовое значение) становится корневым коммутатором протокола STP. Если у всех коммутаторов одинаковый приоритет, то корневым становится коммутатором с наименьшим MAC-адресом. Выберите значение в ниспадающем списке. Чем меньшее числовое значение будет выбрано, тем выше будет приоритет у этого моста. Параметр Bridge Priority определяет корневой мост, который, в свою очередь, определяет параметры Hello Time, Max Age и Forwarding Delay.
Hello Time	Временной интервал в секундах между конфигурационными сообщениями BPDU (блоки данных мостового протокола), генерируемыми корневым коммутатором. Диапазон допустимых значений – от 1 до 10 секунд.

Таблица 44 Экран Advanced Application > Spanning Tree Protocol > MRSTP (продолжение)

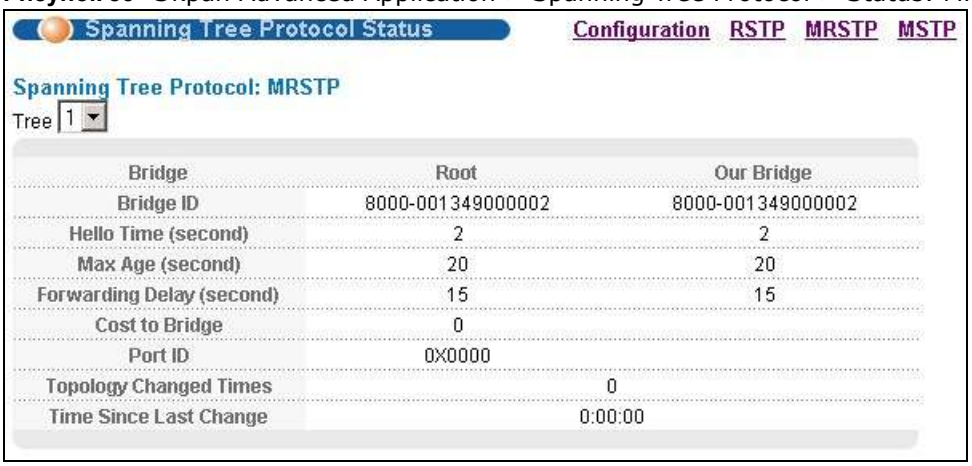
ПОЛЕ	ОПИСАНИЕ
Max Age	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая сообщений BPDU, прежде чем он предпримет попытку произвести настройку заново. Все порты коммутатора (за исключением назначенных портов) должны получать сообщения BPDU через регулярные промежутки времени. Любой порт с устаревшей информацией протокола STP (содержащейся в последнем сообщении BPDU) становится назначенным портом для подключенной локальной сети. Если это корневой порт, то новый корневой порт выбирается из портов коммутатора, подключенных к сети. Диапазон допустимых значений – от 6 до 40 секунд.
Forwarding Delay	Временной интервал (в секундах), в течение которого 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. 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.
Edge	Установите этот переключатель, чтобы выбрать для порта роль граничного порта, если он напрямую подключен к компьютеру. Граничный порт немедленно меняет свое первоначальное состояние как порта STP с блокирующего на пересылающее, минуя состояния прослушивания и запоминания, сразу после выбора этого порта в качестве граничного или после изменения состояния соединения на этом порту. Примечание: Граничный порт перестает быть таковым, как только он получает блок данных мостового протокола (BPDU).
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 – для получения дополнительной информации см. табл. 39 на стр. 119.
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.

13.7 Состояние протокола MRSTP

Чтобы отобразить следующий экран состояния, выберите пункт **Advanced Application** > **Spanning Tree Protocol** в навигационной панели. Более подробную информацию о MRSTP можно найти в разд. 13.1 на стр. 118.

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

Рисунок 85 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP



Поля экрана описаны в следующей таблице.

Таблица 45 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.
Bridge ID	Уникальный идентификатор данного моста, состоящий из уровня приоритета моста и MAC-адреса. Если коммутатор является корневым, то в полях **Root** и **Our Bridge** указывается один и тот же идентификатор.
Hello Time (second)	Временной интервал (в секундах), в течение которого корневой коммутатор передает конфигурационное сообщение. Значения параметров Hello Time, Max Age и Forwarding Delay определяет корневой мост.
Max Age (second)	Максимальное время (в секундах), в течение которого коммутатор может простаивать, не получая конфигурационного сообщения, прежде чем он предпримет попытку произвести настройку заново.
Forwarding Delay (second)	Время (в секундах), в течение которого корневой коммутатор ожидает перед сменой состояний (то есть от Listening к Learning и затем к Forwarding). Примечание: Состояние «Listening» не используется в RSTP.
Cost to Bridge	Стоимость пути от корневого порта на данном коммутаторе к корневому коммутатору.
Port ID	Уровень приоритета и номер порта на коммутаторе, через который этот коммутатор должен связываться с корнем покрывающего дерева.

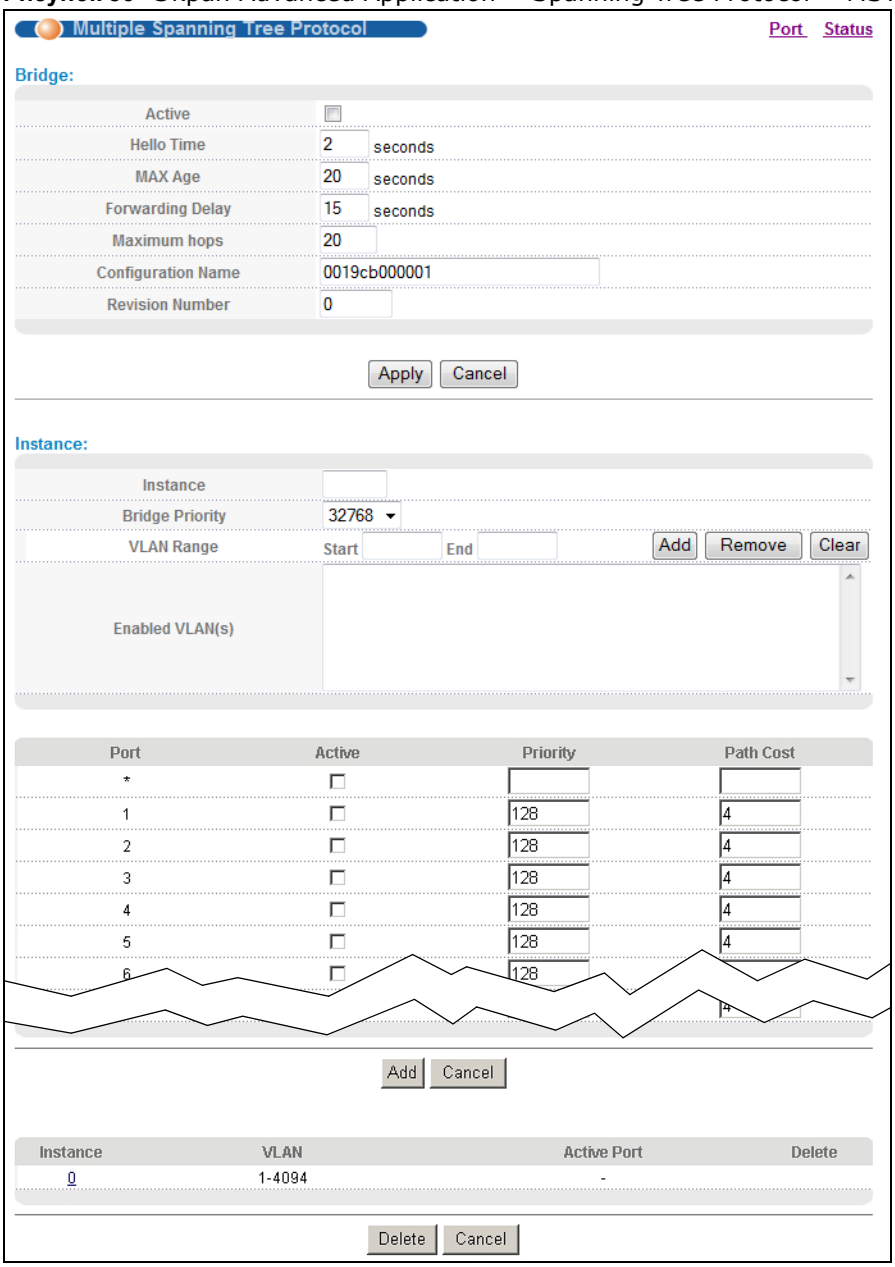
Таблица 45 Экран Advanced Application > Spanning Tree Protocol > Status: MRSTP

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

13.8 Настройка протокола MSTP

Чтобы настроить протокол MSTP, выберите пункт **MSTP** на экране **Advanced Application** > **Spanning Tree Protocol**. Более подробную информацию о MSTP можно найти в разд. «Протокол MSTP» на стр. 121.

Рисунок 86 Экран Advanced Application > Spanning Tree Protocol > MSTP



Поля экрана описаны в следующей таблице.

Таблица 46 Экран Advanced Application > Spanning Tree Protocol > MSTP

ПОЛЕ	ОПИСАНИЕ
Port	Нажмите **Port**, чтобы открыть экран **MSTP Port** (см. рис. 87 на стр. 134).
Status	Нажмите **Status**, чтобы отобразить экран состояния **MSTP Status** (см. рис. 88 на стр. 135).

Таблица 46 Экран Advanced Application > Spanning Tree Protocol > MSTP (продолжение)

ПОЛЕ	ОПИСАНИЕ
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 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. Диапазон допустимых значений – от 4 до 30 секунд. Как правило: Примечание: 2 * (Forward Delay – 1) >= Max Age >= 2 * (Hello Time + 1)
Maximum hops	Введите количество переходов (от 1 до 255) в регионе MSTP, после которого блок данных BPDU будет отбрасываться, и информация порта будет считаться устаревшей.
Configuration Name	Введите имя-описание (до 32 символов) для региона MST.
Revision Number	Введите идентификационный номер конфигурации региона. Этот номер должен быть одинаковым на всех устройствах, принадлежащих одному региону.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Instance	В этом разделе определяются параметры MSTI (экземпляра покрывающего дерева).
Instance	Введите номер, используемый для идентификации данного экземпляра MST на коммутаторе. Данный коммутатор поддерживает номера экземпляров в диапазоне 0-15.
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).

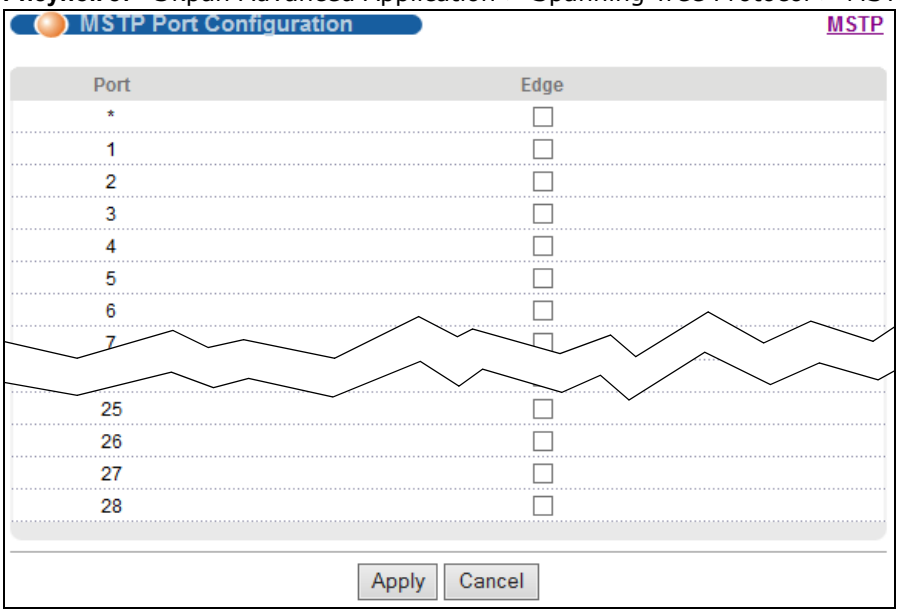
Таблица 46 Экран Advanced Application > Spanning Tree Protocol > MSTP (продолжение)

ПОЛЕ	ОПИСАНИЕ
VLAN Range	Введите начальный идентификатор диапазона идентификаторов VLAN, который необходимо добавить или удалить из области редактирования диапазонов VLAN, в поле **Start**. Введите конечный идентификатор диапазона идентификаторов VLAN, который необходимо добавить или удалить из области редактирования диапазонов VLAN, в поле **End**. Затем нажмите: • **Add** – чтобы добавить данный диапазон идентификаторов VLAN к списку связанных с данным экземпляром MST. • **Remove** – чтобы удалить данный диапазон идентификаторов VLAN из списка связанных с данным экземпляром MST. • **Clear** – чтобы удалить все сети VLAN из списка связанных с данным экземпляром MST.
Enabled VLAN(s)	В данном поле отображаются сети VLAN, связанные с данным экземпляром MST.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите данный переключатель, чтобы добавить данный порт к данному экземпляру MST.
Priority	Здесь можно определить приоритет для каждого из портов. Уровень приоритета определяет, какой из портов нужно отключить, когда на нескольких портах коммутатора образуется петля. Порты с более высоким значением приоритета отключаются первыми. Допустимый диапазон значений – от 0 до 255, по умолчанию устанавливается уровень приоритета 128.
Path Cost	Стоимость пути – стоимость передачи кадра в локальную сеть через этот порт. Данное значение рекомендуется выбирать в зависимости от скорости моста. Чем ниже скорость, тем выше стоимость – для получения дополнительной информации см. табл. 39 на стр. 119.
Add	Нажмите **Add**, чтобы сохранить данный экземпляр MST в оперативной памяти коммутатора. Это изменение будет утеряно в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.
Instance	В этом поле отображается идентификатор экземпляра MST.
VLAN	В данном поле отображается идентификатор VID (или диапазоны идентификаторов VID), связанные с данным экземпляром MST.
Active Port	В данном поле отображаются порты, включенные в данный экземпляр MST.
Delete	В столбце **Delete** установите переключатели правил, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

13.9 Настройка порта для протокола MSTP

Чтобы открыть экран состояния, изображенный на рисунке ниже, выберите в навигационной панели **Advanced Application** > **Spanning Tree Protocol > MSTP > Port**. Более подробную информацию о MSTP можно найти в разд. «Протокол MSTP» на стр. 121.

Рисунок 87 Экран Advanced Application > Spanning Tree Protocol > MSTP > Port



Поля экрана описаны в следующей таблице.

Таблица 47 Экран Advanced Application > Spanning Tree Protocol > MSTP > Port

ПОЛЕ	ОПИСАНИЕ
MSTP	Для изменения настроек MSTP коммутатора нажмите на **MSTP**.
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.
Edge	Установите этот переключатель, чтобы выбрать для порта роль граничного порта, если он напрямую подключен к компьютеру. Граничный порт немедленно меняет свое первоначальное состояние как порта STP с блокирующего на пересылающее, минуя состояния прослушивания и запоминания, сразу после выбора этого порта в качестве граничного или после изменения состояния соединения на этом порту. Примечание: Граничный порт перестает быть таковым, как только он получает блок данных мостового протокола (BPDU).
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.

13.10 Состояние протокола MSTP

Чтобы отобразить следующий экран состояния, выберите пункт **Advanced Application** > **Spanning Tree Protocol** в навигационной панели. Более подробную информацию о MSTP можно найти в разд. «Протокол MSTP» на стр. 121.

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

Рисунок 88 Экран Advanced Application > Spanning Tree Protocol > Status: MSTP

Поля экрана описаны в следующей таблице.

Таблица 48 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.

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

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

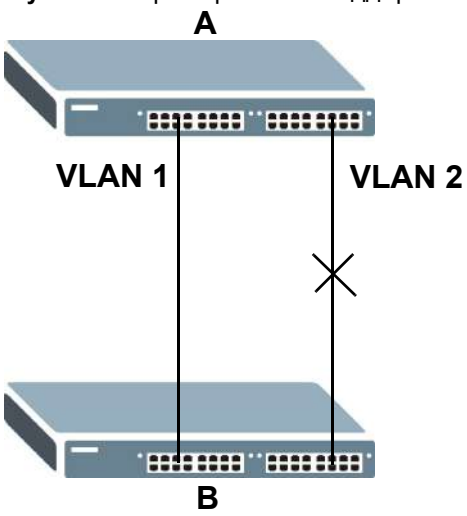
13.11 Справочная техническая информация

Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

13.11.1 Пример сети с поддержкой MSTP

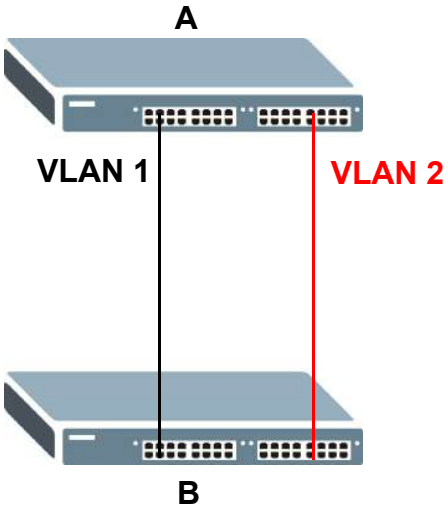
На приведенном ниже рисунке показан пример сети, в которой на двух коммутаторах настроены две сети VLAN. В случае использования на коммутаторах протокола STP или RSTP канал для VLAN 2 будет заблокирован, так как протоколы STP и RSTP допускают наличие только одного канала и блокируют избыточные каналы.

Рисунок 89 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 90 Пример сети с поддержкой MSTP



13.11.2 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:

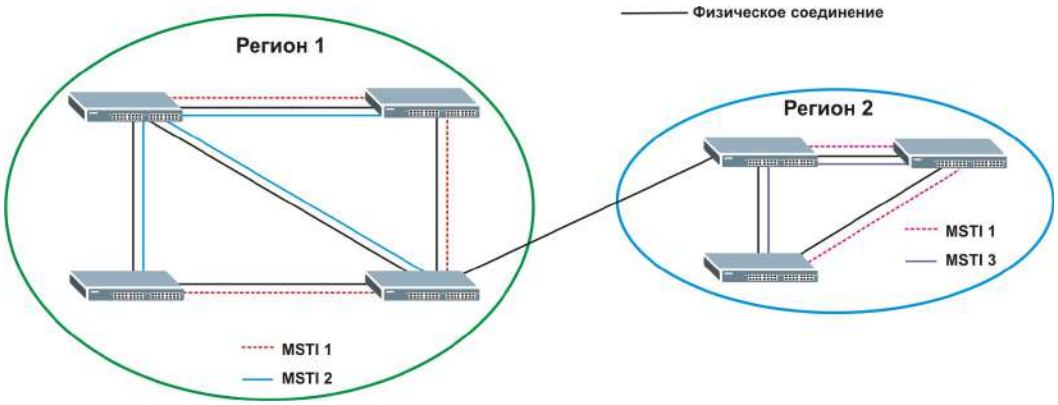
- Имя региона MST
- Номер версии в качестве уникального номера региона MST
- Связывание VLAN с конкретным экземпляром MST

13.11.3 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.

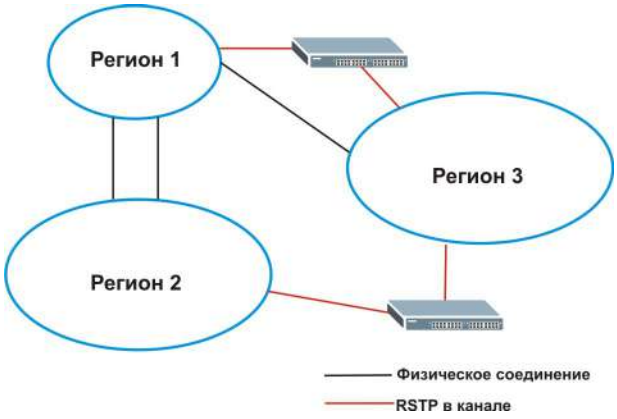
Рисунок 91 Экземпляры MSTI в различных регионах



13.11.4 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 92 Пример сети с использованием MSTP и традиционного протокола RSTP



14

Управление пропускной способностью

14.1 Обзор

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

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

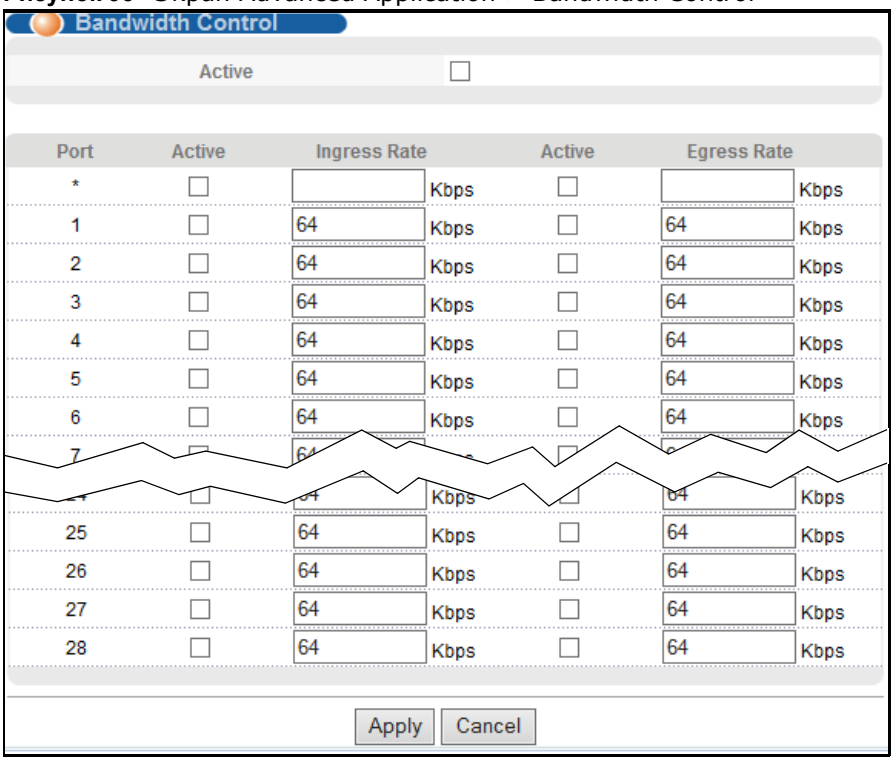
14.1.1 О чем рассказывается в этой главе

С помощью экрана **Bandwidth Control** (разд. 14.2 на стр. 140) можно ограничить пропускную способность для трафика, проходящего через коммутатор.

14.2 Настройка управления пропускной способностью

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

Рисунок 93 Экран Advanced Application > Bandwidth Control



Поля экрана описаны в следующей таблице.

Таблица 49 Экран Advanced Application > Bandwidth Control

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить управление пропускной способностью на коммутаторе.
Port	В этом поле отображается номер порта.
*	Настройки в этой строке применяются ко всем портам. Эту строку необходимо использовать лишь в том случае, если настройки всех портов должны быть одинаковыми. С помощью этой строки можно сначала назначить общие для всех портов настройки, а затем внести необходимые изменения на уровне отдельного порта. Примечание: Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы активировать ограничения скорости для входящего трафика на этом порту.
Ingress Rate	Укажите максимальную разрешенную пропускную способность в килобитах в секунду (кбит/с) для входящего потока трафика через этот порт. Примечание: Ограничение входящей скорости применяется только к трафику уровня 2.
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.

Таблица 49 Экран Advanced Application > Bandwidth Control (продолжение)

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

15

Контроль широковещательных штормов

15.1 Обзор функции контроля широковещательных штормов

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

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

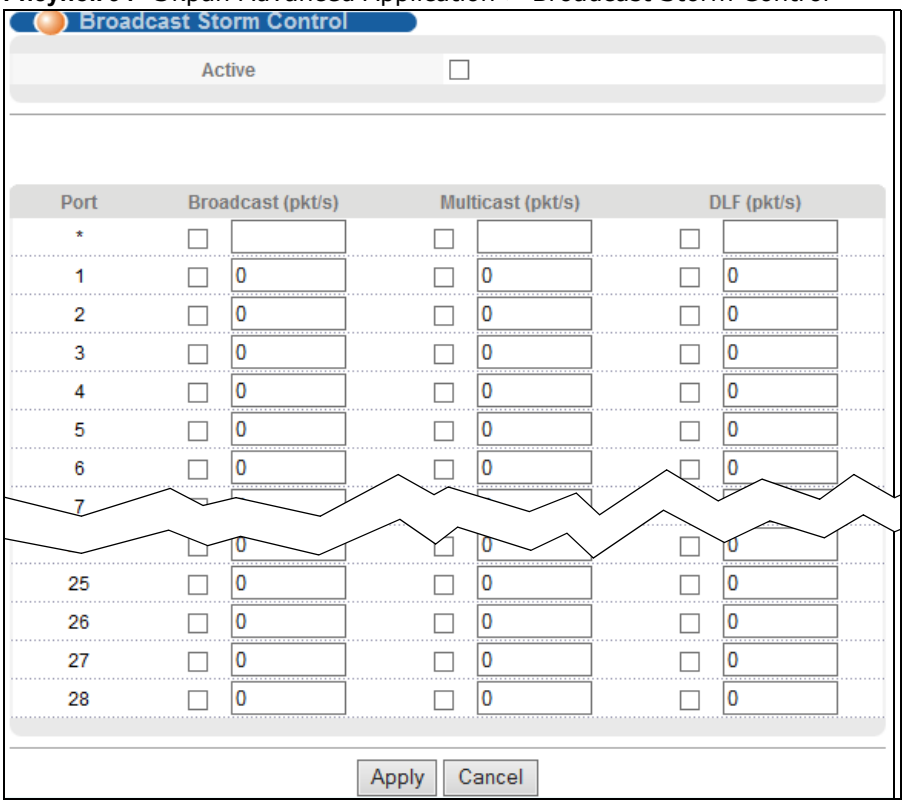
15.1.1 О чем рассказывается в этой главе

С помощью экрана **Broadcast Storm Control** (разд. 15.2 на стр. 143) можно ограничить количество широковещательных, пакетов многоадресной рассылки и DLF-пакетов (destination lookup failure), которые коммутатор принимает в секунду на данных портах.

15.2 Настройка функции контроля широковещательных штормов

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

Рисунок 94 Экран Advanced Application > Broadcast Storm Control



Поля экрана описаны в следующей таблице.

Таблица 50 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 пакетов многоадресной рассылки, 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 сбросить все поля.

16

Зеркальное копирование

16.1 Обзор зеркального копирования

В данной главе описаны экраны настройки 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.

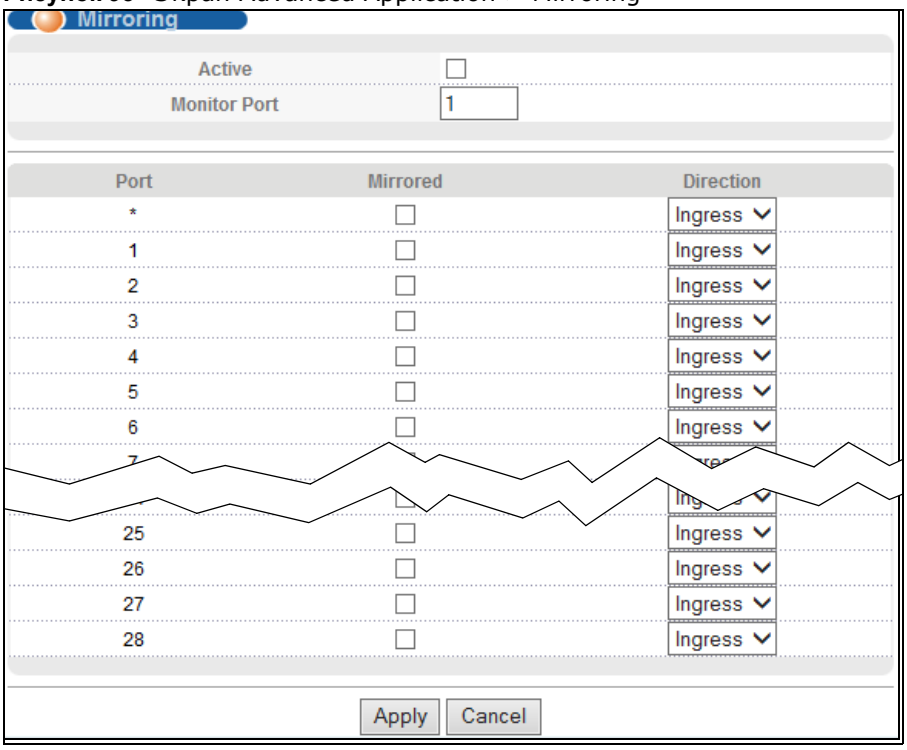
16.1.1 О чем рассказывается в этой главе

С помощью экрана **Mirroring** (разд. 16.2 на стр. 145) можно выбрать контрольный порт и определить поток трафика, который будет копироваться на контрольный порт.

16.2 Настройка зеркального копирования портов

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 95 Экран Advanced Application > Mirroring



Поля экрана описаны в следующей таблице.

Таблица 51 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 сбросить все поля.

17

Агрегация каналов

17.1 Обзор

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

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.

17.1.1 О чем рассказывается в этой главе

- С помощью экрана **Link Aggregation Status** (разд. 17.2 на стр. 148) можно просмотреть список портов, включенных в группу, портов, осуществляющих в данный момент передачу данных как один логический канал в группе портов и т.д.
- С помощью экрана **Link Aggregation Setting** (разд. 17.3 на стр. 150) можно активировать статическую агрегацию каналов.
- С помощью экрана **Link Aggregation Control Protocol** (разд. 17.4 на стр. 151) можно активировать протокол LACP (Link Aggregation Control Protocol, протокол управления агрегацией каналов).

17.1.2 Что необходимо знать

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

Примечание: 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. 17.5.1 на стр. 153.

Динамическая агрегация каналов

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

Стандарт IEEE 802.3ad описывает протокол управления агрегацией каналов (LACP) для динамического создания групп портов и управления ими.

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.

Идентификатор агрегации каналов

Идентификатор агрегации протокола LACP включает в себя[1]:

Таблица 52 Идентификатор агрегации каналов: локальный коммутатор

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

Таблица 53 Идентификатор агрегации каналов: коммутатор-партнер

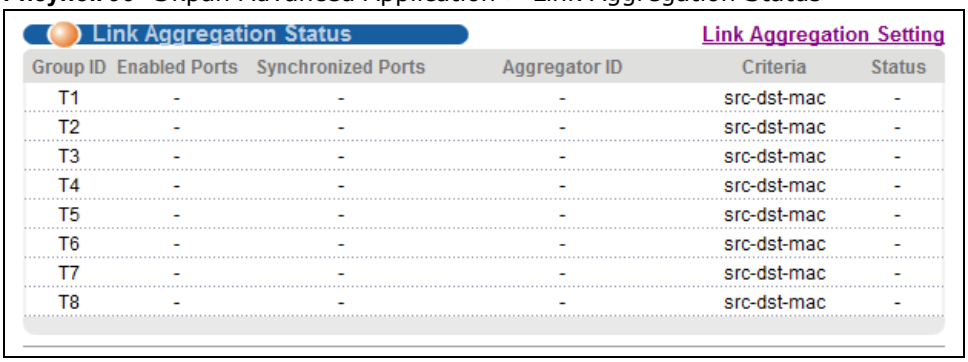
ПРИОРИТЕТ СИСТЕМЫ	MAC-АДРЕС	КЛЮЧ	ПРИОРИТЕТ ПОРТА	НОМЕР ПОРТА
0000	00-00-00-00-00-00	0000	00	0000

17.2 Состояние агрегации каналов

Выберите в навигационной панели **Advanced Application** > **Link Aggregation**. По умолчанию появится экран **Link Aggregation Status**. Дополнительную информацию можно найти в разд. 17.1 на стр. 147.

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

Рисунок 96 Экран Advanced Application > Link Aggregation Status



Поля экрана описаны в следующей таблице.

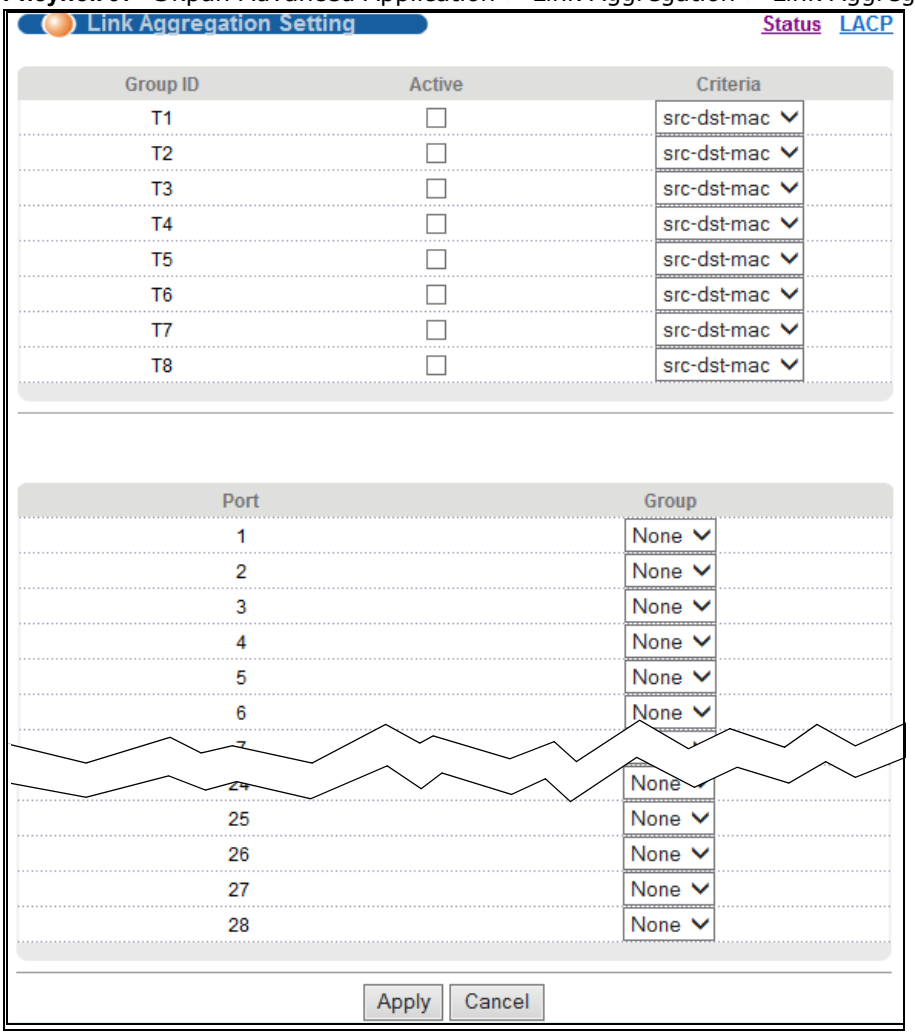
Таблица 54 Экран Advanced Application > Link Aggregation Status

ПОЛЕ	ОПИСАНИЕ
Group ID	В этом поле отображается идентификатор группы, который определяет группу портов, то есть логический канал, объединяющий несколько портов.
Enabled Ports	Порты, настроенные в меню **Link Aggregation** как члены группы портов. Номер порта (или номера портов) отображаются только в том случае, если данная группа портов активирована, и имеется порт, принадлежащий этой группе.
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. «Идентификатор агрегации каналов» на стр. 148. Этот идентификатор отображается только в том случае, если имеется порт, принадлежащий этой группе, и для данной группы активирован протокол LACP.
Criteria	Это поле показывает алгоритм распределения исходящего трафика, используемый данной группой портов. Пакеты, имеющие одинаковый адрес источника и/или одинаковый адрес назначения, направляются по одному каналу в рамках группы портов. опция **src-mac** означает, что коммутатор распределяет трафик исходя из MAC-адреса источника пакета. опция **dst-mac** означает, что коммутатор распределяет трафик исходя из MAC-адреса назначения пакета. опция **src-dst-mac** означает, что коммутатор распределяет трафик по сочетанию MAC-адресов источника и назначения пакета. опция **src-ip** означает, что коммутатор распределяет трафик исходя из IP-адреса источника пакета. опция **dst-ip** означает, что коммутатор распределяет трафик исходя из IP-адреса назначения пакета. опция **src-dst-ip** означает, что коммутатор распределяет трафик по сочетанию IP-адресов источника и назначения пакетов.
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.

17.3 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. 17.1 на стр. 147.

Рисунок 97 Экран Advanced Application > Link Aggregation > Link Aggregation Setting



Поля экрана описаны в следующей таблице.

Таблица 55 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.

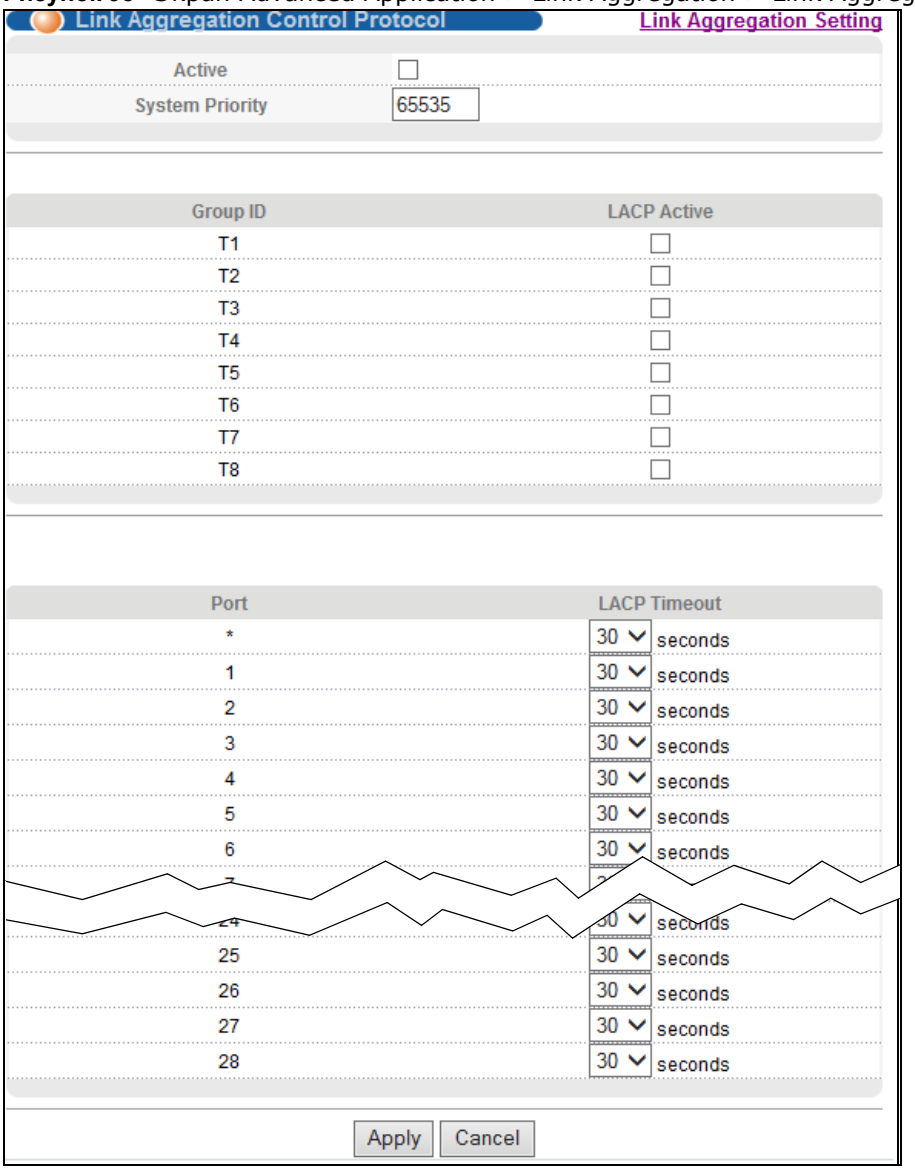
Таблица 55 Экран Advanced Application > Link Aggregation > Link Aggregation Setting

ПОЛЕ	ОПИСАНИЕ
Criteria	Выберите алгоритм распределения исходящего трафика. Пакеты, имеющие одинаковый адрес источника и/или одинаковый адрес назначения, направляются по одному каналу в рамках группы портов. По умолчанию коммутатор использует тип распределения **src-dst-mac**. Если коммутатор находится за маршрутизатором, то MAC-адрес назначения или источника пакета будет изменен. В этом случае необходимо выбрать на коммутатор опцию распределения трафика по IP-адресу, чтобы функция группировки портов работала нормально. Выберите опцию **src-mac**, чтобы распределение трафика осуществлялось по MAC-адресу источника пакета. Выберите опцию **dst-mac**, чтобы распределение трафика осуществлялось по MAC-адресу назначения пакета. Выберите опцию **src-dst-mac**, чтобы распределение трафика осуществлялось по сочетанию MAC-адресов источника и назначения пакетов. Выберите опцию **src-ip**, чтобы распределение трафика осуществлялось по IP-адресу источника пакета. Выберите опцию **dst-ip**, чтобы распределение трафика осуществлялось по IP-адресу назначения пакета. Выберите опцию **src-dst-ip**, чтобы распределение трафика осуществлялось по сочетанию IP-адресов источника и назначения пакетов.
Port	В этом поле отображается номер порта.
Group	Выберите группу портов, которой принадлежит порт. Примечание: Если для определенного порта на коммутатор включена функция безопасности порта и настроены параметры безопасности, то включить такой порт в активную группу портов 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.

17.4 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. «Динамическая агрегация каналов» на стр. 147.

Рисунок 98 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



Поля экрана описаны в следующей таблице.

Таблица 56 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

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

Таблица 56 Экран Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

ПОЛЕ	ОПИСАНИЕ
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.

17.5 Справочная техническая информация

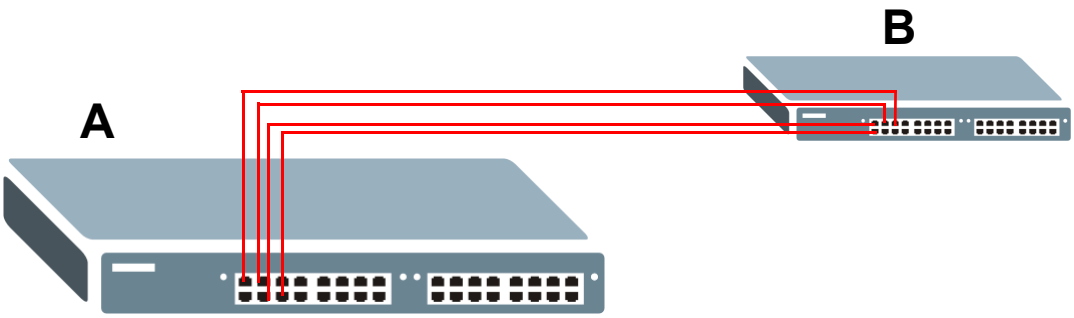
Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

17.5.1 Пример статического группирования портов

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

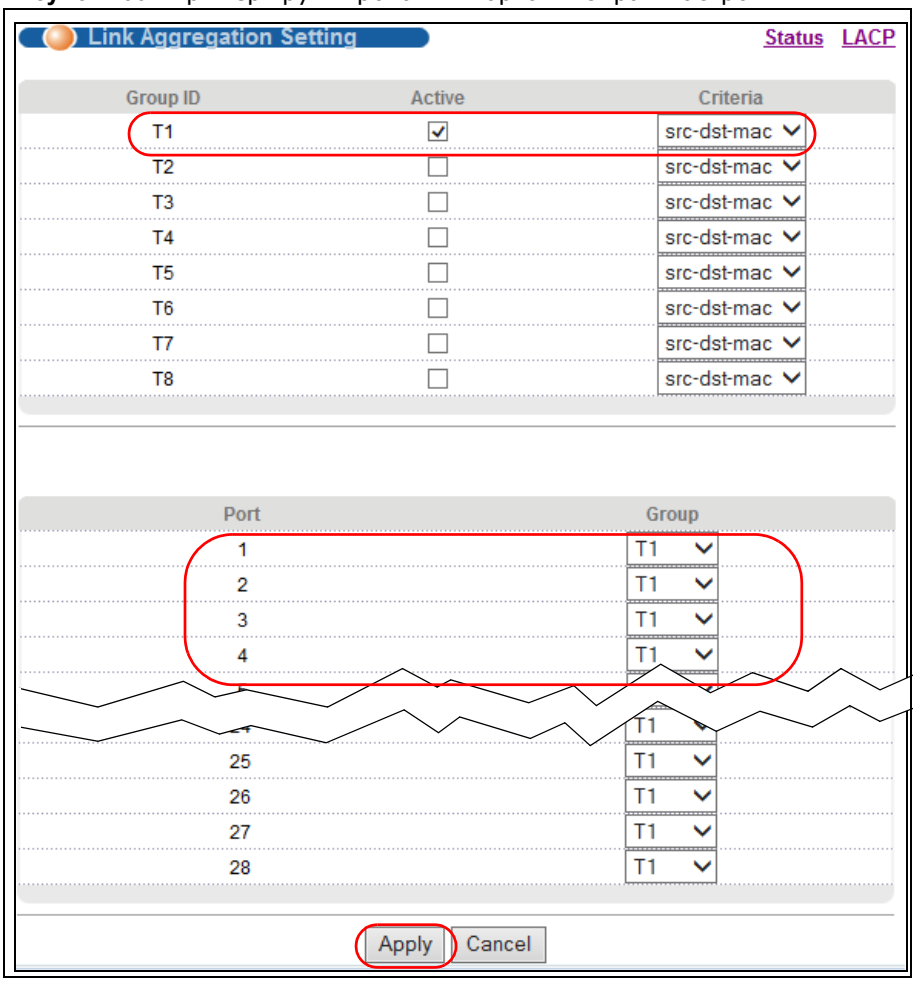
1 **Выполните физические подключения** – подключите все порты, которые должны войти в группу, к одному и тому же пункту назначения. На приведенном ниже рисунке показано подключение портов 2-5 коммутатора **A** к коммутатору **B**.

Рисунок 99 Пример группирования портов – физические подключения



2 **Настройте статическую группу портов** – выберите пункт **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting**. На этом экране активируйте группу портов **T1**, выберите алгоритм распределения трафика, который будет использовать эта группа, и порты, которые следует включить в эту группу, как показано на рисунке ниже. После этого нажмите **Apply**.

Рисунок 100 Пример группирования портов – экран настройки



Процедура настройки группы портов 1 (**T1**) завершена.

18

Аутентификация портов

18.1 Обзор аутентификации портов

В этой главе описан метод аутентификации IEEE 802.1x.

Механизм аутентификации портов позволяет проверять права доступа клиентов к портам коммутатора с использованием внешнего сервера (сервера аутентификации). Данный коммутатор поддерживает следующий метод аутентификации портов:

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

18.1.1 О чем рассказывается в этой главе

- С помощью экрана **Port Authentication** (разд. 18.2 на стр. 156) можно проверить, активирована ли аутентификация портов IEEE 802.1x.
- С помощью экрана **802.1x** (разд. 18.3 на стр. 156) можно активировать функцию безопасности IEEE 802.1x.

18.1.2 Что необходимо знать

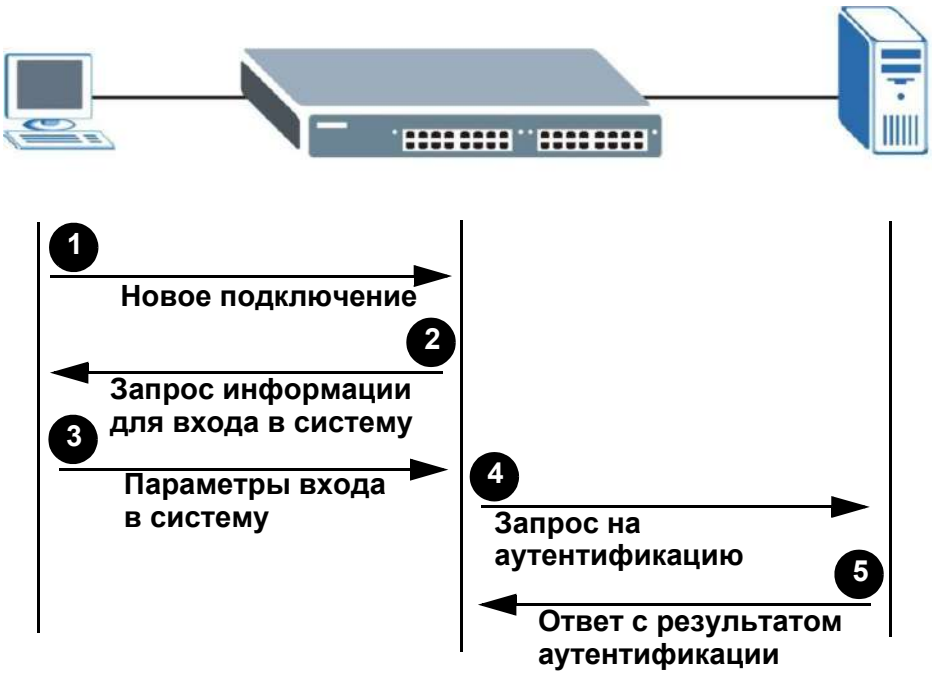
Проверка прав пользователя при аутентификации по схеме IEEE 802.1x осуществляется с использованием протокола RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139). Дополнительную информацию о настройках сервера RADIUS можно найти в разд. «RADIUS и TACACS+» на стр. 206.

Аутентификация на основе IEEE 802.1x

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

2. На момент написания данного руководства не все операционные системы поддерживают стандарт IEEE 802.1x. Обратитесь к документации по операционной системе. Если операционная система не поддерживает стандарт 802.1x, может потребоваться установка программного обеспечения клиента 802.1x.

Рисунок 101 Процесс аутентификации на основе IEEE 802.1x



18.2 Настройка аутентификации портов

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

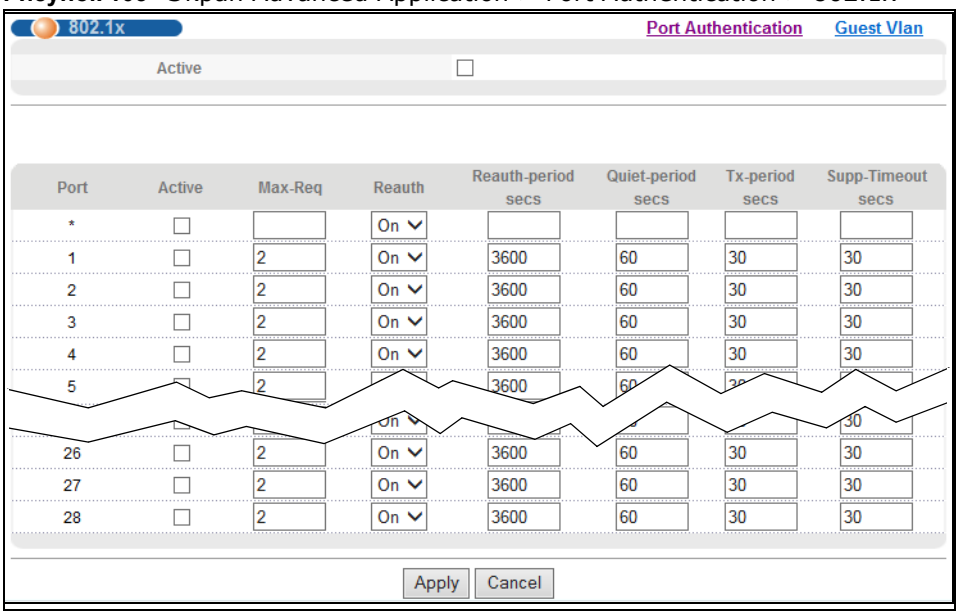
Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Advanced Application** > **Port Authentication**.

Рисунок 102 Экран Advanced Application > Port Authentication

18.3 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 открыть экран настроек, изображенный на рисунке ниже.

Рисунок 103 Экран Advanced Application > Port Authentication > 802.1x



Поля экрана описаны в следующей таблице.

Таблица 57 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.
Max-Req	Укажите, сколько попыток аутентификации клиентов должен совершить коммутатор прежде, чем отправить порты, от которых не поступил отклик, в гостевую сеть VLAN. По умолчанию значение этого поля равно 2. Это означает, что коммутатор будет пытаться аутентифицировать клиента дважды. То есть если клиент не ответил на первый запрос аутентификации, коммутатор отправит еще один запрос. Если клиент не ответит и на второй запрос, то коммутатор отправит клиента в гостевую сеть VLAN. Для прохождения повторной аутентификации на коммутаторе клиенту нужно будет послать новый запрос.
Reauth	Укажите, требуется ли пользователю периодически вводить заново свое пользовательское имя и пароль, чтобы оставаться подключенным к порту.
Reauth-period secs	Укажите период времени, по истечении которого пользователю потребуется заново ввести свое пользовательское имя и пароль, чтобы оставаться подключенным к порту.

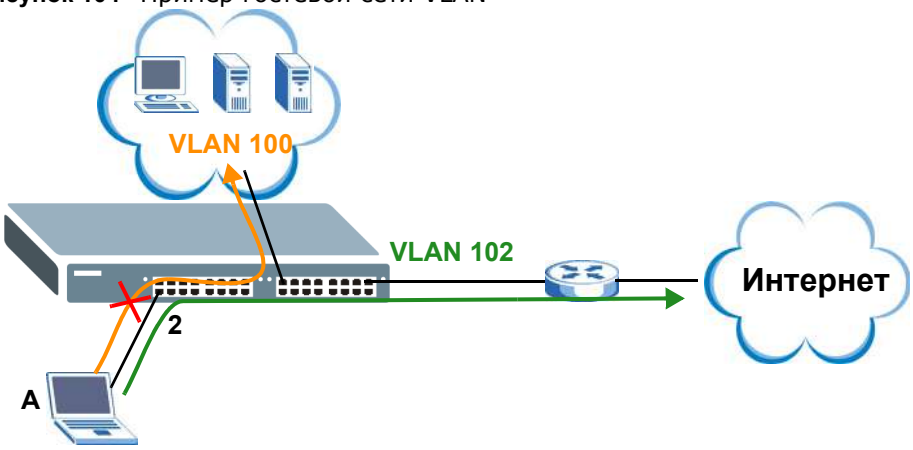
Таблица 57 Экран Advanced Application > Port Authentication > 802.1x (продолжение)

ПОЛЕ	ОПИСАНИЕ
Quiet-period secs	Укажите, сколько секунд порт остается в состоянии HELD и отвергает новые запросы на аутентификацию от подключенного клиента после неудачной попытки обмена аутентификационными сообщениями.
Tx-period secs	Укажите период времени в секундах, в течение которого коммутатор ожидает ответа клиента, прежде чем повторно отправить клиенту запрос на идентификацию.
Supp-Timeout secs	Укажите период времени в секундах, в течение которого коммутатор ожидает ответа клиента на запрос вызова, прежде чем отправить повторный запрос.
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.

18.3.1 Экран Guest VLAN

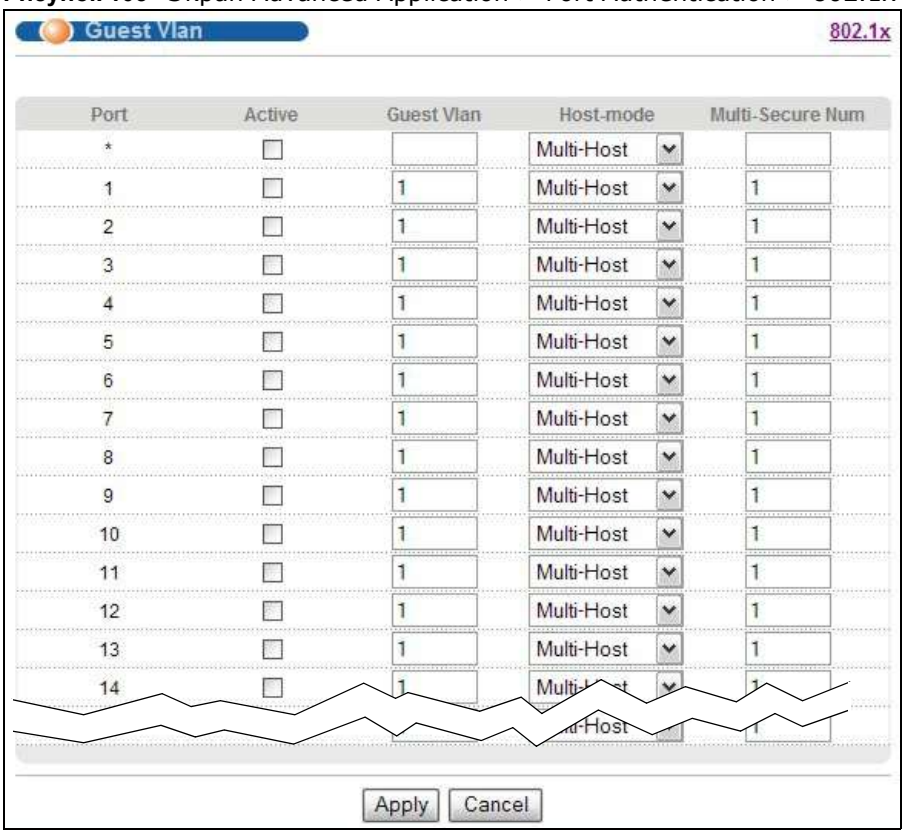
Если на коммутаторе и его портах включена функция аутентификации 802.1x, то коммутатор запрещает клиентам, предоставляющим некорректные учетные данные, доступ через указанные порты. Возможности коммутатора позволяют выбрать одну сеть VLAN в качестве гостевой. Если включить функцию гостевой сети VLAN (в данном примере – сети **102**) на определенном порту (в данном примере – порту **2**), то определенный пользователь (в данном примере – **пользователь A**), который не поддерживает стандарт IEEE 802.1x с или не может указать правильные имя пользователя и пароль, все равно сможет получить доступ к коммутатору через этот порт, но будет направлен в гостевую сеть VLAN. То есть пользователи, не прошедшие аутентификацию, смогут получить доступ к ограниченному количеству сетевых ресурсов в той же гостевой сети VLAN, такой, как сеть Интернет. Набор прав, назначенных гостевой сети VLAN, зависит от того, какие параметры сетевой администратор задаст для коммутаторов или маршрутизаторов при описании функции гостевой сети.

Рисунок 104 Пример гостевой сети VLAN



С помощью этого экрана можно активировать гостевую сеть VLAN и назначить ее определенному порту. На экране **Port Authentication > 802.1x** нажмите **Guest Vlan**, чтобы открыть экран настроек, изображенный на рисунке ниже.

Рисунок 105 Экран Advanced Application > Port Authentication > 802.1x > Guest VLAN



Поля экрана описаны в следующей таблице.

Таблица 58 Экран Advanced Application > Port Authentication > 802.1x > Guest VLAN

ПОЛЕ	ОПИСАНИЕ
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. Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить функцию гостевой сети VLAN для данного порта. Клиенты, которые не смогли пройти аутентификацию, попадают в гостевую сеть VLAN и могут получать ограниченный набор услуг.
Guest Vlan	Гостевая сеть VLAN – это предварительно созданная на коммутаторе сеть VLAN, которая позволяет пользователям, не прошедшим аутентификацию, получить ограниченный доступ к сетевым ресурсам через коммутатор. Кроме того, необходимо включить аутентификацию IEEE 802.1x на коммутаторе и ассоциированных портах. Укажите число, которое идентифицирует гостевую сеть VLAN. Удостоверьтесь, что эта сеть VLAN распознается в сети.

Таблица 58 Экран Advanced Application > Port Authentication > 802.1x > Guest VLAN

ПОЛЕ	ОПИСАНИЕ
Host-mode	Укажите, каким образом коммутатор аутентифицирует пользователей в том случае, если два и более пользователей подключаются к данному порту (используя концентратор). При выборе опции **Multi-Host** устройство будет выполнять аутентификацию только первого пользователя, подключившегося к данному порту. Если первый пользователь указывает правильные данные для входа, то всем последующим пользователям разрешается доступ к этому порту без аутентификации. Если первый пользователь указывает неверные данные для входа, то все пользователи будут направлены в гостевую сеть VLAN. Если первый пользователь, прошедший аутентификацию, выполняет выход из системы или отключается от данного порта, то устройство блокирует остальных пользователей до тех пор, пока кто-нибудь из них не пройдет аутентификацию снова. При выборе опции **Multi-Secure** устройство будет выполнять аутентификацию каждого пользователя, который подключается к данному порту.
Multi-Secure Num	Если в поле **Host-mode** выбрана опция **Multi-Secure**, то в этом поле необходимо указать максимальное количество пользователей, которое коммутатор будет аутентифицировать на этом порту.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

19

Средства безопасности портов

19.1 Обзор средств безопасности портов

В данной главе описана настройка функций 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.

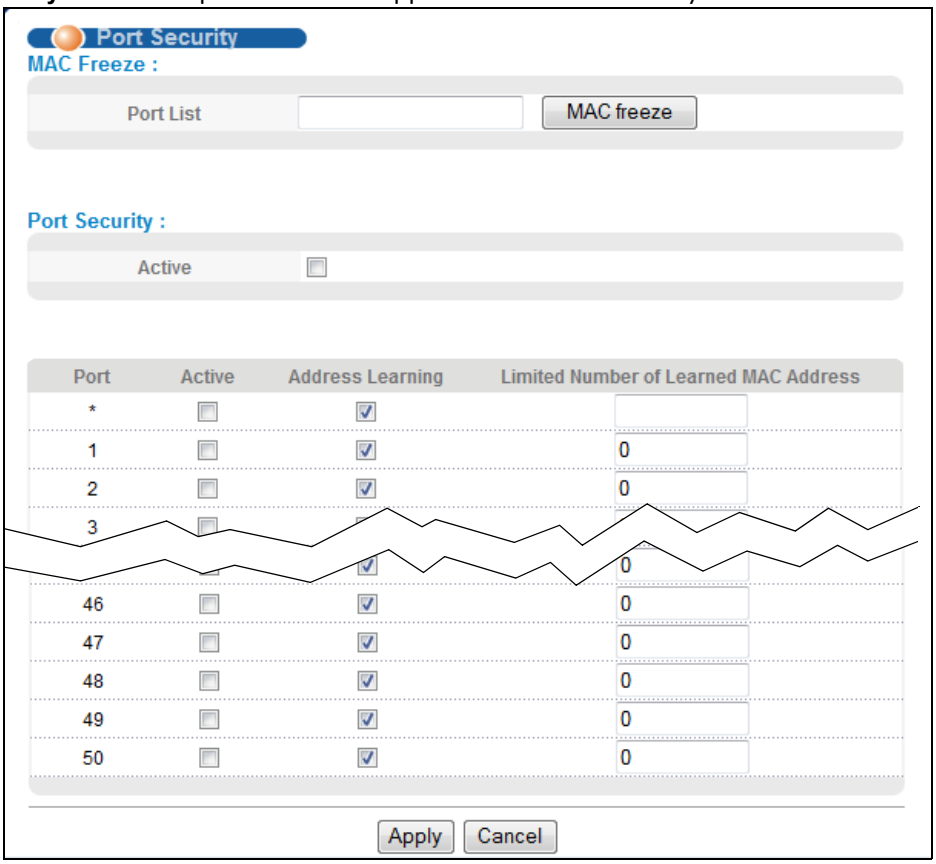
19.1.1 О чем рассказывается в этой главе

С помощью экрана **Port Security** (разд. 19.2 на стр. 161) можно включить функцию безопасности портов и отключить запоминание MAC-адресов. Кроме того, здесь можно включить функцию безопасности порта для определенного порта.

19.2 Настройка средств безопасности портов

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

Рисунок 106 Экран Advanced Application > Port Security



Поля экрана описаны в следующей таблице.

Таблица 59 Экран Advanced Application > Port Security

ПОЛЕ	ОПИСАНИЕ
Port List	Укажите порты (разделенные запятой), для которых необходимо включить функцию безопасности портов и отключить запоминание MAC-адресов. После нажатия **MAC freeze** все ранее запомненные MAC-адреса для указанных портов станут статическими и будут отображаться на экране **Static MAC Forwarding**.
MAC freeze	Нажмите **MAC freeze**, чтобы коммутатор автоматически установил переключатели **Active** и снял выделение с переключателей **Address Learning** только для портов, указанных в списке **Port list**.
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.

Таблица 59 Экран Advanced Application > Port Security (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.
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.

20

Классификация

20.1 Обзор

В этой главе описывается настройка на коммутаторе функции классификации пакетов. Кроме того, в ней рассматриваются концепции управления качеством обслуживания (Quality of Service, QoS) и классификатора в том виде, в котором они реализованы на коммутаторе.

20.1.1 О чем рассказывается в этой главе

С помощью экрана **Classifier** (разд. 20.2 на стр. 165) можно создать классификаторы и просмотреть сводную информацию о конфигурации классификаторов. После настройки классификации можно определить действия (политики), применяемые к отвечающим правилам трафику.

20.1.2 Что необходимо знать

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 создать классификатор, который будет отбирать в отдельный поток трафик порта определенного протокола (например, Telnet).

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

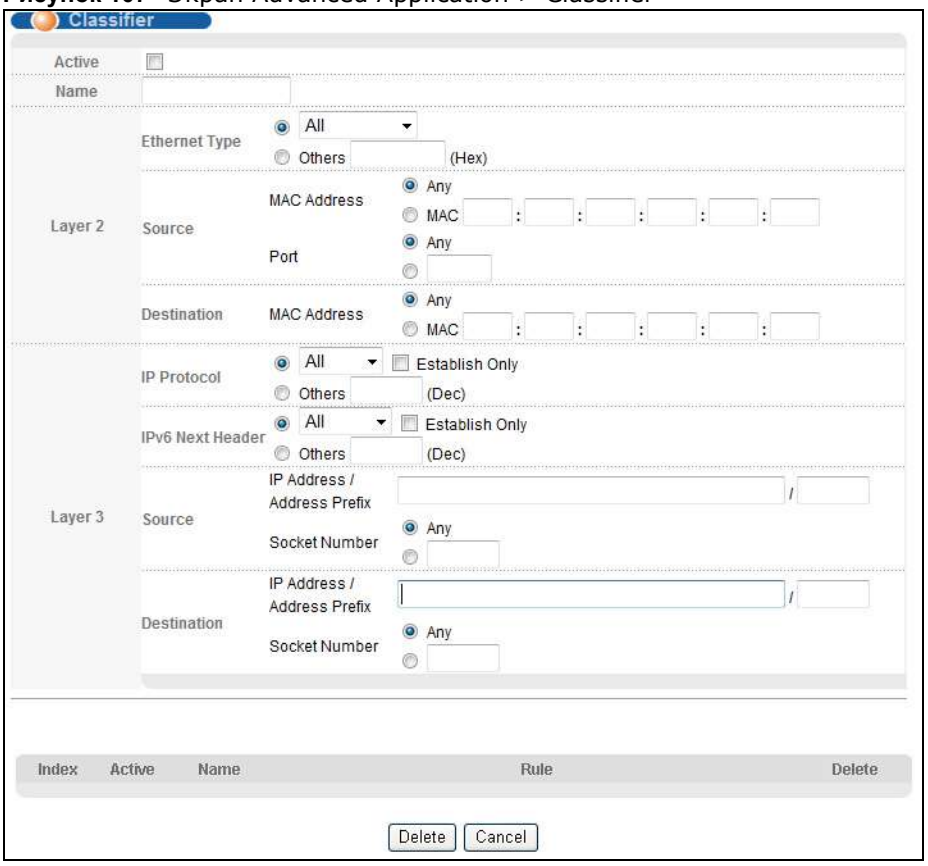
1. Настройка классификации для сортировки трафика между различными потоками.
2. Настройка правил политики, определяющих действия над классифицированными потоками трафика (настройка правил политики описана в гл. 21 на стр. 170).

20.2 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. 21 на стр. 170.

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

Рисунок 107 Экран Advanced Application > Classifier



Поля экрана описаны в следующей таблице.

Таблица 60 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.
Layer 2 В этом разделе приводятся поля, позволяющие настроить классификацию на уровне 2.	
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. 62 на стр. 167.
Source	

Таблица 60 Экран Advanced Application > Classifier (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.	
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. 63 на стр. 168. Для типа протокола **TCP** можно установить переключатель **Establish Only**. В этом случае коммутатор будет отбирать только пакеты, отправляемые для установления TCP-соединений.
IPv6 Next Header	Выберите тип протокола IPv6 или опцию **Other** и введите 8-разрядное значение поля Next Header для пакета IPv6. Поле Next Header аналогично полю Protocol для протокола IPv4 Protocol. Значение протокола для IPv6 выбирается из диапазона от 1 до 255. Для типа протокола **TCP** можно установить переключатель **Establish Only**. Это означает, что коммутатор будет идентифицировать пакеты, которые инициируют или подтверждают (устанавливают) TCP-соединения.
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. Маска подсети может быть представлена в виде 32-битного числа. Например, маску подсети «255.255.255.0» можно записать в двоичном виде как «11111111.11111111.11111111.00000000», и для нее количество единичных битов будет равно 24.
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. Дополнительную информацию можно найти в табл. 64 на стр. 168.
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.
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. Дополнительную информацию можно найти в табл. 64 на стр. 168.

Таблица 60 Экран Advanced Application > Classifier (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	Нажмите **Clear**, чтобы вернуться к заводским настройкам.

20.2.1 Просмотр и изменение настроек 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**.

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

Рисунок 108 Экран Advanced Application > Classifier: итоговая таблица

Поля экрана описаны в следующей таблице.

Таблица 61 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.
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 62 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

Таблица 62 Распространенные типы Ethernet и номера протоколов

ТИП ETHERNET	НОМЕР ПРОТОКОЛА
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Протоколом IP предусмотрено поле, называемое «Protocol», в котором указывается протокол следующего уровня. Некоторые наиболее распространенные типы протоколов и соответствующие номера протоколов приводятся в следующей таблице. Полный список можно найти по адресу: http://www.iana.org/assignments/protocol-numbers.

Таблица 63 Распространенные типы протокола IP и номера протоколов

ТИП ПРОТОКОЛА	НОМЕР ПРОТОКОЛА
ICMP	1
TCP	6
UDP	17
EGP	8
L2TP	115

Наиболее часто используемые номера портов TCP и UDP приводятся в следующей таблице:

Таблица 64 Распространенные номера портов TCP и UDP

ИМЯ ПРОТОКОЛА	НОМЕР ПОРТА TCP/UDP
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110

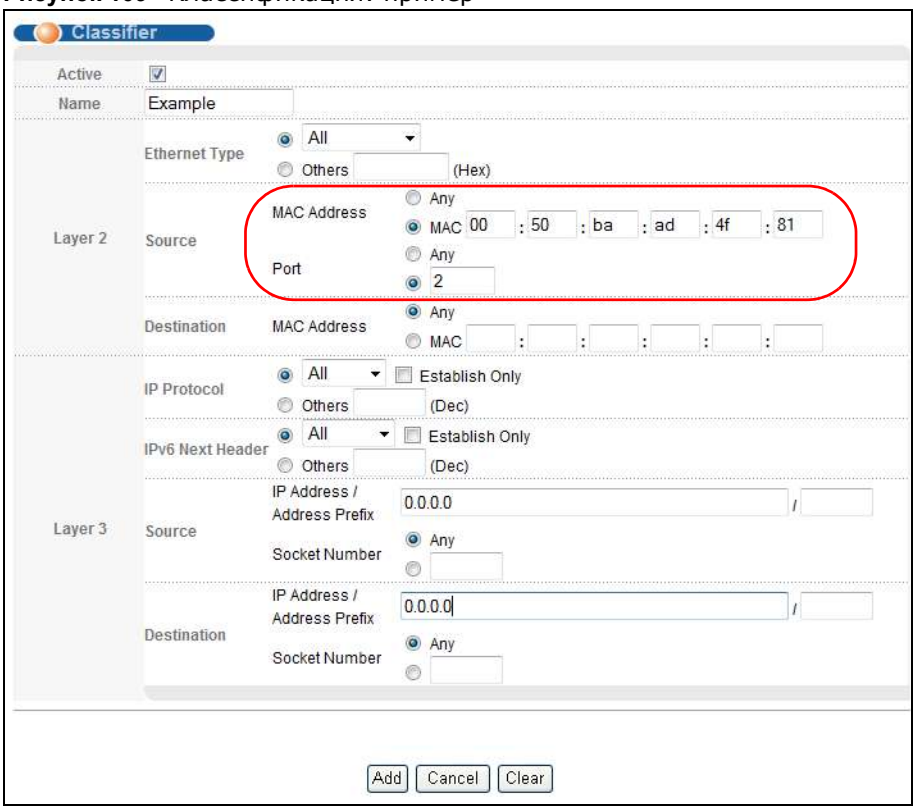
Информацию о часто используемых номерах портов можно найти в прил. A на стр. 385.

20.3 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 109 Классификация: пример



21

Правила политики

21.1 Обзор правил политики

В данной главе описана настройка правил политики.

С помощью классификации трафик делится на потоки в соответствии с установленными критериями (дополнительную информацию можно найти в гл. 20 на стр. 164). Правила политики обеспечивают надлежащую обработку потоков трафика в сети.

21.1.1 О чем рассказывается в этой главе

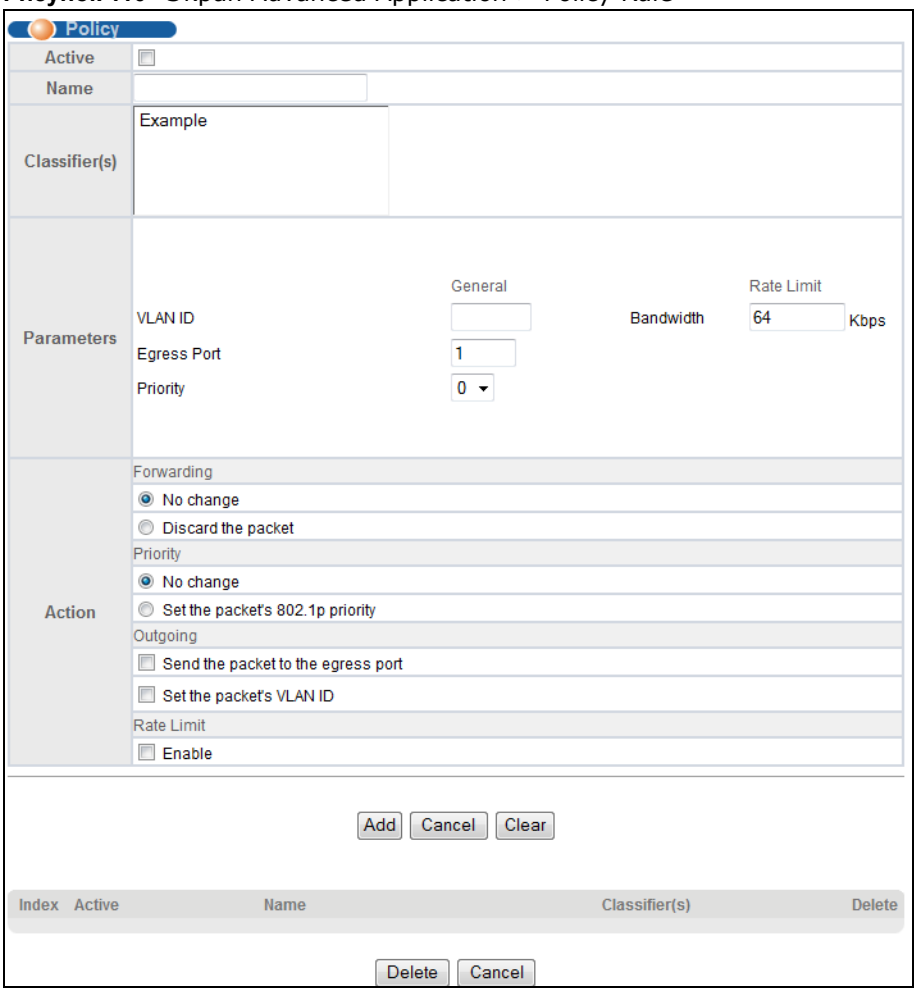
С помощью экрана **Policy** (разд. 21.2 на стр. 170) можно активировать определенную политику и отобразить активные классификаторы, созданные при помощи экрана **Classifier**.

21.2 Настройка правил политики

Прежде всего необходимо настроить классификацию на экране **Classifier**. Дополнительную информацию можно найти в разд. 20.2 на стр. 165.

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

Рисунок 110 Экран Advanced Application > Policy Rule



Поля экрана описаны в следующей таблице.

Таблица 65 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].
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.
Priority	Укажите уровень приоритета.

Таблица 65 Экран Advanced Application > Policy Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Rate Limit	Имеется возможность настроить желаемую пропускную способность, выделяемую для потока трафика. Трафик, поступающий со скоростью, превышающий максимальную выделенную пропускную способность (в случаях перегрузки сети), отбрасывается.
Bandwidth	Укажите пропускную способность в килобитах в секунду (кбит/с). Введите значение в диапазоне от 64 до 1000000.
Action Укажите действия, выполняемые коммутатором над соответствующим классифицированным потоком трафика. Примечание: Для данного правила политики можно указать только одно действие (пару). Для того, чтобы коммутатор выполнял несколько действий в отношении одного и того же потока трафика, необходимо создать несколько классификаторов с одинаковыми критериями и применить различные правила политик. К примеру, у вас есть несколько классификаторов, которые идентифицируют один и тот же поток трафика, и для каждого из них создано собственное правило политики. Если действия политик конфликтуют друг с другом (**Discard the packet**, **Send the packet to the egress port** и **Rate Limit**), то коммутатор применяют только правила политик с действиями **Discard the packet** и **Send the packet to the egress port** в зависимости от имен классификаторов. Чем длиннее имя классификатора, тем выше его приоритет. Если имена двух классификаторов имеют одинаковую длину, то приоритет классификаторов будет зависеть от регистра символа. Буквы в нижнем регистре (например, a и b) имеют более высокий приоритет по сравнению с заглавными буквами (например, A и B) в имени классификатора. Например, классификаторы с именами «class 2», «class a» или «class B» имеют более высокий приоритет по отношению к классификаторам с именами «class 1» или «class A». Предположим, у вас имеется два классификатора (Class 1 и Class 2), которые идентифицируют весь трафик, приходящий с MAC-адреса 11:22:33:44:55:66 через порт 3. Если Политика 1 применяется к Классу 1 с действием «Отбрасывать пакеты», а Политика 2 применяется к Классу 2 с действием «Пересылать пакеты на исходящий порт», то коммутатор будет выполнять пересылку пакетов. Если Политика 1 применяется к Классу 1 с действием «Отбрасывать пакеты», а Политика 2 применяется к Классу 2 с действием «Включить ограничение пропускной способности», то коммутатор будет сразу отбрасывать пакеты. Если Политика 1 применяется к Классу 1 с действием «Пересылать пакеты на исходящий порт», а Политика 2 применяется к Классу 2 с действием «Включить ограничение пропускной способности», то коммутатор будет выполнять пересылку пакетов.	
Forwarding	Выберите **No change** для пересылки пакетов. Выберите **Discard the packet** для отбрасывания пакетов.
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.
Outgoing	Выберите **Send the packet to the egress port**, чтобы передать пакет на исходящий порт. Выберите **Set the packet's VLAN ID**, чтобы выполнить замену идентификатора сети VLAN на значение, указанное в поле **VLAN ID**.
Rate Limit	Выберите **Enable**, чтобы активировать ограничение пропускной способности для потоков трафика.
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.

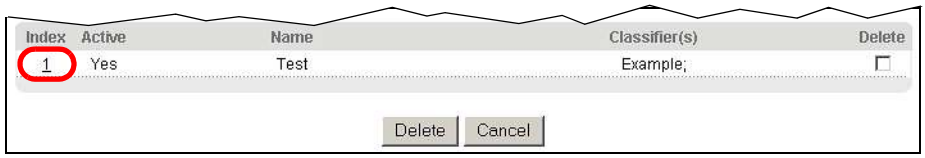
Таблица 65 Экран Advanced Application > Policy Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Cancel	Нажмите **Cancel**, чтобы сбросить поля к предыдущим значениям.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
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.
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.
Delete	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.
Cancel	В этом поле отображается номер политики. Нажмите на этот номер, чтобы отредактировать политику.

21.2.1 Просмотр и изменение 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**.

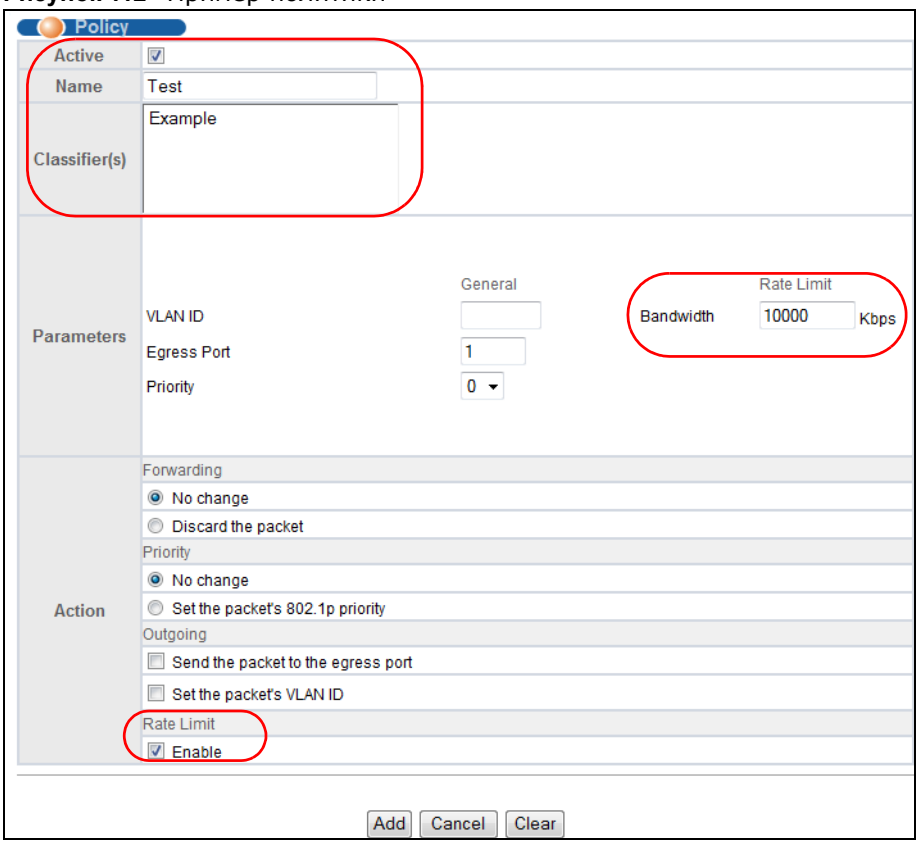
Рисунок 111 Экран Advanced Application > Policy Rule: итоговая таблица



21.3 Пример политики

На приведенном ниже рисунке показан пример экрана **Policy**, на котором настроена политика ограничения пропускной способности для потока трафика, классифицированного с использованием классификатора **Example** (см. разд. 20.3 на стр. 168).

Рисунок 112 Пример политики



22

Метод организации очередей

22.1 Обзор методов организации очередей

В данной главе описаны поддерживаемые методы 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**.

22.1.1 О чем рассказывается в этой главе

С помощью экрана **Queueing Method** (разд. 22.2 на стр. 176) можно установить приоритеты для очередей коммутатор. Это позволит распределить пропускную способность между различными очередями трафика.

22.1.2 Что необходимо знать

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.

Строгая очередь приоритетов (SPQ)

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

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). 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.

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.

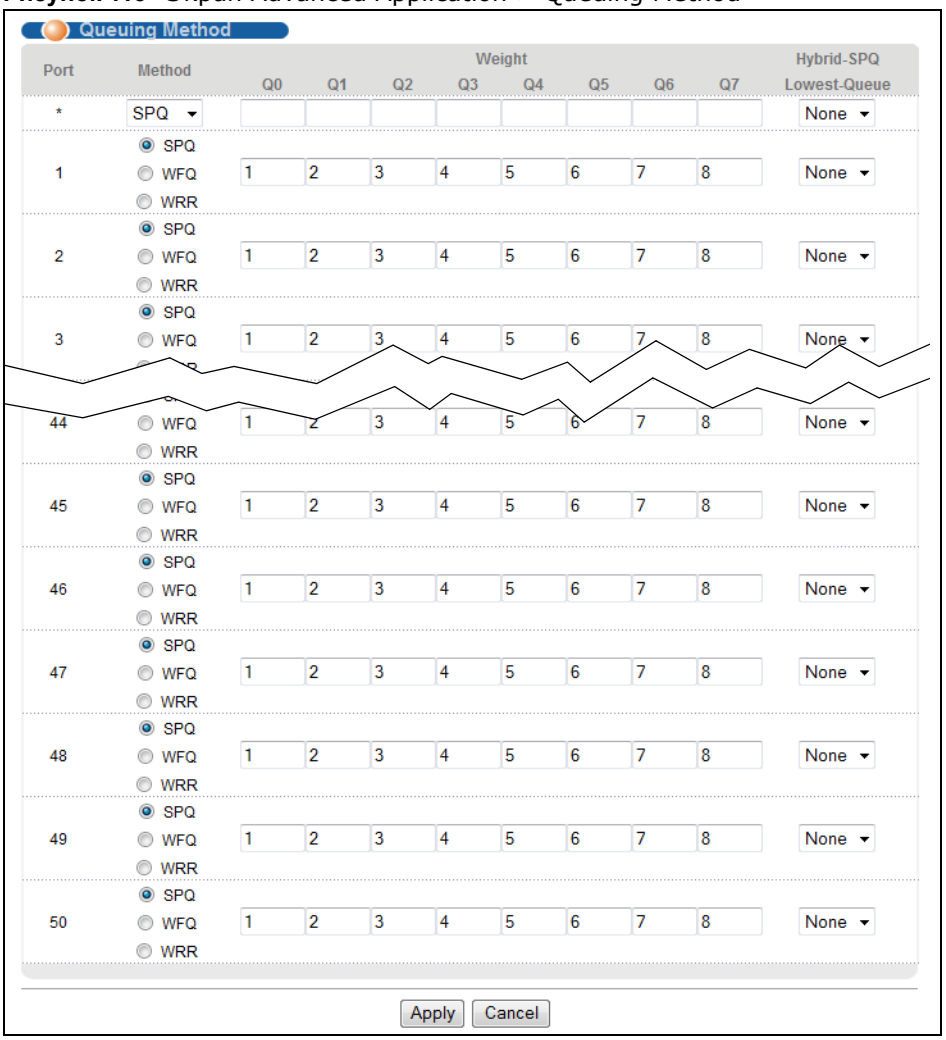
Алгоритм взвешенного циклического обслуживания (WRR) использует тот же метод, что и простое циклическое обслуживание, но он обрабатывает очереди на основе их уровня приоритета и веса очереди (число, которое вводится в поле **Weight**), а не фиксированной доли пропускной способности. Алгоритм WRR запускается 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.

22.2 Настройка метода организации очередей

С помощью экрана можно задать приоритеты для очередей коммутатора. Это позволит распределить пропускную способность между различными очередями трафика.

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

Рисунок 113 Экран Advanced Application > Queuing Method



Поля экрана описаны в следующей таблице.

Таблица 66 Экран Advanced Application > Queuing Method

ПОЛЕ	ОПИСАНИЕ
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.

Таблица 66 Экран Advanced Application > Queuing Method (продолжение)

ПОЛЕ	ОПИСАНИЕ
Method	Выберите одну из опций **SPQ** (Strictly Priority Queuing), **WFQ** (Weighted Fair Queuing) или **WRR** (Weighted Round Robin). 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.
Weight	В случае выбора метода **WFQ** или **WRR** в этих полях указываются веса очередей. Пропускная способность распределяется между очередями в зависимости от их веса.
Hybrid-SPQ Lowest-Queue	Данное поле используется только в случае выбора **WFQ** или **WRR**. Выберите очередь (от **Q0** до **Q7**), начиная с которой коммутатор будет использовать для данного порта алгоритм **SPQ**. Например, если выбрать **Q5**, то коммутатор будет обслуживать трафик в очередях **Q5**, **Q6** и **Q7** с использованием алгоритма **SPQ**. Выберите в этом поле опцию **None**, чтобы в любом случае использовать для данного порта алгоритмы **WFQ** или **WRR**.
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

Многоадресная рассылка

23.1 Обзор многоадресной рассылки

В данной главе описана настройка различных функций многоадресной рассылки.

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). Многоадресная рассылка (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 многоадресной рассылки. 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.

23.1.1 О чем рассказывается в этой главе

- С помощью экрана **Multicast Setup** (разд. 23.2 на стр. 183) можно активировать функцию отслеживания IGMP, при котором трафик группы многоадресной рассылки пересылается только на порты, входящие в соответствующую группу.
- С помощью экрана **IPv4 Multicast Status** (разд. 23.3 на стр. 184) можно просмотреть информацию о группах многоадресной рассылки.
- С помощью экрана **IPv6 Multicast Status** (разд. 23.5 на стр. 190) можно просмотреть информацию о группах многоадресной рассылки.
- С помощью экрана **MLD Snooping-proxy** (разд. 23.5.1 на стр. 190) можно включить на данном агрегирующем порту сбор и передачу сведений об изменениях групп на подключенный маршрутизатор многоадресной рассылки и пересылку сообщений MLD на другие агрегирующие порты. Более подробную информацию о многоадресной рассылке можно найти в разд. 23.1 на стр. 179
- С помощью экранов **MVR** (разд. 23.6 на стр. 198) можно создать сети VLAN многоадресной рассылки и выбрать для каждой из таких сетей порты (или порты) приемников и порт источника.

23.1.2 Что необходимо знать

Ознакомьтесь с приведенной ниже информацией о многоадресной рассылке, которая поможет в работе с экранами, описанными в этой главе.

IP-адреса многоадресной рассылки

В IPv4 адрес многоадресной рассылки позволяет устройству отправлять пакеты определенной группе хостов (группе многоадресной рассылки) в отличной подсети. IP-адрес многоадресной

рассылки определяет группу получателей трафика, а не конкретное получающее устройство. В качестве IP-адресов многоадресной рассылки используются IP-адреса класса D (от 224.0.0.0 до 239.255.255.255). Некоторые IP-адреса многоадресной рассылки зарезервированы IANA для особых целей (более подробную информацию можно найти на сайте IANA).

Отслеживание многоадресного трафика IGMP

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

Данный коммутатор направляет многоадресный трафик, предназначенный для групп многоадресной рассылки (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 многоадресного трафика, проходящего через коммутатор.

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 многоадресной рассылки 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 многоадресной рассылки только в таких виртуальных локальных сетях VLAN, которые были явным образом добавлены как VLAN отслеживания многоадресного трафика IGMP.

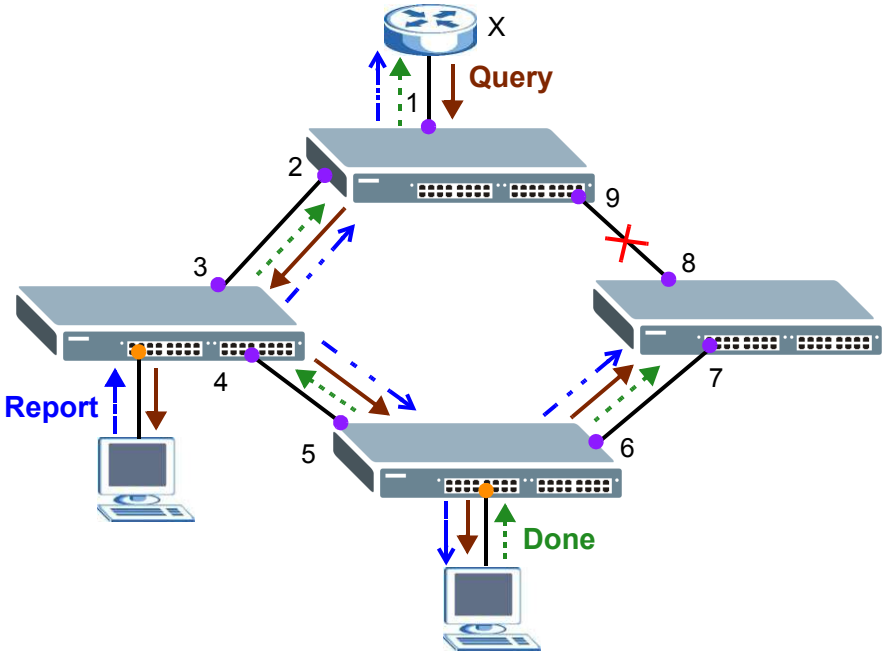
Прокси отслеживания MLD

Прокси отслеживания MLD – это внутрифирменная функция ZyXEL. Прокси MLD IPv6 допускает наличие только одного агрегирующего интерфейса на коммутаторе, а прокси отслеживания MLD поддерживает два и более агрегирующих портов на коммутаторе. Агрегирующий порт прокси отслеживания MLD может передавать сведения об изменениях групп на подключенный коммутатор многоадресной рассылки и пересылать сообщения MLD на другие агрегирующие порты. Этот механизм бывает особенно полезен в сетях, использующих протокол STP для организации резервных соединений между коммутаторами и, кроме того, он выполняет функции отслеживания и проксирования MLD. Прокси отслеживания MLD, как и прокси MLD, позволяет минимизировать количество управляющих сообщений MLD и тем самым повысить производительность сети.

В случае использования прокси отслеживания MLD, если один агрегирующий порт запомнен через механизм отслеживания, то все остальные агрегирующие порты на том же устройстве

будут добавлены в ту же группу. Если один агрегирующий порт запрашивает выход из группы, то все остальные агрегирующие порты на том же устройстве также будут удалены из группы.

В приведенном ниже примере использования прокси отслеживания MLD все подключенные агрегирующие порты (1 ~7) рассматриваются как один интерфейс. STP блокирует соединение между портами 8 и 9, чтобы разорвать петлю. При поступлении запроса от маршрутизатора (**X**), либо сообщения MLD Done или Report с любого агрегирующего порта, коммутатор перешлет это сообщение в широковещательном режиме на все подключенные агрегирующие порты.



Сообщения MLD

Маршрутизатор или коммутатор многоадресной рассылки периодически отправляет общие запросы хостам MLD для актуализации таблицы многоадресной рассылки. Если хост MLD хочет присоединиться к группе многоадресной рассылки, он отправляет сообщение MLD Report для данного адреса.

Сообщение MLD Done является аналогом сообщения IGMP Leave. Если хост MLD хочет выйти из группы многоадресной рассылки, он может отправить сообщение Done маршрутизатору или коммутатору. Если в качестве режима выхода из группы выбрана опция, отличная от **Immediate**, маршрутизатор или коммутатор отправляет сообщение, адресованное определенной группе, на тот порт, на котором было получено сообщение Done, чтобы определить, должны ли другие устройства, подключенные к этому порту, оставаться в этой группе.

Обзор MVR

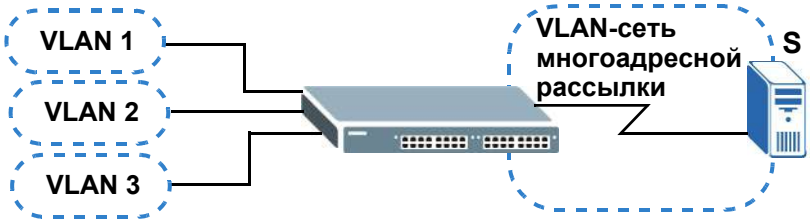
Механизм регистрации VLAN-сети многоадресной рассылки (Multicast VLAN Registration, MVR) предназначен для случаев, когда требуется передавать многоадресный трафик через Ethernet-сеть провайдера услуг, имеющую конфигурацию кольца (например, для приложений «мультимедиа по требованию» – MoD).

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

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

Пример сети показан на следующем рисунке. Информация о сети VLAN абонента (**1**, **2** и **3**) сокрыта от потокового мультимедийного сервера, **S**. Кроме того, информация о сети VLAN многоадресной рассылки видна только коммутатору и **S**.

Рисунок 114 Пример сети с поддержкой MVR



Типы портов MVR

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

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 многоадресной рассылки (такие как маршрутизаторы или серверы многоадресной рассылки) во VLAN-сети многоадресной рассылки. Благодаря этому устройства многоадресной рассылки могут обновлять таблицу пересылки многоадресного трафика и включать или отключать пересылку многоадресного трафика на порты приемников.

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

Как работает механизм MVR

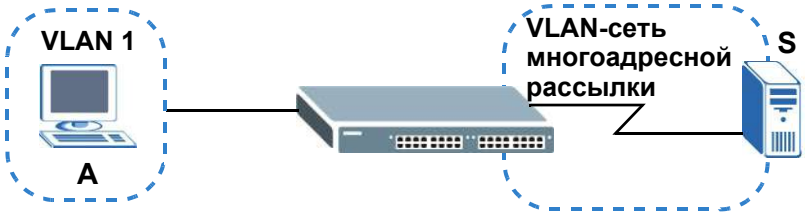
Приведенный ниже рисунок иллюстрирует пример с многоадресной рассылкой телевизионного контента, когда абонентское устройство (такое как компьютер) в сети VLAN 1 принимает через коммутатор многоадресный трафик от сервера потокового мультимедиа **S**. Через порт,

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 многоадресной рассылки. Если IGMP-запрос соответствует одному из настроенных на коммутаторе адресов групп многоадресной рассылки MVR, в таблице пересылки коммутатора создается запись. В ней абонентская VLAN включается в список пунктов назначения для пересылки указанного трафика многоадресной рассылки.

Если абонент переключается на другой канал или выключает компьютер, на коммутатор направляется Leave-сообщение IGMP для выхода из группы многоадресной рассылки. 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 многоадресной рассылки. В противном случае коммутатор удаляет порт приемника из таблицы пересылки.

Рисунок 115 Пример с многоадресной рассылкой телевидения посредством MVR



23.2 Настройка многоадресной рассылки

С помощью этого экрана можно настроить параметры IGMP для IPv4 или MLD для IPv6, а также параметры сетей VLAN многоадресной рассылки. Выберите в навигационной панели **Advanced Application** > **Multicast**.

Рисунок 116 Экран Advanced Application > Multicast Setup

Поля экрана описаны в следующей таблице.

Таблица 67 Экран Advanced Application > Multicast Setup

ПОЛЕ	ОПИСАНИЕ
IPv4 Multicast	С помощью этой ссылки можно открыть экраны для настройки отслеживания IGMP и фильтрации IGMP для IPv4.
IPv6 Multicast	С помощью этой ссылки можно открыть экраны для настройки отслеживания MLD и фильтрации MLD для IPv6.
MVR	С помощью этой ссылки можно открыть экраны для создания сетей VLAN многоадресной рассылки.

23.3 Экран IPv4 Multicast Status

Чтобы открыть экран, изображенный на рисунке ниже, нажмите **Advanced Application > Multicast > IPv4 Multicast**. На этом экране приведена информация о группах многоадресной рассылки IPv4. Более подробную информацию о многоадресной рассылке можно найти в разд. 23.1 на стр. 179.

Рисунок 117 Экран Advanced Application > Multicast > IPv4 Multicast

Поля экрана описаны в следующей таблице.

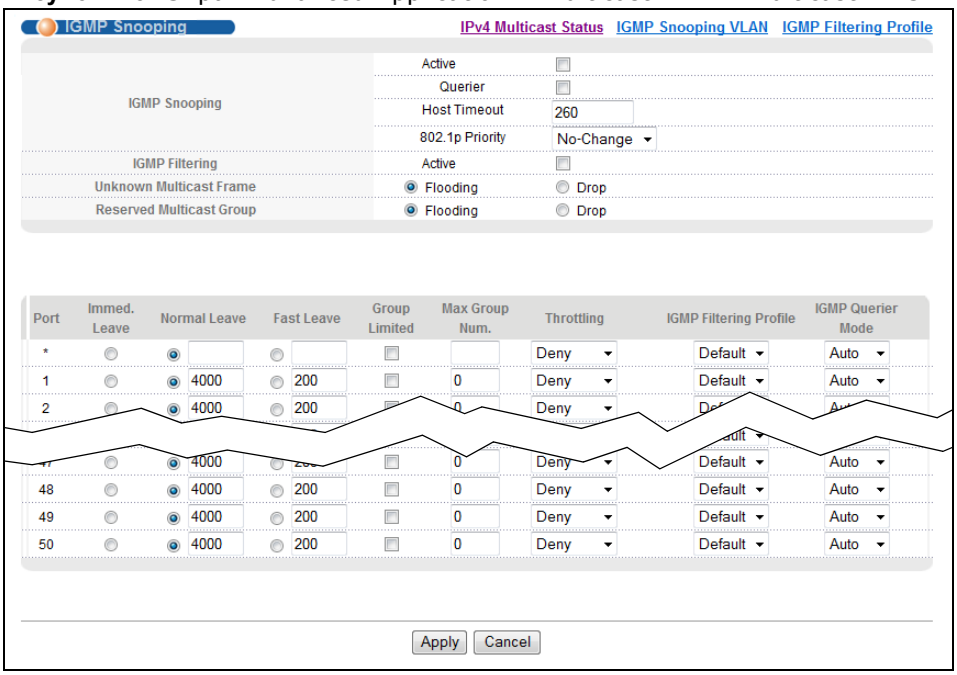
Таблица 68 Экран Advanced Application > Multicast > IPv4 Multicast

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

23.3.1 Экран IGMP Snooping

Перейдите по ссылке **IGMP Snooping** на экране **Advanced Application > Multicast > IPv4 Multicast**, чтобы открыть экран, изображенный на рисунке ниже. Более подробную информацию о многоадресной рассылке можно найти в разд. 23.1 на стр. 179.

Рисунок 118 Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping



Поля экрана описаны в следующей таблице.

Таблица 69 Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

ПОЛЕ	ОПИСАНИЕ
IGMP Snooping	С помощью этих настроек можно задать параметры отслеживания IGMP.
Active	Выбор **Active** активирует отслеживание многоадресного трафика IGMP, при котором трафик группы многоадресной рассылки пересылается только на порты, входящие в соответствующую группу.
Querier	Выбор этой опции разрешает коммутатору рассылать сообщения типа IGMP General Query сетям VLAN с подключенными хостами многоадресной рассылки.
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.
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. При включении фильтрации IGMP необходимо создать и назначить профили фильтрации IGMP тем портам, которым необходимо разрешить присоединение к группам многоадресной рассылки.
Unknown Multicast Frame	Выберите действие, выполняемое коммутатором при получении неизвестного кадра многоадресной рассылки. **Drop** – отбрасывание кадра. **Flooding** – пересылка кадра на все порты.
Reserved Multicast Group	Диапазон IP-адресов от 224.0.0.0 до 224.0.0.255 зарезервирован исключительно для многоадресной рассылки в локальной сети. Например, адрес 224.0.0.1 предназначен для всех хостов в сегменте локальной сети, а адрес 224.0.0.9 используется для рассылки маршрутной информации протокола RIP всем маршрутизаторам RIP v2, находящимся в одном сегменте сети. Маршрутизатор многоадресной рассылки не будет пересылать пакет, IP-адрес назначения которого находится в указанном выше диапазоне, в другие сети. Дополнительную информацию можно найти на сайте IANA. В эту группу также входят MAC-адреса многоадресной рассылки уровня 2, используемые протоколами Cisco уровня 2, 01:00:0C:CC:CC:CC и 01:00:0C:CC:CC:CD. Выберите действие, выполняемое коммутатором при получении кадра с зарезервированным адресом многоадресной рассылки. **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. Изменения в данной строке сразу же копируются на все порты.
Immed. Leave	Выбор данной опции заставляет коммутатор удалять данный порт из дерева многоадресной рассылки 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 69 Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

ПОЛЕ	ОПИСАНИЕ
Normal Leave	Укажите значение тайм-аута режима обычного покидания (normal leave) для IGMP в миллисекундах (выбирается из диапазона от 200 до 6 348 800). При выборе этой опции коммутатор будет использовать указанный тайм-аут при обновлении таблицы маршрутизации для данного порта. В режиме обычного покидания при получении сообщения IGMP Leave от хоста, подключенного к данному порту, коммутатор пересылает это сообщение маршрутизатору многоадресной рассылки. Затем маршрутизатор многоадресной рассылки посылает сообщение IGMP Group-Specific Query (GSQ), чтобы определить, должны ли остаться другие хосты, подключенные к данному порту, в конкретной группе многоадресной рассылки; коммутатор пересылает сообщение с запросом всем хостам, подключенным к данному порту, и ожидает сообщений IGMP Report от хостов для обновления таблицы маршрутизации. Это поле определяет время, которое коммутатор выжидает после получения IGMP-сообщения Leave от хоста перед удалением записи об участии в группе IGMP.
Fast Leave	Укажите тайм-аута режима быстрого покидания для IGMP в миллисекундах (выбирается из диапазона от 200 до 6 348 800). При выборе этой опции коммутатор будет использовать указанный тайм-аут при обновлении таблицы маршрутизации для данного порта. В режиме быстрого покидания сразу после получения сообщения Leave IGMP от хоста на данном порту коммутатор посылает сообщение IGMP Group-Specific Query (GSQ), чтобы определить, должны ли остаться другие хосты, подключенные к данному порту, в конкретной группе многоадресной рассылки. Эта опция помогает ускорить процесс покидания. Это поле определяет время, которое коммутатор выжидает после получения IGMP-сообщения Leave от хоста перед удалением записи об участии в группе IGMP.
Group Limited	Выбор данной опции позволяет ограничить число групп многоадресной рассылки, к которым разрешено присоединиться данному порту.
Max Group Num.	Введите число групп многоадресной рассылки, к которым разрешено присоединиться данному порту. После регистрации порта в указанном количестве групп многоадресной рассылки все последующие Join-сообщения IGMP от данного порта отбрасываются.
Throttling	Параметр IGMP throttling определяет алгоритм обработки коммутатором сообщений IGMP Report при вступлении порта в максимально возможное количество групп IGMP. При выборе опции **Deny** коммутатор будет отбрасывать все новые отчеты о присоединении IGMP, полученные через данный порт, пока не истечет срок жизни действующей записи в таблице маршрутизации многоадресной рассылки. При выборе опции **Replace** существующая запись в таблице маршрутизации многоадресной рассылки будет заменена новым сообщением (или сообщениями) IGMP Report, полученными через данный порт.
IGMP Filtering Profile	Выберите имя профиля фильтрации IGMP, который будет использоваться для данного порта. Значение **Default** запрещает порту присоединение к любым группам многоадресной рассылки. Профили фильтрации IGMP можно создать на экране **Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile**.

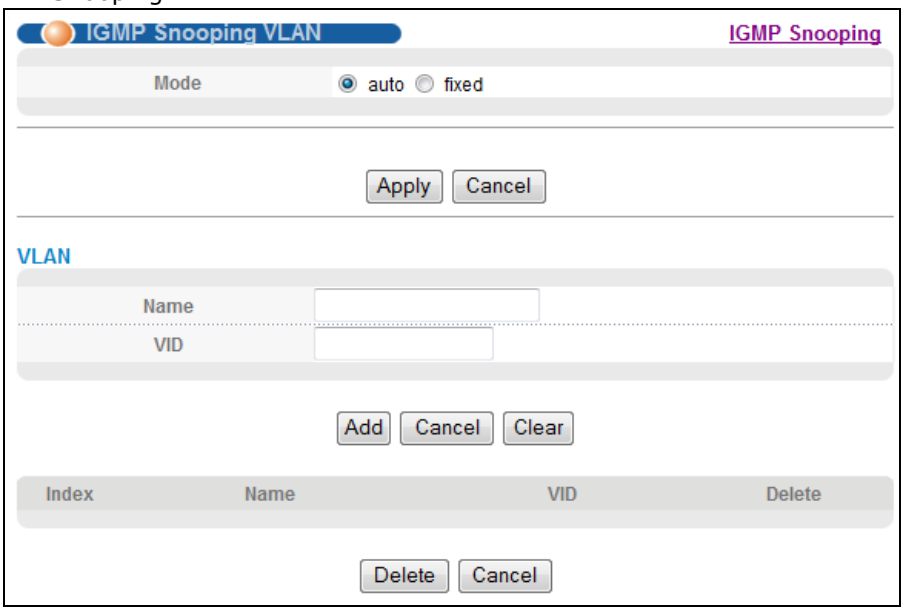
Таблица 69 Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

ПОЛЕ	ОПИСАНИЕ
IGMP Querier Mode	Query-порт IGMP коммутатор рассматривает в качестве порта, к которому подключен маршрутизатор (или сервер) многоадресной рассылки 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 многоадресной рассылки 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.

23.4 Экран IGMP Snooping VLAN

Выберите в навигационной панели **Advanced Application > Multicast > IPv4 Multicast**. Перейдите по ссылке **IGMP Snooping**, а затем по ссылке **IGMP Snooping VLAN**, чтобы открыть экран, изображенный на рисунке ниже. Дополнительную информацию о VLAN отслеживания многоадресного трафика IGMP можно найти в разд. «Отслеживание многоадресного трафика IGMP и сети VLAN» на стр. 180.

Рисунок 119 Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN



Поля экрана описаны в следующей таблице.

Таблица 70 Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

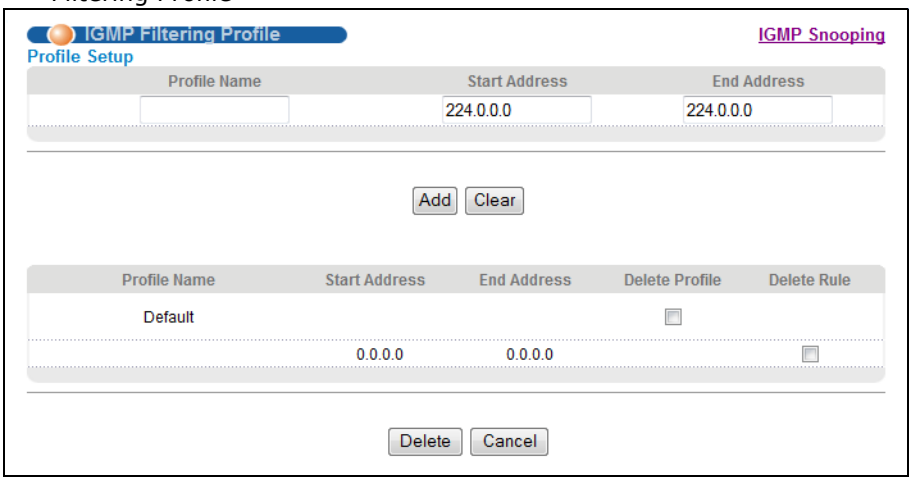
ПОЛЕ	ОПИСАНИЕ
Mode	Выберите **auto**, чтобы коммутатор автоматически получал информацию об участии в группе многоадресной рассылки для любых сетей VLAN. Выберите **fixed**, чтобы коммутатор получал информацию об участии в группе многоадресной рассылки только для указанных ниже сетей VLAN. И в автоматическом (**auto**), и в фиксированном (**fixed**) режимах коммутатор может запомнить информацию не более чем о 16 сетях VLAN (в том числе не более чем о пяти сетях VLAN, созданных на экране **MVR**). Так, если на экране **MVR** была настроена одна VLAN-сеть многоадресной рассылки, 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. Вначале необходимо включить функцию отслеживания IGMP на экране **Multicast > IPv4 Multicast > IGMP Snooping**.
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. Не допускается использовать тот же идентификатор VLAN ID, что и на экране **MVR**.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это порядковый номер записи сети VLAN для отслеживания IGMP в таблице. Щелчок на порядковом номере позволяет отобразить более подробную информацию или изменить настройки.
Name	В этом поле отображается имя-описание группы VLAN.
VID	В этом поле отображается идентификационный номер группы VLAN.
Delete	В столбце **Delete** установите переключатели напротив записей, которые нужно удалить, и нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

23.4.1 Экран IGMP Filtering Profile

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

Выберите в навигационной панели **Advanced Application > Multicast > IPv4 Multicast**. Перейдите по ссылке **IGMP Snooping**, а затем по ссылке **IGMP Filtering Profile**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 120 Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile



Поля экрана описаны в следующей таблице.

Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > 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 многоадресной рассылки.
Start Address	Введите начальный адрес диапазона IP-адресов многоадресной рассылки, который необходимо включить в профиль фильтрации IGMP.
End Address	Введите конечный адрес диапазона IP-адресов многоадресной рассылки, который необходимо включить в профиль фильтрации IGMP. Чтобы добавить единственный IP-адрес многоадресной рассылки, укажите его и в поле **Start Address**, и в поле **End Address**.
Add	Нажатие на этот значок позволяет создать новую запись. Это действие позволяет сохранить изменения настроек 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.

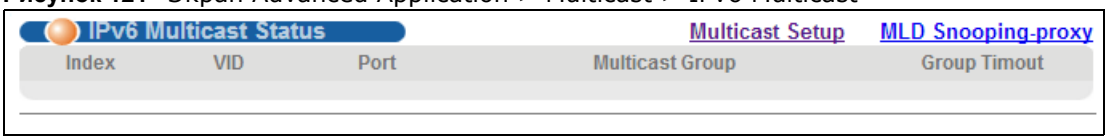
Экран Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

ПОЛЕ	ОПИСАНИЕ
Profile Name	В этом поле отображается имя-описание профиля.
Start Address	В этом поле отображается начальный адрес диапазона IP-адресов многоадресной рассылки.
End Address	В этом поле отображается конечный адрес диапазона IP-адресов многоадресной рассылки.
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**.

23.5 Экран IPv6 Multicast Status

Выберите в меню **Advanced Application > Multicast > IPv6 Multicast**, чтобы открыть экран, изображенный ниже. Этот экран содержит информацию о группах многоадресной рассылки IPv6. Более подробную информацию о многоадресной рассылке можно найти в разд. 23.1 на стр. 179.

Рисунок 121 Экран Advanced Application > Multicast > IPv6 Multicast



Поля экрана, изображенного на рисунке выше, описаны в следующей таблице.

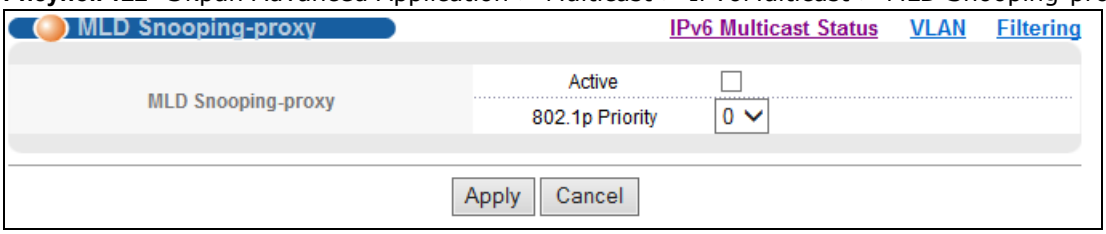
Таблица 71 Экран Advanced Application > Multicast > IPv6 Multicast

ПОЛЕ	ОПИСАНИЕ
Index	Порядковый номер записи.
VID	В этом поле отображается идентификатор VLAN-сети многоадресной рассылки.
Port	В этом поле отображается номер порта, принадлежащего группе многоадресной рассылки.
Multicast Group	В этом поле отображаются IP-адреса группы многоадресной рассылки.
Group Timeout	Это поле показывает время (в секундах), по истечении которого коммутатор удаляет запись об участии в группе MLD при отсутствии сообщений Report от данного порта.

23.5.1 Экран MLD Snooping-proxy

Перейдите по ссылке **MLD Snooping-proxy** на экране **Advanced Application > Multicast > IPv6 Multicast**, чтобы открыть экран, изображенный на рисунке ниже. Более подробную информацию о многоадресной рассылке можно найти в разд. 23.1 на стр. 179.

Рисунок 122 Экран Advanced Application > Multicast > IPv6Multicast > MLD Snooping-proxy



Поля экрана, изображенного на рисунке выше, описаны в следующей таблице.

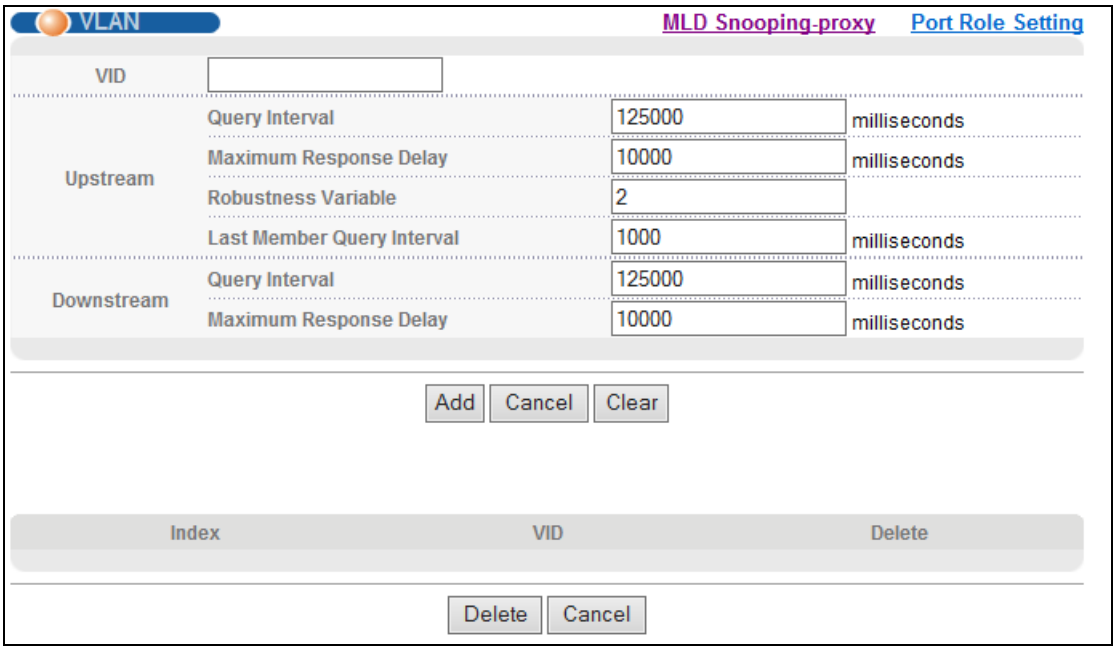
Таблица 72 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy

ПОЛЕ	ОПИСАНИЕ
MLD Snooping-proxy	С помощью этих настроек можно задать параметры прокси отслеживания MLD.
Active	Выберите опцию Active, чтобы активировать прокси отслеживания MLD на коммутаторе с целью уменьшения количества управляющих сообщений MLD и улучшения производительности сети.
802.1p Priority	Выберите уровень приоритета (из диапазона от 0 до 7), на который коммутатор меняет приоритет в исходящих сообщениях MLD.
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.

23.5.2 Экран MLD Snooping-proxy VLAN

Перейдите по ссылке **VLAN** на экране **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy**, чтобы открыть экран, изображенный на рисунке ниже. Более подробную информацию о многоадресной рассылке можно найти в разд. 23.1 на стр. 179.

Рисунок 123 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN



Поля экрана, изображенного на рисунке выше, описаны в следующей таблице.

Таблица 73 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

ПОЛЕ	ОПИСАНИЕ
VID	Введите идентификатор сети VLAN, в которой необходимо активировать прокси отслеживания MLD, и выполните настройку соответствующих параметров.
Upstream	
Query Interval	Укажите временной интервал (в миллисекундах) между сообщениями-запросами общего характера, которые посылает коммутатор, подключенный к агрегирующему порту. Значение в этом поле должно в точности совпадать со значением, указанным в параметрах подключенного коммутатора многоадресной рассылки. Это значение используется при расчете периода времени, в течение которого запись об участии в отслеживании MLD (полученная только на агрегирующем порту) может существовать в таблице маршрутизации. При получении сообщения MLD Report коммутатор устанавливает период тайм-аута для записи равным величине, рассчитываемой по формуле T = (QI*RV) + MRD, где T = тайм-аут, QI = интервал между запросами, RV = переменная отказоустойчивости (Robustness Variable), MRD = максимальная задержка ответа.

Таблица 73 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

ПОЛЕ	ОПИСАНИЕ
Maximum Response Delay	Укажите временной интервал (в миллисекундах), в течение которого маршрутизатор, подключенный к агрегирующему порту, ожидает ответа на сообщение-запрос общего характера MLD. Значение в этом поле должно в точности совпадать со значением, указанным в параметрах подключенного коммутатора многоадресной рассылки. Это значение используется при расчете периода времени, в течение которого запись об участии в отслеживании MLD (полученная только на агрегирующем порту) может существовать в таблице маршрутизации. При получении сообщения MLD Report коммутатор устанавливает период тайм-аута для записи равным величине, рассчитываемой по формуле T = (QI*RV) + MRD, где T = тайм-аут, QI = интервал между запросами, RV = переменная отказоустойчивости, MRD = максимальная задержка ответа. При получении сообщения MLD Done коммутатор устанавливает срок жизни записи как функцию от значений **Last Member Query Interval** и **Robustness Variable**
Robustness Variable	Укажите количество запросов. Запись адреса многоадресной рассылки (полученная только на агрегирующем порту посредством отслеживания) удаляется из таблицы маршрутизации при отсутствии ответа на заданное количество запросов, отправленных маршрутизатором, подключенным к агрегирующему порту. Значение в этом поле должно в точности совпадать со значением, указанным в параметрах подключенного коммутатора многоадресной рассылки. Это значение используется при расчете периода времени, в течение которого запись об участии в отслеживании MLD (полученная только на агрегирующем порту) может существовать в таблице маршрутизации.
Last Member Query Interval	Укажите временной интервал (в секундах) между запросами MLD с указанием группы, которые отправляет агрегирующий порт после получения сообщения MLD Done. Значение в этом поле должно в точности совпадать со значением, указанным в параметрах подключенного коммутатора многоадресной рассылки. Это значение используется при расчете периода времени, в течение которого запись об участии в отслеживании MLD (полученная только на агрегирующем порту) может существовать в таблице маршрутизации после получения сообщения Done. При получении сообщения MLD Done коммутатор устанавливает срок жизни записи как функцию от значений **Last Member Query Interval** и **Robustness Variable**.
Downstream	
Query Interval	Укажите временной интервал (в миллисекундах) между сообщениями-запросами общего характера, которые посылает нисходящий порт.
Maximum Response Delay	Укажите максимальный период времени (в миллисекундах), в течение которого коммутатор ожидает ответа на сообщение-запрос общего характера, отправленное нисходящим портом.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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.

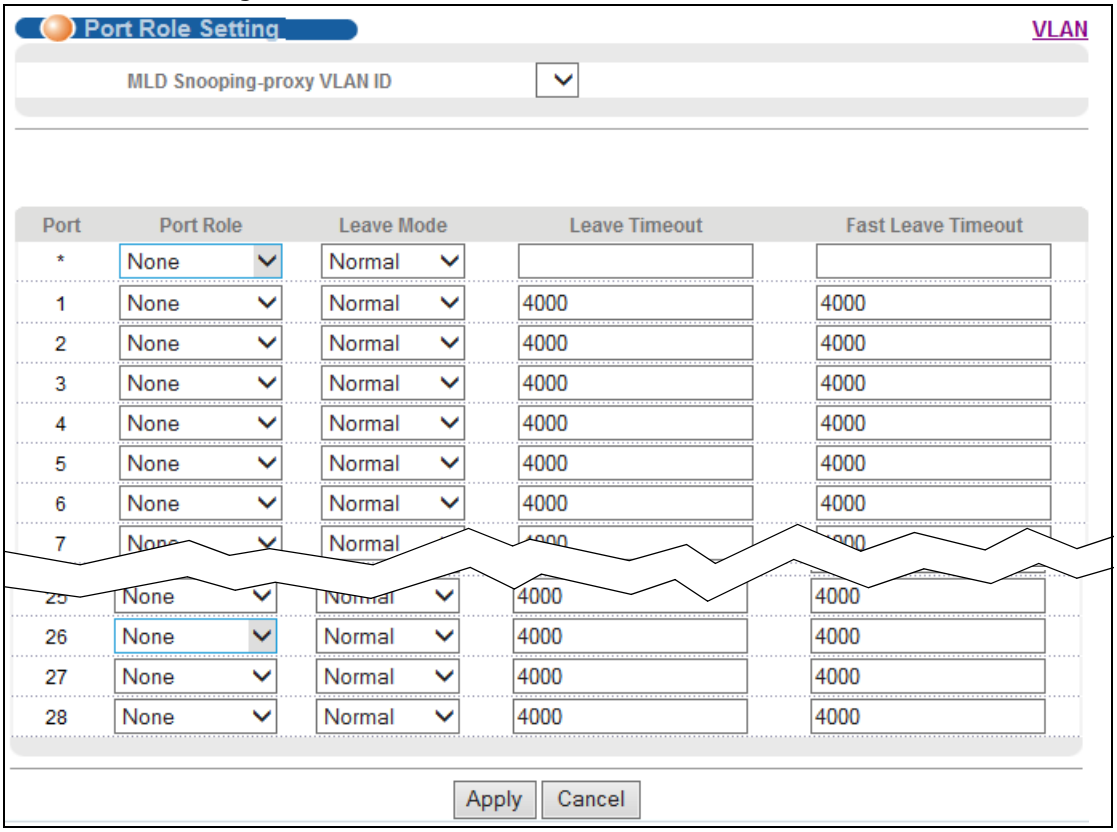
Таблица 73 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

ПОЛЕ	ОПИСАНИЕ
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это поле содержит порядковый номер записи сети VLAN прокси отслеживания MLD в данной таблице. Щелчок на порядковом номере позволяет отобразить более подробную информацию или изменить настройки.
VID	В этом поле отображается идентификационный номер группы VLAN.
Delete	В столбце **Delete** установите переключатели напротив записей, которые нужно удалить.
Delete	Нажмите **Delete**, чтобы навсегда удалить запись, выбранную в столбце Delete.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

23.5.3 Экран MLD Snooping-proxy VLAN Port Role Setting

Перейдите по ссылке **Port Role Setting** на экране **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN**, чтобы открыть экран, изображенный на рисунке ниже. Более подробную информацию о многоадресной рассылке можно найти в разд. 23.1 на стр. 179.

Рисунок 124 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Port Role Setting



Поля экрана, изображенного на рисунке выше, описаны в следующей таблице.

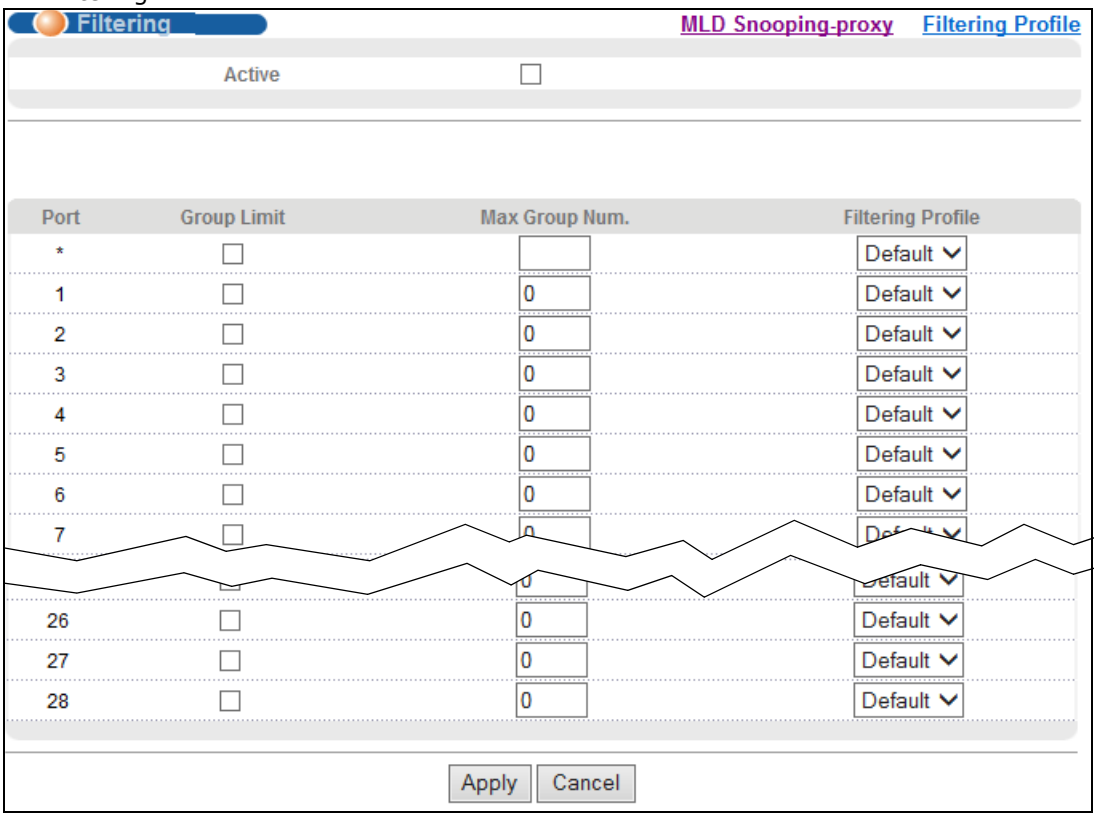
Таблица 74 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Port Role Setting

ПОЛЕ	ОПИСАНИЕ
MLD Snooping-proxy VLAN ID	Выберите идентификатор сети VLAN, для которой необходимо настроить параметры прокси отслеживания MLD для определенного 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. Изменения в данной строке сразу же копируются на все порты.
Port Role	Порт коммутатора может играть в MLD роль либо нисходящего (**Downstream**), либо агрегирующего (**Upstream**) порта. Нисходящий порт подключается к хостам MLD и выступает в качестве маршрутизатора многоадресной рассылки, который отправляет запросы MLD и слушает сообщения Report и Done от хоста MLD. Агрегирующий порт подключается к маршрутизатору многоадресной рассылки и функционирует в качестве хоста, отправляющего сообщения Report или Done в ответ на запросы от маршрутизатора многоадресной рассылки. В противном случае, если порт не будет включен в группу многоадресной рассылки или не принадлежит этой сети VLAN, выберите опцию **None**.
Leave Mode	Выберите режим покидания для указанного нисходящего порта (или портов) в данной сети VLAN. Это поле указывает на то, удаляет ли коммутатор запись об участии в отслеживании MLD (полученную через нисходящий порт) немедленно (**Immediate**), или ожидает сообщения MLD Report до истечения времени тайм-аута обычного (**Normal**) или быстрого (**Fast**) покидания при получении сообщения MLD Leave на данном порту от какого-либо хоста.
Leave Timeout	Укажите обычное время тайм-аута покидания для отслеживания MLD (в миллисекундах), которое коммутатор использует при обновлении таблицы маршрутизации указанного нисходящего порта (или портов). Значение в этом поле показывает, сколько секунд коммутатор ожидает сообщения MLD Report, прежде чем удалить запись об участии в отслеживании MLD (полученную через нисходящий порт), при получении сообщения MLD Done через этот порт от какого-либо хоста.
Fast Leave Timeout	Укажите время тайм-аута быстрого покидания (в миллисекундах) для указанного нисходящего порта (или портов). Значение в этом поле показывает, сколько секунд коммутатор ожидает сообщения MLD Report, прежде чем удалить запись об участии в отслеживании MLD (полученную через нисходящий порт), при получении сообщения MLD Done через этот порт от какого-либо хоста.
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.

23.5.4 Экран MLD Snooping-proxy VLAN Filtering

С помощью этого экрана можно настроить параметры фильтрации MLD коммутатора. Перейдите по ссылке **Filtering** на экране **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 125 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering



Поля экрана, изображенного на рисунке выше, описаны в следующей таблице.

Таблица 75 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering

ПОЛЕ	ОПИСАНИЕ
Active	Выберите эту опцию, чтобы включить фильтрацию MLD 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. Изменения в данной строке сразу же копируются на все порты.
Group Limit	Выбор данной опции позволяет ограничить число групп многоадресной рассылки, к которым разрешено присоединиться данному порту.

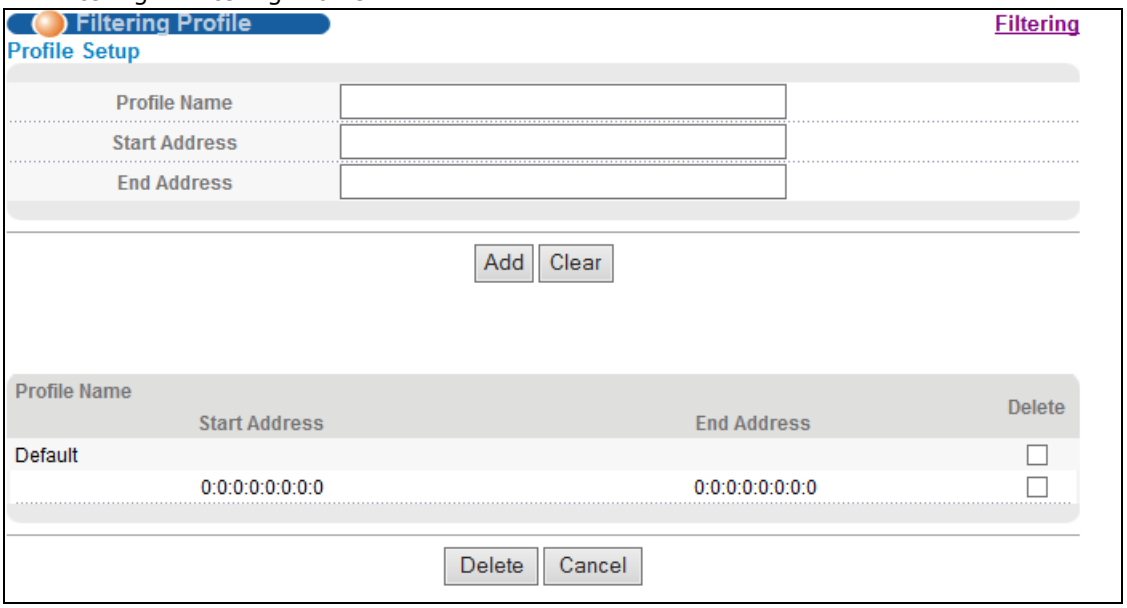
Таблица 75 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering

ПОЛЕ	ОПИСАНИЕ
Max Group Num.	Введите число групп многоадресной рассылки, к которым разрешено присоединиться данному порту. После регистрации порта в указанном количестве групп многоадресной рассылки все новые сообщения MLD Report, приходящие на этот порт, будут отбрасываться.
Filtering Profile	Выберите имя профиля фильтрации MLD, который будет использоваться для данного порта. Значение **Default** запрещает порту присоединение к любым группам многоадресной рассылки. Для создания профилей фильтрации MLD можно использовать экран **Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile**.
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.

23.5.5 Экран MLD Snooping-proxy VLAN Filtering Profile

С помощью этого экрана можно создать профиль фильтрации MLD и задать диапазон адресов многоадресной рассылки. Перейдите по ссылке **Filtering Profile** на экране **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 126 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile



Поля экрана, изображенного на рисунке выше, описаны в следующей таблице.

Таблица 76 Экран Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > 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 многоадресной рассылки.
Start Address	Введите начальный адрес диапазона адресов многоадресной рассылки IPv6, который необходимо включить в профиль фильтрации MLD.
End Address	Введите конечный адрес диапазона адресов многоадресной рассылки IPv6, который необходимо включить в профиль фильтрации MLD. Чтобы добавить единственный адрес многоадресной рассылки IPv6, укажите его и в поле **Start Address**, и в поле **End Address**.
Add	Нажатие на этот значок позволяет создать новую запись. Это действие позволяет сохранить изменения настроек 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 адресов многоадресной рассылки IPv6.
End Address	В этом поле отображается конечный адрес диапазона адресов многоадресной рассылки IPv6.
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**.
Delete	Нажмите **Delete**, чтобы навсегда удалить записи, выбранные в столбце Delete.
Cancel	Нажатие на кнопку **Cancel** снимает выделения с переключателей в столбцах **Delete Profile**/**Delete Rule**.

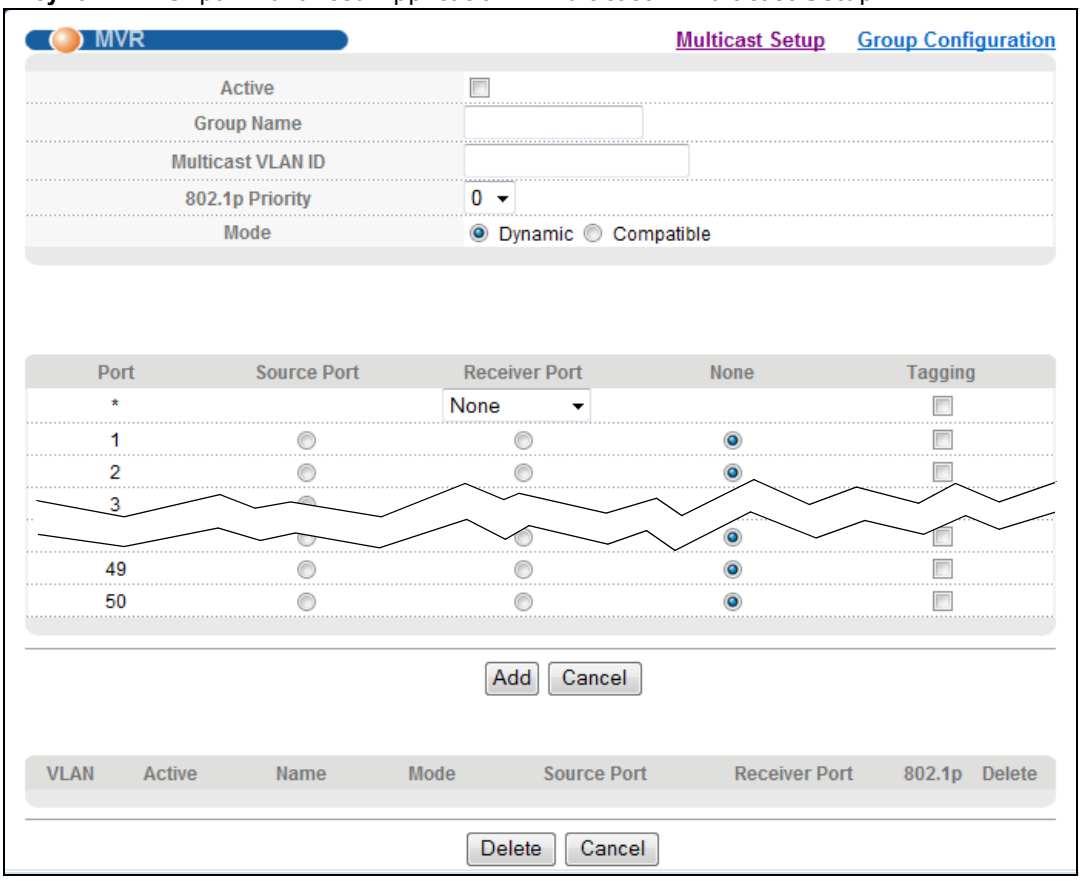
23.6 Общие настройки MVR

Создать VLAN-сети многоадресной рассылки и выбрать для каждой VLAN-сети многоадресной рассылки порты приемников и порт источника можно на экране **MVR**. Перейдите по ссылке **Advanced Application > Multicast** > **Multicast Setup > MVR**, чтобы открыть экран, изображенный на рисунке ниже.

Примечание: На коммутаторе можно создать не более пяти сетей VLAN многоадресной рассылки и не более 256 правил многоадресной рассылки.

Примечание: При создании на данном экране сети VLAN многоадресной рассылки коммутатор автоматически создает статическую VLAN (с тем же идентификатором VID).

Рисунок 127 Экран Advanced Application > Multicast > Multicast Setup > MVR



Поля экрана описаны в следующей таблице.

Таблица 77 Экран Advanced Application > Multicast > Multicast Setting > MVR

ПОЛЕ	ОПИСАНИЕ
Active	Выберите данный переключатель для включения MVR, чтобы использовать одну единственную VLAN-сеть многоадресной рассылки для различных абонентских VLAN в сети.
Group Name	Введите имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать этот маршрут.
Multicast VLAN ID	Введите идентификатор сети VLAN (от 1 до 4094) для VLAN-сети многоадресной рассылки.
802.1p Priority	Выберите уровень приоритета (из диапазона от 0 до 7), на который коммутатор заменяет приоритет в исходящих управляющих пакетах IGMP или MLD (принадлежащих к данной сети VLAN многоадресной рассылки).
Mode	Укажите режим MVR для коммутатора. Можно выбрать значения **Dynamic** (динамический) и **Compatible** (режим совместимости). При выборе опции **Dynamic** сообщения IGMP Report или сообщения MLD будут рассылаться на все порты источников MVR в сети VLAN многоадресной рассылки. При выборе опции **Compatible** коммутатор не будет рассылать сообщения IGMP Report и сообщения MLD.

Таблица 77 Экран Advanced Application > Multicast > Multicast Setting > MVR (продолжение)

ПОЛЕ	ОПИСАНИЕ
Port	В этом поле отображается 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. 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 многоадресной рассылки. Все порты источников должны принадлежать к одной VLAN-сети многоадресной рассылки.
Receiver Port	Выберите данную опцию, чтобы назначить данный порт в качестве порта приемника MVR, который только принимает трафик многоадресной рассылки.
None	Выберите данную опцию, если данный порт не участвует в механизме MVR. Через такой порт трафик многоадресной рассылки 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 эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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 многоадресной рассылки. Щелкните на порядковом номере, чтобы изменить настройки.
Active	Данное поле показывает, включена ли поддержка группы многоадресной рассылки.
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 многоадресной рассылки, выберите нужные сети в столбце **Delete** и нажмите на кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

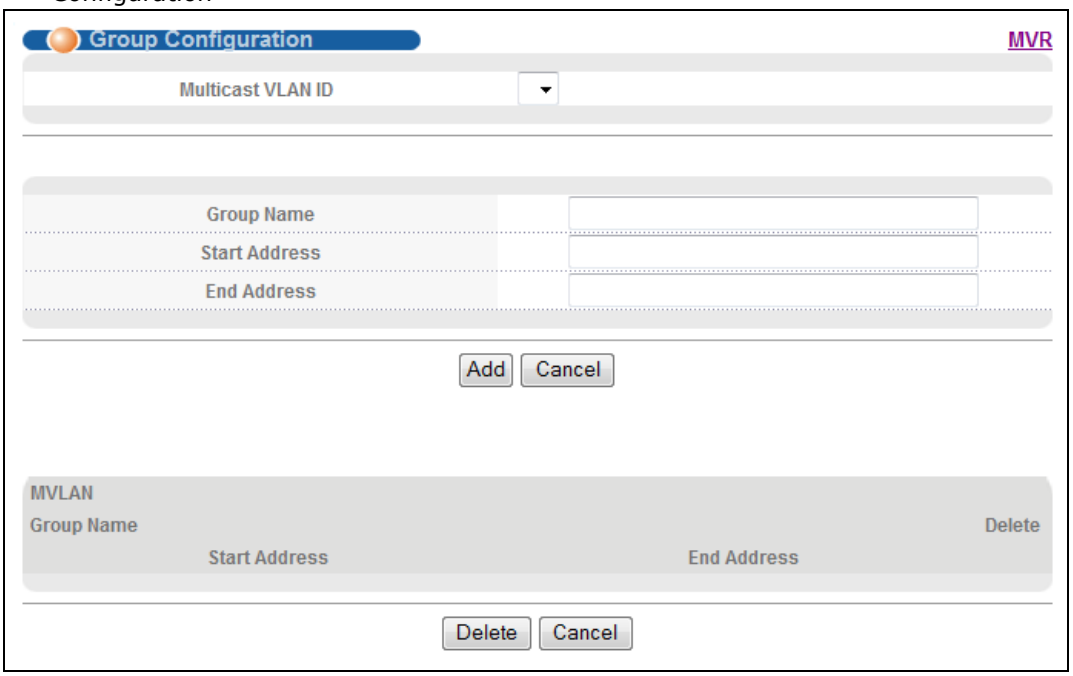
23.6.1 Настройка группы MVR

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

С помощью этого экрана можно задать IP-адреса группы многоадресной рассылки MVR. Перейдите по ссылке **Group Configuration** на экране **MVR**.

Примечание: Порт может принадлежать нескольким сетям VLAN многоадресной рассылки. Однако, IP-адреса различных групп многоадресной рассылки не должны перекрываться.

Рисунок 128 Экран Advanced Application > Multicast > Multicast Setup > MVR > Group Configuration



Поля экрана описаны в следующей таблице.

Таблица 78 Экран Advanced Application > Multicast > Multicast Setting > MVR > Group Configuration

ПОЛЕ	ОПИСАНИЕ
Multicast VLAN ID	Выберите из ниспадающего списка идентификатор VLAN-сети многоадресной рассылки (настроенный на экране **MVR**).
Group Name	Введите имя-описание для идентификации.
Start Address	Введите начальный IP-адрес группы многоадресной рассылки в виде десятичных чисел, разделенных точками. Более подробную информацию об IP-адресах многоадресной рассылки можно найти в разд. «IP-адреса многоадресной рассылки» на стр. 179.
End Address	Введите конечный IP-адрес группы многоадресной рассылки в виде десятичных чисел, разделенных точками. Если в группу многоадресной рассылки 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 многоадресной рассылки можно найти в разд. «IP-адреса многоадресной рассылки» на стр. 179.
Add	Нажатие на этот значок позволяет создать новую запись. Это действие позволяет сохранить изменения настроек 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 многоадресной рассылки.
Group Name	В этом поле отображается имя-описание для данной настройки.
Start Address	В этом поле отображается начальный IP-адрес группы многоадресной рассылки.

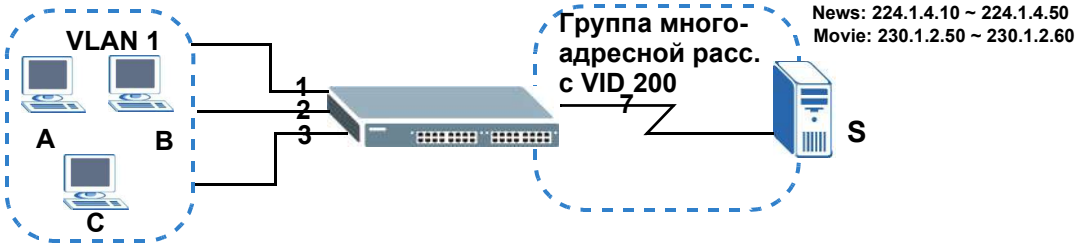
Таблица 78 Экран Advanced Application > Multicast > Multicast Setting > MVR > Group Configuration (продолжение)

ПОЛЕ	ОПИСАНИЕ
End Address	В этом поле отображается конечный IP-адрес группы многоадресной рассылки.
Delete	Выберите записи, которые нужно удалить, в столбце **Delete** и нажмите кнопку **Delete**, чтобы удалить выбранные записи из таблицы. При удалении сети VLAN многоадресной рассылки все группы многоадресной рассылки в данной сети VLAN также будут удалены.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей в таблице.

23.6.2 Пример настройки MVR

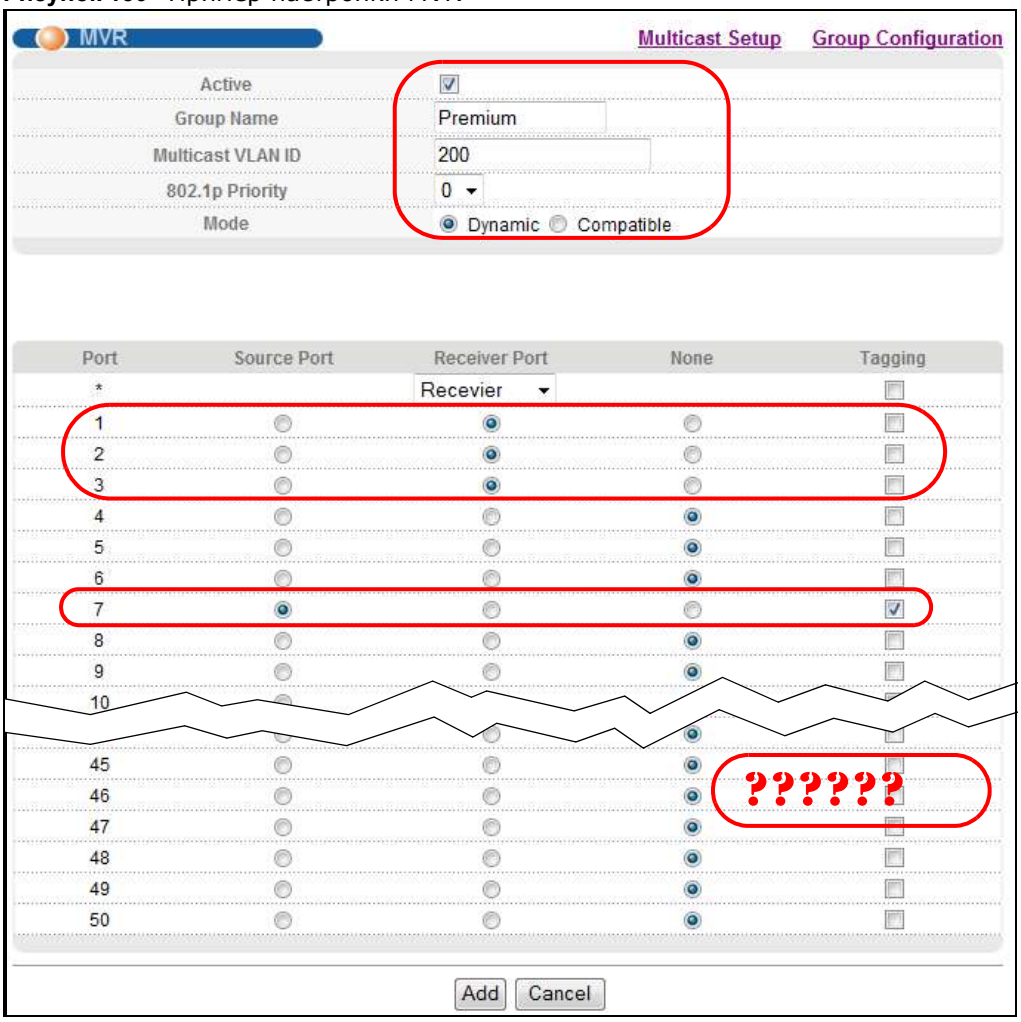
На приведенном ниже рисунке показан пример сети, в которой порты 1, 2 и 3 коммутатора принадлежат VLAN 1. Кроме того, порт 7 принадлежит к группе многоадресной рассылки с идентификатором VID 200 для получения многоадресного трафика (каналы **News** и **Movie**) от удаленного потокового мультимедийного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

Рисунок 129 Пример настройки MVR



Для создания настроек MVR на коммутаторе необходимо создать сеть VLAN многоадресной рассылки на экране **MVR** и назначить порты приемников и источников.

Рисунок 130 Пример настройки MVR



Чтобы коммутатор пересылал трафик группы многоадресной рассылки абонентам, необходимо определить настройки группы многоадресной рассылки на экране **Group Configuration**. На следующем рисунке показан пример настройки двух групп многоадресной рассылки IPv4 (**News** и **Movie**) для сети VLAN многоадресной рассылки 200.

Рисунок 131 Пример настройки групп MVR

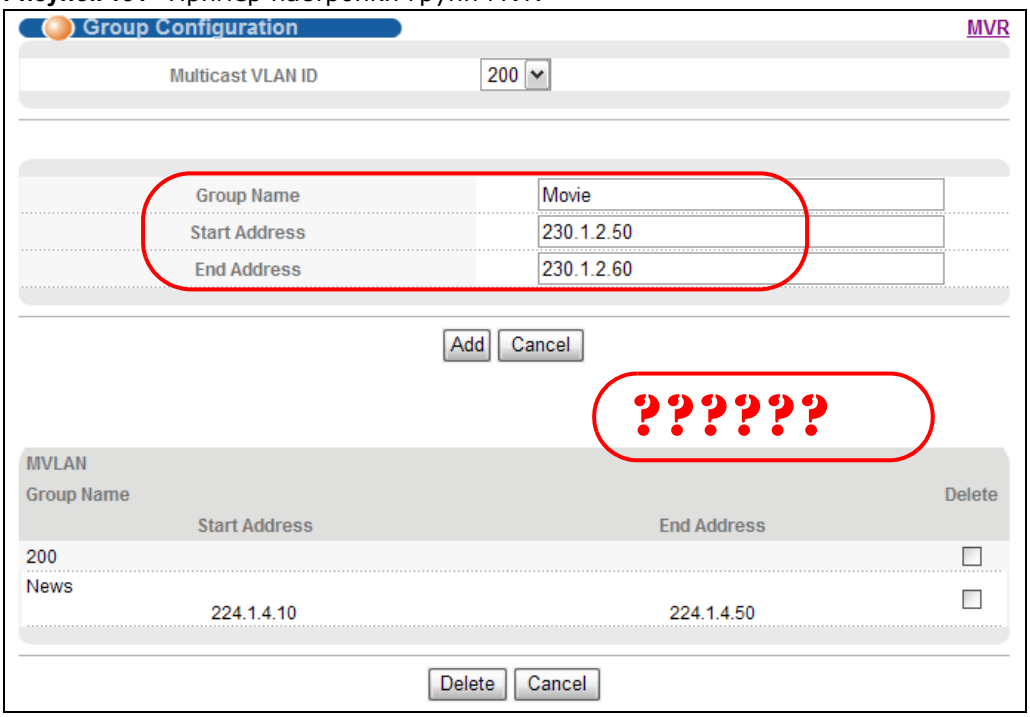
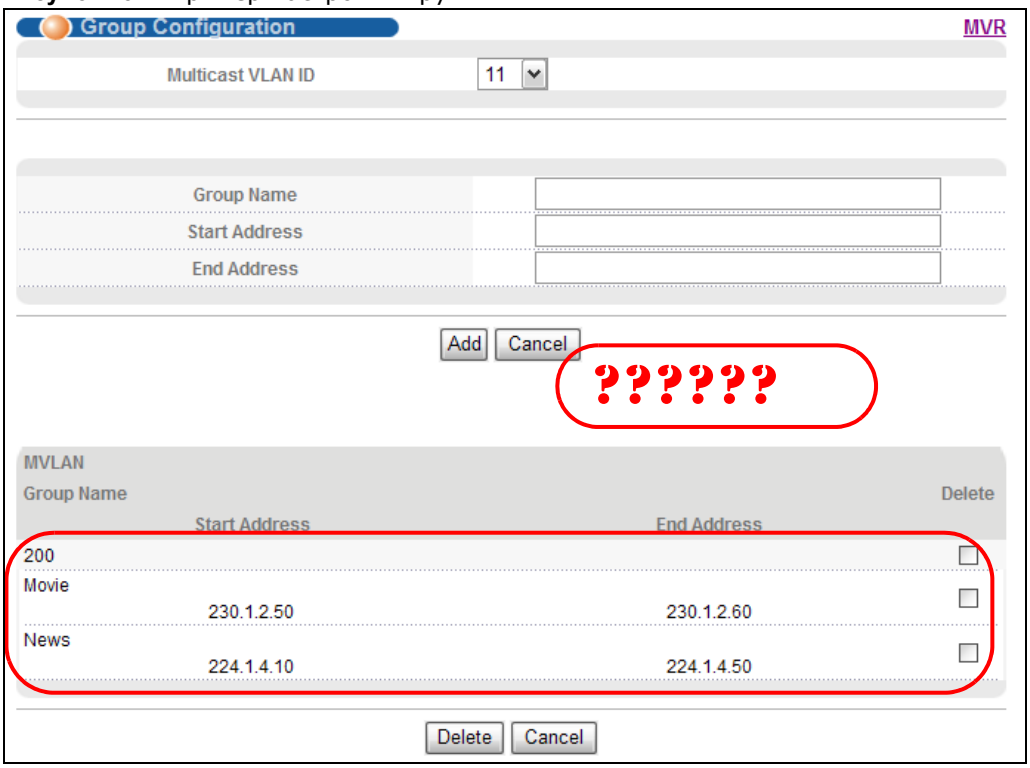


Рисунок 132 Пример настройки групп MVR



24

Аутентификация, авторизация и учет

24.1 Обзор функций аутентификации, авторизации и учета

В этой главе описана настройка функций аутентификации и авторизации на коммутаторе.

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. «RADIUS и TACACS+» на стр. 206) и TACACS+ (Terminal Access Controller Access-Control System Plus, см. разд. «RADIUS и TACACS+» на стр. 206).

Рисунок 133 Сервер AAA

24.1.1 О чем рассказывается в этой главе

- С помощью экрана **AAA** (разд. 24.2 на стр. 206) можно включить аутентификацию и/или авторизацию на коммутаторе.
- С помощью экрана **Radio Server Setup** (разд. 24.3 на стр. 207) можно настроить параметры сервера RADIUS.
- С помощью экрана **TACACS+ Server Setup** (разд. 24.4 на стр. 209) можно настроить параметры аутентификации TACACS+.
- С помощью экрана **AAA Setup** (разд. 24.5 на стр. 211) можно выбрать методы, используемые для аутентификации пользователей, пытающихся получить доступ к коммутатору, и указать, какую базу данных коммутатор должен использовать в первую очередь.

24.1.2 Что необходимо знать

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.

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. 37 на стр. 322).

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 79 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.

24.2 Экраны AAA

Экраны **AAA** позволяют включить аутентификацию и/или авторизацию на коммутаторе. В первую очередь необходимо настроить параметры сервера аутентификации (RADIUS и/или TACACS+), а затем указать приоритетный вариант аутентификации и включить авторизацию.

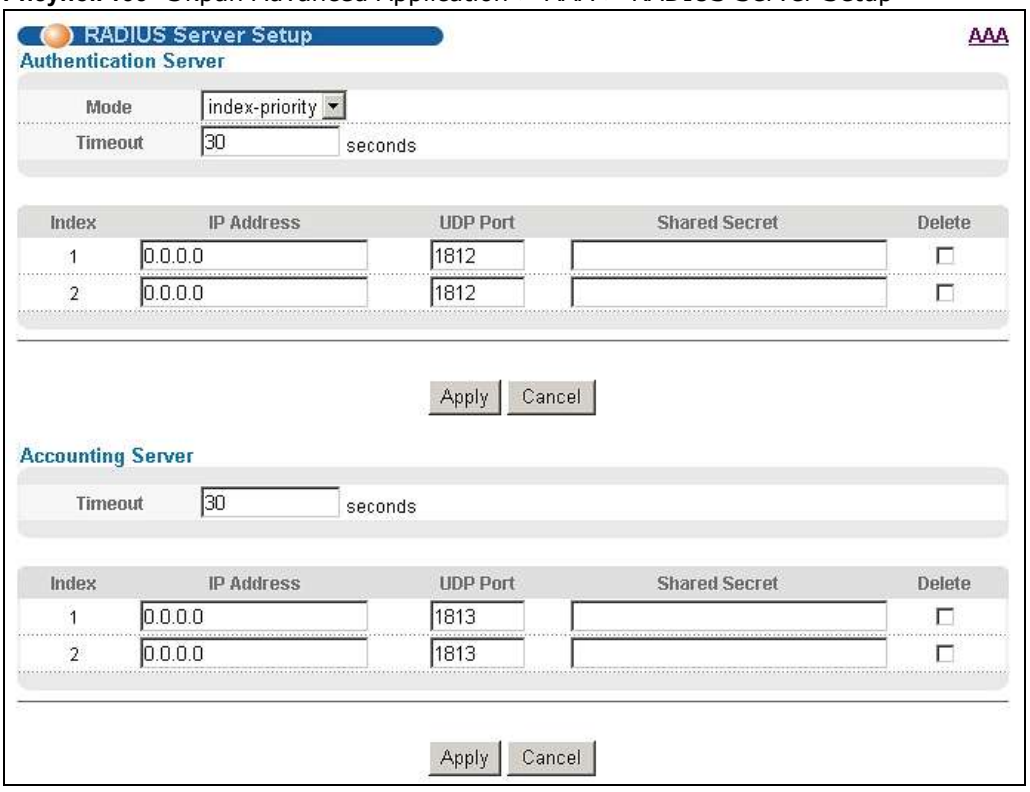
Выберите в навигационной панели **Advanced Application** > **AAA**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 134 Экран Advanced Application > AAA

24.3 Настройка сервера RADIUS

Изображенный ниже экран служит для ввода настроек сервера RADIUS. В разд. «RADIUS и TACACS+» на стр. 206 можно найти дополнительную информацию о серверах RADIUS, а в разд. 24.6.2 на стр. 215 – информацию об атрибутах RADIUS, используемых функциями аутентификации на коммутаторе.Перейдите по ссылке **RADIUS Server Setup** на экране **AAA**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 135 Экран Advanced Application > AAA > RADIUS Server Setup



Поля экрана описаны в следующей таблице.

Таблица 80 Экран Advanced Application > AAA > RADIUS Server Setup

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

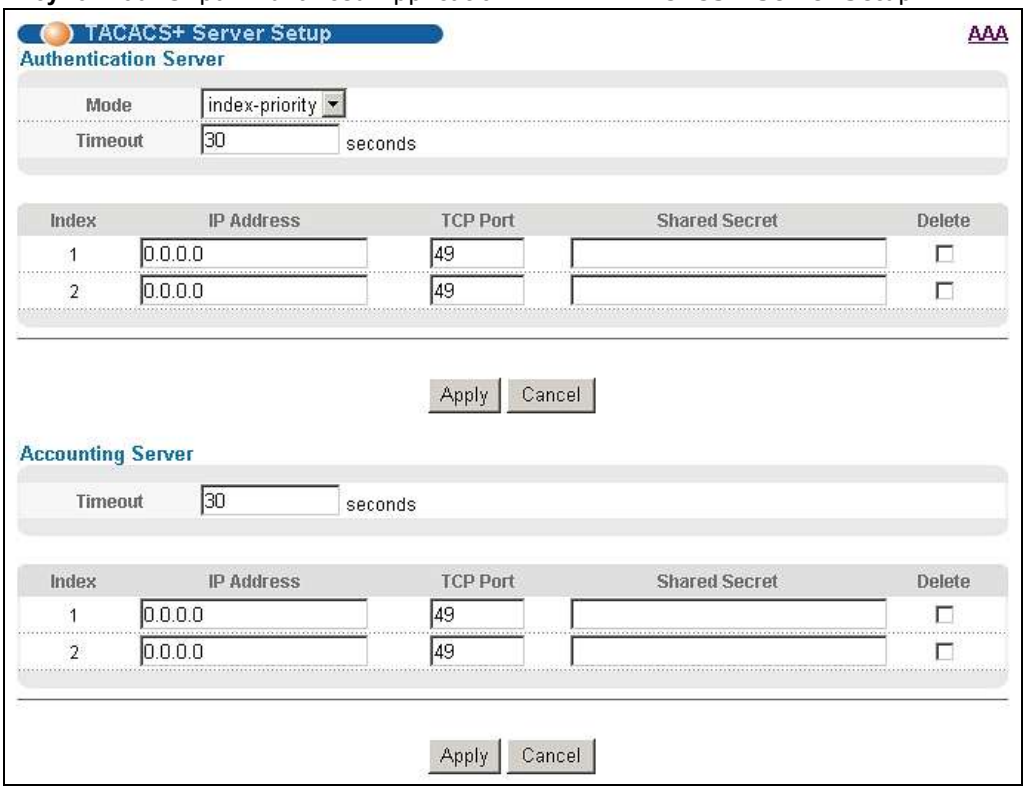
Таблица 80 Экран Advanced Application > AAA > RADIUS Server Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.

24.4 Настройка сервера TACACS+

Настройки сервера TACACS+ вводятся на показанном ниже экране. Более подробную информацию о серверах TACACS+ можно найти в разд. «RADIUS и TACACS+» на стр. 206. Перейдите по ссылке **TACACS+ Server Setup** на экране **AAA**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 136 Экран Advanced Application > AAA > TACACS+ Server Setup



Поля экрана описаны в следующей таблице.

Таблица 81 Экран Advanced Application > AAA > 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.
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.

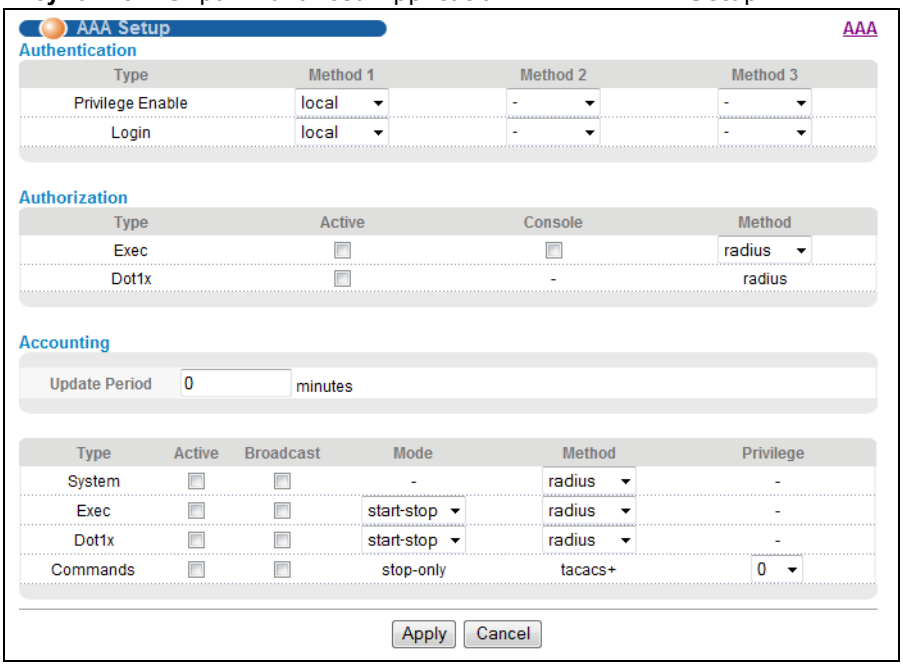
Таблица 81 Экран Advanced Application > AAA > TACACS+ Server Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.

24.5 Настройка AAA

С помощью этого экрана можно настроить параметры аутентификации и авторизации для коммутатора. Перейдите по ссылке **AAA Setup** на экране **AAA**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 137 Экран Advanced Application > AAA > AAA Setup



Поля экрана описаны в следующей таблице.

Таблица 82 Экран Advanced Application > AAA > AAA 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). Настройка привилегий доступа учетных записей посредством команд (см. Справочное руководство по интерфейсу командной строки) для **локальной** аутентификации. **TACACS+** и **RADIUS** представляют собой внешние серверы. Прежде чем установить приоритет, убедитесь, что соответствующая база данных правильно настроена. Для аутентификации уровня привилегий 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 уровня привилегий учетных записей администраторов, их необходимо указать в полях **Method 2** и **Method 3**. Выберите **local**, чтобы коммутатор проверял привилегии доступа, настроенные для локальной аутентификации. Выберите **radius** или **tacacs+**, чтобы коммутатор проверял привилегии доступа с использованием внешних серверов.
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. В случае выбора **tacacs+** для проверки учетных записей администраторов коммутатор будет обращаться к серверам TACACS+.
Authorization	С помощью этого раздела можно настроить параметры авторизации для коммутатора.
Type	Укажите, предоставляет ли коммутатор пользователям следующие услуги. • **Exec**: Разрешить администратору, который выполняет вход на коммутатор через Telnet или SSH, наличие иного уровня прав доступа, назначенного внешним сервером. • **Dot1x**: Разрешить клиенту IEEE 802.1x, наличие иных ограничений пропускной способности или иного идентификатора сети VLAN, назначенного внешним сервером.

Таблица 82 Экран Advanced Application > AAA > AAA Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы активировать функцию авторизации для указанных типов событий.
Console	Установите этот переключатель, чтобы разрешить администратору, который выполняет вход на коммутатор через консольный порт, наличие иного уровня прав доступа, назначенного внешним сервером.
Method	Выберите метод (RADIUS или TACACS+) для авторизации событий определенного типа. RADIUS является единственным методом авторизации для клиентов IEEE 802.1x.
Accounting	С помощью этого раздела можно настроить параметры учета для данного коммутатора.
Update Period	Периодичность в минутах, с которой коммутатор отправляет на сервер учета обновленную информацию. Данное значение используется только в том случае, если записей **Exec** или **Dot1x** выбрана опция **start-stop**.
Type	Данный коммутатор поддерживает отправку на сервер(ы) учета следующих типов событий: • **System** – при выборе этой опции коммутатор будет передавать информацию о следующих системных событиях: загрузка системы, отключение системы, включение учета на системе, отключение учета на системе. • **Exec** – при выборе этой опции коммутатор будет передавать информацию о входе и выходе администратора через консольный порт, telnet или SSH. • **Dot1x** – при выборе этой опции коммутатор будет передавать информацию о начале сессий клиентами IEEE 802.1x (аутентификация на коммутаторе), завершении сессий и промежуточных обновлениях состояния сессий. • **Commands** – при выборе этой опции коммутатор будет передавать информацию при выполнении на коммутаторе команд с указанным или более высоким уровнем привилегий.
Active	Установите этот переключатель, чтобы активировать функцию учета для указанных типов событий.
Broadcast	Установите данный переключатель, чтобы коммутатор передавал учетную информацию сразу на все настроенные серверы учета. Если этот переключатель не установлен, и у вас имеется два сервера учета, коммутатор будет передавать информацию на первый сервер учета, и только при отсутствии ответа от первого сервера попытается передать информацию на второй сервер учета.
Mode	Данный коммутатор поддерживает два режима регистрации событий входа в систему. Выберите одну из опций: • **start-stop** – коммутатор будет передавать на сервер учета информацию в момент начала пользовательской сессии, на ее протяжении (если она длится дольше, чем указано в поле **Update Period**) и в момент ее завершения. • **stop-only** – коммутатор будет передавать на сервер учета информацию только в момент завершения пользовательской сессии.
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, учетная информация о которых должна передаваться коммутатором. Коммутатор будет передавать учетную информацию при выполнении на коммутаторе команд с указанным или более высоким уровнем привилегий.

Таблица 82 Экран Advanced Application > AAA > AAA Setup (продолжение)

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

24.6 Справочная техническая информация

Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

24.6.1 Специальный атрибут производителя

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

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

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

Примечание: 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 83 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.

24.6.1.1 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 требуется настроить, приведены в следующей таблице. Значения, выделенные в таблице полужирным шрифтом, являются фиксированными в соответствии с RFC 3580.

Таблица 84 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.

24.6.2 Поддерживаемые атрибуты RADIUS

Атрибуты RADIUS представляют собой данные, используемые для определения конкретных элементов аутентификации 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.

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

24.6.3 Атрибуты, используемые для аутентификации

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

24.6.3.1 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

24.6.3.2 Атрибуты, используемые для входа пользователей

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

24.6.3.3 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

25

Защита от подмены IP-адресов

25.1 Обзор

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

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
- Идентификатор сети VLAN
- 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.

25.1.1 О чем рассказывается в этой главе

- С помощью экрана **IP Source Guard** (разд. 25.2 на стр. 218) можно посмотреть на текущие привязки для функций отслеживания DHCP и инспекции ARP-пакетов.
- С помощью экрана **IP Source Guard Static Binding** (разд. 25.3 на стр. 219) можно управлять статическими привязками для функций отслеживания DHCP и инспекции ARP-пакетов.
- С помощью экрана **DHCP Snooping** (разд. 25.4 на стр. 221) можно ознакомиться с различными статистическими данными из базы данных отслеживания DHCP.
- С помощью экрана **DHCP Snooping Configure** (разд. 25.5 на стр. 224) можно включить отслеживание DHCP на коммутаторе (но не для конкретных сетей VLAN), указать сеть VLAN, в которой располагается DHCP-сервер по умолчанию, а также настроить базу данных отслеживания.
- С помощью экрана **DHCP Snooping Port Configure** (разд. 25.5.1 на стр. 226) можно указать, какие порты являются доверенными, а какие – нет для отслеживания DHCP.
- С помощью экрана **DHCP VLAN Configure** (разд. 25.5.2 на стр. 228) можно включить отслеживание DHCP для каждой сети VLAN и указать, должен ли коммутатор добавлять информацию опции 82 агента ретрансляции DHCP в запросы DHCP, которые коммутатор ретранслирует на сервер DHCP в каждой сети VLAN.
- С помощью экрана **DHCP Snooping VLAN Port Configure** (разд. 25.5.3 на стр. 229) можно применить различные профили опции 82 DHCP к определенным портам в сети VLAN.

- С помощью экрана **ARP Inspection Status** (разд. 25.6 на стр. 230) можно ознакомиться с текущим списком фильтров по MAC-адресам, созданных в связи с обнаружением коммутатором несанкционированного пакета ARP.
- С помощью экрана **ARP Inspection VLAN Status** (разд. 25.7 на стр. 231) можно ознакомиться с различными статистическими данными о пакетах ARP в каждой сети VLAN.
- С помощью экрана **ARP Inspection Log Status** (разд. 25.8 на стр. 232) можно просмотреть сообщения журнала, которые были сгенерированы пакетами ARP и еще не были отправлены на сервер syslog.
- С помощью экрана **ARP Inspection Configure** (разд. 25.9 на стр. 234) можно включить инспекцию пакетов ARP 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.
- С помощью экрана **ARP Inspection Port Configure** (разд. 25.9.1 на стр. 235) можно указать, какие порты являются доверенными, а какие – нет для инспекции пакетов ARP.
- С помощью экрана **ARP Inspection VLAN Configure** (разд. 25.9.2 на стр. 237) можно включить инспекцию ARP для каждой сети VLAN и указать, в какие момент коммутатор должен генерировать сообщения журналов при получении пакетов ARP из каждой сети VLAN.

25.1.2 Что необходимо знать

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.

25.2 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 138 Экран Advanced Application > IP Source Guard

Поля экрана описаны в следующей таблице.

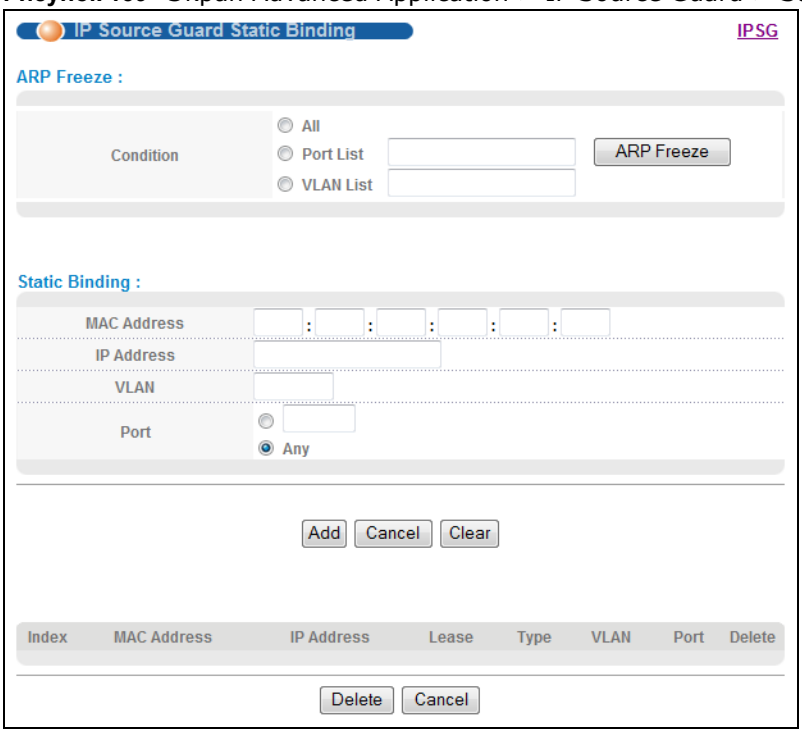
Таблица 85 Экран Advanced Application > IP Source Guard

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.

25.3 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 139 Экран Advanced Application > IP Source Guard > Static Binding



Поля экрана описаны в следующей таблице.

Таблица 86 Экран Advanced Application > IP Source Guard > Static Binding

ПОЛЕ	ОПИСАНИЕ
ARP Freeze	Функция ARP Freeze позволяет автоматически создавать статические привязки на основе текущих записей ARP (либо полученных динамически, либо статических) до тех пор, пока таблица привязок коммутатора не заполнится. Примечание: Для использования функции ARP Freeze необходимо выбрать в качестве режима запоминания ARP опцию **ARP-Request** на экране **IP Application > ARP Setup > ARP Learning**.
Condition	**All** – Если выбрать эту опцию и нажать кнопку **ARP Freeze**, коммутатор будет автоматически добавлять все текущие записи ARP в таблицу статических привязок. **Port List** – При выборе этой опции потребуется ввести список портов, используя в качестве разделителя запятую. После нажатия кнопки **ARP Freeze** коммутатор будет добавлять записи ARP, полученные на определенном порту (или портах) в таблицу статических привязок. **VLAN List** – При выборе этой опции потребуется указать список идентификаторов сетей VLAN, используя в качестве разделителя запятую. После нажатия кнопки **ARP Freeze** коммутатор будет добавлять записи ARP для указанных сетей VLAN в таблицу статических привязок.
Static Binding	
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.

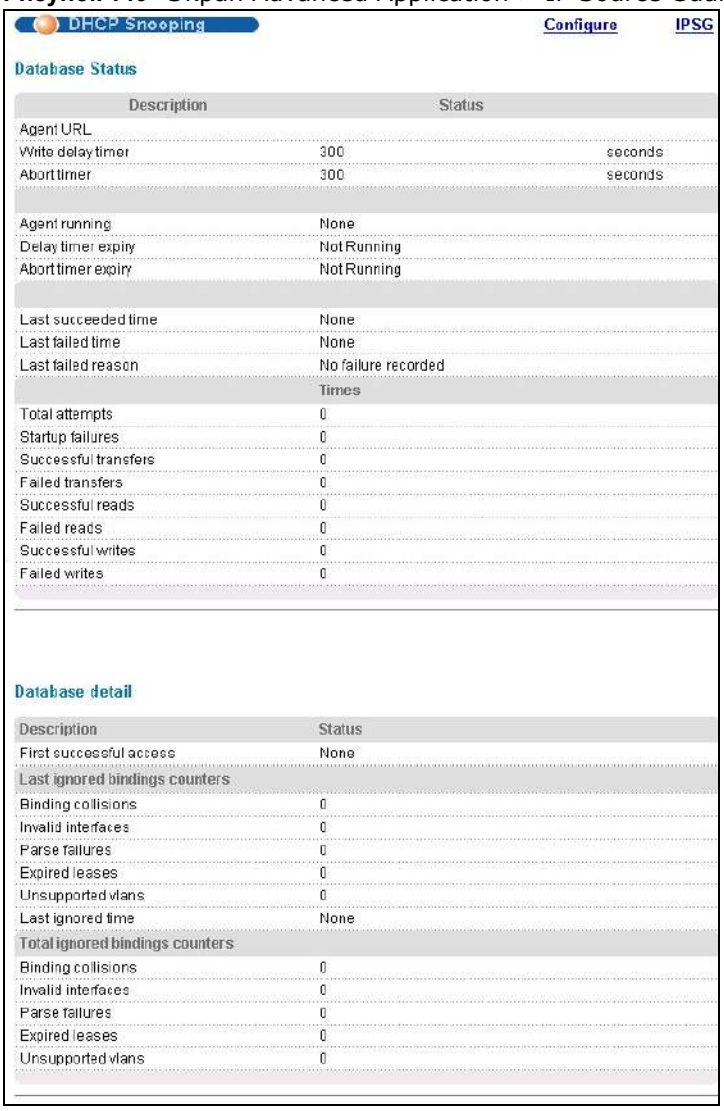
Таблица 86 Экран Advanced Application > IP Source Guard > Static Binding (продолжение)

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

25.4 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 140 Экран Advanced Application > IP Source Guard > DHCP Snooping



Поля экрана описаны в следующей таблице.

Таблица 87 Экран Advanced Application > IP Source Guard > 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. 25.5 на стр. 224.
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.

Таблица 87 Экран Advanced Application > IP Source Guard > DHCP Snooping (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.
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.

Таблица 87 Экран Advanced Application > IP Source Guard > DHCP Snooping (продолжение)

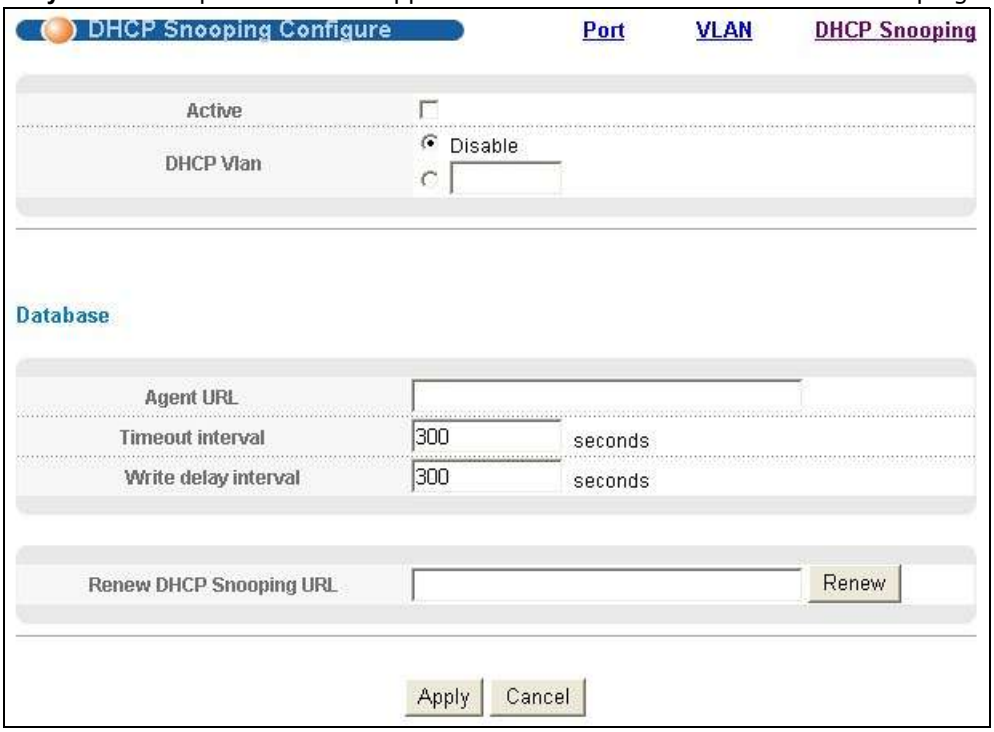
ПОЛЕ	ОПИСАНИЕ
Last ignored bindings counters	В этом разделе отображается количество случаев и причины, по которым коммутатором были проигнорированы привязки при последней попытке считывания привязок из базы данных отслеживания DHCP. Эти счетчики можно сбросить посредством перезапуска коммутатора или при помощи команд интерфейса командной строки. См. Справочное руководство по интерфейсу командной строки.
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 коммутатора 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 при помощи команд интерфейса командной строки. См. Справочное руководство по интерфейсу командной строки.
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 коммутатора 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.

25.5 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 141 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure



Поля экрана описаны в следующей таблице.

Таблица 88 Экран Advanced Application > IP Source Guard > 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 при включенном DHCP отсутствуют доверенные порты, то запросы DHCP выполняться не будут.
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. 25.5.2 на стр. 228). 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.

Таблица 88 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure

ПОЛЕ	ОПИСАНИЕ
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. 25.4 на стр. 221).
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.

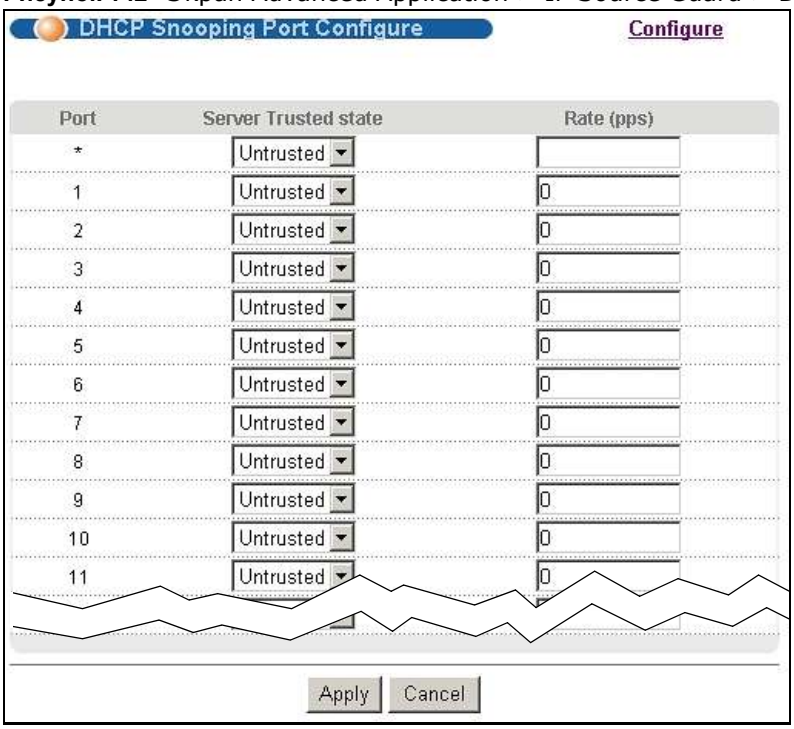
25.5.1 Настройка портов отслеживания DHCP

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

Примечание: Если при включенной функции отслеживания DHCP отсутствуют доверенные порты, то запросы DHCP не могут попасть на сервер 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 142 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port



Поля экрана описаны в следующей таблице.

Таблица 89 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port

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.

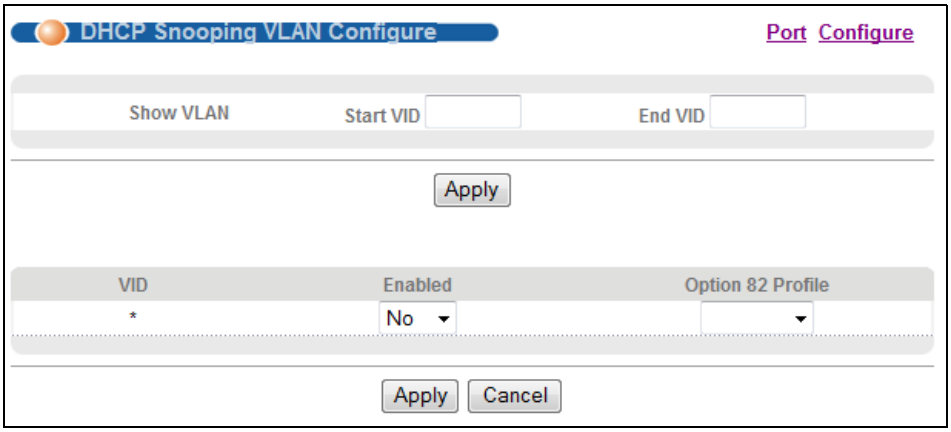
Таблица 89 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port

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.

25.5.2 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. 35 на стр. 304) 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 143 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN



Поля экрана описаны в следующей таблице.

Таблица 90 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN

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.

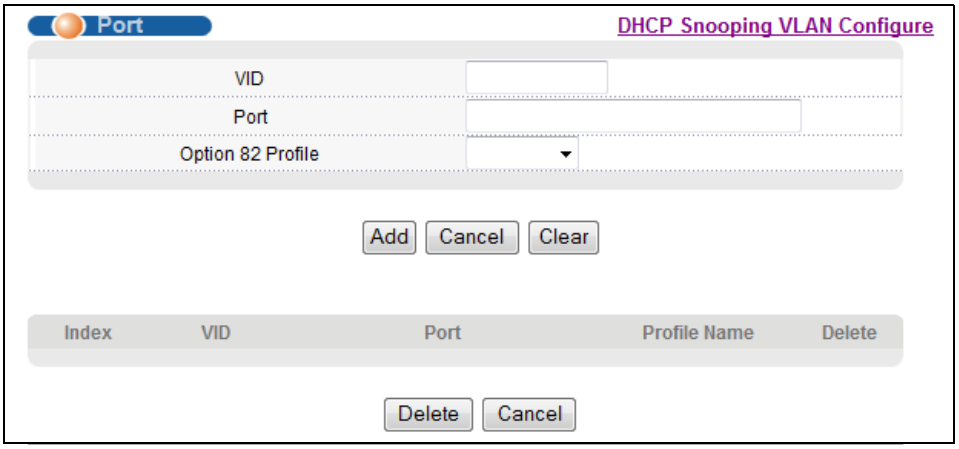
Таблица 90 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
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 при включенном DHCP отсутствуют доверенные порты, то запросы DHCP выполняться не будут.
Option 82 Profile	Выберите заранее созданный профиль опции 82 DHCP, который коммутатор применяет ко всем портам в указанной сети (или сетях) VLAN. Коммутатор добавляет определенную информацию (такую, как номер слота, номер порта, идентификатор сети VLAN и/или имя системы), указанную в профиле, в запросы DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN. Выбрать сеть VLAN DHCP можно на экране **DHCP Snooping Configure** (см. разд. 25.5 на стр. 224).
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.

25.5.3 Настройка порта сети VLAN отслеживания DHCP

С помощью этого экрана можно применить различные профили опции 82 DHCP к определенным портам в сети VLAN. Чтобы открыть этот экран, перейдите по ссылке **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN > Port.**

Рисунок 144 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN > Port



Поля экрана описаны в следующей таблице.

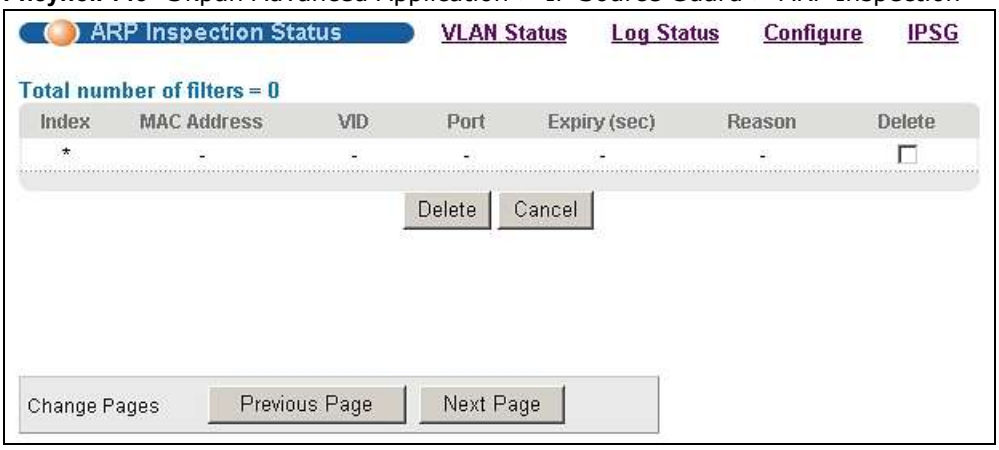
Таблица 91 Экран Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN > Port

ПОЛЕ	ОПИСАНИЕ
VID	Укажите идентификатор сети VLAN, параметры которой требуется настроить.
Port	Введите список портов, к которым необходимо применить указанный профиль опции 82 DHCP. В этом поле можно указать два и более портов, разделенных (без пробелов) символами запятой (,) или дефиса (-). Например, запись «3-5» будет означать порты 3, 4 и 5. Чтобы указать порты 3, 5 и 7, введите в этом поле значение «3,5,7».
Option 82 Profile	Выберите заранее созданный профиль опции 82, который коммутатор применяет к указанным портам в данной сети VLAN. коммутатор добавляет определенную информацию (такую, как номер слота, номер порта, идентификатор сети VLAN и/или имя системы), указанную в профиле, в запросы DHCP, которые он ретранслирует в сеть VLAN DHCP, если таковая указана, или в сеть VLAN. Выбрать сеть VLAN DHCP можно на экране **DHCP Snooping Configure** (см. разд. 25.5 на стр. 224). Профиль, выбранный на этом экране, имеет приоритет по отношению к профилю, выбранному на экране **DHCP Snooping > Configure > VLAN**.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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 на данную кнопку, чтобы сбросить значения из последней выбранной записи, или, если ничего не было выбрано, очистить перечисленные выше поля.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	В этом поле отображается порядковый номер каждой записи. Нажмите на этот номер, чтобы изменить настройки.
VID	Это поле показывает идентификатор сети VLAN, которой принадлежит данный порт (или порты).
Port	Это поле показывает порт (или порты), к которым коммутатор применяет данные настройки.
Profile Name	Это поле отображает профиль опции 82 DHCP, который коммутатор применяет к указанному порту (или портам).
Delete	Выберите записи, которые нужно удалить, в столбце **Delete** и нажмите кнопку **Delete**, чтобы удалить выбранные записи из таблицы.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей **Delete**.

25.6 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 145 Экран Advanced Application > IP Source Guard > ARP Inspection



Поля экрана описаны в следующей таблице.

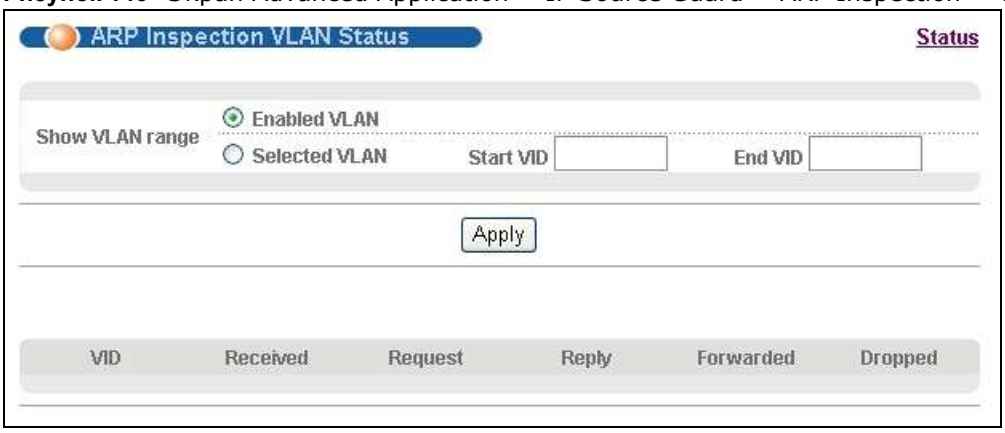
Таблица 92 Экран Advanced Application > IP Source Guard > ARP Inspection

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

25.7 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 146 Экран Advanced Application > IP Source Guard > ARP Inspection > VLAN Status



Поля экрана описаны в следующей таблице.

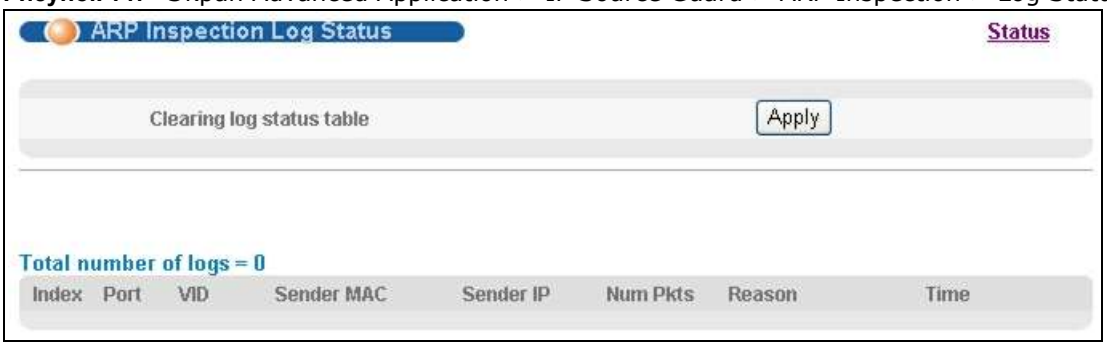
Таблица 93 Экран Advanced Application > IP Source Guard > ARP Inspection > VLAN Status

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.
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.

25.8 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 147 Экран Advanced Application > IP Source Guard > ARP Inspection > Log Status



Поля экрана описаны в следующей таблице.

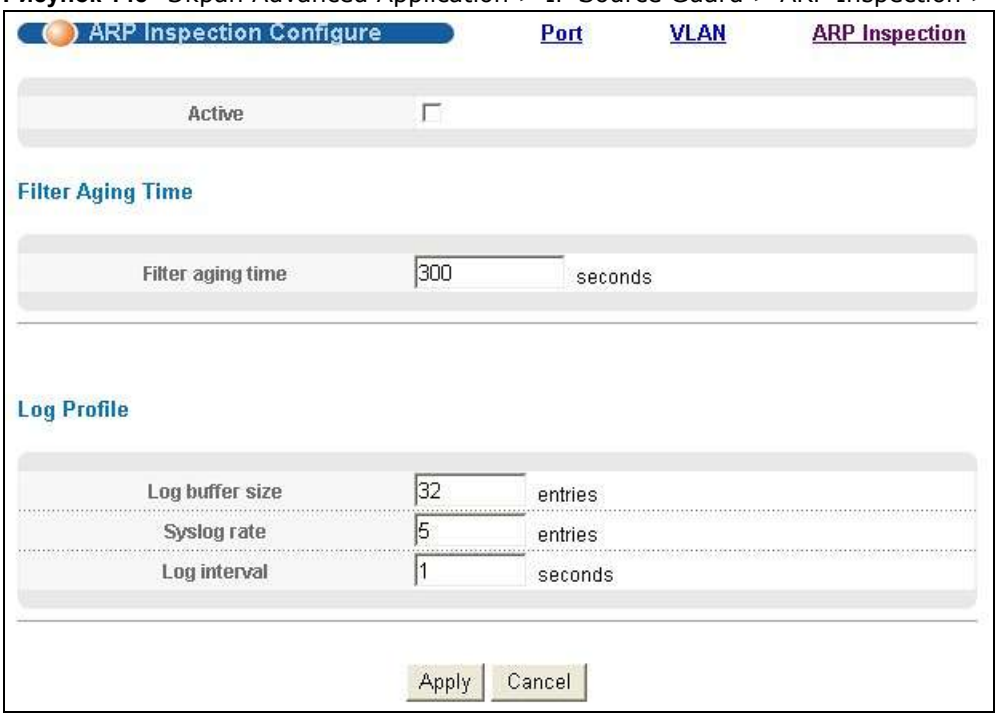
Таблица 94 Экран Advanced Application > IP Source Guard > ARP Inspection > Log Status

ПОЛЕ	ОПИСАНИЕ
Clearing log status table	Нажатие на **Apply** позволяет удалить все сообщения контрольного журнала, сгенерированные пакетами ARP, которые еще не были отправлены на сервер syslog.
Total number of logs	В данном поле отображается количество сообщений контрольного журнала, сгенерированных пакетами ARP, которые еще не были отправлены на сервер syslog. В случае отбрасывания одного или нескольких сообщений контрольного журнала из-за недоступности буфера соответствующие записи помечаются как **overflow**, с указанием текущего количества отброшенных сообщений.
Index	В этом поле отображается порядковый номер сообщения контрольного журнала.
Port	В этом поле отображается порт источника пакета ARP.
VID	В этом поле отображается идентификатор VLAN источника пакета ARP.
Sender MAC	В этом поле отображается MAC-адрес источника пакета ARP.
Sender IP	В этом поле отображается IP-адрес источника пакета ARP.
Num Pkts	В этом поле отображается количество пакетов ARP, консолидированных в данном сообщении контрольного журнала. Данный коммутатор консолидирует в одно сообщение идентичные сообщения контрольного журнала, сгенерированные пакетами ARP, за установленный период консолидации. Это период настраивается на экране **ARP Inspection Configure**.См. разд. 25.9 на стр. 234.
Reason	В этом поле отображается причина, по которой было сгенерировано сообщение в журнале. **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. 25.9.2 на стр. 237.
Time	В этом поле отображается время, в которое было сгенерировано сообщение контрольного журнала.

25.9 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 148 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure



Поля экрана описаны в следующей таблице.

Таблица 95 Экран Advanced Application > IP Source Guard > 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. Укажите период времени (от 1 до 2147483647 секунд), в течение которого фильтр по MAC-адресам будет действовать на коммутаторе с момента обнаружения коммутатором несанкционированного пакета ARP. По истечении этого времени фильтр MAC-адресов автоматически удаляется коммутатором. Чтобы фильтр MAC-адреса действовал постоянно, необходимо ввести в это поле значение 0.
Log Profile	

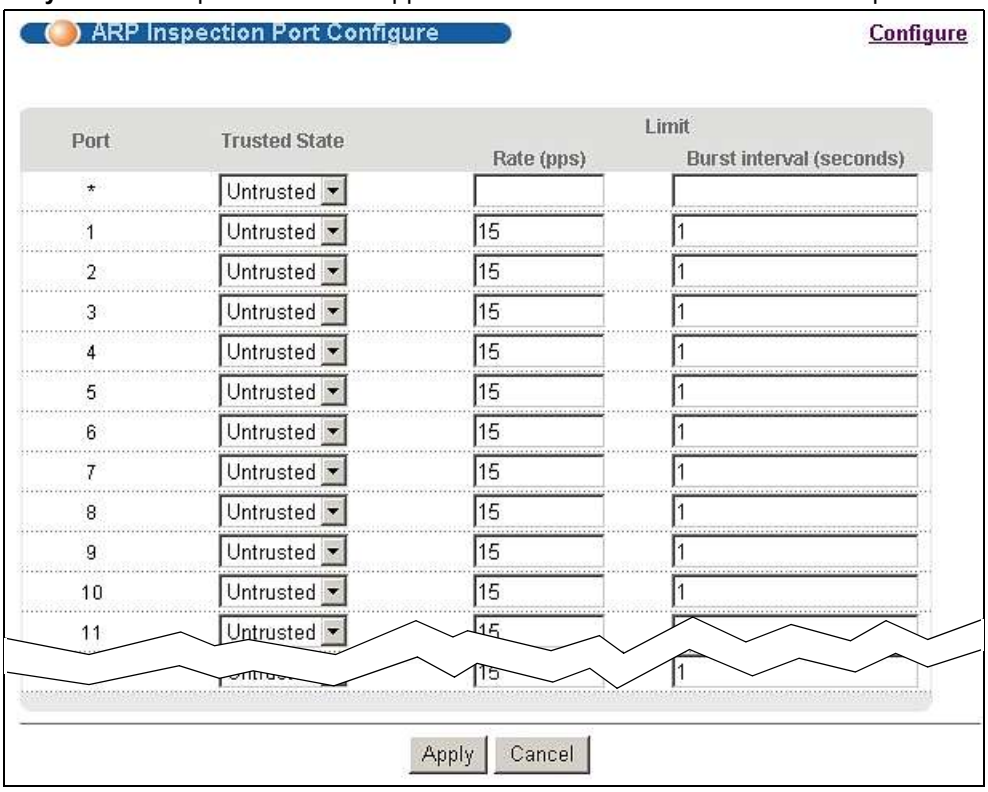
Таблица 95 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure

ПОЛЕ	ОПИСАНИЕ
Log buffer size	Введите максимальное количество сообщений контрольного журнала (от 1 до 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. 25.8 на стр. 232.
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. 40 на стр. 361). 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 5 сообщений 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.

25.9.1 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 149 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port



Поля экрана описаны в следующей таблице.

Таблица 96 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

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.

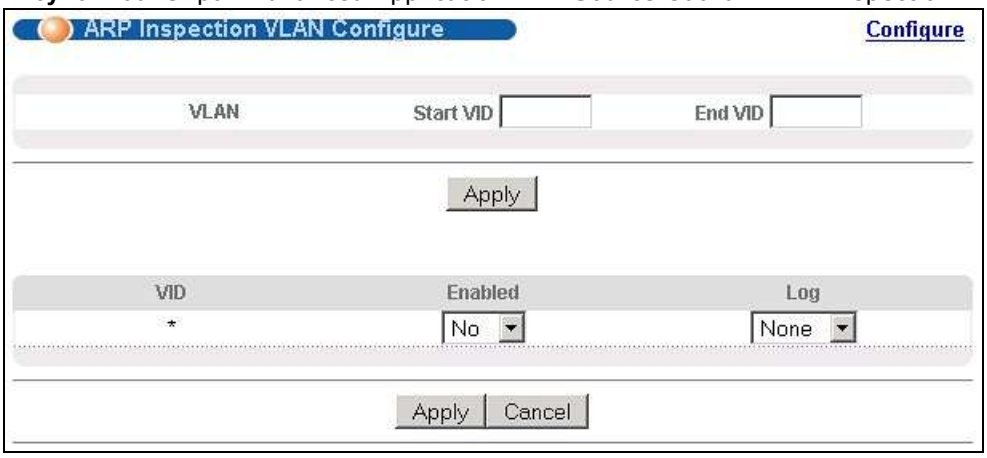
Таблица 96 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > Port

ПОЛЕ	ОПИСАНИЕ
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 будет принимать не более 15 пакетов ARP в течение каждого 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).
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.

25.9.2 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 150 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN



Поля экрана описаны в следующей таблице.

Таблица 97 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN

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.

Таблица 97 Экран Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN (продолжение) (продолжение)

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

25.10 Справочная техническая информация

Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

25.10.1 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.

25.10.1.1 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.

Примечание: Если при включенном DHCP отсутствуют доверенные порты, то запросы DHCP выполняться не будут.

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.

25.10.1.2 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 151 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.

25.10.1.3 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. 35 на стр. 304.

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. 35 на стр. 304).

25.10.1.4 Настройка отслеживания DHCP

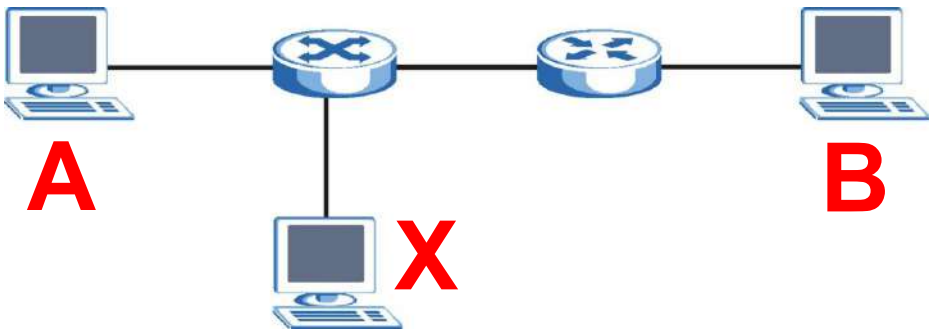
Чтобы настроить на коммутаторе функцию отслеживания DHCP, выполните следующие действия.

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.

25.10.2 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 152 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 связь между компьютером **A** и компьютером **B** полностью осуществляется через компьютер **X**. Компьютер **X** может считывать и изменять информацию, передаваемую между указанными двумя компьютерами.

25.10.2.1 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. 12 на стр. 116).

- 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 результатах команд **ARP Inspection** и не видны на экранах и в результатах команд **MAC Address Filter**.

25.10.2.2 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.

25.10.2.3 Системный журнал Syslog

При пересылке или отбрасывании пакетов ARP коммутатор может отправлять сообщения системного журнала syslog на указанный сервер syslog (гл. 40 на стр. 361). В целях большей эффективности коммутатор может консолидировать сообщения контрольного журнала и отправлять их партиями.

25.10.2.4 Настройка инспекции ARP-пакетов

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

1 Настройте отслеживание DHCP. См. разд. 25.10.1.4 на стр. 240.

Примечание: 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.

26

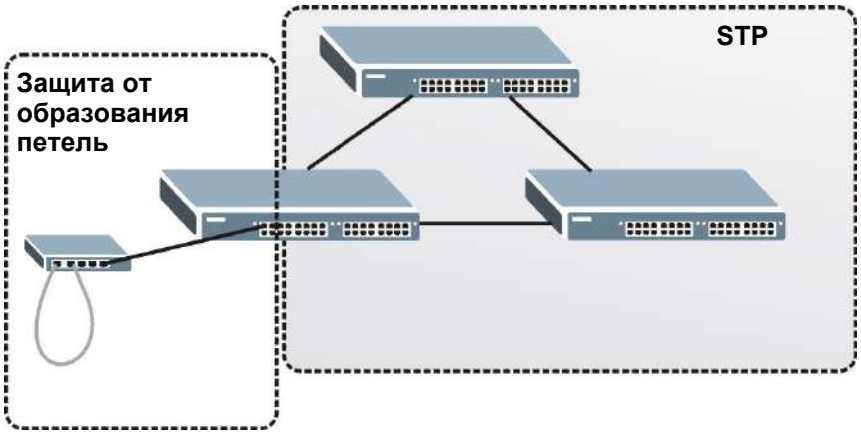
Защита от образования петель

26.1 Обзор функции защиты от образования петель

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

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 153 Защита от образования петель и STP



Дополнительную информацию можно найти в разд. 26.1.2 на стр. 243.

26.1.1 О чем рассказывается в этой главе

С помощью экрана **Loop Guard** (разд. 26.2 на стр. 245) можно включить функцию защиты от образования петель на коммутаторе и определенных портах.

26.1.2 Что необходимо знать

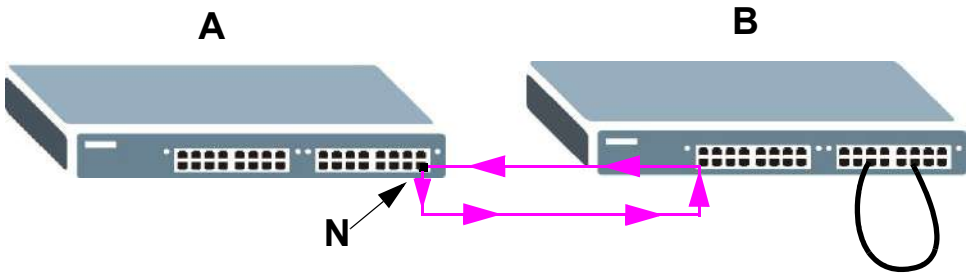
Функция защиты от образования петель предназначена специально для устранения проблем на границе сети. Проблема может возникнуть при подключении порта к коммутатору, на котором образовалась петля. Петля образуется в результате человеческой ошибки. Она возникает, когда два порта коммутатора оказываются 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 рисунке ниже изображен порт **N** коммутатора **A**, подключенный к коммутатору **B**. Коммутатор **B** находится в состоянии петли. При выходе широковещательных или многоадресных сообщений из порта **N** и их поступлении на коммутатор **B** эти сообщения вновь направляются на порт **N** коммутатора **A**, после их ретрансляции коммутатором B.

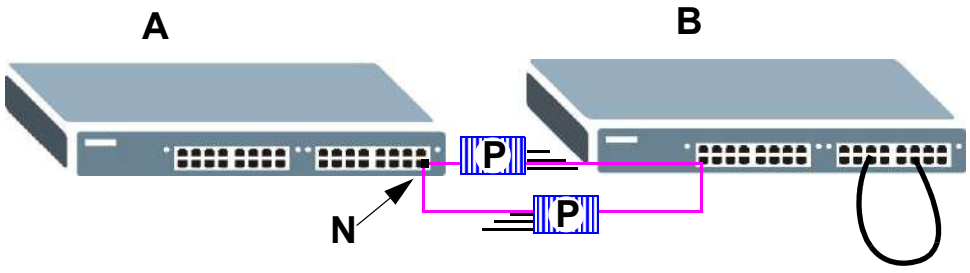
Рисунок 154 Коммутатор с петлей



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.

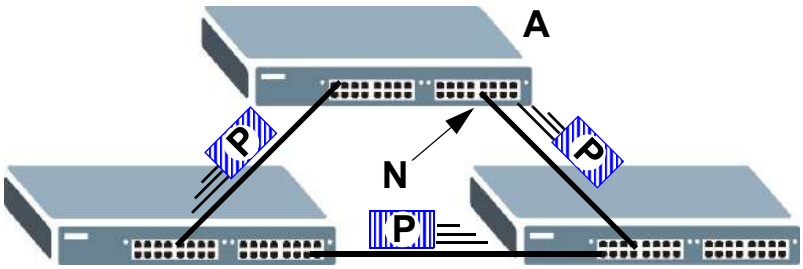
На рисунке ниже изображен порт **N** коммутатора **A** с включенной функцией защиты от образования петель, который посылает пробный пакет **P** на коммутатор **B**. Поскольку коммутатор **B** находится в состоянии петли, пробный пакет **P** возвращается на порт **N** коммутатора **A**. Затем коммутатор закрывает порт **N**, чтобы оградить остальную часть сети от влияния коммутатора, находящегося в состоянии петли.

Рисунок 155 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 будет закрывать порт **N** всякий раз, когда пробный пакет возвращается на коммутатор.

Рисунок 156 Защита от образования петель – петля в сети



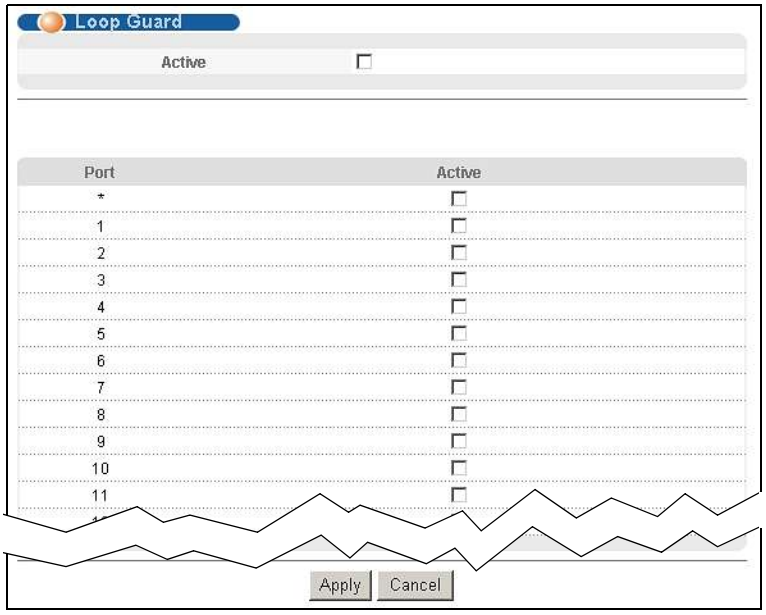
Примечание: После устранения проблемы с петлей в сети отключенный порт можно снова активировать через web-конфигуратор (см. разд. 8.7 на стр. 70) или при помощи команд (см. Справочное руководство по интерфейсу командной строки).

26.2 Настройка защиты от образования петель

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

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

Рисунок 157 Экран Advanced Application > Loop Guard



Поля экрана описаны в следующей таблице.

Таблица 98 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.

27

Туннелирование протоколов уровня 2

27.1 Обзор туннелирования протоколов уровня 2

В этой главе описан процесс настройки туннелирования протоколов уровня 2 на коммутаторе.

Туннелирование протоколов уровня 2 (L2PT) используется на граничных устройствах провайдеров услуг.

27.1.1 О чем рассказывается в этой главе

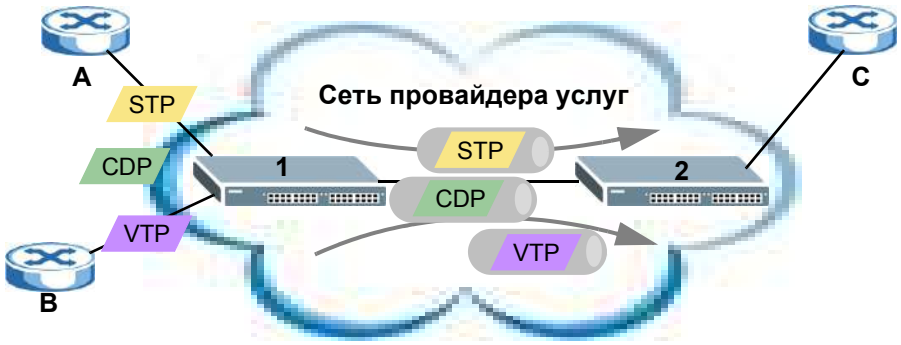
С помощью экрана **Layer 2 Protocol Tunnel** (разд. 27.2 на стр. 248) можно включить на коммутаторе туннелирование протоколов уровня 2 и указать MAC-адрес, который коммутатор будет использовать для инкапсуляции пакетов протоколов уровня 2 посредством замены в них MAC-адреса назначения.

27.1.2 Что необходимо знать

Туннелирование протоколов уровня 2 (L2PT) используется на граничных устройствах провайдеров услуг.

Функция L2PT позволяет граничным коммутаторам (**1** и **2** на рисунке ниже) туннелировать пакеты протоколов уровня 2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) и VTP (VLAN Trunking Protocol), циркулирующие между коммутаторами клиента (**A**, **B** и **C** на рисунке ниже), подключенными через сеть провайдера услуг. Граничный коммутатор инкапсулирует пакеты протоколов уровня 2 с помощью определенного MAC-адреса перед тем, как отправлять их через сеть провайдера услуг на другие граничные коммутаторы.

Рисунок 158 Сетевой сценарий туннелирования протоколов уровня 2

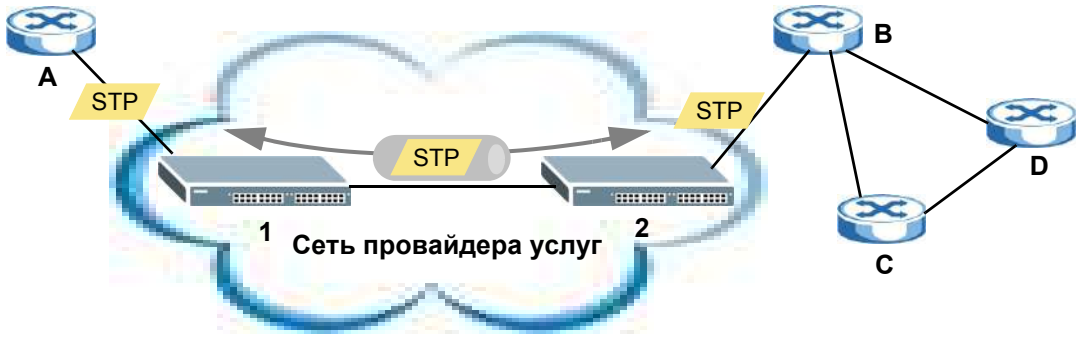


Если в приведенном ниже примере включить функцию L2PT для протокола STP, коммутаторы **A**, **B**, **C** и **D** будут находиться в одном и том же покрывающем дереве, несмотря на то, что

коммутатор **A** не подключен напрямую к коммутаторам **B**, **C** и **D**. Информация об изменении топологии может распространяться через сеть провайдера услуг.

Чтобы эмулировать топологию типа «точка-точка» между двумя коммутаторами клиента, находящимися на различных площадках, например, **A** и **B**, можно включить функцию туннелирования протоколов на граничных коммутаторах **1** и **2** для протоколов PAgP (Port Aggregation Protocol), LACP или UDLD (UniDirectional Link Detection).

Рисунок 159 Пример сети с использованием L2PT



27.1.2.1 Режим туннелирования протоколов уровня 2

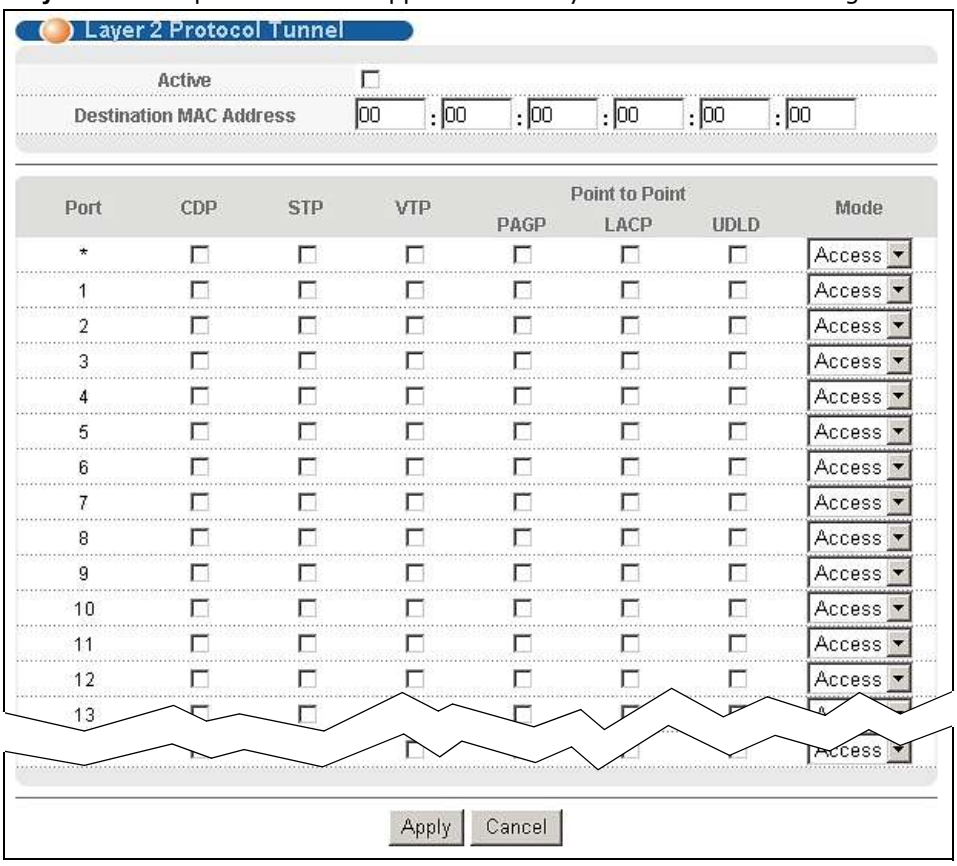
Каждый порт может использовать два режима туннелирования протоколов уровня 2, **Access** (Доступ) и **Tunnel** (Туннель).

- Порт доступа **Access** – это входящий порт на граничном устройстве провайдера услуг (**1** или **2** на рис. 159 на стр. 248), который подключен к коммутатору клиента (**A** или **B**). Коммутатор инкапсулирует пакеты протокола уровня 2, принимаемые через порт доступа, и пересылает их на туннельные порты.
- Туннельный порт **Tunnel** – это исходящий порт на граничном устройстве сети провайдера услуг, который подключен к другому коммутатору провайдера услуг. Входящие инкапсулированные пакеты протокола уровня 2, принимаемые через туннельный порт, декапсулируются и пересылаются на порт доступа.

27.2 Настройка туннелирования протоколов уровня 2

Выберите в навигационной панели **Advanced Application** > **Layer 2 Protocol Tunneling**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 160 Экран Advanced Application > Layer 2 Protocol Tunneling



Поля экрана описаны в следующей таблице.

Таблица 99 Экран Advanced Application > Layer 2 Protocol Tunneling

ПОЛЕ	ОПИСАНИЕ
Active	Выберите эту опцию, если требуется включить туннелирование протоколов уровня 2 на коммутаторе.
Destination MAC Address	Укажите MAC-адрес, который коммутатор будет использовать для инкапсуляции пакетов уровня 2 путем замены в них MAC-адреса назначения. Примечание: В этом поле можно указать как одноадресный, так и MAC-адрес многоадресной рассылки. При использовании MAC-адреса одноадресной рассылки удостоверьтесь, что он отсутствует в таблице адресов коммутатора в сети провайдера услуг. Примечание: Все граничные коммутаторы в сети провайдера услуг должны использовать для инкапсуляции один и тот же MAC-адрес.
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.
CDP	При выборе этой опции коммутатор будет туннелировать пакеты CDP (Cisco Discovery Protocol) с тем, чтобы обеспечить обнаружение других устройств Cisco в сети провайдера услуг.

Таблица 99 Экран Advanced Application > Layer 2 Protocol Tunneling (продолжение)

ПОЛЕ	ОПИСАНИЕ
STP	При выборе этой опции коммутатор будет туннелировать пакеты STP (Spanning Tree Protocol) с тем, чтобы обеспечить нормальное функционирование протокола STP в сети провайдера услуг и возможность создания покрывающих деревьев на основе информации о мостах изо всех сетей, локальных и удаленных.
VTP	При выборе опции коммутатор будет туннелировать пакеты VTP (VLAN Trunking Protocol) с тем, чтобы все клиентские коммутаторы могли использовать одинаковую конфигурацию VLAN во всей сети провайдера услуг.
Point to Point	коммутатор поддерживает туннелирование протоколов PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) и UDLD (UniDirectional Link Detection) для топологии типа «точка-точка». И PAgP, и UDLD являются внутрифирменными протоколами канального уровня Cisco. PAgP аналогичен LACP и используется для организации автоматической логической агрегации портов Ethernet. UDLD служит для определения физического статуса соединения и обнаружения однонаправленных каналов.
PAGP	При выборе этой опции коммутатор будет пересылать пакеты PAgP партнерским устройствам для автоматической установки соединения и создания логической агрегации портов.
LACP	При выборе этой опции коммутатор будет пересылать пакеты LACP партнерским устройствам для динамического создания групп портов и управления ими.
UDLD	При выборе этой опции коммутатор будет пересылать пакеты UDLD на порт партнерского устройства, к которому он подключен, для отслеживания физического статуса соединения.
Mode	При выборе опции **Access** коммутатор будет инкапсулировать входящие пакеты протоколов уровня 2 и пересылать их на туннельный порт (или порты). Опцию **Access** следует выбирать для входящих портов на границе сети провайдера услуг. Примечание: Включить туннелирование для протоколов уровня 2 STP, LACP, VTP, CDP, UDLD и PAGP можно только на портах доступа. Опцию **Tunnel** следует выбирать только для граничных устройств сети провайдера услуг. В этм случае коммутатор будет декапсулировать инкапсулированные пакеты протоколов уровня 2, полученные через туннельный порт, путем подмены текущего MAC-адреса назначения на исходный и последующей их пересылки на порт доступа. Если данная функция не включена на порту доступа, то пакеты для этих протоколов будут отбрасываться.
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

PPPoE

28.1 Обзор промежуточных агентов PPPoE

В этой главе рассказывается о том, каким образом коммутатор предоставляет серверу терминации PPPoE дополнительную информацию, которую тот может использовать для идентификации и аутентификации клиента PPPoE.

Промежуточный агент PPPoE (PPPoE Intermediate Agent, PPPoE IA) используется в процессе взаимодействия между сервером и клиентами PPPoE. Он помогает серверу PPPoE идентифицировать и аутентифицировать клиентов путем добавления информации об абонентской линии в пакеты обнаружения PPPoE, поступающие от клиентов, в разрезе отдельных портов и сочетаний «порт-сеть VLAN», перед тем, как переслать их на сервер PPPoE.

28.1.1 О чем рассказывается в этой главе

- Экран **PPPoE** (разд. 28.2 на стр. 254) служит для настройки основных параметров PPPoE.
- С помощью экрана **Intermediate Agent** (разд. 28.3 на стр. 254) можно включить на коммутаторе промежуточный агент PPPoE.
- С помощью экрана **PPPoE IA Per-Port** (разд. 28.3.1 на стр. 255) можно задать состояние отдельных портов и настроить для них субопции промежуточных агентов PPPoE.
- С помощью экрана **PPPoE IA Per-Port Per-VLAN** (разд. 28.3.2 на стр. 257) можно настроить параметры промежуточных агентов PPPoE, которые применяются к определенной сети VLAN на определенном порту.
- С помощью экрана **PPPoE IA for VLAN**(разд. 28.3.3 на стр. 258) можно включить промежуточный агент PPPoE для определенной сети VLAN.

28.1.2 Что необходимо знать

Ознакомьтесь с информацией о протоколе ARP, которая поможет при работе с экранами, описанными в этой главе.

28.1.2.1 Формат тегов промежуточных агентов PPPoE

При включенном промежуточном агенте PPPoE коммутатор добавляет тег с информацией от производителя в пакеты PADI (PPPoE Active Discovery Initialization) и PADR (PPPoE Active

Discovery Request), приходящие от клиентов PPPoE. Этот тег описан в RFC 2516 и для данной функции имеет следующий формат.

Таблица 100 Формат тега с информацией от производителя для промежуточного агента PPPoE

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

Значение поля Tag_Type для тегов с информацией от производителя равно 0x0105, как указано в RFC 2516. Значение поля Tag_Len указывает на длину полей Value, i1 и i2. Значением поля Value является 32-разрядное число 0x00000DE9, которое соответствует записи IANA «ADSL Forum». Поля i1 и i2 представляют собой субопции промежуточного агента PPPoE, которые содержат дополнительную информацию о клиенте PPPoE.

28.1.2.2 Формат субопций

Существует два типа субопций: «Agent Circuit ID Sub-option» и «Agent Remote ID Sub-option». Они имеют следующие форматы.

Таблица 101 Формат субопции PPPoE IA Circuit ID: Строка, вводимая пользователем

Субопция	Длина	Значение
0x01 (1 байт)	N (1 байт)	Строка (63 байта)

Таблица 102 Формат субопции PPPoE IA Remote ID

Субопция	Длина	Значение
0x02 (1 байт)	N (1 байт)	MAC-адрес или строка (63 байта)

Значение 1 в первом поле идентифицирует субопцию Agent Circuit ID, а значение 2 – субопцию Agent Remote ID. Следующее поле определяет длину поля. Данный коммутатор воспринимает строку Circuit ID, введенную вручную для сети VLAN на данном порту, как значение первого приоритета, а строку Circuit ID, указанную для порта – как значение второго приоритета. Если не указать ни одной строки, определяемой пользователем, то коммутатор будет помещать в субопцию Agent Remote ID MAC-адрес клиента PPPoE.

Гибкий синтаксис Circuit ID за счет использования строк-идентификаторов и переменных

Если не указать строку Circuit ID для определенной сети VLAN на определенном порту или для определенного порта, коммутатор будет добавлять заданные пользователем строку-идентификатор и переменные в субопцию Agent Circuit ID. В качестве переменных можно использовать идентификатор слота клиента PPPoE, номер порта клиента PPPoE и/или идентификатор сети VLAN в пакете PPPoE.

В качестве разделителя для строк-идентификаторов, идентификаторов слотов, номеров портов и идентификаторов сети VLAN ID можно использовать символ «решетки» (#), двоеточие (;), точку (.), запятую (,), прямую косую черту (/) и пробел. Субопция Agent Circuit ID может выглядеть, например, так «коммутатор/07/0123». Это означает, что пакеты PPPoE

приходят от клиента PPPoE, который подключен к порту 7 коммутатора и входит в сеть VLAN 123.

Таблица 103 Формат субопции PPPoE IA Circuit ID: Использование строк-идентификаторов и переменных

Субопция	Длина	Значение						
0x01 (1 байт)	N (1 байт)	Строка-идентификатор (53 байта)	Разделитель (1 байт)	Идентификатор слота (1 байт)	Разделитель (1 байт)	Номер порта (2 байта)	Разделитель (1 байт)	VLAN ID (4 байта)

Синтаксис Circuit ID по умолчанию (WT-101)

Если не указать строку Circuit ID для определенной сети VLAN на определенном порту или для определенного порта и отключить опцию гибкого синтаксиса Circuit ID на экране **PPPoE > Intermediate Agent**, то коммутатор будет автоматически генерировать строку Circuit ID в соответствии с правилами синтаксиса Circuit ID по умолчанию, описанными в документе DSL Forum Working Text (WT)-101. Идентификатором узла доступа по умолчанию является имя хоста промежуточного агента PPPoE, подстрока «eth» обозначает «Ethernet».

Таблица 104 Формат субопции PPPoE IA Circuit ID: Описан в документе WT-101

Субопция	Длина	Значение								
0x01 (1 байт)	N (1 байт)	Идентификатор узла доступа (20 байт)	Тип антенны (1 байт)	eth (3 байта)	Тип антенны (1 байт)	Идентификатор слота (1 байт)	/ (1 байт)	Номер порта (2 байта)	: (1 байт)	VLAN ID (4 байта)

28.1.2.3 Состояние порта

Промежуточный агент PPPoE 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 или инспекции ARP-пакетов. Существует возможность указать субопции агента (circuit ID и remote ID), которые коммутатор будет добавлять в пакеты PADI и PADR, приходящие от клиентов PPPoE.

Доверенные порты подключаются к серверам PPPoE.

- Если сервер PPPoE посылает пакет PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation) или PADT (PPPoE Active Discovery Terminate), и он приходит на доверенный порт, то коммутатор пересылает его на все остальные порты.
- Если пакет PADI или PADR приходит от клиента PPPoE на доверенный порт, то коммутатор пересылает его на другие доверенные порты.

Примечание: Если включить промежуточный агент PPPoE и не определить ни одного доверенного порта, коммутатор будет отбрасывать все пакеты обнаружения PPPoE.

Не заслуживающие доверия порты подключаются к абонентам.

- Если пакет PADI, PADR или PADT приходит от клиента PPPoE на не заслуживающий доверия порт, то коммутатор добавляет к нему тег с информацией от производителя, а затем пересылает пакет на доверенные порты.

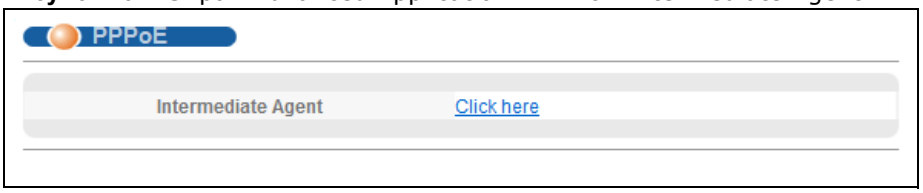
- коммутатор отбрасывает пакеты PADO и PADS, пришедшие от сервера PPPoE на не заслуживающий доверия порт.

28.2 Экран PPPoE

С помощью этого экрана можно настроить параметры промежуточного агента PPPoE на коммутаторе.

Выберите в навигационной панели **Advanced Application** > **PPPoE**, чтобы открыть экран, изображенный на рисунке ниже. Перейдите по ссылке **Click Here**, чтобы открыть экран **Intermediate Agent**.

Рисунок 161 Экран Advanced Application > PPPoE Intermediate Agent

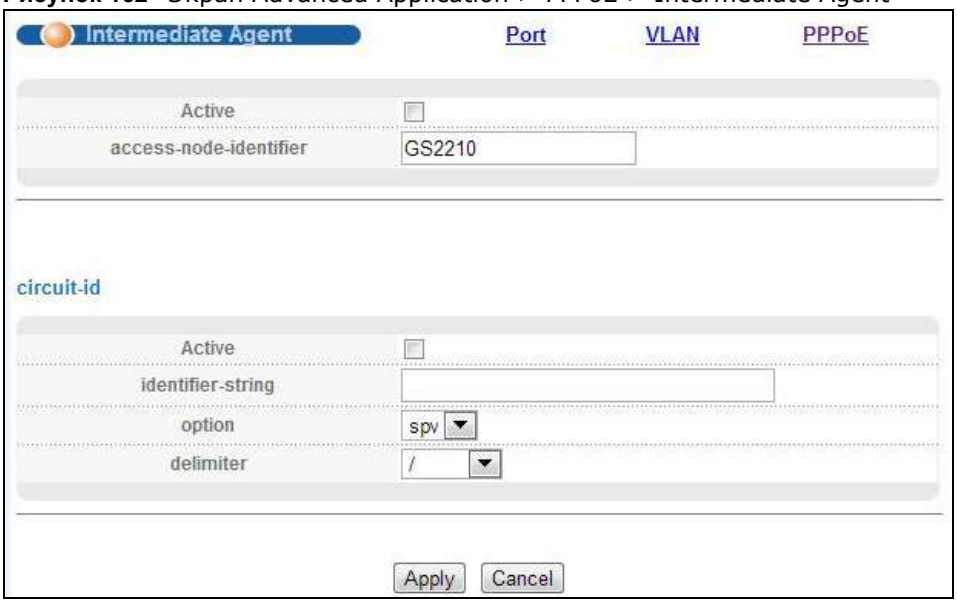


28.3 Экран PPPoE Intermediate Agent

С помощью этого экрана можно настроить механизм предоставления коммутатором дополнительной информации об абонентах серверу терминации PPoE, которую последний может использовать для идентификации и аутентификации клиентов PPPoE.

Выберите в навигационной панели **Advanced Application** > **PPPoE > Intermediate Agent**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 162 Экран Advanced Application > PPPoE > Intermediate Agent



Поля экрана описаны в следующей таблице.

Таблица 105 Экран Advanced Application > PPPoE > Intermediate Agent

ПОЛЕ	ОПИСАНИЕ
Active	Выберите эту опцию, чтобы включить промежуточный агент PPPoE на коммутатор в целом.
access-node-identifier	Введите строку, состоящую не более чем из 20 ASCII-символов, для идентификации промежуточного агента PPPoE. Строка также может содержать дефисы (-) и пробелы. По умолчанию в качестве идентификатора выбирается имя хоста коммутатора.
circuit-id	В этом разделе можно указать содержимое поля Circuit ID в пакетах PADI и PADR. Значение Circuit ID, указанное для конкретного порта или для конкретной сети VLAN на определенном порту, имеет приоритет перед этим значением. Значение Circuit ID, указанное для конкретного порта (на экране **Advanced Application > PPPoE > Intermediate Agent > Port**) или для конкретной сети VLAN на определенном порту (на экране **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN**) имеет приоритет перед этим значением. Таким образом, если предполагается настроить параметры PPPoE IA Per-Port или Per-Port Per-VLAN, эти поля нужно оставить пустыми и задать настройки circuit-id и remote-id на экране Per-Port или Per-Port Per-VLAN.
Active	При выборе этой опции коммутатор будет добавлять строку-идентификатор, задаваемую пользователем, и переменные (указанные в поле **option**) в пакеты PADI или PADR, приходящие от клиентов PPPoE. Если не выбирать данную опцию и не настроить какой-либо строки Circuit ID (при помощи команд интерфейса командной строки) на коммутаторе, то коммутатор будет использовать строку, указанную в поле **access-node-identifier**.
identifier-string	Укажите строку, которую коммутатор будет добавлять в субопцию Agent Circuit ID. Примечание может содержать до 53 ASCII-символов. В этом поле можно использовать пробелы.
option	Выберите переменные, которые коммутатор будет генерировать и добавлять в субопцию Agent Circuit ID. Для выбора доступны следующие варианты переменных: **sp**, **sv**, **pv** и **spv**, которые описывают сочетания «слот-порт», «слот-сеть VLAN», «порт-сеть VLAN» и «слот-порт-сеть VLAN» соответственно. В качестве значения слота коммутатор добавляет ноль в пакеты PADI и PADR.
delimiter	Выберите разделитель, который будет отделять строку-идентификатор, идентификатор слота, номер порта и/или идентификатор сети VLAN друг от друга. В качестве разделителя можно использовать символ «решетка» (**#**), точку с запятой (**;**), точку (**.**), запятую (**,**), прямую косую черту (**/**) или пробел.
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.

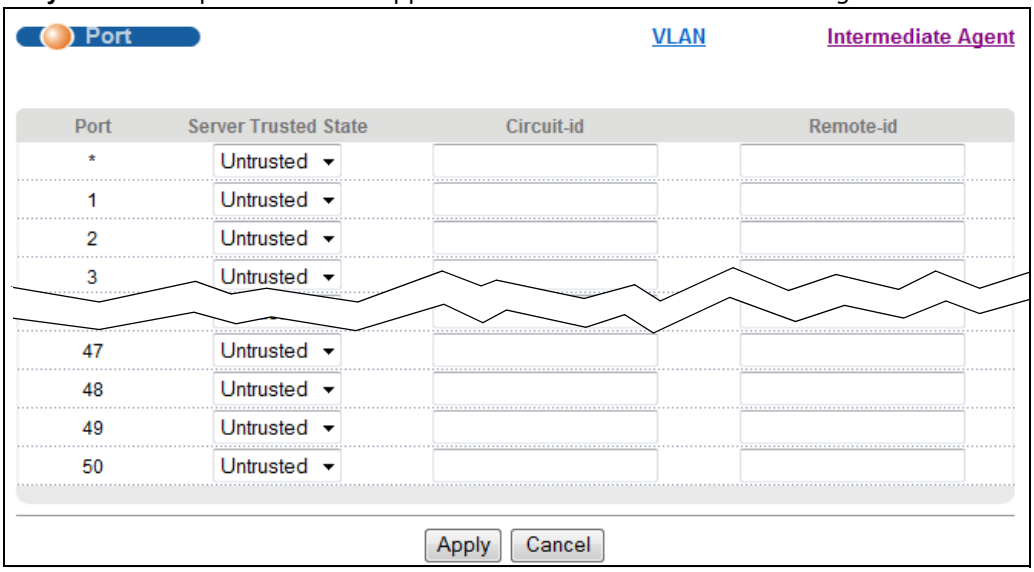
28.3.1 Экран PPPoE IA Per-Port

С помощью этого экрана можно выбрать доверенные и не заслуживающие доверия порты и указать, что коммутатор должен добавлять дополнительную информацию в пакеты обнаружения PPPoE, поступающие от клиентов PPPoE на определенные порты.

Примечание: коммутатор будет отбрасывать все пакеты PPPoE, если отключить промежуточный агент PPPoE на коммутаторе и не определить ни одного доверенного порта.

Перейдите по ссылке **Port** на экране **Intermediate Agent**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 163 Экран Advanced Application > PPPoE > Intermediate Agent > Port



Поля экрана описаны в следующей таблице.

Таблица 106 Экран Advanced Application > PPPoE > Intermediate Agent > Port

ПОЛЕ	ОПИСАНИЕ
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. Изменения в данной строке сразу же копируются на все порты.
Server Trusted State	Выберите, будет ли данный порт считаться доверенным (**Trusted**) или не заслуживающим доверия (**Untrusted**). Доверенными являются порты каскадирования, подключенные к серверам PPPoE. Если сервер PPPoE посылает пакет PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation) или PADT (PPPoE Active Discovery Terminate), и он приходит на доверенный порт, то коммутатор пересылает его на все остальные порты. Если пакет PADI или PADR приходит от клиента PPPoE на доверенный порт, то коммутатор пересылает его на другие доверенные порты. Не заслуживающими доверия являются исходящие порты, подключенные к абонентам. Если пакет PADI, PADR или PADT приходит от клиента PPPoE на не заслуживающий доверия порт, то коммутатор добавляет к нему тег с информацией от производителя, а затем пересылает пакет на доверенные порты. коммутатор отбрасывает пакеты PADO и PADS, пришедшие от сервера PPPoE на не заслуживающий доверия порт.
Circuit-id	Введите строку, состоящую не более чем из 63 ASCII-символов, которые коммутатор добавляет в субопцию Agent Circuit ID для пакетов обнаружения PPPoE, полученных на этом порту. В этом поле можно использовать пробелы. Строка Circuit, заданная для определенной сети VLAN на определенном порту (на экране **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN**), имеет наивысший приоритет.

Таблица 106 Экран Advanced Application > PPPoE > Intermediate Agent > Port (продолжение)

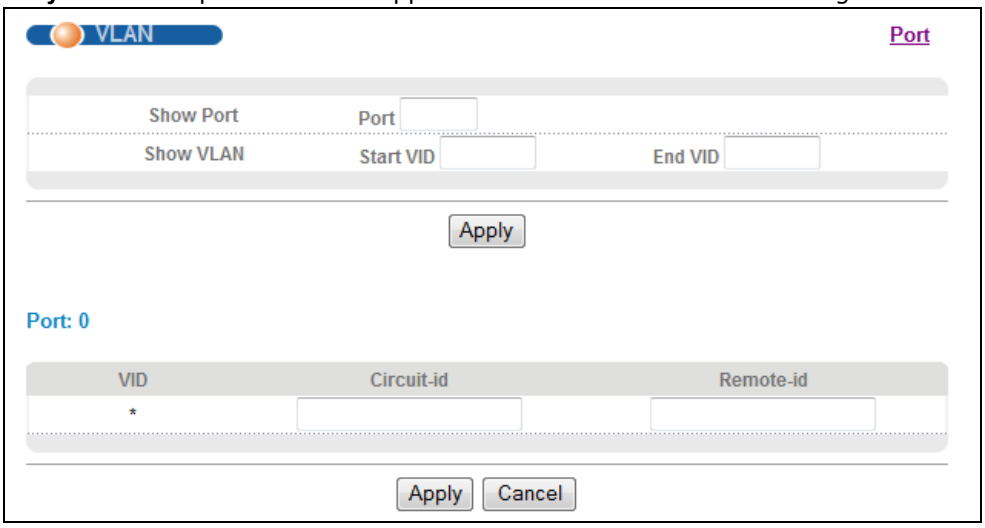
ПОЛЕ	ОПИСАНИЕ
Remote-id	Введите строку, состоящую не более чем из 63 ASCII-символов, которые коммутатор добавляет в субопцию Agent Remote ID для пакетов обнаружения PPPoE, полученных на этом порту. В этом поле можно использовать пробелы. Если не указать строку здесь или в поле **Remote-id** для определенной сети VLAN на определенном порту, то коммутатор будет автоматически использовать MAC-адрес клиента PPPoE. Строка Remote ID, заданная для определенной сети VLAN на определенном порту (на экране **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN**), имеет наивысший приоритет.
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.

28.3.2 Экран PPPoE IA Per-Port Per-VLAN

С помощью этого экрана можно задать настройки промежуточного агента PPPoE, которые будут применяться к определенной сети VLAN на определенном порту.

Перейдите по ссылке **VLAN** на экране **Intermediate Agent > Port**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 164 Экран Advanced Application > PPPoE > Intermediate Agent > Port > VLAN



Поля экрана описаны в следующей таблице.

Таблица 107 Экран Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

ПОЛЕ	ОПИСАНИЕ
Show Port	Введите номер порта, чтобы вывести на экран настройки промежуточного агента PPPoE для указанных сетей VLAN на данном порту.
Show VLAN	В данном разделе можно выбрать сети VLAN, для настройки параметров которых служит раздел ниже.

Таблица 107 Экран Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

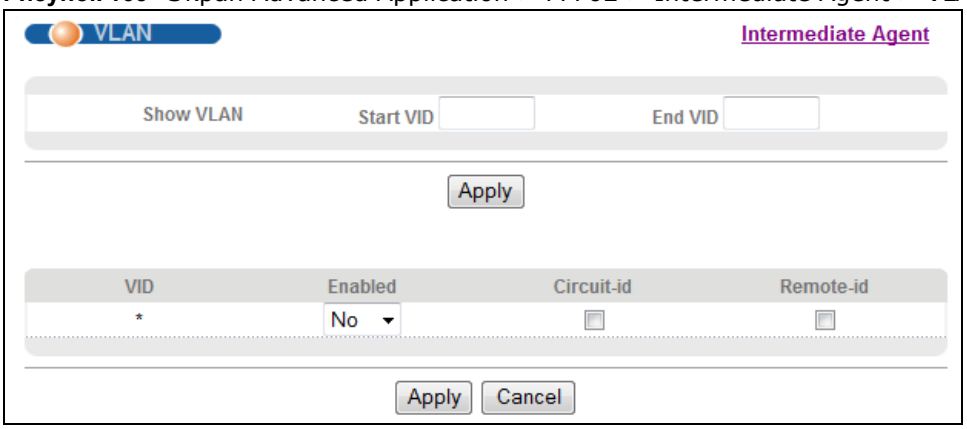
ПОЛЕ	ОПИСАНИЕ
Start VID	Укажите наименьший из диапазона идентификаторов сетей VLAN, настройку которых необходимо произвести в разделе ниже.
End VID	Укажите наибольший из диапазона идентификаторов сетей VLAN, настройку которых необходимо произвести в разделе ниже.
Apply	Нажмите **Apply**, чтобы отобразить сети VLAN из указанного диапазона в разделе ниже.
Port	Это поле отображает номер порта, указанный выше.
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.
*	С помощью этой строки можно применить настройки одновременно ко всем сетям VLAN. Примените общие для всех сетей VLAN настройки с помощью этой строки, а затем внесите необходимые корректировки на уровне отдельных сетей VLAN. Изменения в данной строке сразу же копируются во все сети VLAN.
Circuit-id	Введите строку, состоящую не более чем из 63 ASCII-символов, которые коммутатор добавляет в субопцию Agent Circuit ID для данной сети VLAN на указанном порту. В этом поле можно использовать пробелы. Значение Circuit ID, указанное в этом поле, имеет наивысший приоритет.
Remote-id	Введите строку, состоящую не более чем из 63 ASCII-символов, которые коммутатор добавляет в субопцию Agent Remote ID для данной сети VLAN на указанном порту. В этом поле можно использовать пробелы. Если не указать строку здесь или в поле **Remote-id** для определенного порта, то коммутатор будет автоматически использовать MAC-адрес клиента PPPoE. Значение Remote ID, указанное в этом поле, имеет наивысший приоритет.
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.

28.3.3 Промежуточный агент PPPoE для сети VLAN

С помощью этого экрана можно включить промежуточного агента PPPoE для определенной сети VLAN, а также указать, должен ли коммутатор присоединять строку Circuit ID и/или строку Remote ID к пакетам обнаружения PPPoE, приходящим из определенной сети VLAN.

Перейдите по ссылке **VLAN** на экране **Intermediate Agent**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 165 Экран Advanced Application > PPPoE > Intermediate Agent > VLAN



Поля экрана описаны в следующей таблице.

Таблица 108 Экран Advanced Application > PPPoE > Intermediate Agent > VLAN

ПОЛЕ	ОПИСАНИЕ
Show VLAN	В данном разделе можно выбрать сети VLAN, для настройки параметров которых служит раздел ниже.
Start VID	Укажите наименьший из диапазона идентификаторов сетей VLAN, настройку которых необходимо произвести в разделе ниже.
End VID	Укажите наибольший из диапазона идентификаторов сетей VLAN, настройку которых необходимо произвести в разделе ниже.
Apply	Нажмите **Apply**, чтобы отобразить сети VLAN из указанного диапазона 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.
*	С помощью этой строки можно применить настройки одновременно ко всем сетям VLAN. Примените общие для всех сетей VLAN настройки с помощью этой строки, а затем внесите необходимые корректировки на уровне отдельных сетей VLAN. Изменения в данной строке сразу же копируются во все сети VLAN.
Enabled	Выберите эту опцию, чтобы включить промежуточного агента PPPoE в определенной сети VLAN.
Circuit-id	Выберите эту опцию, что применить настройки Circuit ID к определенной сети VLAN.
Remote-id	Выберите эту опцию, что применить настройки Remote ID к определенной сети 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.

29

Отключение ошибок

29.1 Обзор функции отключения ошибок

В этой главе рассказывается о том, как настроить ограничение скорости для управления пакетами на определенном порту и определить действия, которые коммутатор должен выполнять на определенном порту при обнаружении заранее описанной ошибки (например, отключить порт или остановить отправку пакетов). Кроме того, здесь показано, как настроить автоматический откат действия на коммутаторе после исчезновения ошибки.

29.1.1 О чем рассказывается в этой главе

- С помощью экрана **Errdisable Status** (разд. 29.2 на стр. 260) можно увидеть, были ли обнаружены коммутатором контрольные пакеты, превысившие ограничение скорости, установленное для данного порта, а также ознакомиться с сопутствующей информацией.
- С помощью экрана **CPU Protection** (разд. 29.3 на стр. 262) можно установить максимально допустимое число контрольных пакетов (ARP, BPDU и/или IGMP), которые коммутатор может принять или передать через определенный порт.
- С помощью экрана **Errdisable Detect** (разд. 29.4 на стр. 263) можно включить режим обнаружения коммутатором контрольных пакетов (Errdisable Detect), превышающих ограничение скорости, установленное для данного порта, и выбрать действие, которое необходимо выполнить в случае превышения допустимой скорости.
- С помощью экрана **Errdisable Recovery** (разд. 29.5 на стр. 264) можно установить на коммутаторе режим автоматического отката действия при исчезновении ошибки (Errdisable Recovery).

С помощью этого экрана можно изменить настройки, связанные с отключением ошибок. Выберите в навигационной панели **Advanced Application > Errdisable**, чтобы открыть экран, изображенный ниже.

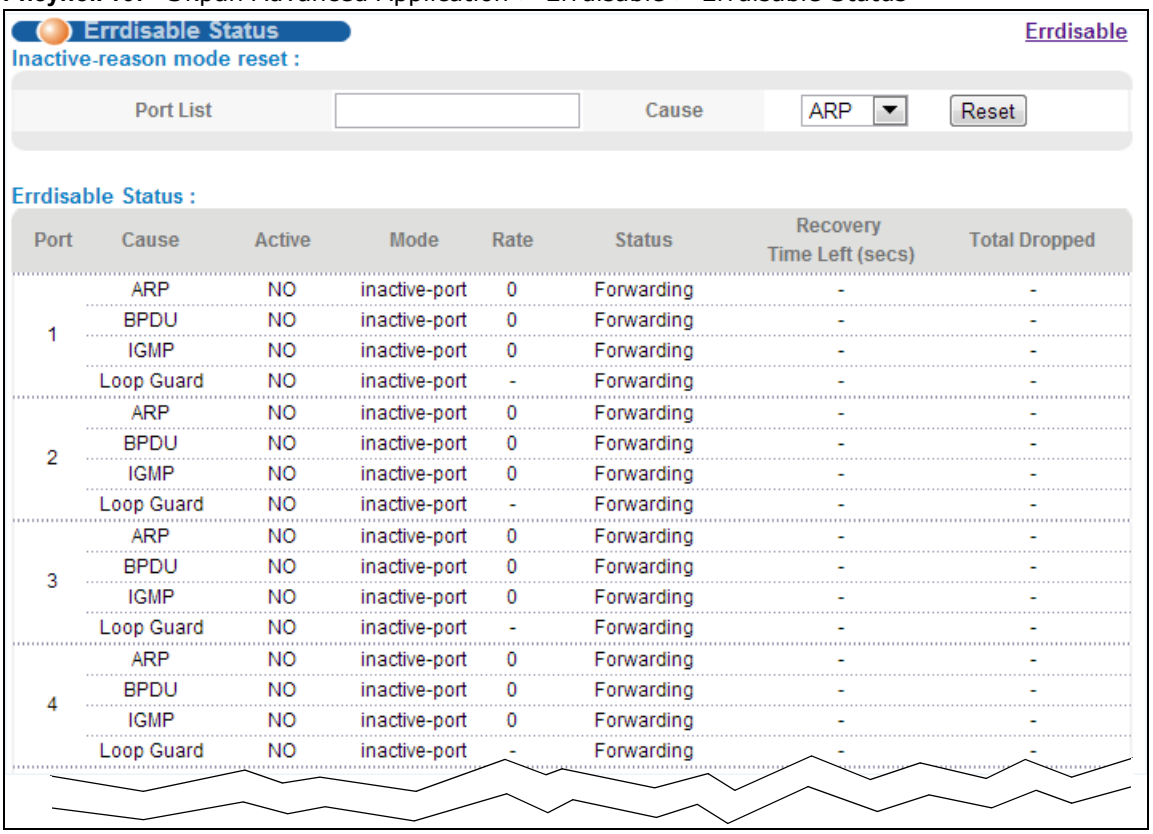
Рисунок 166 Экран Advanced Application > Errdisable

29.2 Экран Error-Disable Status

С помощью этого экрана можно определить, были ли обнаружены коммутатором контрольные пакеты, превысившие ограничение скорости, установленное для данного порта, а также ознакомиться с сопутствующей информацией. Перейдите по ссылке **Click here** рядом с

надписью **Errdisable Status** на экране **Advanced Application > Errdisable**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 167 Экран Advanced Application > Errdisable > Errdisable Status



Поля экрана описаны в следующей таблице.

Таблица 109 Экран Advanced Application > Errdisable > Errdisable Status

ПОЛЕ	ОПИСАНИЕ
Inactive-reason mode reset	
Port List	Укажите порты (разделенные запятой), для которых необходимо сбросить статус Inactive Reason.
Cause	Выберите причину режима Inactive Reason, который необходимо сбросить.
Reset	Нажмите кнопку Reset, чтобы включить режим обработки пакетов ARP, BPDU или IGMP вместо их игнорирования, если порт (или порты) находится в режиме Inactive Reason.
Errdisable Status	
Port	Здесь указывается номер порта, для которого необходимо задать статус Errdisable.
Cause	Здесь указывается причина режима Errdisable Detect или Errdisable Recovery на коммутаторе.
Active	Это поле указывает на то, обнаруживает ли коммутатор пакеты ARP, BPDU, IGMP и LOOP GUARD в данный момент на указанном порту.

Таблица 109 Экран Advanced Application > Errdisable > Errdisable Status (продолжение)

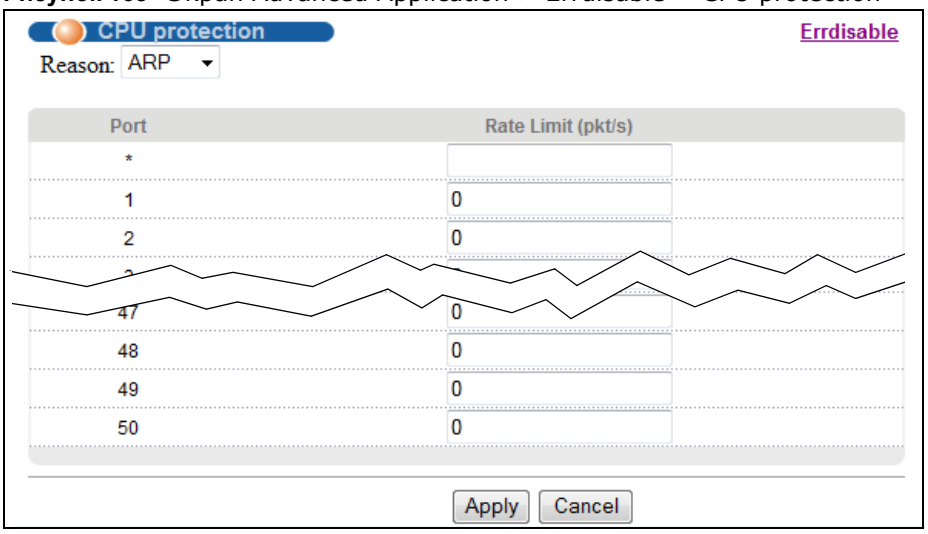
ПОЛЕ	ОПИСАНИЕ
Mode	Это поле указывает режим причины. • **inactive-port** – коммутатор отключает порт, через который приходят контрольные пакеты. • **inactive-reason** – коммутатор отбрасывает все указанные контрольные пакеты (такие, как BPDU), приходящие через этот порт. • **rate-limitation** – коммутатор отбрасывает дополнительные контрольные пакеты, которые указанный порт (или порты) должен обработать за одну секунду.
Rate	Этот порт показывает, сколько контрольных пакетов может принять или передать указанный порт за одну секунду. Это значение можно изменить с помощью поля CPU Protection. **0** означает отсутствие ограничений по скорости.
Status	Это поле показывает статус Errdisable • **Forwarding**: Данный коммутатор осуществляет пересылку пакетов. Режиму ограничения скорости всегда соответствует статус **Forwarding**. • **Err-disable**: коммутатор отключает порт, через который приходят контрольные пакеты (inactive-port) или отбрасывает указанные контрольные пакеты (inactive-reason)
Recovery Time	Это поле показывает интервал времени (в секундах), по истечении которого порт (или порты) снова станет активным по завершении режима Errdisable Recovery.
Total Dropped	Это поле показывает общее количество пакетов, отброшенных портом, на котором скорость пакетов превышает установленные для данного режима ограничения скорости.

29.3 Экран CPU Protection Configuration

С помощью этого экрана можно ограничить максимальное количество контрольных пакетов (ARP, BPDU и/или IGMP), которые коммутатор может принять или передать через определенный порт. Перейдите по ссылке **Click Here** рядом с надписью **CPU protection** на экране **Advanced Application > Errdisable**, чтобы открыть экран, изображенный на рисунке ниже.

Примечание: По завершении настроек на этом экране не забудьте включить режим обнаружения ошибок для интересующих контрольных пакетов на экране **Advanced Application** > **Errdisable** > **Errdisable Detect**.

Рисунок 168 Экран Advanced Application > Errdisable > CPU protection



Поля экрана описаны в следующей таблице.

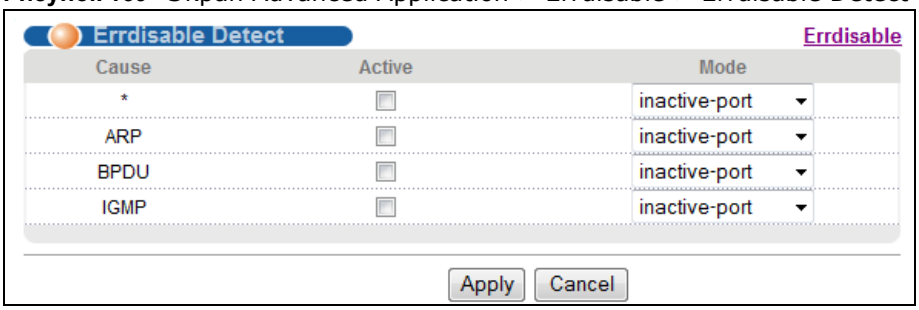
Таблица 110 Экран Advanced Application > Errdisable > CPU protection

ПОЛЕ	ОПИСАНИЕ
Reason	Выберите тип контрольного пакета, для которого будут выполнены настройки.
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, если потребуется, внести необходимые изменения на уровне отдельного порта. Изменения в данной строке сразу же копируются на все порты.
Rate Limit (pkt/s)	Укажите число из диапазона от 0 до 256, которое определяет, сколько контрольных пакетов может принять или передать указанный порт за одну секунду. **0** означает отсутствие ограничений по скорости. Необходимо указать действие, которое коммутатор будет выполнять при превышении ограничения скорости. Дополнительную информацию можно найти в разд. 29.4 на стр. 263.
Apply	Нажмите **Apply**, чтобы сохранить изменения в оперативной памяти коммутатора. Эти настройки будут утеряны в случае выключения коммутатора или перебоя в подаче питания, поэтому по завершении настройки необходимо нажать на ссылке **Save** в верхней навигационной панели для сохранения изменений в энергонезависимой памяти.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

29.4 Настройки режима Error-Disable Detect

С помощью этого экрана можно включить на коммутаторе режим обнаружения превышения ограничения скорости, установленного для контрольных пакетов на данном порту, и указать действие, которое необходимо выполнить в случае превышения допустимой скорости. Перейдите по ссылке **Click Here** рядом со ссылкой **Errdisable Detect** на экране **Advanced Application > Errdisable**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 169 Экран Advanced Application > Errdisable > Errdisable Detect



Поля экрана описаны в следующей таблице.

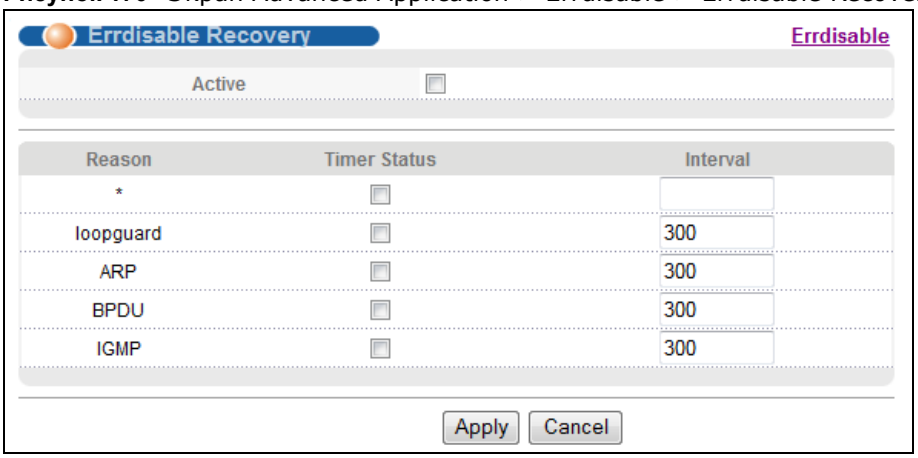
Таблица 111 Экран Advanced Application > Errdisable > Errdisable Detect

ПОЛЕ	ОПИСАНИЕ
Cause	Это поле показывает типы контрольных пакетов, которые могут вызвать перегрузку процессора.
*	С помощью этой строки можно применить настройки одновременно ко всем типам контрольных пакетов. С помощью этой строки можно назначить общие для всех типов контрольных пакетов настройки, а затем, если потребуется, внести необходимые изменения на уровне отдельного типа. Изменения в данной строке сразу же копируются для всех типов контрольных пакетов.
Active	При выборе этой опции коммутатор будет отслеживать превышение ограничения скорости, установленного для контрольных пакетов определенного типа, и выполнять указанное ниже действие, если такое превышение обнаружено.
Mode	Выберите действие, которое коммутатор должен выполнить, если количество контрольных пакетов превышает ограничение скорости, установленное для данного порта на экране **Advanced Application > Errdisable > CPU protection**. • **inactive-port** – коммутатор отключает порт, через который приходят контрольные пакеты. • **inactive-reason** – коммутатор отбрасывает все указанные контрольные пакеты (такие, как BPDU), приходящие через этот порт. • **rate-limitation** – коммутатор отбрасывает дополнительные контрольные пакеты, которые указанный порт (или порты) должен обработать за одну 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.

29.5 Настройки режима восстановления после ошибок Error-Disable Recovery

С помощью этого экрана можно установить на коммутаторе режим автоматического отката действия при исчезновении ошибки. Перейдите по ссылке **Click Here** рядом со ссылкой **Errdisable Recovery** на экране **Advanced Application > Errdisable**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 170 Экран Advanced Application > Errdisable > Errdisable Recovery



Поля экрана описаны в следующей таблице.

Таблица 112 Экран Advanced Application > Errdisable > Errdisable Recovery

ПОЛЕ	ОПИСАНИЕ
Active	Выберите эту опцию, чтобы включить функцию восстановления после ошибок на коммутаторе.
Reason	Это поле отображает список поддерживаемых функциональных возможностей, которые позволяют коммутатору отключать определенный порт или отбрасывать приходящие на него пакеты в соответствии с функциональными требованиями и настройками действий.
*	С помощью этой строки можно применить настройки одновременно ко всем типам контрольных пакетов. С помощью этой строки можно назначить общие для всех типов контрольных пакетов настройки, а затем, если потребуется, внести необходимые изменения на уровне отдельного типа. Изменения в данной строке сразу же копируются для всех типов контрольных пакетов.
Timer Status	При выборе этой опции коммутатор будет ожидать заданное количество времени перед тем, как активировать порт или разрешить прохождение через него определенных пакетов после возникновения ошибки. Снимите выделение с переключателя, чтобы отключить это правило.
Interval	Укажите длительность временного интервала в секундах (из диапазона от 30 до 2592000).
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

Частные сети VLAN

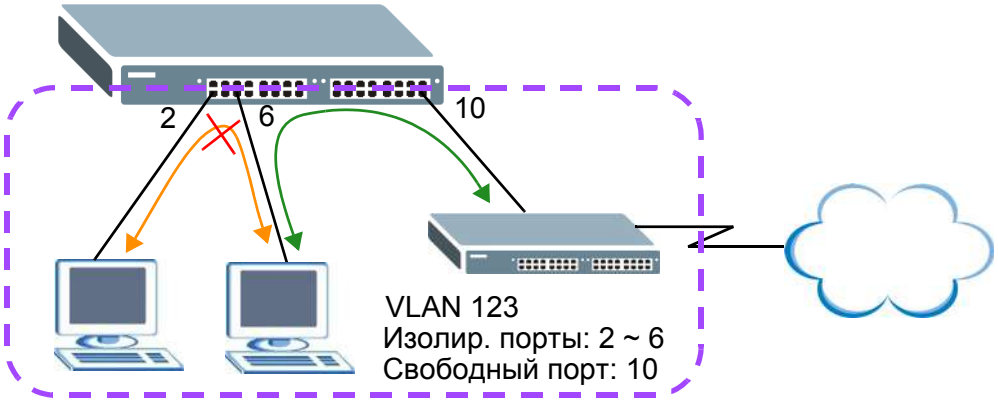
В этой главе рассказывается о настройках коммутатора, позволяющих запретить связь между портами в определенной сети VLAN.

30.1 Обзор частных сетей VLAN

Функция частных сетей VLAN предлагает простой вариант изоляции портов в пределах определенной сети VLAN. Порты, которые не нужно изолировать в данной сети VLAN, необходимо добавить в список свободных портов. Остальные порты в данной сети VLAN коммутатор автоматически добавляет в список изолированных портов и блокирует трафик между изолированными портами. Свободный порт может поддерживать связь с любым портом в той же сети VLAN. Изолированный порт может поддерживать связь только со свободными портами.

Примечание: В каждой сети VLAN допускается наличие только одной частной сети VLAN.

Рисунок 171 Пример частной сети VLAN

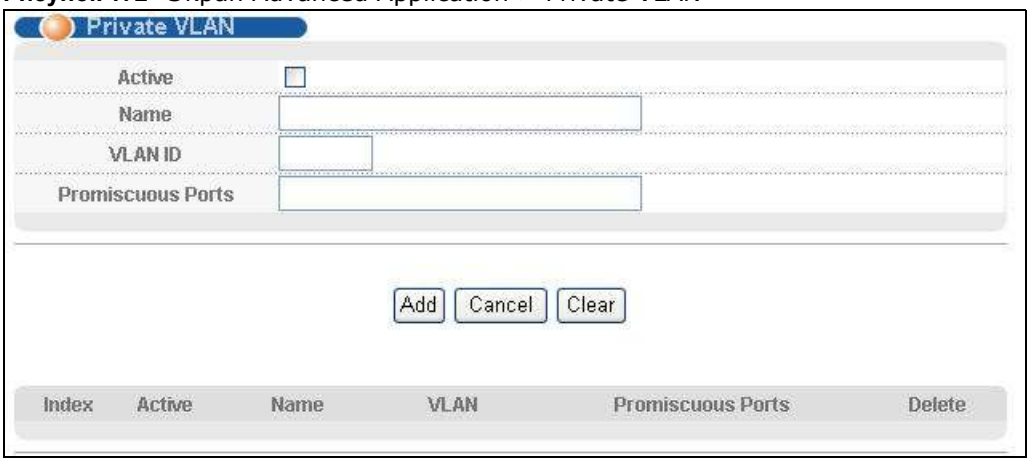


Примечание: В сети VLAN, внутри которой создана частная сеть VLAN, необходимо как минимум один порт включить в список свободных портов. В противном случае данная сеть VLAN будет отрезана от остальной сети.

30.2 Создание и настройка частной сети VLAN

Выберите в навигационной панели **Advanced Application** > **Private VLAN**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 172 Экран Advanced Application > Private VLAN



Поля экрана описаны в следующей таблице.

Таблица 113 Экран Advanced Application > Private VLAN

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы активировать частную сеть VLAN внутри сети VLAN.
Name	Введите имя-описание (до 32 отображаемых ASCII-символов), по которому можно идентифицировать этот маршрут.
VLAN ID	Укажите идентификатор сети VLAN из диапазона от 1 до 4094. Настраиваемое правило будет применено к сети VLAN с указанным идентификатором.
Promiscuous Ports	Укажите номера портов, которые могут поддерживать связь с любыми портами в той же сети VLAN. Все остальные порты в этой сети VLAN будут добавлены в список изолированных портов и смогут обмениваться трафиком только с портами, указанными в этом поле.
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	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Это порядковый номер правила.
Active	Это поле указывает на то, активировано ли данное правило.
Name	Это поле содержит имя-описание данного правила.
VLAN	Это поле указывает на сеть VLAN, к которой применяется данное правило.
Promiscuous Ports	Это поле отображает список портов, которые могут поддерживать связь с любыми портами в пределах одной сети VLAN.
Delete	В столбце **Delete** установите переключатели правил, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей **Delete**.

31

Green Ethernet («Зеленый» Ethernet)

В этой главе рассказывается о том, с помощью каких настроек коммутатора можно уменьшить энергопотребление его портов.

31.1 Обзор функции Green Ethernet («Зеленый» Ethernet)

Функция Green Ethernet сокращает энергопотребление портов с помощью следующих опций.

IEEE 802.3az Energy Efficient Ethernet (EEE)

Если на коммутаторе включена опция EEE, оба конца канала поддерживают EEE, и в канале отсутствует трафик, порт переходит в режим Low Power Idle (LPI). В режиме LPI отключаются некоторые функции физического уровня (в канале наступает «тишина») для экономии энергии. Периодически порт транслирует сигнал REFRESH с тем, чтобы обеспечить сохранение связи с партнером по каналу. При появлении трафика порт посылает партнеру по каналу сигнал WAKE, чтобы вернуть канал в активный режим.

Auto Power Down (Автоматические снижение мощности)

Опция **Auto Power Down** отключает практически все функции физического уровня порта, если на порту отсутствует соединение, поэтому порт потребляет энергию исключительно для периодической проверки статуса соединения. При обнаружении подключения к порту порт выходит из режима **Auto Power Down** и переходит в обычный режим.

Short Reach (Короткие соединения)

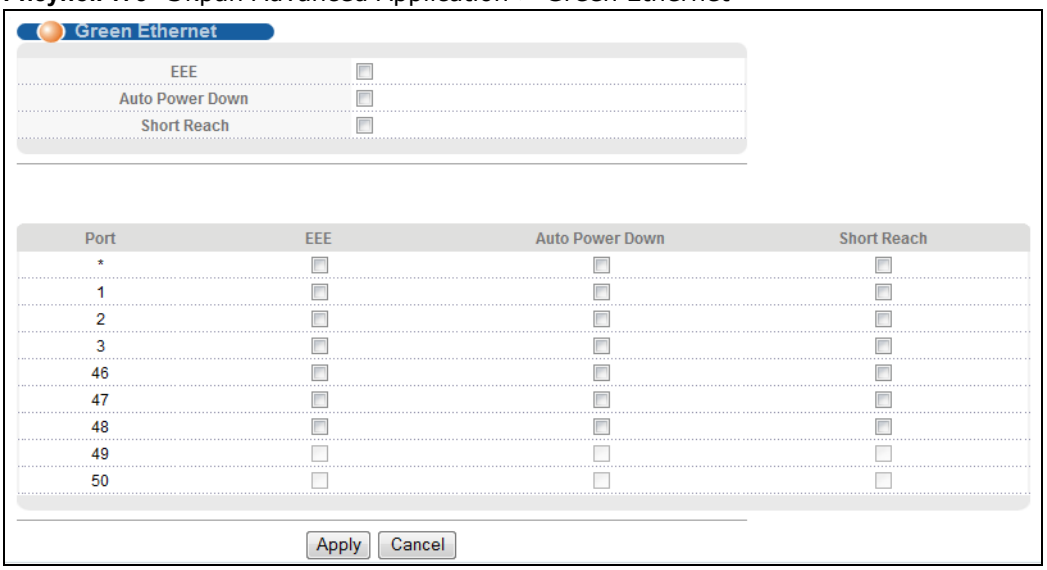
В традиционной сети Ethernet при передаче данных задействуется объем мощности, достаточный для поддержки кабелей максимальной длины. В кабелях меньшей длины рассеивается меньше мощности, поэтому функция **Short Reach** позволяет снизить энергопотребление за счет регулировки мощности, выделяемой на каждый порт, в зависимости от длины кабеля, подключенного к этому порту.

31.2 Настройка функции Green Ethernet

Выберите в навигационной панели **Advanced Application** > **Green Ethernet**, чтобы открыть экран, изображенный на рисунке ниже.

Примечание: Опции EEE, Auto Power Down и Short Reach не поддерживаются для портов каскадирования.

Рисунок 173 Экран Advanced Application > Green Ethernet



Поля экрана описаны в следующей таблице.

Экран Advanced Application > Green Ethernet

ПОЛЕ	ОПИСАНИЕ
EEE	Установите этот переключатель, чтобы включить опцию Energy Efficient Ethernet на уровне всего коммутатора.
Auto Power Down	Установите этот переключатель, чтобы включить опцию Auto Power Down на уровне всего коммутатора.
Short Reach	Установите этот переключатель, чтобы включить опцию Short Reach на уровне всего коммутатора.
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, если потребуется, внести необходимые изменения на уровне отдельного порта. Изменения в данной строке сразу же копируются на все порты.
EEE	Установите этот переключатель, чтобы включить опцию Energy Efficient Ethernet для данного порта.
Auto Power Down	Установите этот переключатель, чтобы включить опцию Auto Power Down для данного порта.
Short Reach	Установите этот переключатель, чтобы включить опцию Short Reach для данного 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.

31

Протокол Link Layer Discovery Protocol (LLDP)

32.1 Обзор протокола LLDP

Протокол обнаружения канального уровня LLDP (Link Layer Discovery Protocol) – это протокол уровня 2. Он позволяет сетевым устройствам сообщать о своем присутствии и возможностях другим устройствам в локальной сети. Кроме того, он позволяет сохранять и обновлять информацию об устройствах, непосредственно подключенных к данному устройству. Это помогает администратору следить за изменениями в сети и своевременно выполнять соответствующие процедуры по изменению конфигурации и управлению сетью. Информация об устройстве инкапсулируется в блоки данных LLDP (LLDPDU) в формате полей TLV (Type, Length, Value – тип, длина, значение). Информация об устройствах, содержащаяся в принятых блоках данных LLDP, сохраняется в стандартной базе управляющей информации MIB.

Данный коммутатор поддерживает следующие базовые управляющие поля TLV.

- Конец блока LLDPDU (обязательное)
- Идентификатор шасси (обязательное)
- Идентификатор порта (обязательное)
- Срок жизни (обязательное)
- Описание порта (опциональное)
- Название системы (опциональное)
- Описание системы (опциональное)
- Возможности системы (опциональное)
- Адрес управления (опциональное)

Данный коммутатор также поддерживает поля TLV стандарта IEEE 802.1 и IEEE 802.3 с организационной спецификой.

Специфические поля TLV стандарта IEEE 802.1:

- Поле TLV для идентификатора сети VLAN на основе портов (опциональное)
- Поле TLV для идентификатора сети VLAN на основе портов и протоколов (опциональное)

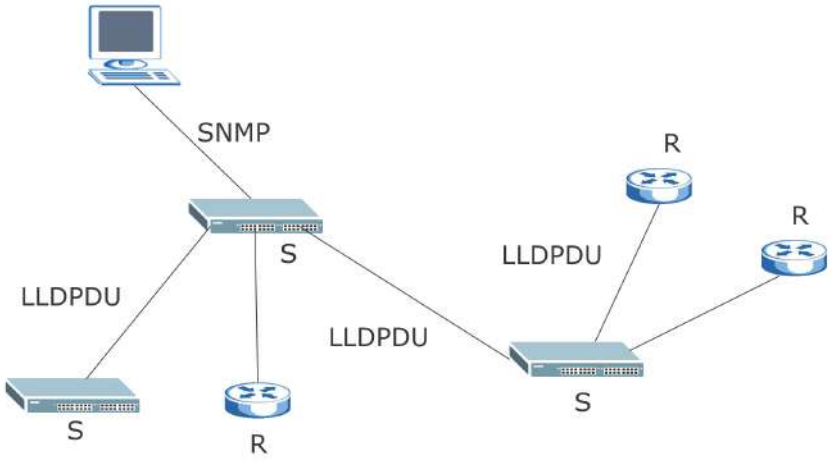
Специфические поля TLV стандарта IEEE 802.3:

- Поле TLV для конфигурации/статуса MAC/PHY
- Поле TLV для питания через MDI (опциональное, только для моделей с поддержкой PoE)
- Поле TLV для агрегации каналов (опциональное)
- Поле TLV для максимального размера кадра (опциональное)

Опциональные поля TLV вставляются между TLV Time To Live («Срок жизни») и TLV End of LLDPDU («Конец блока LLDPDU»).

На следующем рисунке показано, как сетевые устройства, коммутаторы и маршрутизаторы (S и R), обмениваются информацией о себе посредством блоков LLDPDU, а администратор сети может запрашивать эту информацию по протоколу SNMP (Simple Network Management Protocol).

Рисунок 174 Обзор протокола LLDP



32.2 Обзор LLDP-MED

Протокол обнаружения канального уровня для мультимедийных конечных устройств LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) – это расширение стандартного протокола LLDP, разработанное подкомитетом TR-41.4 Ассоциации телекоммуникационной отрасли (Telecommunications Industry Association, TIA). Это расширение описывает дополнительные возможности обнаружения, например, для приложений VoIP, располагая которыми администраторы сетей могут более эффективно управлять топологией сети. В отличие от традиционного протокола LLDP, который имеет некоторые ограничения при работе с несколькими прикладными устройствами, LLDP-MED позволяет получить точное представление о сетевой топологии. LLDP-MED поддерживает конечные устройства трех классов:

Класс I: Контроллеры IP-коммуникаций или другие серверы, связанные с коммуникациями

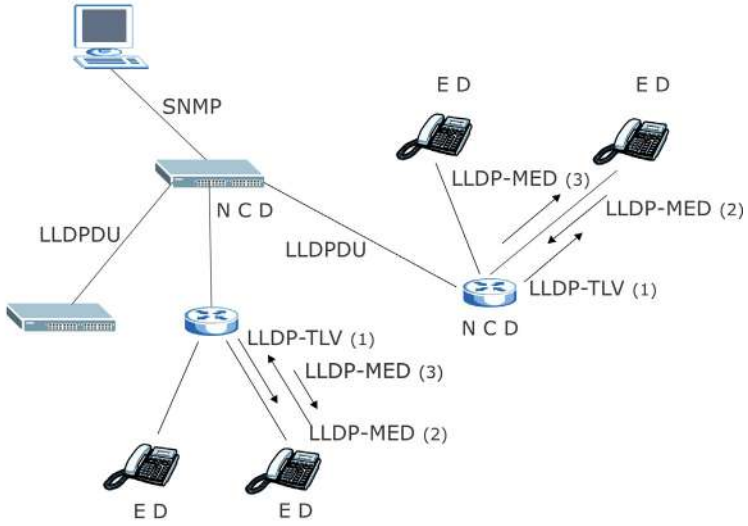
Класс II: Голосовые шлюзы, мосты для конференц-связи или мультимедийные серверы

Класс III: IP-телефоны, программные телефоны для ПК, коммуникационные устройства для конечных пользователей, поддерживающие мультимедийные возможности IP

На следующем рисунке показано, как, используя протокол LLDP-MED, устройства обеспечения сетевого взаимодействия (network connectivity devices, NCD), коммутаторы и маршрутизаторы, передают TLV LLDP конечным устройствам (endpoint device, ED), таким, как первый IP-телефон (1), чтобы получить информацию о типе устройства и его возможностях, затем получают эту информацию в формате TLV LLDP-MED от конечных устройств (2), после чего передают TLV LLDP-MED (3) для конфигурирования конечного устройства, в частности, для обновления

сетевых политик и информации о местонахождении. Такие блоки LLDPDU периодически обновляют сведения о статусе и конфигурации, поэтому с помощью LLDP-MED администраторы сети могут проверить результаты конфигурирования с помощью дистанционного статуса. Актуализация дистанционного статуса происходит при получении TLV LLDP-MED от конечных устройств.

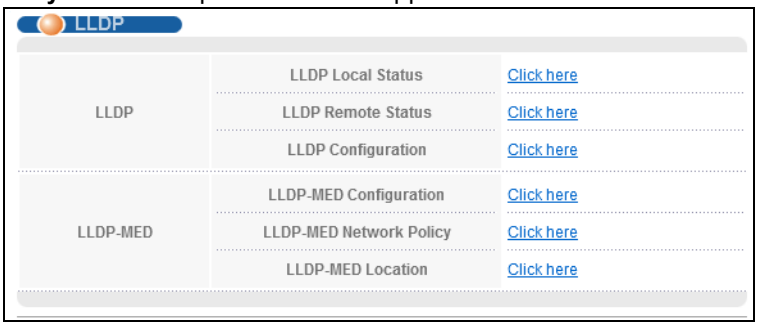
Рисунок 175 Обзор LLDP-MED



32.3 Экраны для настройки LLDP

Выберите в навигационной панели **Advanced Application** > **LLDP**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 176 Экран Advanced Application > LLDP



Поля экрана описаны в следующей таблице.

Таблица 114 Экран Advanced Application > LLDP

ПОЛЕ	ОПИСАНИЕ
LLDP	
LLDP Local Status	С помощью этой ссылки можно открыть экран, содержащий информацию о настройках LLDP для коммутатора.
LLDP Remote Status	С помощью этой ссылки можно открыть экран, содержащий информацию LLDP, полученную от соседних устройств.

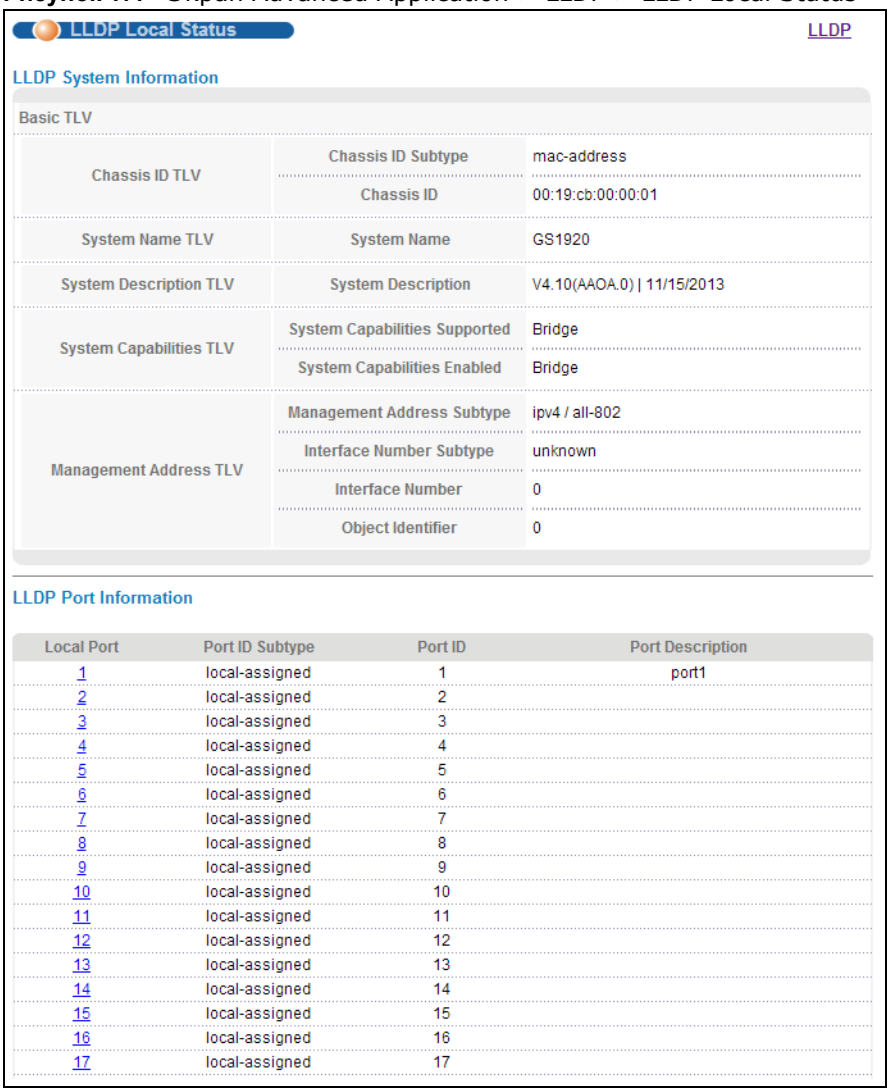
Таблица 114 Экран Advanced Application > LLDP (продолжение)

ПОЛЕ	ОПИСАНИЕ
LLDP Configuration	С помощью этой ссылки можно открыть экран для настройки параметров LLDP.
LLDP-MED	
LLDP-MED Configuration	С помощью этой ссылки можно открыть экран для настройки параметров LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices).
LLDP-MED Network Policy	С помощью этой ссылки можно открыть экран для настройки параметров сетевых политик LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices).
LLDP-MED Location	С помощью этой ссылки можно открыть экран для настройки параметров местонахождения LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices).

32.4 Экран LLDP Local Status

Этот экран отображает сводную информацию о статусе LLDP на данном коммутаторе. Перейдите по ссылке **Advanced Application** > **LLDP > LLDP Local Status (Click Here)**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 177 Экран Advanced Application > LLDP > LLDP Local Status



LLDP Local Status

LLDP

LLDP System Information

Basic TLV

Chassis ID TLV	Chassis ID Subtype	mac-address
	Chassis ID	00:19:cb:00:00:01
System Name TLV	System Name	GS1920
System Description TLV	System Description	V4.10(AAOA.0) | 11/15/2013
System Capabilities TLV	System Capabilities Supported	Bridge
	System Capabilities Enabled	Bridge
Management Address TLV	Management Address Subtype	ipv4 / all-802
	Interface Number Subtype	unknown
	Interface Number	0
	Object Identifier	0

LLDP Port Information

Local Port	Port ID Subtype	Port ID	Port Description
1	local-assigned	1	port1
2	local-assigned	2	
3	local-assigned	3	
4	local-assigned	4	
5	local-assigned	5	
6	local-assigned	6	
7	local-assigned	7	
8	local-assigned	8	
9	local-assigned	9	
10	local-assigned	10	
11	local-assigned	11	
12	local-assigned	12	
13	local-assigned	13	
14	local-assigned	14	
15	local-assigned	15	
16	local-assigned	16	
17	local-assigned	17	

Поля экрана описаны в следующей таблице.

Таблица 115 Экран Advanced Application > LLDP > LLDP Local Status

ПОЛЕ	ОПИСАНИЕ
Basic TLV	
Chassis ID TLV	Это поле показывает идентификатор шасси локального коммутатора, то есть коммутатора, параметры которого настраиваются. Идентификатор шасси определяется своим подтипом. Chassis ID Subtype – это поле указывает на то, каким образом осуществляется идентификация шасси удаленного коммутатора. Chassis ID – Это поле отображает идентификатор шасси локального коммутатора. Идентификатор шасси определяется своим подтипом.
System Name TLV	Это поле показывает имя хоста коммутатора.
System Description TLV	Это поле показывает описание системы, то есть версию встроенного программного обеспечения коммутатора.

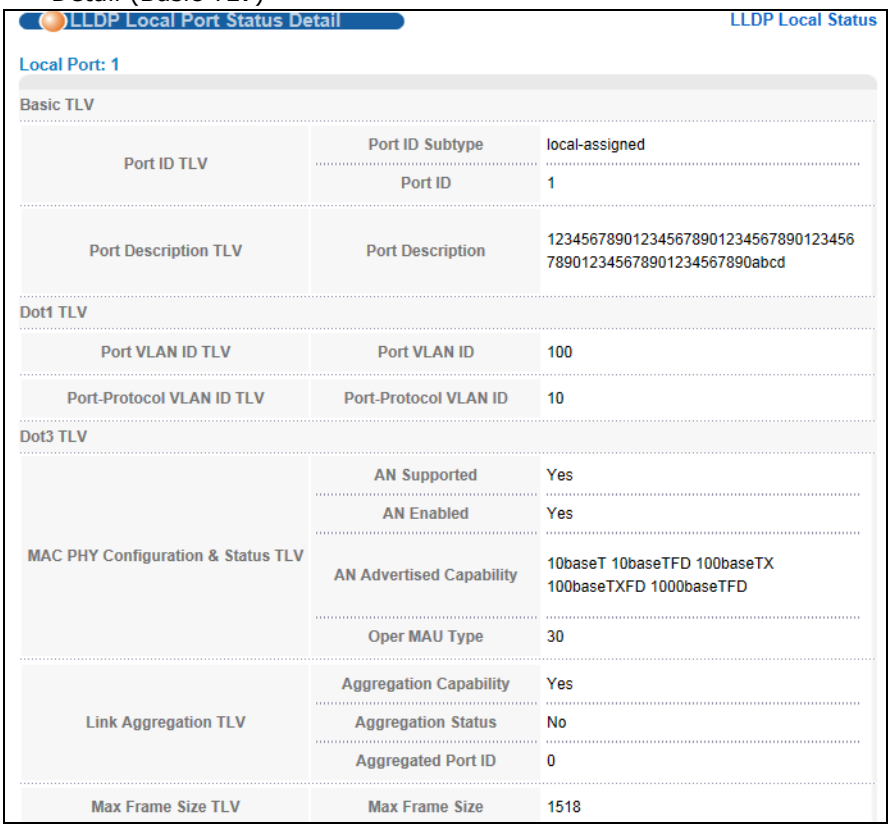
Таблица 115 Экран Advanced Application > LLDP > LLDP Local Status

ПОЛЕ	ОПИСАНИЕ
System Capabilities TLV	Это поле отображает системные возможности, которые поддерживает локальный коммутатор и которые на нем активированы. • System Capabilities Supported – Bridge (Поддерживаемые системные возможности – Мост) • System Capabilities Enabled – Bridge (Активированные системные возможности – Мост)
Management Address TLV	Поле Management Address TLV указывает на адрес, ассоциированный с локальным агентом LLDP, который можно использовать для связи с сущностями более высоких уровней при обнаружении устройств с использованием средств управления сетью. Данное поле TLV может также включать в себя номер системного интерфейса и идентификатор объекта (OID), которые ассоциированы с данным адресом управления Данное поле отображает настройки адреса управления для указанного порта (или портов). • Management Address Subtype – ipv4 / all-802 [Подтип адреса управления – ipv4 / all-802] • Interface Number Subtype – unknown [Подтип номера интерфейса – неизвестен] • Interface Number – 0 (not supported) [Номер интерфейса – 0 (не поддерживается)] • Object Number – 0 (not supported) [Номер объекта – 0 (не поддерживается)]
LLDP Port Information	Этот раздел содержит информацию о локальных портах.
Local Port	Это поле показывает номер локального порта, который получает блоки LLDPDU от удаленного устройства. Щелкните по номеру порта, чтобы просмотреть подробную информацию о статусе LLDP данного порта на экране **LLDP Local Port Status Detail**.
Port ID Subtype	Это поле указывает на способ идентификации поля Port ID.
Port ID	Это поле содержит специфический идентификатор для порта, с которого был передан данный блок LLDPDU, в формате строки из алфавитно-цифровых символов.
Port Description	Это поле отображает описание порта, которое коммутатор будет анонсировать с данного порта.

32.4.1 Подробная информация о статусе LLDP для локальных портов

На этом экране отображается подробная информация о статусе LLDP для каждого порта коммутатора. Перейдите по ссылке **Advanced Application** > **LLDP > LLDP Local Status**, а затем щелкните по номеру порта, например, 1 (Port) в столбце Local port, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 178 Экран Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (Basic TLV)



LLDP Local Port Status Detail

LLDP Local Status

Local Port: 1

Basic TLV		
Port ID TLV	Port ID Subtype	local-assigned
	Port ID	1
Port Description TLV	Port Description	12345678901234567890123456789012345678901234567890123456789abcd
Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	100
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	10
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	Yes
	AN Enabled	Yes
	AN Advertised Capability	10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD
	Oper MAU Type	30
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	No
	Aggregated Port ID	0
Max Frame Size TLV	Max Frame Size	1518

Рисунок 179 Экран Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (MED TLV)

MED TLV

Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	VLAN ID 10, tagged, L2-priority 7, DSCP 63
	Voice-Signaling	VLAN ID 100, tagged, L2-priority 2, DSCP 10
	Guest-Voice	VLAN ID 20, tagged, L2-priority 3, DSCP 12
	Guest-Voice-Signaling	VLAN ID 0, untagged, L2-priority 0, DSCP 0
	Softphone-Voice	VLAN ID 200, tagged, L2-priority 1, DSCP 1
	Video-Conferencing	VLAN ID 0, untagged, L2-priority 0, DSCP 0
	Streaming-Video	VLAN ID 300, tagged, L2-priority 4, DSCP 20
	Video-Signaling	VLAN ID 400, tagged, L2-priority 6, DSCP 55
Location Identification TLV	Coordinate-base LCI	latitute north 24.0 longitute east 120.0 altitute meter 13.0 datum WGS84
	Civic LCI	country TW city HSINCHU building ZYXEL
	ELIN	1234567890

Поля экрана описаны в следующей таблице.

Таблица 116 Экран Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

ПОЛЕ	ОПИСАНИЕ
Basic TLV	Это поле содержит флаги Basic TLV
Port ID TLV	Это поле указывает на конкретный порт, который передал данный кадр LLDP. • Port ID Subtype: Это поле указывает на то, каким образом осуществляется идентификация порта. • Port ID: Это поле содержит идентификатор порта.
Port Description TLV	Это поле отображает описание локального порта.
Dot1 TLV	
Port VLAN ID TLV	Это поле показывает идентификатор сети VLAN, отправляемый в TLV IEEE 802.1 Port VLAN ID.
Port-Protocol VLAN ID TLV	Это поле отображает TLV IEEE 802.1 Port Protocol VLAN ID, которые указывают на статус (активна, неактивна) и поддержку сети VLAN.
Dot3 TLV	
MAC PHY Configuration & Status TLV	TLV MAC/PHY Configuration/Status анонсирует поддерживаемую скорость в битах и возможность поддержки дуплексного режима отправляющим узлом 802.3. Кроме того, данное поле TLV анонсирует текущие режим дуплекса и скорость в битах отправляющего узла. Наконец, данное поле TLV указывает, является ли выбранный параметр результатом автосогласования при установлении соединения или ручной настройки. • AN Supported – Показывает, поддерживает ли данный порт функцию автосогласования. • AN Enabled – Текущий статус автосогласования порта. • AN Advertised Capability – Указывает на возможности порта в части автосогласования. • Oper MAU Type – Текущий тип MAU (Medium Attachment Unit) порта
Link Aggregation TLV	Поле Link Aggregation TLV показывает, поддерживает ли данный канал возможность агрегации, участвует ли канал в агрегации в данный момент, и, если да, указывает агрегационный идентификатор порта. • Aggregation Capability – Текущие возможности порта по участию в агрегации. • Aggregation Status – Текущий статус агрегации порта. • Aggregation Port ID – Агрегационный идентификатор данного порта.
Max Frame Size TLV	Это поле показывает максимальный поддерживаемый размер кадра в октетах.
MED TLV	LLDP Media Endpoint Discovery (MED) – это расширение протокола LLDP, которое поддерживает дополнительные возможности по взаимодействию с мультимедийными конечными устройствами. MED поддерживает анонс/обнаружение сетевых политик и обнаружение местонахождения устройств, позволяя создавать базы данных, содержащие сведения о местонахождении устройств, и предоставляя информацию, необходимую для поиска и устранения проблем.
Capabilities TLV	Это поле показывает, какие из полей TLV, относящихся к расширению LLDP-MED, может передавать коммутатор. • Network Policy (Сетевая политика) • Location (Местоположение)
Device Type TLV	Это поле отображает класс устройства LLDP-MED. Тип устройства «Коммутатор Zyxel»: • Network Connectivity (Устройство обеспечения сетевого взаимодействия)

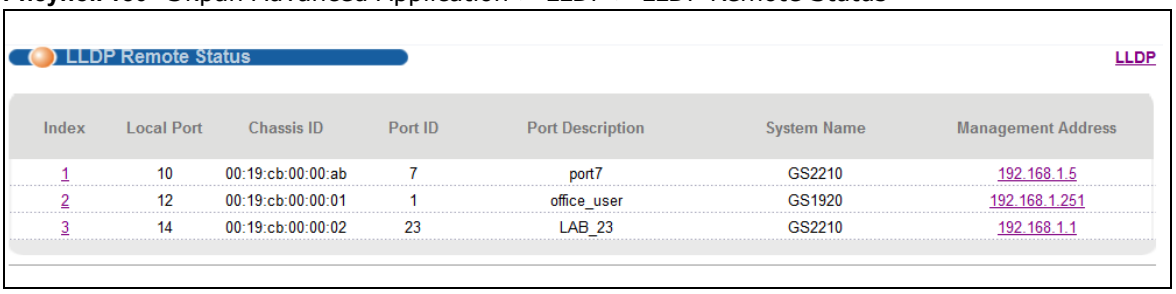
Таблица 116 Экран Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

ПОЛЕ	ОПИСАНИЕ
Network Policy TLV	Это поле показывает сетевую политику для указанного приложения. • Voice (Сеть голосовой связи) • Voice-Signaling (Сигнализация сети голосовой связи) • Guest-Voice (Гостевая сеть голосовой связи) • Guest-Voice-Signaling (Сигнализация в гостевой сети голосовой связи) • Softphone-Voice (Голосовая связь для программного телефона) • Video-Conferencing (Видеоконференцсвязь) • Streaming-Video (Потоковая передача видео) • Video-Signaling (Сигнализация при передаче видео)
Location Identification TLV	Это поле содержит информацию о местонахождении абонента, совершающего вызов, которое определяется по таким параметрам, как ELIN (Emergency Location Identifier Number) или IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). • Civic LCI – IETF Geopriv Civic Address based Location Configuration Information (Информация о конфигурации местоположения на основе городского адреса IETF Geopriv Civic Address) • ELIN – (Emergency Location Identifier Number, идентификатор местоположения для экстренных служб) • Coordinate-based LCI – координаты широты, долготы и высоты, содержащиеся в информации о конфигурации местоположения (LCI)

32.5 Удаленный статус LLDP

Этот экран содержит сводную информацию о статусе LLDP для каждого соединения LLDP с соседними коммутаторами. Перейдите по ссылке **Advanced Application** > **LLDP > LLDP Remote Status (Click Here)**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 180 Экран Advanced Application > LLDP > LLDP Remote Status



Поля экрана описаны в следующей таблице.

Таблица 117 Экран Advanced Application > LLDP > LLDP Remote Status

ПОЛЕ	ОПИСАНИЕ
Index	Это поле показывает количество удаленных устройств, подключенных к коммутатору. Щелкните на порядковом номере, чтобы просмотреть подробный статус LLDP для данного удаленного устройства на экране **LLDP Remote Port Status Detail**.
Local Port	Это поле содержит номер порта локального коммутатора, который получил блок LLDPDU от удаленного устройства.

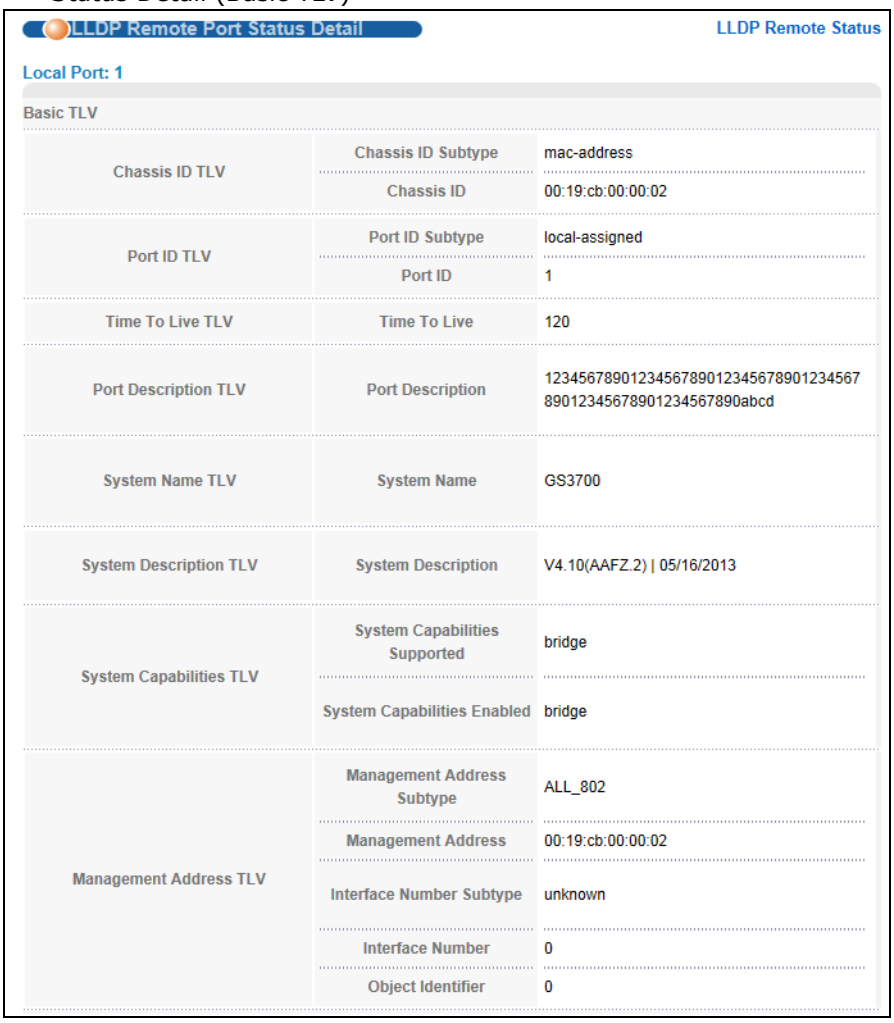
Таблица 117 Экран Advanced Application > LLDP > LLDP Remote Status

ПОЛЕ	ОПИСАНИЕ
Chassis ID	Это поле показывает идентификатор шасси удаленного устройства, ассоциированного с передающим агентом LLDP. Идентификатор шасси определяется своим подтипом. Например, в этой роли может выступать MAC-адрес удаленного устройства.
Port ID	Это поле содержит специфический идентификатор для порта, с которого был передан данный блок LLDPDU, в формате строки из алфавитно-цифровых символов. Идентификатор порта определяется своим подтипом.
Port Description	Это поле содержит описание порта, с которого был передан данный блок LLDPDU.
System Name	Это поле показывает имя системы удаленного устройства.
Management Address	Это поле показывает адрес управления удаленного устройства. В этом качестве может выступать MAC-адрес или IP-адрес. Пользователь может непосредственно перейти по гиперссылке IP-адреса.

32.5.1 Подробная информация о статусе удаленных портов LLDP

Этот экран отображает подробную информацию о статусе LLDP, полученную от удаленного устройства. Перейдите по ссылке **Advanced Application** > **LLDP > LLDP Remote Status (Click Here)**, а затем щелкните по порядковому номеру, например, 1, в столбце Index на экране **LLDP Remote Status**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 181 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)



В таблице, приведенной ниже, описаны поля из раздела Basic TLV для данного экрана.

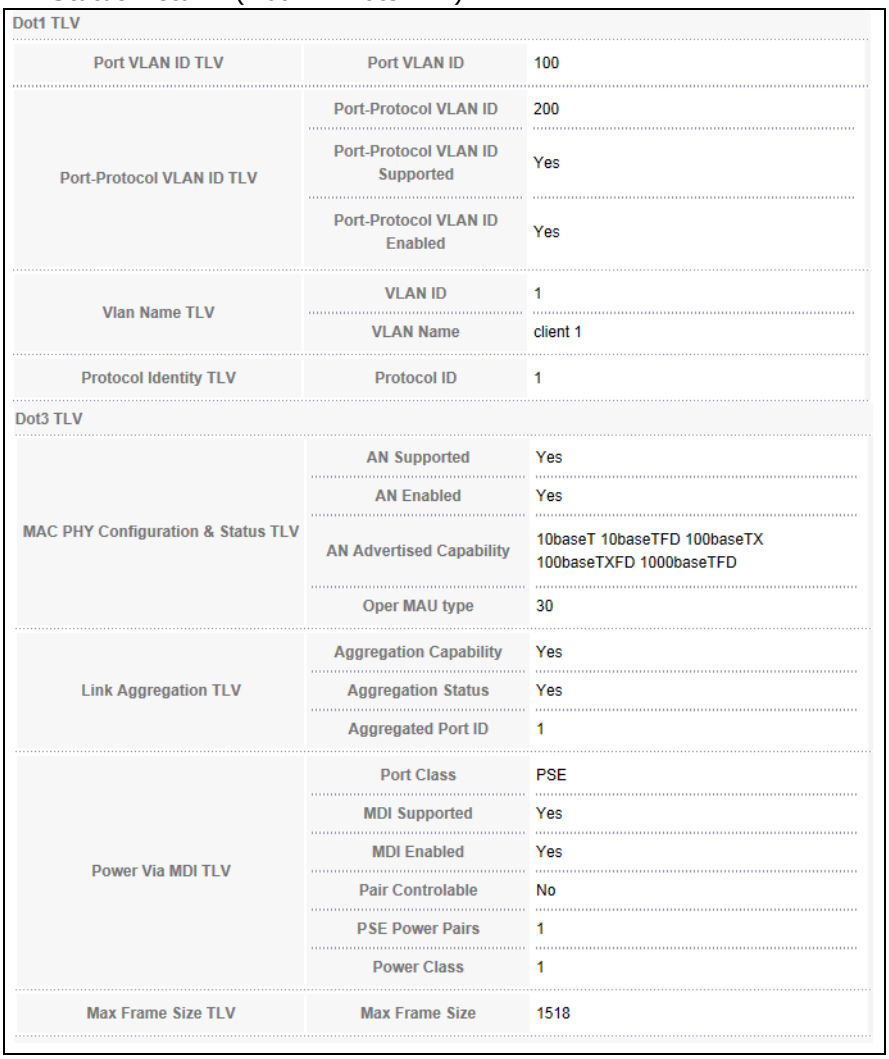
Таблица 118 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

ПОЛЕ	ОПИСАНИЕ
Basic TLV	
Chassis ID TLV	• Chassis ID Subtype – это поле указывает на метод идентификации шасси удаленного устройства. • Chassis ID – это поле показывает идентификатор шасси удаленного устройства. Идентификатор шасси определяется своим подтипом
Port ID TLV	• Port ID Subtype – это поле указывает на метод идентификации порта удаленного устройства. • Port ID – это поле показывает идентификатор порта удаленного устройства. Идентификатор порта определяется своим подтипом.
Time To Live TLV	Это поле показывает множитель времени жизни (TTL) кадров LLDP. При истечении соответствующего времени TTL информация о соседних устройствах на данном устройстве устаревает и отбрасывается. Для расчета значения TTL необходимо умножить множитель TTL на интервал передачи кадров LLDP.
Port Description TLV	Это поле содержит описание удаленного порта.

Таблица 118 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

ПОЛЕ	ОПИСАНИЕ
System Name TLV	Это поле показывает имя системы удаленного устройства.
System Description TLV	Это поле содержит описание системы для удаленного устройства.
System Capabilities TLV	Это поле отображает системные возможности, которые поддерживает удаленное устройство и которые на нем активированы. • System Capabilities Supported (Поддерживаемые системные возможности) • System Capabilities Enabled (Активированные системные возможности)
Management Address TLV	Это поле показывает параметры адреса управления удаленного устройства. • Management Address Subtype (Подтип адреса управления) • Management Address (Адрес управления) • Interface Number Subtype (Подтип номера интерфейса) • Interface Number (Номер интерфейса) • Object Identifier (Идентификатор объекта)

Рисунок 182 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail> (Dot 1 и Dot3 TLV)



В таблице, приведенной ниже, описаны поля из разделов Dot1 и Dot3 для данного экрана.

Таблица 119 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

ПОЛЕ	ОПИСАНИЕ
Dot1 TLV	
Port VLAN ID TLV	Это поле показывает идентификатор сети VLAN данного порта на удаленном устройстве.
Port-Protocol VLAN ID TLV	Это поле содержит TLV IEEE 802.1 Port Protocol VLAN ID, который указывает, имеется ли для данного порта идентификатор сети VLAN, активирована ли она, и поддерживается ли она для порта удаленного коммутатора, который отправил данный блок LLDPDU. • Port-Protocol VLAN ID • Port-Protocol VLAN ID Supported • Port-Protocol VLAN ID Enabled
Vlan Name TLV	Это поле отображает идентификатор сети VLAN и имя порта удаленного устройства. • VLAN ID • VLAN Name
Protocol Identity TLV	Наличие поля Protocol Identity TLV позволяет коммутатору анонсировать определенные протоколы, доступные через данный порт.
Dot3 TLV	
MAC PHY Configuration & Status TLV	TLV MAC/PHY Configuration/Status анонсирует поддерживаемую скорость в битах и возможность поддержки дуплексного режима отправляющим узлом 802.3. Кроме того, данное поле TLV анонсирует текущие режим дуплекса и скорость в битах отправляющего узла. Наконец, данное поле TLV указывает, является ли выбранный параметр результатом автосогласования при установлении соединения или ручной настройки. • AN Supported – Показывает, поддерживает ли данный порт функцию автосогласования. • AN Enabled – Текущий статус автосогласования порта. • AN Advertised Capability – Указывает на возможности порта в части автосогласования. • Oper MAU Type – Текущий тип MAU (Medium Attachment Unit) порта
Link Aggregation TLV	Поле Link Aggregation TLV показывает, поддерживает ли данный канал возможность агрегации, участвует ли канал в агрегации в данный момент, и, если да, указывает агрегационный идентификатор порта. • Aggregation Capability – Текущие возможности порта по участию в агрегации. • Aggregation Status – Текущий статус агрегации порта. • Aggregation Port ID – Агрегационный идентификатор данного порта.
Power Via MDI TLV	Поле Power Via MDI TLV позволяет анонсировать и обнаруживать поддержку питания MDI со стороны порта удаленного устройства, отправившего данное сообщение, с помощью средств управления сетью. • Port Class (Класс порта) • MDI Supported (Функция MDI поддерживается) • MDI Enabled (Функция MDI активирована) • Pair Controlable (Парный контроль) • PSE Power Pairs (Пары питания PSE) • Power Class (Класс питания)
Max Frame Size TLV	Это поле показывает максимальный поддерживаемый размер кадра в октетах.

Рисунок 183 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

MED TLV

Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	VLAN ID 10, tagged, known, L2-priority 7, DSCP 63
	Voice-Signaling	VLAN ID 100, tagged, known, L2-priority 2, DSCP 10
	Guest-Voice	VLAN ID 20, tagged, known, L2-priority 3, DSCP 12
	Guest-Voice-Signaling	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Softphone-Voice	VLAN ID 200, tagged, known, L2-priority 1, DSCP 1
	Video-Conferencing	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Streaming-Video	VLAN ID 300, tagged, known, L2-priority 4, DSCP 20
	Video-Signaling	VLAN ID 400, tagged, known, L2-priority 6, DSCP 55
Location Identification TLV	Coordinate-base LCI	latitude north 0.0 longitude east 0.9995 altitude meters 0.0 datum NAD83-MLLW
	Civic LCI	country TW city HSINCHU building ZYXEL
	ELIN	1234567890
Inventory TLV	Hardware Revision	V20131114 | 11/14/2013
	Software Revision	V4.10(AAOA.0) | 11/15/2013
	Firmware Revision	V4.10(AAOA.0) | 11/15/2013
	Model Name	GS3700-HP
	Manufacturer	123456789

В таблице, приведенной ниже, описаны поля из раздела MED TLV для данного экрана.

Таблица 120 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

ПОЛЕ	ОПИСАНИЕ
MED TLV	LLDP Media Endpoint Discovery (MED) – это расширение протокола LLDP, которое поддерживает дополнительные возможности по взаимодействию с мультимедийными конечными устройствами. MED поддерживает анонс/обнаружение сетевых политик и обнаружение местонахождения устройств, позволяя создавать базы данных, содержащие сведения о местонахождении устройств, и предоставляя информацию, необходимую для поиска и устранения проблем.
Capabilities TLV	Это поле описывает возможности MED, которые поддерживает удаленный порт. • Network Policy (Сетевая политика) • Location (Местоположение) • Extend Power via MDI PSE (Расширенные возможности подачи питания с использованием MDI PSE) • Extend Power via MDI PSE (Расширенные возможности подачи питания с использованием MDI PD) • Inventory Management (Управление инвентарной информацией)
Device Type TLV	Классы конечных устройств LLDP-MED: • Endpoint Class I (Класс конечного устройства I) • Endpoint Class II (Класс конечного устройства II) • Endpoint Class III (Класс конечного устройства III) • Network Connectivity (Устройство обеспечения сетевого взаимодействия)
Network Policy TLV	Это поле показывает сетевую политику для указанного приложения. • Voice (Сеть голосовой связи) • Voice-Signaling (Сигнализация сети голосовой связи) • Guest-Voice (Гостевая сеть голосовой связи) • Guest-Voice-Signaling (Сигнализация в гостевой сети голосовой связи) • Softphone-Voice (Голосовая связь для программного телефона) • Video-Conferencing (Видеоконференцсвязь) • Streaming-Video (Потоковая передача видео) • Video-Signaling (Сигнализация при передаче видео)
Location Identification TLV	Это поле показывает информацию о местонахождении абонента, совершающего вызов, на основании следующих параметров: • Coordinate-based LCI – координаты широты, долготы и высоты, содержащиеся в информации о конфигурации местоположения (LCI) • Civic LCI – IETF Geopriv Civic Address based Location Configuration Information (Информация о конфигурации местоположения на основе городского адреса IETF Geopriv Civic Address) • ELIN – (Emergency Location Identifier Number, идентификатор местоположения для экстренных служб)

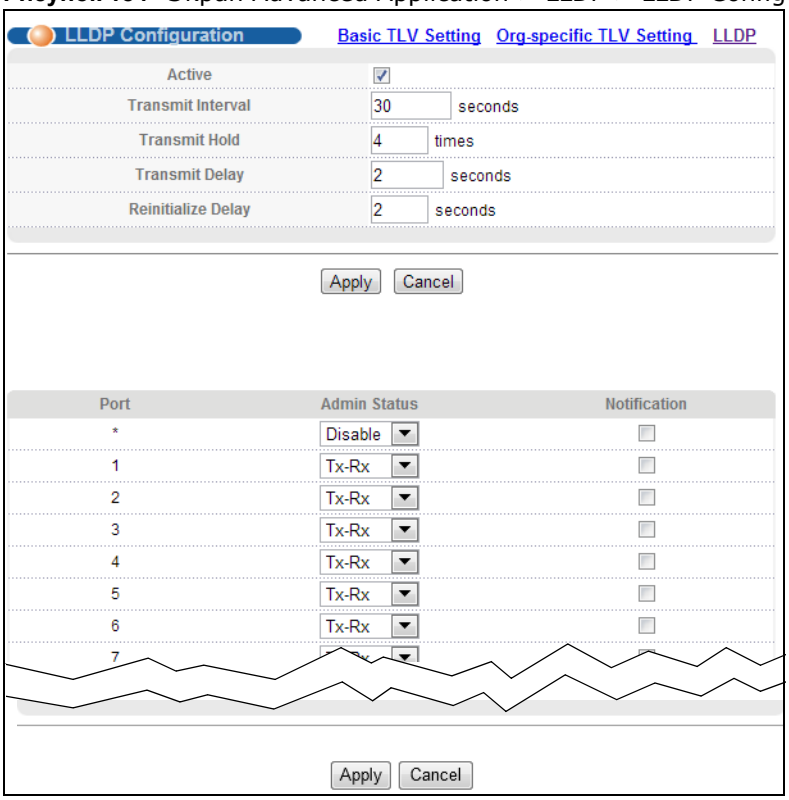
Таблица 120 Экран Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

ПОЛЕ	ОПИСАНИЕ
Inventory TLV	Большинство моделей IP-телефонов не поддерживают протоколы управления, такие, как SNMP, поэтому для предоставления инвентарной информации устройствам обеспечения сетевого взаимодействия, например, коммутатору, используются инвентарные TLV LLDP-MED. Поле Inventory TLV может содержать следующую информацию. • Hardware Revision (Номер ревизии устройства) • Software Revision (Номер ревизии программного обеспечения) • Firmware Revision (Номер ревизии встроенного программного обеспечения) • Model Name (Наименование модели) • Manufacturer (Производитель) • Serial Number (Серийный номер) • Asset ID (Идентификатор ресурса)
Extended Power via MDI TLV	Поле Extended Power Via MDI Discovery позволяет мультимедийным конечным точкам, например, IP-телефонам, и устройствам обеспечения сетевого взаимодействия, таким, как коммутатор, анонсировать подробную информацию о поддержке дополнительных методов подачи питания. • Power Type – использует ли устройство в данный момент основной или резервный источник питания (использование резервного источника может сообщить конечному устройству о необходимости перехода в режим экономии питания). • Power Source – работает ли конечное устройство в данный момент от внешнего источника питания. • Power Priority – приоритеты конечного устройства в получении питания от различных источников (устройство обеспечения сетевого взаимодействия может использовать эту опцию при выстраивании приоритетов, определяющих, какие устройства должны продолжать работать при проблемах с электричеством) • Power Value – требования к питанию в единицах ватт в текущей конфигурации

32.6 Настройки протокола LLDP

С помощью этого экрана можно настроить глобальные параметры LLDP на коммутаторе. Перейдите по ссылке **Advanced Application** > **LLDP > LLDP Configuration (Click Here)**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 184 Экран Advanced Application > LLDP > LLDP Configuration



Поля экрана описаны в следующей таблице.

Таблица 121 Экран Advanced Application > LLDP > LLDP Configuration

ПОЛЕ	ОПИСАНИЕ
Active	Выберите эту опцию, чтобы активировать поддержку протокола LLDP на коммутаторе. По умолчанию этот переключатель установлен.
Transmit Interval	Укажите периодичность отправки пакетов LLDP коммутатором (в секундах).
Transmit Hold	Укажите множитель срока жизни (TTL) для кадров LLDP. При истечении соответствующего времени TTL информация о соседних устройствах на данном устройстве устаревает и отбрасывается. Для расчета значения TTL необходимо умножить множитель TTL на интервал передачи пакетов LLDP.
Transmit Delay	Укажите задержку (в секундах) между последовательными сообщениями LLDPDU, инициированными в результате изменений значения и статуса в базе данных MIB коммутатора.
Reinitialize Delay	Укажите период ожидания в секундах, по истечении которого LLDP выполняет инициализацию на определенном порту.
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.
Port	Это поле показывает номер порта, для которого действует данная конфигурация LLDP. * означает «все порты».

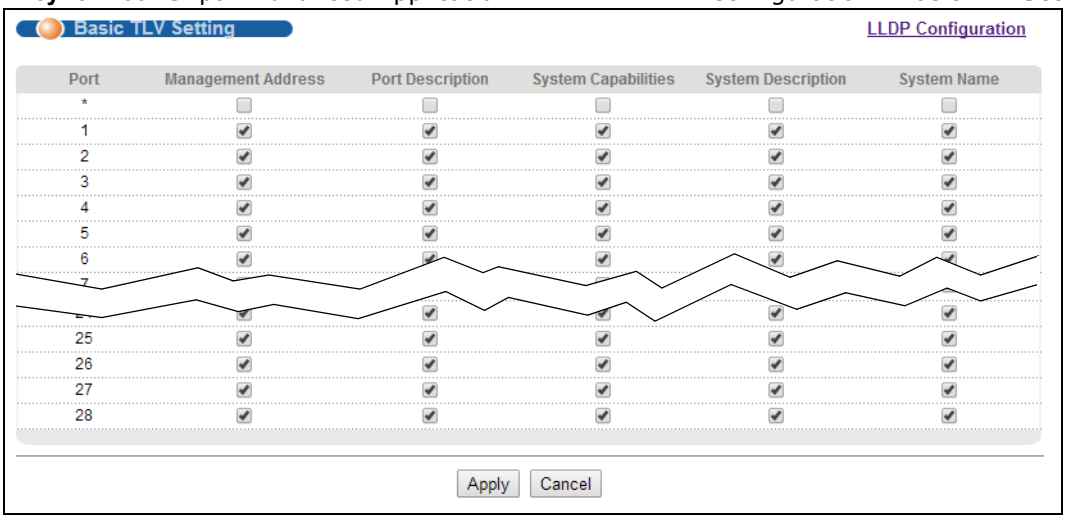
Таблица 121 Экран Advanced Application > LLDP > LLDP Configuration

ПОЛЕ	ОПИСАНИЕ
Admin Status	Укажите, разрешена ли передача и/или прием сообщений LLDP через данный порт. • Disable – запрещена • Tx-Only – разрешена только передача • Rx-Only – разрешен только прием • Tx-Rx – разрешены и передача, и прием
Notification	Укажите, включена ли для данного порта поддержка уведомлений LLDP.
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.

32.6.1 Настройки Basic TLV для конфигурации LLDP

С помощью этого экрана можно настроить параметры Basic TLV. Перейдите по ссылке **Advanced Application** > **LLDP > LLDP Configuration (Click Here) > Basic TLV Setting**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 185 Экран Advanced Application > LLDP > LLDP Configuration> Basic TLV Setting



Поля экрана описаны в следующей таблице.

Таблица 122 Экран Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

ПОЛЕ	ОПИСАНИЕ
Port	Это поле отображает номер порта, для которого выполняется настройка параметров LLDP. Чтобы применить изменяемые параметры для всех портов одновременно, установите переключатели в строке *. По умолчанию все переключатели в строке * установлены.
Management Address	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений Management Address через данный порт (или порты).
Port Description	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений Port Description через данный порт (или порты).

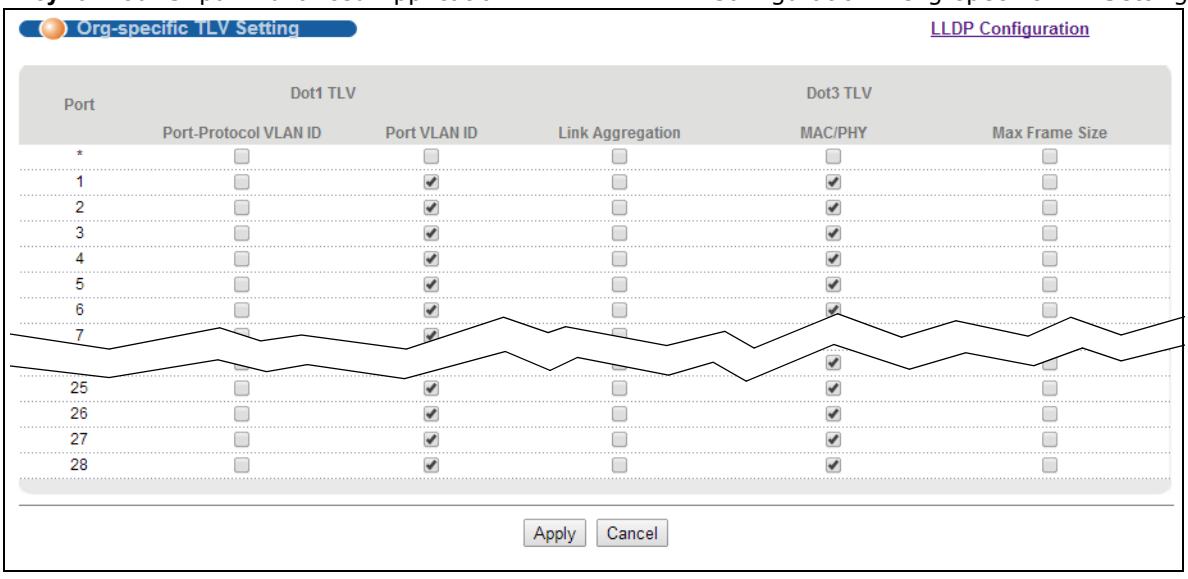
Таблица 122 Экран Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

ПОЛЕ	ОПИСАНИЕ
System Capabilities	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений System Capabilities через данный порт (или порты).
System Description	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений System Description через данный порт (или порты).
System Name	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений System Name через данный порт (или порты).
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.

32.6.2 Настройка специфичных для организаций полей TLV в конфигурации LLDP

С помощью этого экрана можно настроить параметры полей TLV, специфичных для организаций. Перейдите по ссылке **Advanced Application** > **LLDP > LLDP Configuration (Click Here) > Org-specific TLV Setting**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 186 Экран Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting



Поля экрана описаны в следующей таблице.

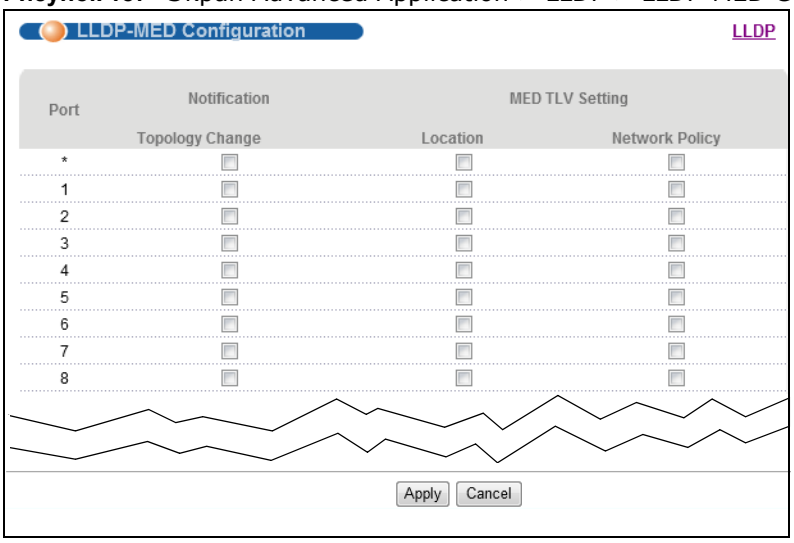
Таблица 123 Экран Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

ПОЛЕ	ОПИСАНИЕ
Port	Это поле отображает номер порта, для которого выполняется настройка параметров LLDP. Чтобы применить изменяемые параметры для всех портов одновременно, установите переключатели в строке *.
Dot1 TLV	
Port-Protocol VLAN ID	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений IEEE 802.1 Port and Protocol VLAN ID через данный порт (или порты).
Port VLAN ID	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений IEEE 802.1 Port VLAN ID через данный порт (или порты). По умолчанию все переключатели в этой строке установлены.
Dot3 TLV	
Power Via MDI TLV	**Примечание**: Только для моделей с поддержкой питания устройств по витой паре (PoE). Поле Power Via MDI TLV позволяет анонсировать и обнаруживать поддержку питания MDI со стороны порта удаленного устройства, отправившего данное сообщение, с помощью средств управления сетью. • Port Class (Класс порта) • MDI Supported (Функция MDI поддерживается) • MDI Enabled (Функция MDI активирована) • Pair Controlable (Парный контроль) • PSE Power Pairs (Пары питания PSE) • Power Class (Класс питания)
Link Aggregation	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений IEEE 802.3 Link Aggregation через данный порт (или порты).
MAC/PHY	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений IEEE 802.3 MAC/PHY Configuration/Status через данный порт (или порты). По умолчанию все переключатели в этой строке установлены.
Max Frame Size	Установите данный переключатель или снимите с него выделение, чтобы разрешить или запретить отправку TLV-сообщений IEEE 802.3 Max Frame Size через данный порт (или порты).
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.

32.7 Настройки LLDP-MED

Перейдите по ссылке **Advanced Application** > **LLDP > LLDP-MED Configuration (Click Here)**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 187 Экран Advanced Application > LLDP > LLDP-MED Configuration



Поля экрана описаны в следующей таблице.

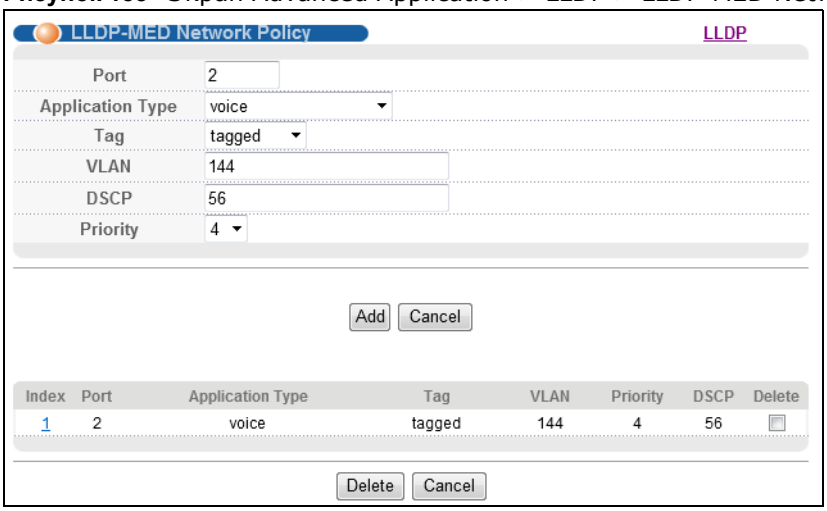
Таблица 124 Экран Advanced Application > LLDP > LLDP-MED Configuration

ПОЛЕ	ОПИСАНИЕ
Port	Это поле отображает номер порта, для которого выполняется настройка параметров LLDP-MED. Установите переключатели в строке *, чтобы применить их ко всем портам одновременно.
Notification	
Topology Change	Выберите эту опцию, чтобы включить поддержку ловушек изменения топологии LLDP-MED для данного порта.
MED TLV Setting	
Location	Выберите эту опцию, чтобы разрешить передачу TLV-сообщений Location LLDP-MED через данный порт.
Network Policy	Выберите эту опцию, чтобы разрешить передачу TLV-сообщений Network Policy LLDP-MED через 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.

32.8 Настройки сетевых политик LLDP-MED

Перейдите по ссылке **Advanced Application** > **LLDP > LLDP-MED Network Policy (Click Here)**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 188 Экран Advanced Application > LLDP > LLDP-MED Network Policy



Поля экрана описаны в следующей таблице.

Таблица 125 Экран Advanced Application > LLDP > LLDP-MED Network Policy

ПОЛЕ	ОПИСАНИЕ
Port	Укажите номер порта, для которого выполняется настройка сетевых политик LLDP-MED.
Application Type	Выберите тип приложения, используемого для данной сетевой политики. • voice (Сеть голосовой связи) • voice-signaling (Сигнализация сети голосовой связи) • guest-voice (Гостевая сеть голосовой связи) • guest-voice-signaling (Сигнализация в гостевой сети голосовой связи) • softphone-voice (Голосовая связь для программного телефона) • video-conferencing (Видеоконференцсвязь) • streaming-video (Потоковая передача видео) • video-signaling (Сигнализация при передаче видео)
Tag	Укажите, нужно ли добавлять или убирать теги в рамках данной сетевой политики. • с тегами (Tagged) • без тегов (Untagged)
VLAN	Укажите идентификационный номер сети VLAN. Он выбирается из диапазона от 1 до 4094. Для кадров с тегом приоритета нужно ввести значение «0».
DSCP	Укажите значение DSCP для данной сетевой политики. Оно выбирается из диапазон от 0 до 63, при этом 0 означает использование значения DSCP по умолчанию.
Priority	Укажите значение приоритета для данной сетевой политики.
Add	После завершения ввода информации о сетевых политиках нажмите Add. В сводной таблице появятся все созданные для коммутатора сетевые политики.
Cancel	Нажмите Cancel, если требуется изменить только что введенную информацию.
Index	Это поле отображает порядковый номер сетевой политики. Нажмите на этот номер, чтобы отредактировать правило.
Port	Это поле отображает номер порта для сетевой политики.
Application Type	Это поле отображает тип приложения для сетевой политики.
Tag	Это поле отображает статус добавления/удаления тегов для сетевой политики.
VLAN	Это поле отображает идентификатор сети VLAN для сетевой политики.
Priority	Это поле отображает значение приоритета для сетевой политики.

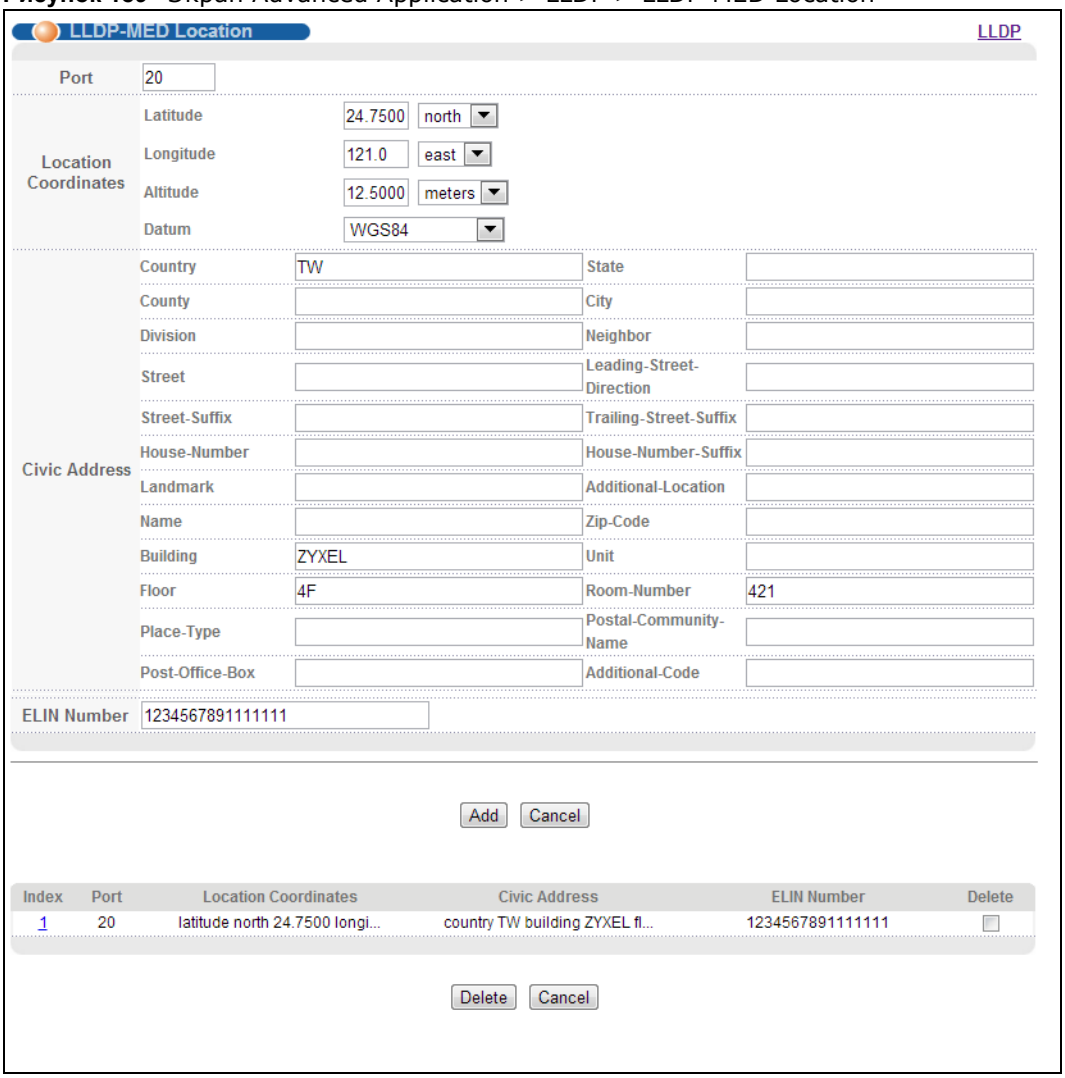
Таблица 125 Экран Advanced Application > LLDP > LLDP-MED Network Policy

ПОЛЕ	ОПИСАНИЕ
DSCP	Это поле отображает значение DSCP для сетевой политики.
Delete	Выберите правила, которые нужно удалить, в столбце Delete и нажмите кнопку Delete.
Cancel	Нажмите Cancel, чтобы снять выделение с переключателей в столбце **Delete**.

32.9 Информация о местоположении LLDP-MED

Перейдите по ссылке **Advanced Application** > **LLDP > LLDP-MED Location (Click Here)**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 189 Экран Advanced Application > LLDP > LLDP-MED Location



Поля экрана описаны в следующей таблице.

Таблица 126 Экран Advanced Application > LLDP > LLDP-MED Location

ПОЛЕ	ОПИСАНИЕ
Port	Укажите номер порта, для которого требуется настроить параметры местоположения в сети LLDP-MED.
Location Coordinates	Протокол LLDP-MED использует географические координаты и городской адрес (Civic Address) для определения местоположения удаленного устройства. Географические координаты включают в себя широту, долготу, высоту и точку отсчета. Городской адрес включает в себя страну, штат, округ, город, улицу и другую сопутствующую информацию.
Latitude	Введите информацию о широте. Значение выбирается в диапазоне от 0º до 90º. Отрицательное значение соответствует югу. • north (северной) • south (южной)
Longitude	Введите информацию о долготе. Значение выбирается в диапазоне от 0º до 180º. Отрицательное значение соответствует западу. • west (западной) • east (восточной)
Altitude	Введите информацию о высоте. Значение выбирается в диапазоне от -2097151 до 2097151 указывается в метрах или в этажах. • meters (метры) • floor (этажи)
Datum	Укажите соответствующую геодезическую точку отсчета, используемую GPS. • WGS84 • NAD83-NAVD88 • NAD83-MLLW

Таблица 126 Экран Advanced Application > LLDP > LLDP-MED Location

ПОЛЕ	ОПИСАНИЕ
Civic Address	Укажите городской адрес (Civic Address), включающий в себя такие сведения, как страна, штат, округ, город, улица, номер дома, почтовый индекс, и другую дополнительную информацию. Городской адрес должен включать в себя как минимум два поля, одним из которых должна быть страна. Допустимая длина поля «Country» (Страна) составляет 2 символа, длина всех остальных полей не должна превышать 32 символа. • Country (Страна) • State (Штат, область) • County (Округ) • City (Город) • Division (Район) • Neighbor (Микрорайон) • Street (Улица) • Leading-Street-Direction (Направление главной улицы) • Street-Suffix (Суффикс улицы) • Trailing-Street-Suffix (Второй суффикс улицы) • House-Number (Номер дома) • House-Number-Suffix (Суффикс номера дома) • Landmark (Общеизвестное название) • Additional-Location (Дополнительные сведения о местоположении) • Name (Название) • Zip-Code (Почтовый код) • Building (Здание) • Unit (Корпус) • Floor (Этаж) • Room-Number (Номер комнаты) • Place-Type (Тип квартиры) • Postal-Community-Name (Название почтового сообщества) • Post-Office-Box (Почтовый ящик) • Additional-Code (Дополнительный код)
ELIN Number	Введите строку из цифр, соответствующую идентификатору ELIN, которые передается во время экстренных вызовов в традиционные системы CAMA или PSAP ISDN на основе портов. Длина значения в этом поле должна лежать в диапазоне от 10 до 25 символов.
Add	После завершения ввода информации о местоположении нажмите Add.
Cancel	Нажмите Cancel, если требуется изменить только что введенную информацию о местоположении.
Index	Это поле отображает порядковый номер конфигурации местоположения. Щелкните по порядковому номеру, чтобы просмотреть или изменить информацию о местоположении.
Port	В этом поле отображается номер порта для данной конфигурации местоположения.
Location Coordinates	Это поле показывает информацию о конфигурации местоположения, в основе которой лежат географические координаты, включающие в себя долготу, широту, высоту и точку отсчета.
Civic Address	Это поле отображает городской адрес (Civic Address), включающий в себя такие сведения, как страна, штат, округ, город, улица, номер дома, почтовый индекс, и другую дополнительную информацию.
ELIN Number	Это поле отображает идентификатор ELIN (Emergency Location Identification Number), который используется для идентификации конечных устройств, участвующих в совершении экстренных вызовов. Длина значения в этом поле должна лежать в диапазоне от 10 до 25 символов.

Таблица 126 Экран Advanced Application > LLDP > LLDP-MED Location

ПОЛЕ	ОПИСАНИЕ
Delete	Выберите местоположения, которые нужно удалить, в столбце Delete и нажмите кнопку Delete.
Cancel	Нажмите Cancel, чтобы снять выделение с переключателей в столбце Delete.

33

Статические маршруты

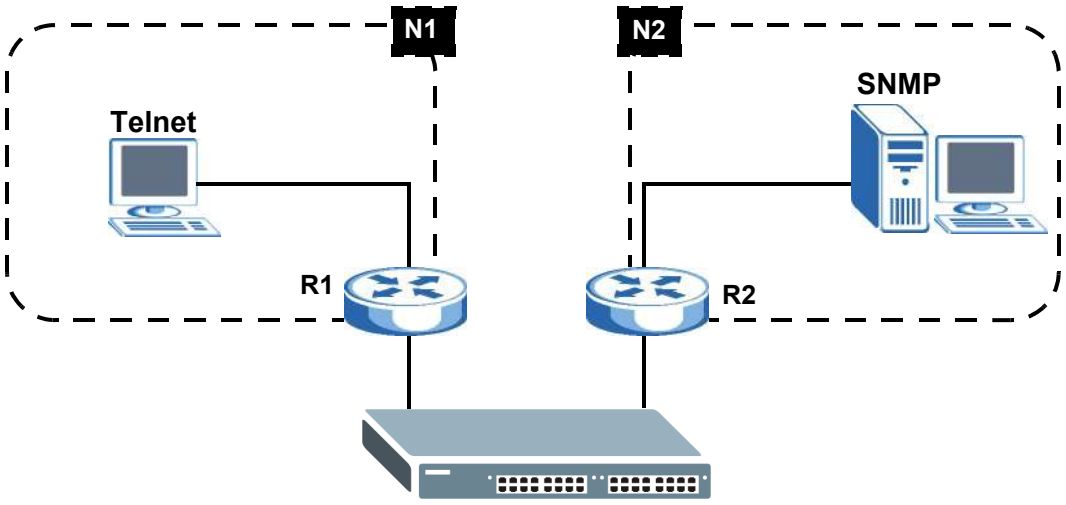
33.1 Обзор статических маршрутов

В данной главе описана настройка статических маршрутов.

Взаимодействие данного коммутатора с управляющими компьютерами осуществляется через IP-подключение (например, с использованием HTTP, Telnet, SSH или SNMP). С помощью статических IP-маршрутов коммутатор может отвечать удаленным станциям управления, недоступным через шлюз по умолчанию. Кроме того, статические маршруты могут использоваться коммутатором для отправки данных на сервер или устройство, недоступные через шлюз по умолчанию, например, для передачи «ловушек» SNMP или использования команды ping при проверке IP-подключения.

На приведенном ниже рисунке показана сессия **Telnet** из сети **N1**. Ответный трафик коммутатор отправляет на шлюз по умолчанию **R1**, который маршрутизирует его к компьютеру управления. Чтобы коммутатор мог отправлять трафик на сервер «ловушек» SNMP, находящийся в сети **N2**, на коммутаторе потребуется настроить статические маршруты.

Рисунок 190 Обзор статических маршрутов



33.1.1 О чем рассказывается в этой главе

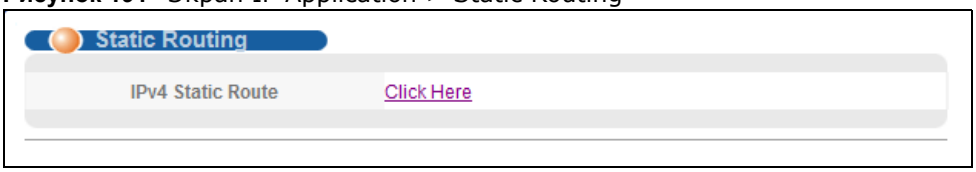
- С помощью экрана **Static Routing** (разд. 33.2 на стр. 298) можно проверить, активирован ли определенный статический маршрут IPv4.
- С помощью экрана **IPv4 Static Route** (разд. 33.3 на стр. 298) можно активировать или деактивировать определенный статический маршрут.

33.2 Статические маршруты

Чтобы активировать статический маршрут IPv4, необходимо задать его параметры на экране **IP Application > Static Routing > IPv4 Static Route**.

Выберите в навигационной панели **IP Application > Static Routing**, чтобы открыть экран, изображенный на рисунке ниже.

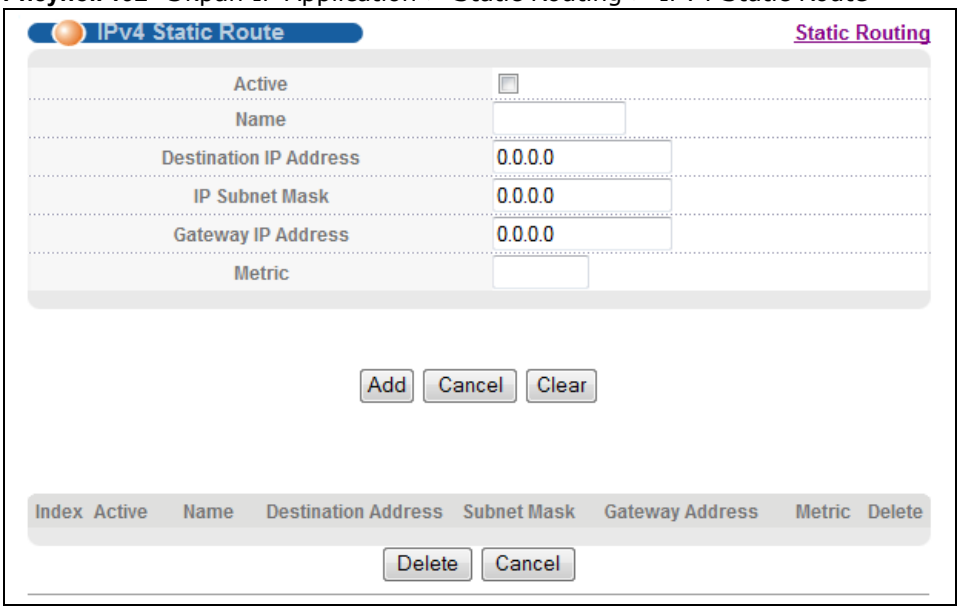
Рисунок 191 Экран IP Application > Static Routing



33.3 Настройка статических маршрутов

Выберите в навигационной панели **IP Application > Static Routing > IPv4 Static Route**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 192 Экран IP Application > Static Routing > IPv4 Static Route



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

Таблица 127 Экран IP Application > Static Routing > IPv4 Static Route

ПОЛЕ	ОПИСАНИЕ
Active	В этом поле можно активировать/деактивировать данный статический маршрут.
Name	Введите имя-описание (до 10 отображаемых ASCII-символов), по которому можно идентифицировать этот маршрут.
Destination IP Address	Сетевой IP-адрес конечного пункта назначения.

Таблица 127 Экран IP Application > Static Routing > IPv4 Static Route (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Subnet Mask	Введите маску подсети для данного направления. 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.
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 сбросить поля к предыдущим значениям.
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**.

34

Дифференцированное обслуживание

34.1 Обзор дифференцированного обслуживания

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

34.1.1 О чем рассказывается в этой главе

- С помощью экрана **DiffServ** (разд. 34.2 на стр. 301) можно активировать функцию дифференцированного обслуживания (DiffServ) для применения правил маркирования или отображения приоритетов IEEE 802.1p на коммутаторе.
- С помощью экрана **DSCP** (разд. 34.3.1 на стр. 303) можно изменить правила соответствия DSCP-IEEE 802.1p.

34.1.2 Что необходимо знать

Ознакомьтесь с приведенной ниже информацией о дифференцированном обслуживании, которая поможет в работе с экранами, описанными в этой главе.

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 193 DiffServ: поле Differentiated Service

DSCP (6 бит)	CU (2 бита)

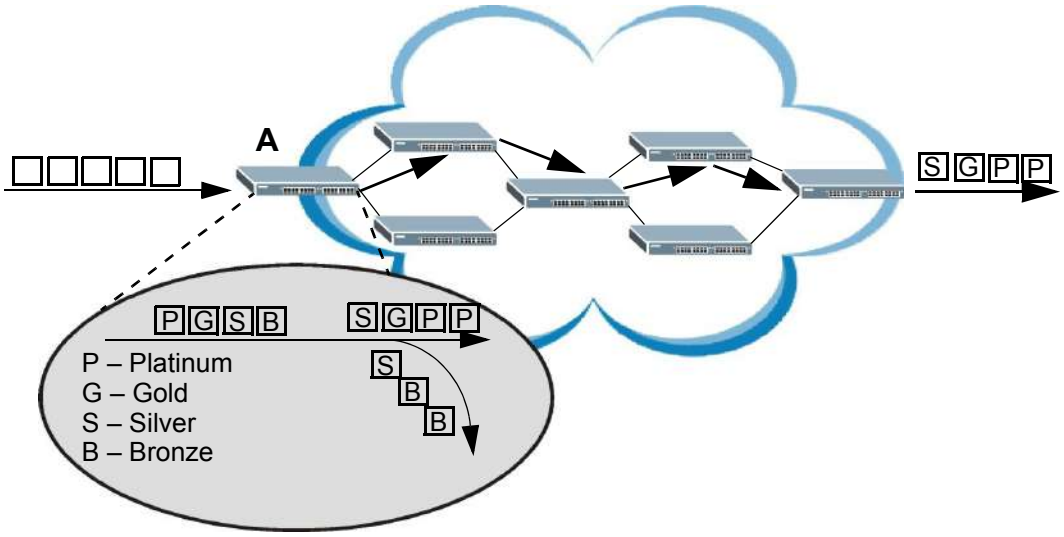
Маркер DSCP обратно совместим с тремя битами приоритета в октете ToS, благодаря чему сетевое устройство с поддержкой ToS, но без поддержки DiffServ не будет конфликтовать с отображением маркера DSCP.

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.

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. 194) 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 194 Сеть с поддержкой DiffServ

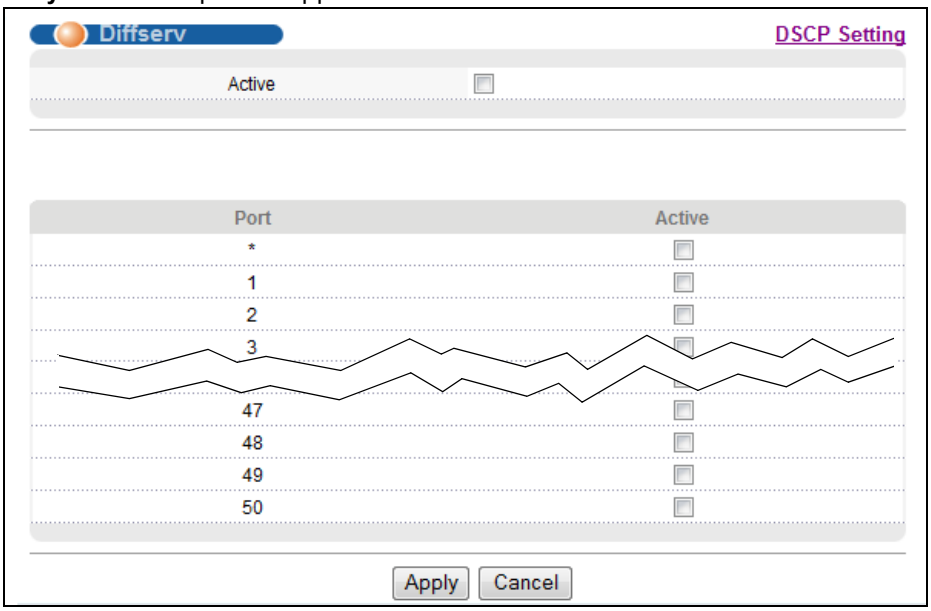


34.2 Активация механизма DiffServ

Активируйте функцию дифференцированного обслуживания (DiffServ), чтобы обеспечить применение правил маркирования или отображения приоритетов IEEE 802.1p на коммутаторе.

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

Рисунок 195 Экран IP Application > DiffServ



Поля экрана описаны в следующей таблице.

Таблица 128 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. Изменения в данной строке сразу же копируются на все порты.
Active	Выберите опцию **Active**, чтобы включить функцию Diffserv для данного 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.

34.3 Настройка отображения маркеров DSCP на приоритеты IEEE 802.1p

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

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

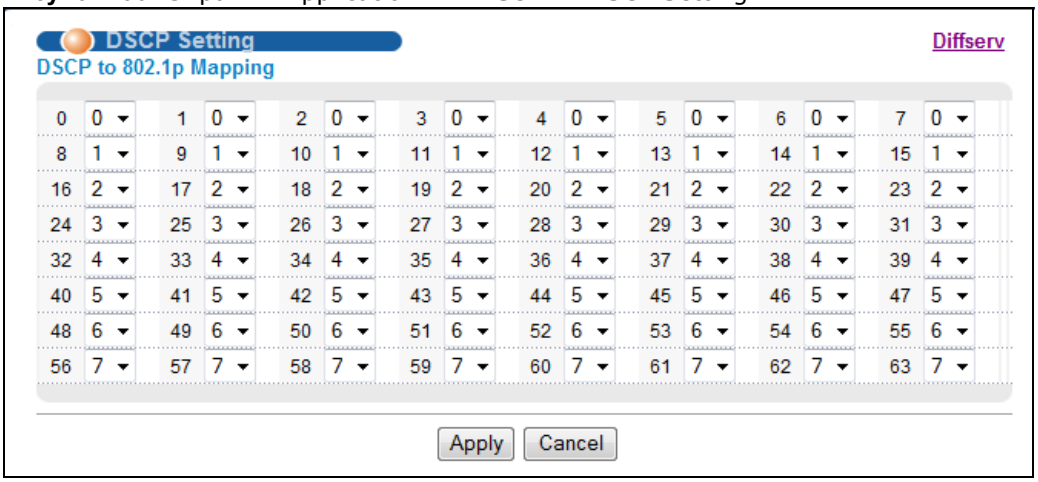
Таблица 129 Отображение маркеров DSCP на приоритеты IEEE 802.1p по умолчанию

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

34.3.1 Настройка DSCP

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

Рисунок 196 Экран IP Application > DiffServ > DSCP Setting



Поля экрана описаны в следующей таблице.

Таблица 130 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.

35

DHCP

35.1 Обзор DHCP

В данной главе описана настройка функции 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. Если настроить коммутатор в качестве агента ретрансляции DHCP, он будет пересылать запросы DHCP на сервер DHCP, находящийся в данной сети. Если не настраивать коммутатор в качестве агента ретрансляции DHCP, потребуется сервер DHCP в широковещательном домене клиентских компьютеров, в противном случае клиентские компьютеры придется настраивать вручную.

35.1.1 О чем рассказывается в этой главе

- С помощью экрана **DHCPv4 Status** (разд. 35.3 на стр. 306) можно отобразить информацию о режиме ретрансляции.
- С помощью экрана **DHCPv4 Relay** (разд. 35.4 на стр. 306) можно включить режим ретрансляции DHCP и настроить его глобальные параметры.
- С помощью экрана **VLAN Setting** (разд. 35.5 на стр. 312) можно настроить параметры DHCP исходя из домена VLAN, в котором находятся клиенты DHCP.
- С помощью экрана **DHCPv6 Relay** (разд. 35.6 на стр. 316) можно включить режим ретрансляции DHCPv6 и настроить его параметры.

35.1.2 Что необходимо знать

Ознакомьтесь с приведенной ниже информацией о DHCP, которая поможет в работе с экранами, описанными в этой главе.

Режимы DHCP

Если в сети уже имеется сервер DHCP, то коммутатор можно настроить для работы в качестве агента ретрансляции DHCP. При получении запроса от компьютера в сети коммутатор связывается с сервером DHCP для получения необходимой информации о настройках протокола IP, а затем передает полученные настройки обратно на компьютер.

Варианты настройки DHCP

Настройки DHCP на коммутаторе 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** – Настройка коммутатора осуществляется на уровне отдельной сети VLAN. На коммутаторе можно настроить ретрансляцию запросов DHCP на различные серверы DHCP в зависимости от того, к какой сети VLAN относятся клиенты.

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 маска подсети) от клиента DHCP к серверу DHCP. После получения клиентом DHCP IP-адреса и его подключения к сети обмен актуализирующей информацией между клиентом DHCP и сервером DHCP производится без участия коммутатора.

Коммутатор можно настроить для работы в качестве глобального агента ретрансляции DHCP. Это означает, что коммутатор будет передавать все запросы DHCP, поступающие изо всех доменов, на один и тот же сервер DHCP. Кроме того, на ретрансляторе можно настроить ретрансляцию информации DHCP в зависимости от сети VLAN, к которой относится клиент.

Информация агента ретрансляции DHCP

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 131 Relay Agent Information

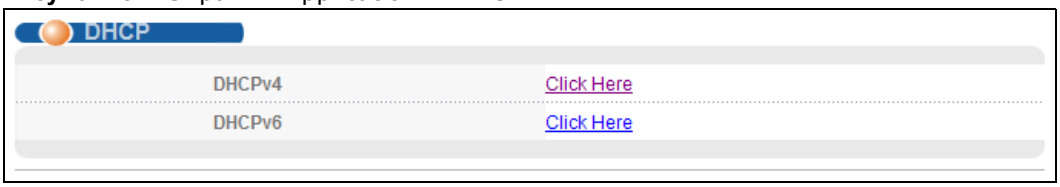
ПОЛЕ	ОПИСАНИЕ
Slot ID	(1 байт) Данное значение всегда равно 0 для автономных коммутаторов.
Port ID	(1 байт) Номер порта, к которому подключен клиент DHCP.
VLAN ID	(2 байта) Идентификатор VLAN, которой принадлежит порт.
Information	(до 64 байт) Опциональное поле только для чтения, которое устанавливается в соответствии с именем системы, настроенным на экране **Basic Settings > General Setup.**

35.2 Настройка DHCP

Выберите в навигационной панели **IP Application** > **DHCP**, чтобы открыть экран, изображенный на рисунке ниже. Перейдите по ссылке рядом с надписью **DHCPv4**, чтобы

открыть экраны, позволяющие настраивать опции ретрансляции DHCPv4 м создавать профили опции 82. Перейдите по ссылке рядом с надписью **DHCPv6**, чтобы открыть экран настройки параметров ретрансляции DHCPv6.

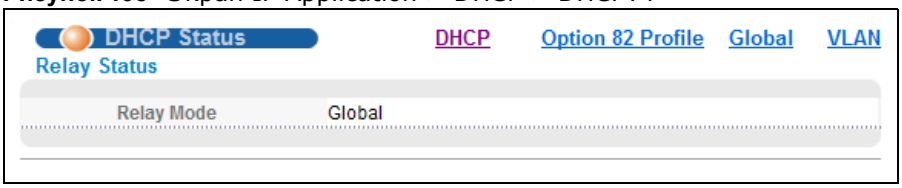
Рисунок 197 Экран IP Application > DHCP



35.3 Статус DHCPv4

Выберите в навигационной панели **IP Application** > **DHCP > DHCPv4**. Откроется экран **DHCP Status**.

Рисунок 198 Экран IP Application > DHCP > DHCPv4



Поля экрана описаны в следующей таблице.

Таблица 132 Экран IP Application > DHCP > DHCPv4

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

35.4 Ретранслятор DHCPv4

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.

35.4.1 Информация агента ретрансляции DHCPv4

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 (Agent Information), известное также, как **Option 82**, в запросы DHCP. Поле **Option 82** располагается в заголовке клиентских DHCP-запросов, ретранслируемых коммутатором на сервер DHCP.

35.4.1.1 Формат информации агента ретрансляции DHCPv4

Опция информации агента ретрансляции DHCP имеет следующий формат.

Таблица 133 Формат опции информации агента ретрансляции DHCP

Код (82)	Длина (N)	i1	i2	...	iN

i1, i2 и iN – это субопции агента ретрансляции DHCP, которые содержат дополнительную информацию о клиенте DHCP. Необходимо указать как минимум одну субопцию.

35.4.1.2 Формат субопций

Существует два типа субопций: «Agent Circuit ID Sub-option» и «Agent Remote ID Sub-option». Они имеют следующие форматы.

Таблица 134 Формат субопции DHCP Relay Agent Circuit ID

Код субопции	Длина	Значение
1 (1 байт)	N (1 байт)	Идентификатор слота, идентификатор порта, идентификатор сети VLAN, имя системы или строка

Таблица 135 Формат субопции DHCP Relay Agent Remote ID

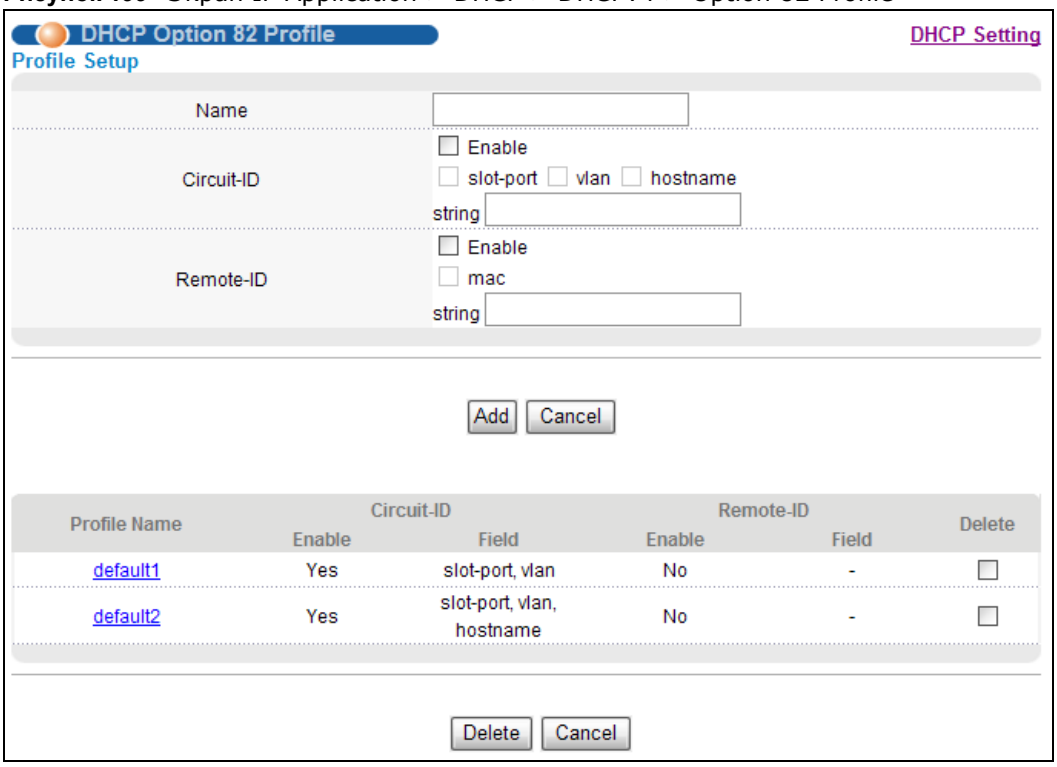
Код субопции	Длина	Значение
2 (1 байт)	N (1 байт)	MAC-адрес или строка

Значение 1 в первом поле идентифицирует субопцию Agent Circuit ID, а значение 2 – субопцию Agent Remote ID. Следующее поле определяет длину поля.

35.4.2 Профиль опции 82 DHCPv4

С помощью этого экрана можно создать профили опции 82 DHCPv4. Выберите в навигационной панели **IP Application > DHCP > DHCPv4** и перейдите по ссылке **Option 82 Profile**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 199 Экран IP Application > DHCP > DHCPv4 > Option 82 Profile



Поля экрана описаны в следующей таблице.

Таблица 136 Экран IP Application > DHCP > DHCPv4 > Option 82 Profile

ПОЛЕ	ОПИСАНИЕ
Name	Введите имя-описание профиля, с помощью которого его можно идентифицировать. Данное поле может содержать до 32 ASCII-символов. В этом поле можно использовать пробелы.
Circuit-ID	В этом разделе можно настроить субопцию Circuit ID, включив в нее информацию о конкретном агенте ретрансляции (данном коммутаторе).
Enable	При выборе этой опции коммутатор будет добавлять субопцию Circuit ID в клиентские запросы DHCP, которые он пересылает на сервер DHCP.
slot-port	При выборе этой опции коммутатор будет добавлять номер порта, к которому подключен клиент DHCP.
vlan	При выборе этой опции коммутатор будет добавлять идентификатор сети VLAN, которой принадлежит данный порт.
hostname	Это имя системы, которое задается на экране **Basic Setting** > **General Setup**. При выборе этой опции коммутатор будет добавлять имя системы в клиентские запросы DHCP, которые он передает на сервер DHCP.
string	Введите строку, содержащую не более 64 ASCII-символов, которую коммутатор будет добавлять в клиентские запросы DHCP. В этом поле можно использовать пробелы.
Remote-ID	В этом разделе можно настроить субопцию Remote ID, включив в нее информацию, которая идентифицирует данный агент ретрансляции (коммутатор).
Enable	При выборе этой опции коммутатор будет присоединять субопцию Remote ID к полю Option 82 в запросах DHCP.
mac	При выборе этой опции коммутатор будет добавлять собственный MAC-адрес в клиентские запросы DHCP, которые он передает на сервер DHCP.

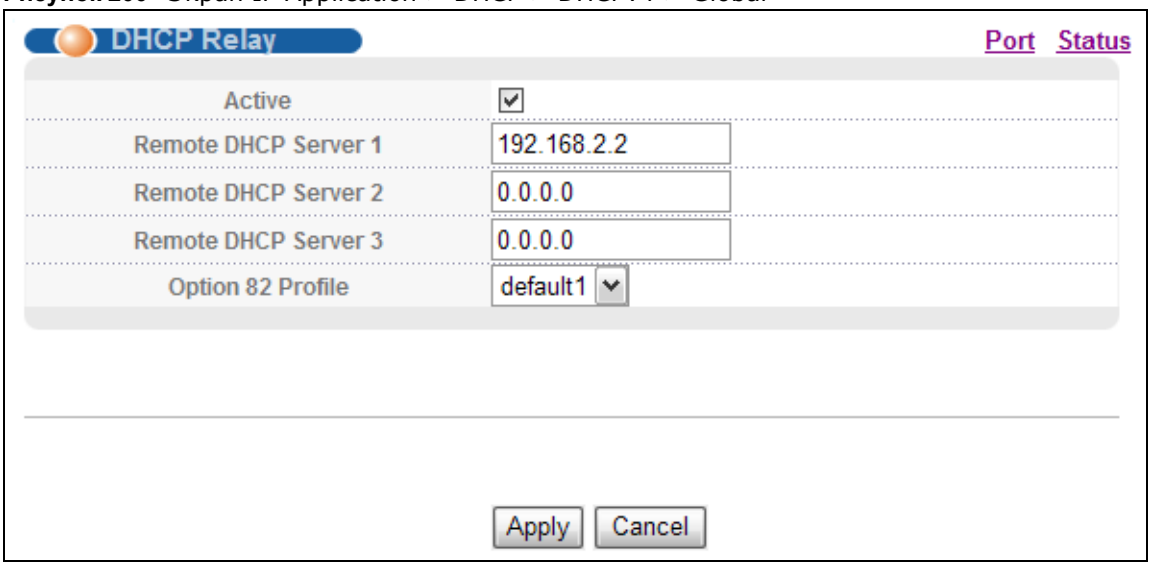
Таблица 136 Экран IP Application > DHCP > DHCPv4 > Option 82 Profile (продолжение)

ПОЛЕ	ОПИСАНИЕ
string	Введите строку, содержащую не более 64 ASCII-символов, которая будет использоваться в качестве субопции Remote ID. В этом поле можно использовать пробелы.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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 вернуться к сохраненным значениям полей.
Profile Name	В этом поле отображается имя-описание профиля. Щелкните по имени, чтобы изменить настройки.
Circuit-ID	
Enable	Это поле указывает на то, добавляется ли субопция Circuit ID в клиентские запросы DHCP.
Field	Это поле отображает информацию, которая попадает в субопцию Circuit ID.
Remote-ID	
Enable	Это поле указывает на то, добавляется ли субопция Remote ID в клиентские запросы DHCP.
Field	Это поле отображает информацию, которая попадает в субопцию Remote ID.
Delete	В столбце **Delete** выберите записи, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей в столбце **Delete**.

35.4.3 Настройка глобальных параметров ретрансляции DHCPv4

С помощью этого экрана можно настроить глобальные параметры ретрансляции DHCPv4. Выберите в навигационной панели **IP Application > DHCP > DHCPv4** и перейдите по ссылке **Global**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 200 Экран IP Application > DHCP > DHCPv4 > Global



Поля экрана описаны в следующей таблице.

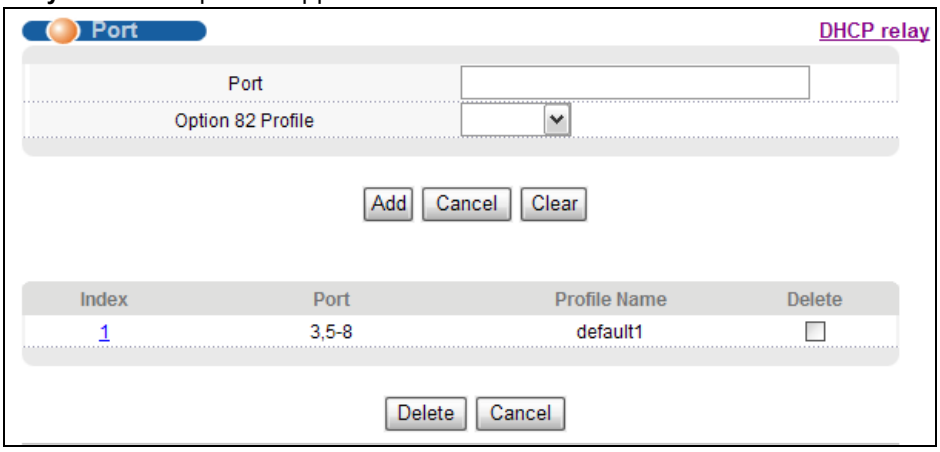
Таблица 137 Экран IP Application > DHCP > DHCPv4 > Global

ПОЛЕ	ОПИСАНИЕ
Active	Установите этот переключатель, чтобы включить ретрансляцию DHCPv4.
Remote DHCP Server 1 .. 3	Введите IP-адрес сервера DHCPv4 в виде десятичных чисел, разделенных точками.
Option 82 Profile	Выберите заранее созданный профиль опции 82 DHCPv4, который коммутатор применяет ко всем портам. Данный коммутатор добавляет субопцию Circuit ID и/или Remote ID, указанные в данном профиле, в запросы DHCP, которые он передает 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.

35.4.4 Глобальные настройки портов ретрансляции DHCPv4

С помощью этого экрана можно применить различные профили опции 82 DHCP к определенным портам коммутатора. Чтобы открыть этот экран, перейдите по ссылке **IP Application > DHCP > DHCPv4 > Global > Port**.

Рисунок 201 Экран IP Application > DHCP > DHCPv4 > Global > Port



Поля экрана описаны в следующей таблице.

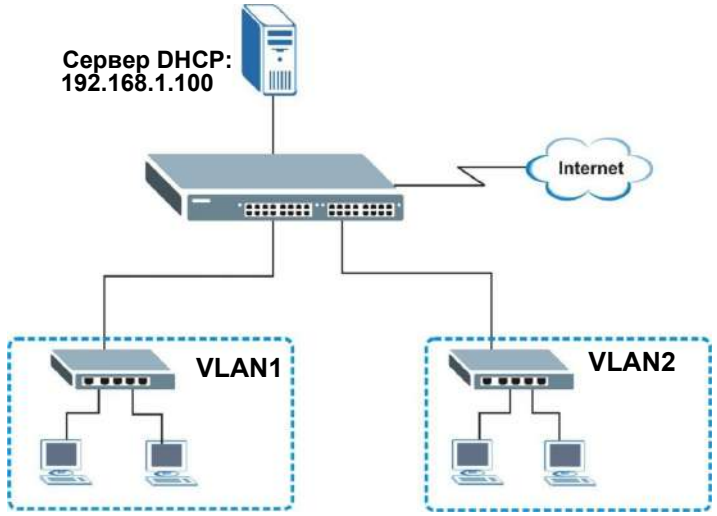
Таблица 138 Экран IP Application > DHCP > DHCPv4 > Global > Port

ПОЛЕ	ОПИСАНИЕ
Port	Введите список портов, к которым необходимо применить указанный профиль опции 82 DHCP. В этом поле можно указать два и более портов, разделенных (без пробелов) символами запятой (,) или дефиса (-). Например, запись «3-5» будет означать порты 3, 4 и 5. Чтобы указать порты 3, 5 и 7, введите в этом поле значение «3,5,7».
Option 82 Profile	Выберите заранее созданный профиль опции 82 DHCP, который коммутатор применяет к указанному порту (или портам). Данный коммутатор добавляет субопцию Circuit ID и/или Remote ID, указанные в данном профиле, в запросы DHCP, которые он передает на сервер DHCP. Профиль, выбранный на этом экране, имеет приоритет по отношению к профилю, выбранному на экране **DHCP > DHCPv4 > Global**.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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 на данную кнопку, чтобы сбросить значения из последней выбранной записи, или, если ничего не было выбрано, очистить перечисленные выше поля.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	В этом поле отображается порядковый номер каждой записи. Нажмите на этот номер, чтобы изменить настройки.
Port	Это поле показывает порт (или порты), к которым коммутатор применяет данные настройки.
Profile Name	Это поле отображает профиль опции 82 DHCP, который коммутатор применяет к указанному порту (или портам).
Delete	Выберите записи, которые нужно удалить, в столбце **Delete** и нажмите кнопку **Delete**, чтобы удалить выбранные записи из таблицы.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей **Delete**.

35.4.5 Пример настройки глобальной ретрансляции DHCP

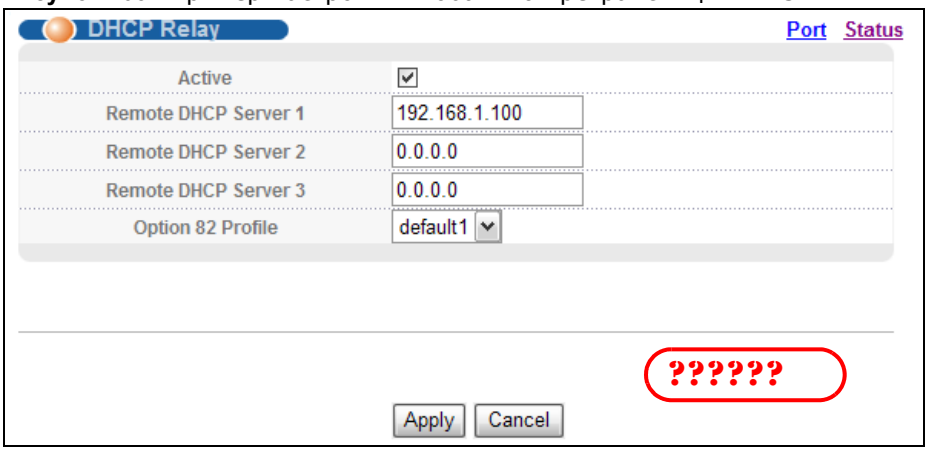
На приведенном ниже рисунке показан пример сети, в которой коммутатор используется для ретрансляции запросов DHCP в доменах **VLAN1** и **VLAN2**. В сети имеется только один сервер DHCP, который обслуживает клиентов DHCP в обоих доменах.

Рисунок 202 Пример сети с глобальной ретрансляцией DHCP



На экране **DHCP Relay** выполняются следующие настройки. Необходимо обязательно выбрать профиль опции 82 DHCP (в данном примере – **default1**), чтобы коммутатор начал передавать дополнительную информацию (например, идентификатор сети VLAN) вместе с запросами DHCP на сервер DHCP. В этом случае сервер DHCP сможет назначать нужные IP-адреса в зависимости от идентификатора VLAN ID.

Рисунок 203 Пример настройки глобальной ретрансляции DHCP

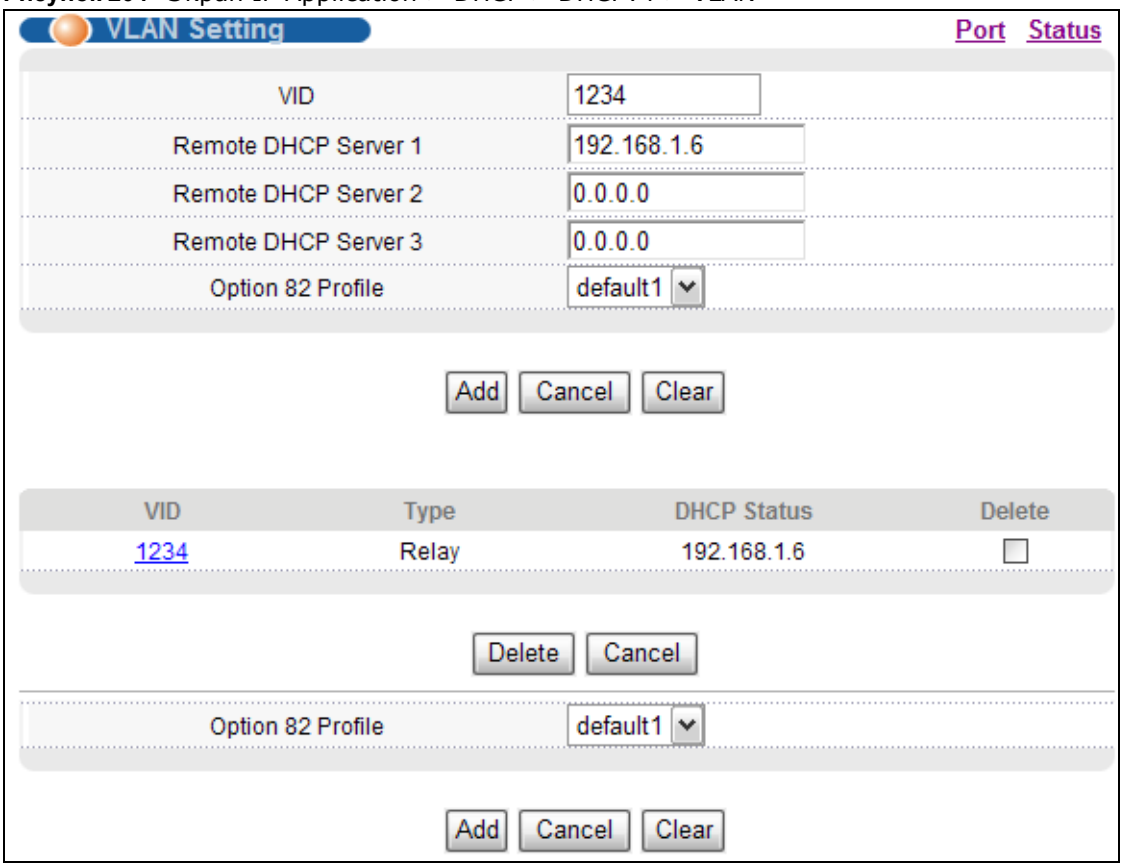


35.5 Настройка DHCPv4 для сетей VLAN

На данном экране можно настроить параметры DHCP для конкретных виртуальных локальных сетей VLAN, к которым относятся клиенты DHCP. Выберите в навигационной панели **IP Application** > **DHCP > DHCPv4**, затем перейдите по ссылке **VLAN** на открывшемся экране **DHCP Status**.

Примечание: 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. 5.2 на стр. 43.

Рисунок 204 Экран IP Application > DHCP > DHCPv4 > VLAN



Поля экрана описаны в следующей таблице.

Таблица 139 Экран IP Application > DHCP > DHCPv4 > VLAN

ПОЛЕ	ОПИСАНИЕ
VID	Введите идентификатор VLAN, к которой относятся данные настройки DHCP.
Remote DHCP Server 1 .. 3	Введите IP-адрес сервера DHCP в виде десятичных чисел, разделенных точками.
Option 82 Profile	Выберите заранее созданный профиль опции 82, который коммутатор применяет ко всем портам в данной сети VLAN. Данный коммутатор добавляет субопцию Circuit ID и/или Remote ID, указанные в данном профиле, в запросы DHCP, которые он передает на сервер DHCP.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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.
VID	В данном поле отображается идентификатор VLAN, к которой относятся настройки DHCP.
Type	В данном поле отображается **Relay** в качестве режима DHCP.

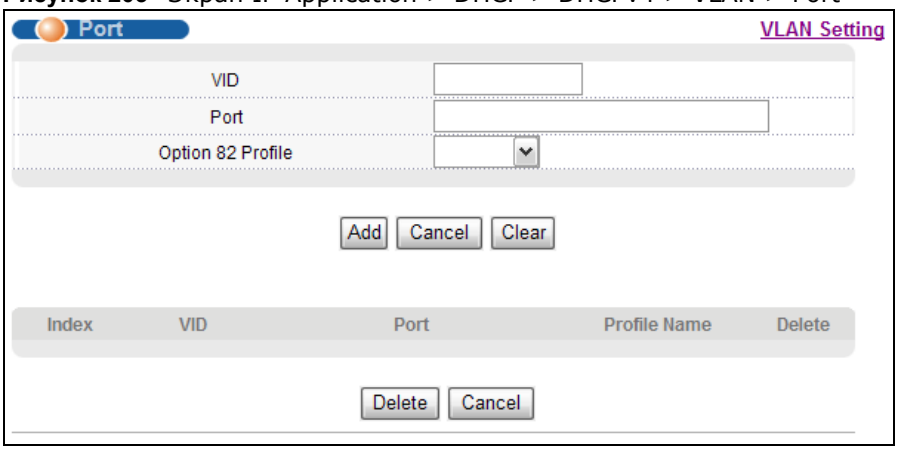
Таблица 139 Экран IP Application > DHCP > DHCPv4 > VLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
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**.

35.5.1 Настройка параметров DHCPv4 для портов сети VLAN

С помощью этого экрана можно применить различные профили опции 82 DHCP к определенным портам в сети VLAN. Чтобы открыть этот экран, перейдите по ссылке **IP Application > DHCP > DHCPv4 > VLAN > Port**.

Рисунок 205 Экран IP Application > DHCP > DHCPv4 > VLAN > Port



Поля экрана описаны в следующей таблице.

Таблица 140 Экран IP Application > DHCP > DHCPv4 > VLAN > Port

ПОЛЕ	ОПИСАНИЕ
VID	Укажите идентификатор сети VLAN, параметры которой требуется настроить.
Port	Введите список портов, к которым необходимо применить указанный профиль опции 82 DHCP. В этом поле можно указать два и более портов, разделенных (без пробелов) символами запятой (,) или дефиса (-). Например, запись «3-5» будет означать порты 3, 4 и 5. Чтобы указать порты 3, 5 и 7, введите в этом поле значение «3,5,7».
Option 82 Profile	Выберите заранее созданный профиль опции 82, который коммутатор применяет к указанным портам в данной сети VLAN. Данный коммутатор добавляет субопцию Circuit ID и/или Remote ID, указанные в данном профиле, в запросы DHCP, которые он передает на сервер DHCP. Профиль, выбранный на этом экране, имеет приоритет по отношению к профилю, выбранному на экране **DHCP > DHCPv4 > VLAN**.

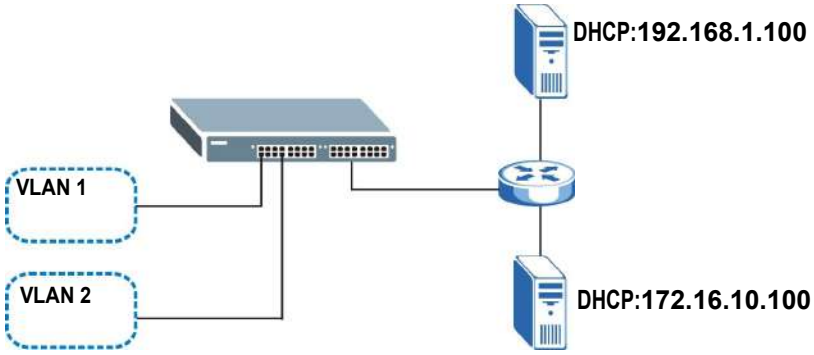
Таблица 140 Экран IP Application > DHCP > DHCPv4 > VLAN > Port (продолжение)

ПОЛЕ	ОПИСАНИЕ
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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 на данную кнопку, чтобы сбросить значения из последней выбранной записи, или, если ничего не было выбрано, очистить перечисленные выше поля.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	В этом поле отображается порядковый номер каждой записи. Нажмите на этот номер, чтобы изменить настройки.
VID	Это поле показывает идентификатор сети VLAN, которой принадлежит данный порт (или порты).
Port	Это поле показывает порт (или порты), к которым коммутатор применяет данные настройки.
Profile Name	Это поле отображает профиль опции 82 DHCP, который коммутатор применяет к указанному порту (или портам) в данной сети VLAN.
Delete	Выберите записи, которые нужно удалить, в столбце **Delete** и нажмите кнопку **Delete**, чтобы удалить выбранные записи из таблицы.
Cancel	Нажмите на данную кнопку, чтобы снять выделение с переключателей **Delete**.

35.5.2 Пример: Ретрансляция DHCP для двух VLAN

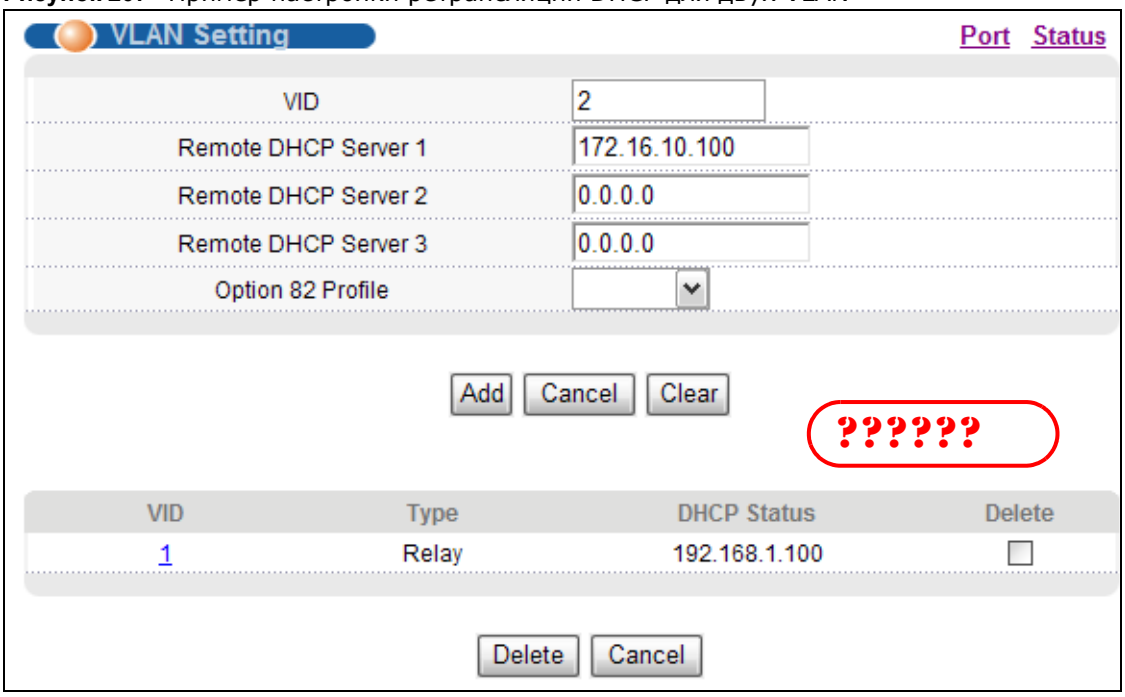
В следующем примере показана сеть группы зданий с двумя виртуальными локальными сетями VLAN (VID 1 и 2). Для обслуживания каждой из сетей VLAN установлено два сервера DHCP. В системе настроена ретрансляция запросов DHCP из комнат общежития (VLAN 1) на сервер DHCP с IP-адресом 192.168.1.100. Запросы из учебных зданий (VLAN 2) направляются на другой сервер DHCP с IP-адресом 172.16.10.100.

Рисунок 206 Ретрансляция DHCP для двух VLAN



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

Рисунок 207 Пример настройки ретрансляции DHCP для двух VLAN



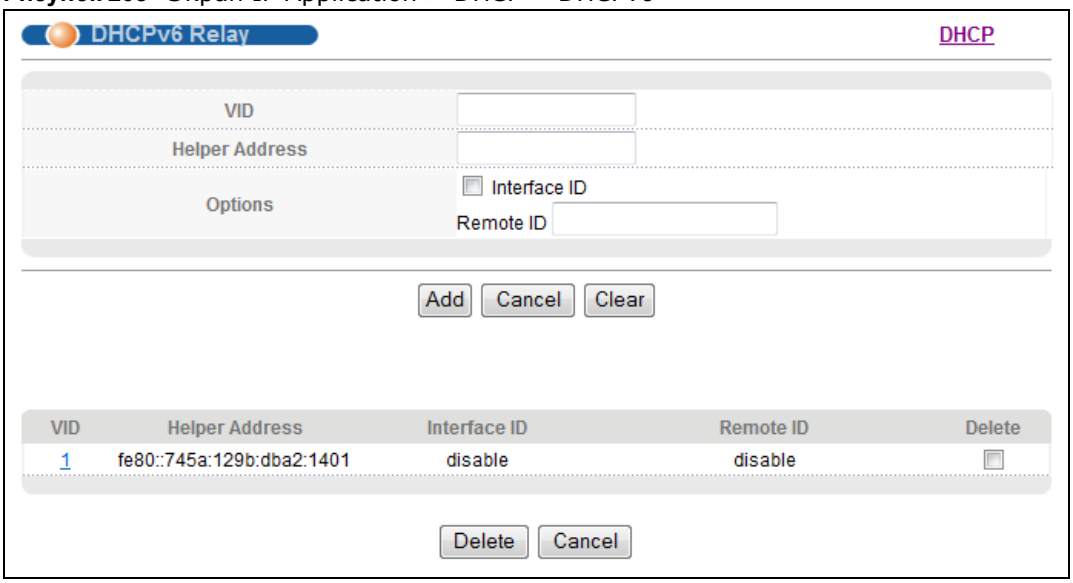
35.6 Ретранслятор DHCPv6

Агент ретрансляции DHCPv6 находится в одной сети с клиентами DHCPv6 и помогает пересылать сообщения между сервером DHCPv6 и клиентами DHCPv6. Если клиент не может использовать собственный адрес link-local и хорошо известный адрес многоадресной рассылки для поиска сервера DHCPv6 в своей сети, то ему нужен агент ретрансляции DHCPv6 для отправки сообщения серверу DHCPv6, находящемуся в другой сети.

Агент ретрансляции DHCPv6 может добавлять опцию удаленной идентификации (remote-ID) и опцию идентификации интерфейса (interface-ID) в сообщения Relay-Forward протокола DHCPv6. Опция remote-ID содержит строку, заданную пользователем, например, имя системы. Опция interface-ID передает серверу DHCPv6 сведения о номере слота, информация о портах и идентификатор VLAN. Опция remote-ID (если она есть) удаляется из сообщений Relay-Reply до момента отправки пакетов агентом ретрансляции клиентам. Сервер DHCPv6 копирует опцию interface-ID из сообщения Relay-Forward в сообщение Relay-Reply и отправляет его агенту ретрансляции. Значение interface-ID не должно меняться даже после перезапуска агента ретрансляции.

С помощью этого экрана можно настроить параметры ретрансляции DHCPv6 для определенной сети VLAN на коммутаторе. Выберите в панели навигации **IP Application > DHCP > DHCPv6**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 208 Экран IP Application > DHCP > DHCPv6



Поля экрана описаны в следующей таблице.

Таблица 141 Экран IP Application > DHCP > DHCPv6

ПОЛЕ	ОПИСАНИЕ
VID	Укажите идентификатор сети VLAN, параметры которой требуется настроить.
Helper Address	Укажите адрес удаленного сервера DHCPv6 для указанной сети VLAN.
Options	
Interface ID	При выборе этой опции коммутатор будет добавлять опцию interface-ID в запросы DHCPv6, приходящие от клиентов в указанной сети VLAN, прежде чем переслать их на сервер DHCPv6.
Remote ID	Введите строку, содержащую не более 64 печатных символов, которая будет использоваться в качестве remote-ID. Данный коммутатор добавляет опцию remote-ID в запросы DHCPv6, приходящие от клиентов в указанной сети VLAN, прежде чем переслать их на сервер DHCPv6.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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 вернуться к сохраненным значениям полей.
Clear	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
VID	Это поле отображает идентификатор сети VLAN (VLAN ID). Щелкните по идентификатору сети VLAN, чтобы изменить настройки.
Helper Address	Это поле отображает адрес IPv6 удаленного сервера DHCPv6 для данной сети VLAN.
Interface ID	Это поле указывает на то, добавляется ли опция interface-ID в запросы DHCPv6, приходящие от клиентов в данной сети VLAN.
Remote ID	Это поле указывает на то, добавляется ли опция remote-ID в запросы DHCPv6, приходящие от клиентов в данной сети VLAN.
Delete	В столбце **Delete** выберите записи, которые нужно удалить, затем нажмите кнопку **Delete**.
Cancel	Нажмите **Cancel**, чтобы снять выделение с переключателей в столбце **Delete**.

36

Настройка ARP

36.1 Обзор протокола 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.

36.1.1 О чем рассказывается в этой главе

С помощью экрана **ARP Learning** (разд. 36.2.1 на стр. 320) можно настроить режим запоминания ARP для каждого отдельного порта.

36.1.2 Что необходимо знать

Ознакомьтесь с информацией о протоколе ARP, которая поможет при работе с экранами, описанными в этой главе.

36.1.2.1 Как работает протокол ARP

Когда входящий пакет, предназначенный для хост-устройства в локальной сети, прибывает на коммутатор, коммутатор ищет его в таблице ARP, и, если адрес удается найти, отправляет пакет на указанное 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.

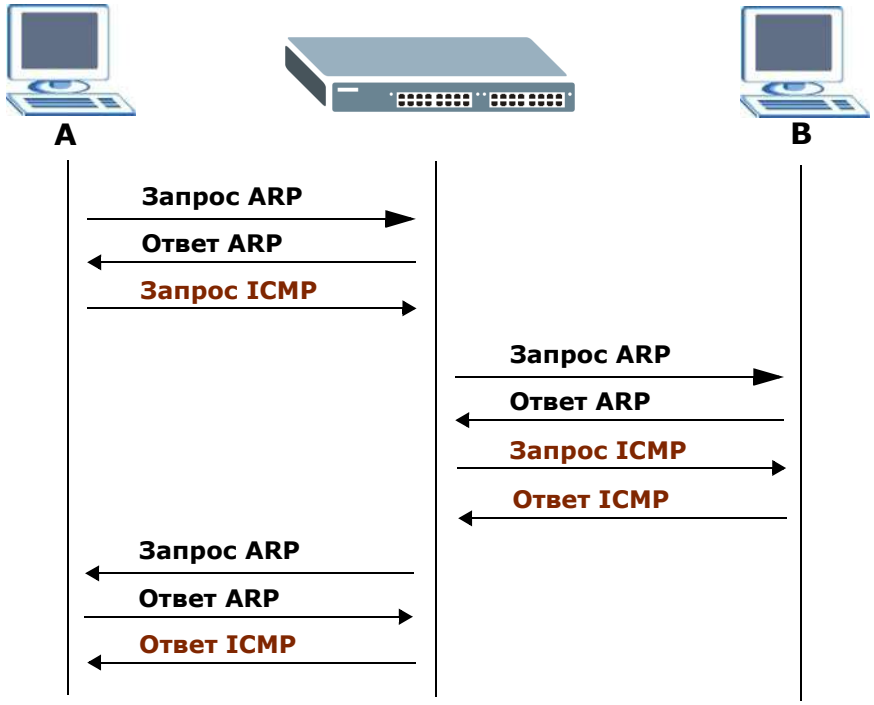
36.1.2.2 Режим запоминания ARP

коммутатор поддерживает три режима запоминания ARP: ARP-Reply, Gratuitous-ARP и ARP-Request.

ARP-Reply

По умолчанию коммутатор работает в режиме запоминания ARP-Reply и обновляет информацию в таблице ARP только при получении ответов ARP на запросы ARP, отправленные самим коммутатором. Это предотвращает возможность подмены информации ARP.

В приведенном ниже примере коммутатор не располагает информацией о соответствии IP-адреса и MAC-адреса для хостов **A** и **B** в таблице ARP, и хост **A** хочет отправить ping-запросы на хост **B**. Хост **A** отправляет запрос ARP на коммутатор, а затем, после получения ответа ARP от коммутатора, отправляет запрос ICMP. коммутатор не находит в таблице ARP записи для хоста **B** и направляет широковещательный запрос ARP всем устройствам в локальной сети. При получении ответа ARP от хоста **B** коммутатор обновляет информацию в таблице ARP и пересылает запрос ICMP хоста **A** хосту **B**. После получения ответа ICMP от хоста **B** коммутатор посылает запрос ARP для получения MAC-адреса хоста **A**, а после получения ответа ARP от хоста **A** вносит соответствующие изменения в таблицу ARP. После этого коммутатор может переслать запрос ICMP хоста **B** хосту **A**.



Gratuitous-ARP

Самообращенный (gratuitous) запрос ARP – это запрос, в котором и IP-адрес источника, и IP-адрес назначения равны IP-адресу устройства, которое посылает данный запрос, а MAC-адрес назначения равен широковещательному адресу. На самообращенный запрос ARP не бывает ответов.

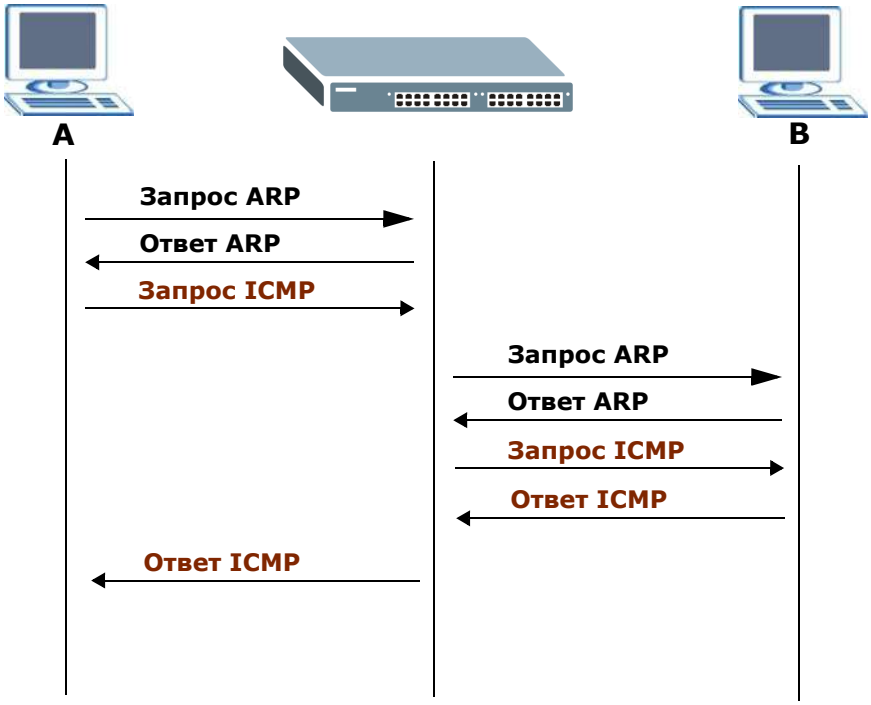
Устройство может отправлять самообращенные пакеты ARP для выявления IP-коллизий. При перезагрузке или смене MAC-адреса устройство также может послать самообращенный запрос ARP, чтобы сообщить другим устройствам в той же сети о необходимости внести в таблицу ARP информацию о новом соответствии.

В режиме запоминания Gratuitous-ARP коммутатор обновляет таблицу ARP либо в результате получения ответа ARP, либо в результате самообращенного запроса ARP.

ARP-Request

коммутатор, работающий в режиме запоминания ARP-Request, обновляет таблицу ARP в результате ответов ARP, самообращенных запросов ARP и обычных запросов ARP.

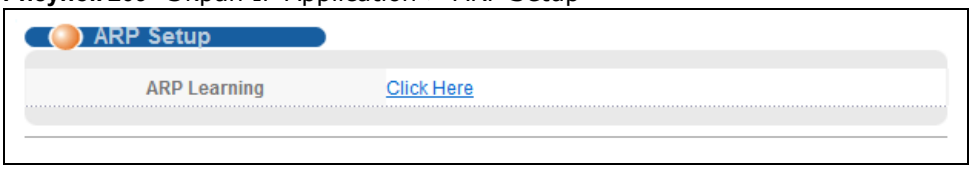
Соответственно, в примере, который показан ниже, коммутатор может выяснить MAC-адрес хоста **A** из запроса ARP, отправленного хостом **A**. Затем коммутатор пересылает ответ ICMP хоста **B** хосту **A** – сразу после получения MAC-адреса хоста **B** и ответа ICMP от него.



36.2 Настройка протокола ARP

Выберите в навигационной панели **IP Application** > **ARP Setup**, чтобы открыть экран, изображенный на рисунке ниже. Перейдите по ссылке рядом с надписью **ARP Learning**, чтобы открыть экран, на котором можно указать режим запоминания ARP для каждого порта.

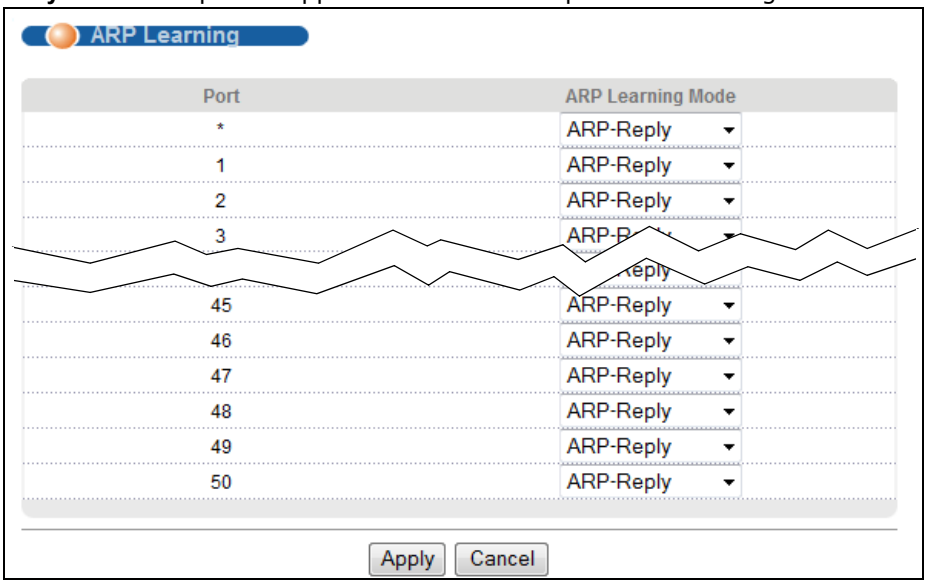
Рисунок 209 Экран IP Application > ARP Setup



36.2.1 Экран ARP Learning

С помощью этого экрана можно указать режим запоминания ARP для каждого порта. Перейдите по ссылке рядом с надписью **ARP Learning** на экране **IP Application** > **ARP Setup**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 210 Экран IP Application > ARP Setup > ARP Learning



Поля экрана описаны в следующей таблице.

Таблица 142 Экран IP Application > ARP Setup > ARP Learning

ПОЛЕ	ОПИСАНИЕ
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. Изменения в данной строке сразу же копируются на все порты.
ARP Learning Mode	Выберите режим запоминания ARP, который коммутатор будет использовать для данного порта. При выборе опции **ARP-Reply** коммутатор будет обновлять таблицу ARP только при получении ответов ARP на запросы ARP, отправленные самим коммутатором. При выборе опции **Gratuitous-ARP** коммутатор будет обновлять таблицу ARP либо в результате ответа ARP, либо в результате самообращенного запроса ARP. При выборе опции **ARP-Request** коммутатор будет обновлять таблицу ARP в результате ответов ARP, самообращенных запросов ARP и обычных запросов ARP.
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

Обслуживание

37.1 Обзор

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

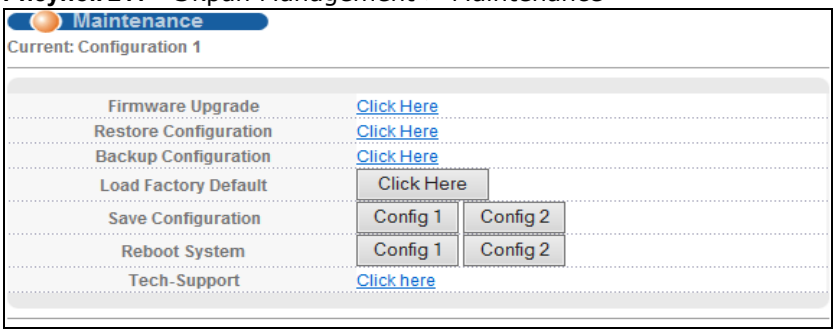
37.1.1 О чем рассказывается в этой главе

- С помощью экрана **Maintenance** (разд. 37.2 на стр. 322) можно загрузить свежую версию встроенного программного обеспечения.
- С помощью экрана **Firmware Upgrade** (разд. 37.3 на стр. 325) можно загрузить свежую версию встроенного программного обеспечения.
- С помощью экрана **Restore Configuration** (разд. 37.4 на стр. 326) можно загрузить сохраненный файл конфигурации устройства.
- С помощью экрана **Backup Configuration** (разд. 37.5 на стр. 327) можно сохранить конфигурацию для использования в дальнейшем.

37.2 Экран Maintenance

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

Рисунок 211 Экран Management > Maintenance



Поля экрана описаны в следующей таблице.

Таблица 143 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 программного 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.
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.
Tech-Support	Перейдите по ссылке **Click Here**, чтобы открыть экран Tech-Support. С помощью этого экрана можно установить пороговые значения утилизации процессора и оперативной памяти для журнальных отчетов и загрузить соответствующие журнальные отчеты для анализа проблем. Журнальные отчеты содержат информацию об истории и текущей утилизации процессорных ресурсов и памяти, а также о возникших сбоях.

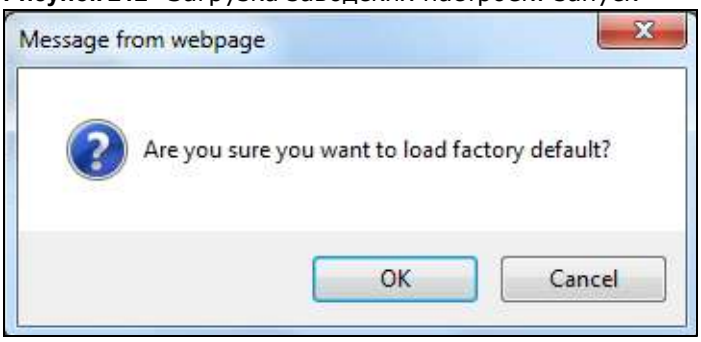
37.2.1 Загрузка заводских настроек по умолчанию

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 212 Загрузка заводских настроек: запуск



3 Нажмите кнопку **Save** в web-конфигураторе в верхней части экрана, чтобы изменения вступили в силу. 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).

37.2.2 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.

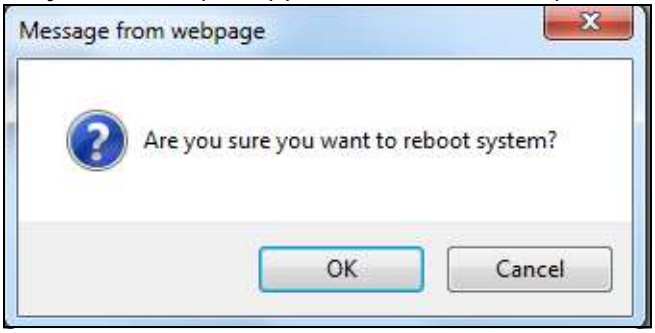
Примечание: Нажатие на кнопки **Apply** и **Add** НЕ сохраняет изменения в постоянной памяти. Все несохраненные изменения будут утеряны после перезагрузки коммутатора.

37.2.3 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 213 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.

37.3 Обновление встроенного программного обеспечения

С помощью следующего экрана можно загрузить на коммутатор свежую версию встроенного программного обеспечения.

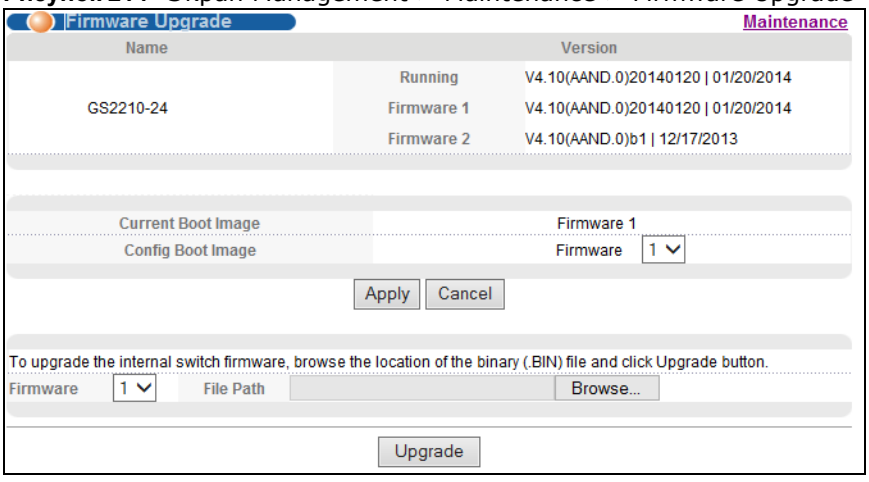
С помощью следующего экрана можно загрузить на коммутатор свежую версию встроенного программного обеспечения. Данный коммутатор поддерживает два образа встроенного программного обеспечения, **Firmware 1** и **Firmware 2**. С помощью этого экрана можно указать, какой образ нужно обновить при передаче встроенного программного обеспечения с использованием web-конфигуратора, и какой образ следует загрузить при запуске коммутатора.

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.

Чтобы открыть приведенный ниже экран, нажмите **Management** > **Maintenance** > **Firmware Upgrade**.

Рисунок 214 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.

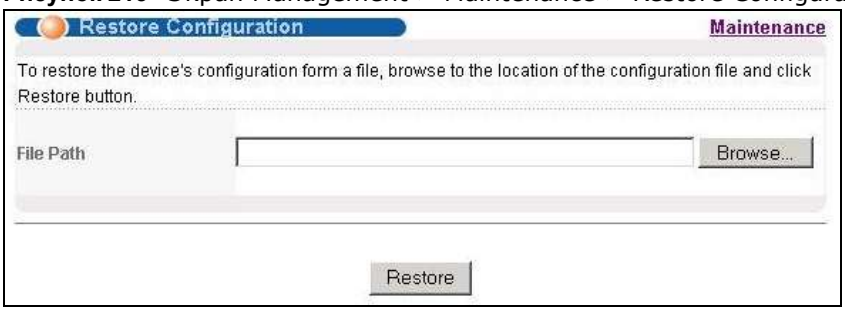
Таблица 144 Экран Management > Maintenance > Firmware Upgrade

ПОЛЕ	ОПИСАНИЕ
Name	Это поле показывает название настраиваемого коммутатора.
Version	коммутатор имеет два набора встроенного программного обеспечения, **Firmware 1** и **Firmware 2**, которые загружены во флэш-память. • Поле **Running** показывает номер версии (и код модели) и дату создания (в формате ММ/ДД/ГГГГ) встроенного программного обеспечения, которое коммутатор использует в настоящий момент (**Firmware 1** или **Firmware 2)**. Информация о встроенном программном обеспечении также отображается на экране System Information, доступном из меню Basic Settings. • Поле **Firmware 1** показывает номер версии, код модели и дату создания в формате ММ/ДД/ГГГГ первого образа программного обеспечения. • Поле **Firmware 2** показывает номер версии, код модели и дату создания в формате ММ/ДД/ГГГГ второго образа программного обеспечения.
Current Boot Image	Это поле указывает на то, какое встроенное программное обеспечение коммутатор использует в настоящий момент (**Firmware 1** или **Firmware 2)**.
Config Boot Image	Выберите, какое встроенное программное обеспечение (**Firmware 1** или **Firmware 2)** необходимо загружать, нажмите Apply и перезагрузите коммутатор, чтобы изменения вступили в силу. Изменения также появятся в поле Current boot image, расположенном выше.
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.
Firmware	Выберите целевой образ для загрузки нового встроенного программного обеспечения (Firmware) **1** или (Firmware) **2**.
File Path	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.
Upgrade	Нажмите **Upgrade**, чтобы загрузить новое встроенное программное обеспечение. Встроенное программное обеспечение вступает в силу только после перезагрузки. Чтобы выполнить перезагрузку, выберите в меню **Management > Maintenance > Reboot System** и перейдите по ссылке **Config 1** или **Config 2** (**Config 1** и **Config 2** – это файлы конфигурации, которые коммутатор должен использовать при перезагрузке).

37.4 Восстановление файла конфигурации

С помощью этого экрана можно восстановить ранее сохраненную конфигурацию с компьютера на коммутаторе, используя экран **Restore Configuration**.

Рисунок 215 Экран Management > Maintenance > Restore Configuration



Введите имя и путь к файлу конфигурации, который необходимо восстановить, в текстовое поле **File Path**, или нажмите **Browse**, чтобы 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.

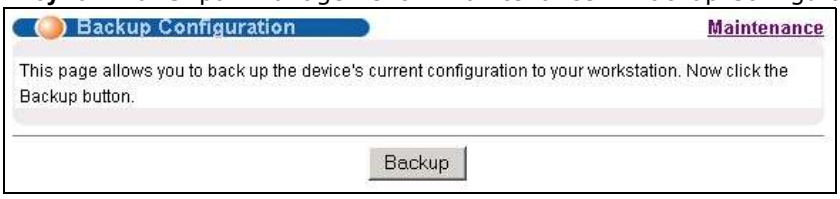
37.5 Резервное копирование файла конфигурации

С помощью этого экрана можно сохранить текущие настройки устройства.

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 216 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.

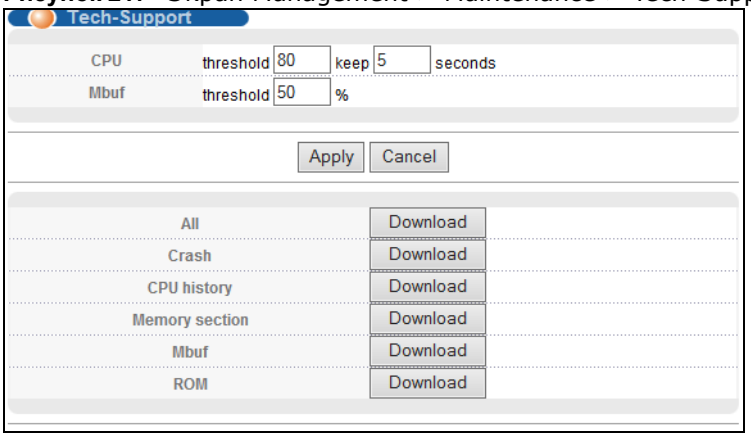
37.6 Функция Tech-Support

Функция Tech-Support – это инструмент расширенного ведения журналов, который позволяет сохранять в журнале такую полезную информацию, как история утилизации процессора,

сведения об использовании оперативной памяти и буфера Mbuf (Memory Buffer) и информацию о сбоях для анализа проблем службой технической поддержки при возникновении неполадок с коммутатором. Меню Tech Support упрощает доступ к соответствующим отчетам; доступ к этой функции также возможен через интерфейс командной строки при помощи команды «Show tech-support».

Перейдите по ссылке **Menu** > **Management** > **Maintenance** > **Tech-Support**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 217 Экран Management > Maintenance > Tech-Support



Для просмотра журнала в корректном формате может потребоваться WordPad или аналогичное приложение. Поля экрана, изображенного на рисунке выше, описаны в следующей таблице.

Таблица 145 Экран Management > Maintenance > Tech-Support

CPU	Выберите число из диапазона от 50 до 100 и введите его в поле CPU threshold, затем введите число из диапазона от 5 до 60 в поле Seconds, после чего нажмите **Apply**. Например, значение 80 в поле CPU threshold и значение 5 в поле Seconds будут означать, что в журнале появится сообщение в том случае, если уровень утилизации процессора превысит 80% и пробудет в таком состоянии в течение не менее 5 секунд. Журнальный отчет хранит данные из журнала об использовании процессора в течение 7 дней и загружен в энергозависимую память (ОЗУ). Эти данные будут потеряны при отключении питания коммутатора, будь-то штатное отключение или результат перебоев с электричеством. По истечении 7 дней происходит ротация журнала, и новые записи заменяют наиболее старые. Чем выше значение в поле CPU threshold, тем меньше сообщений будет создаваться в журнале, и тем меньше данных будет у службы технической поддержки для анализа, и наоборот.
Mbuf	Выберите число из диапазона от 50 до 100 и введите его в поле Mbuf (Memory Buffer) threshold. Журнальный отчет Mbuf хранится во флэш-памяти (то есть в постоянной памяти). Например, значение 50 в поле Mbuf threshold будет означать, что сообщение появится в журнале, если уровень утилизации буфера памяти превысит 50%. Чем выше значение в поле Mbuf threshold, тем меньше сообщений будет создаваться в журнале, и тем меньше данных будет у службы технической поддержки для анализа, и наоборот.

Таблица 145 Экран Management > Maintenance > Tech-Support

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.
All	Перейдите по ссылке **Download**, чтобы просмотреть все журнальные отчеты и ознакомиться со статусом системы. Данный журнальный отчет хранится во флэш-памяти. Если журнальный отчет **All** окажется слишком большим, то журнальные отчеты можно загрузить по отдельности ниже.
Crash	Перейдите по ссылке **Download**, чтобы просмотреть журнальный отчет о сбоях в системе. Данный журнал включает в себя информацию о последнем сбое и хранится во флэш-памяти.
CPU history	Перейдите по ссылке **Download**, чтобы просмотреть журнальный отчет с историей использования процессора. Этот журнал с информацией за последние 7 дней хранится в ОЗУ. Сохраните его, если он нужен, в противном случае он может потеряться при выключении коммутатора или перебоях с электроснабжением.
Memory Section	Перейдите по ссылке **Download**, чтобы просмотреть журнальный отчет о разделах памяти. Данный журнальный отчет хранится во флэш-памяти.
Mbuf	Перейдите по ссылке **Download**, чтобы просмотреть журнальный отчет об использовании буфера памяти. Данный журнал содержит информацию о случаях превышения установленного порогового значения для буфера памяти (Mbuf). Данный журнальный отчет хранится во флэш-памяти.
ROM	Перейдите по ссылке **Download**, чтобы просмотреть журнальный отчет об использовании ПЗУ (Read Only Memory, ROM). Этот отчет хранится во флэш-памяти.

37.7 Справочная техническая информация

Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

37.7.1 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.

37.7.2 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 146 Соглашения об именовании файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Configuration File	config	*.cfg	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.
Firmware	ras	*.bin	Общее имя для встроенного программного обеспечения ZyNOS на коммутаторе.

37.7.2.1 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.

37.7.3 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. Используйте команду `put` для передачи файлов с компьютера на коммутатор, например, команда `put firmware.bin ras` загружает встроенное программное обеспечение, хранящееся на компьютере (firmware.bin), на коммутатор и переименовывает его в «ras». Аналогичным образом, команда `put config.cfg config` загружает файл конфигурации с компьютера

(config.cfg) на коммутатор и переименовывает его в «config». Наконец, команда `get config config.cfg` передает файл конфигурации, хранящийся на коммутаторе, на компьютер и переименовывает его в «config.cfg». Дополнительную информацию о соглашениях в отношении именования файлов можно найти в табл. 146 на стр. 330.

7 Чтобы покинуть строку ftp-команд, введите `quit`.

37.7.4 FTP-клиенты с графическим пользовательским интерфейсом

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

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).

37.7.5 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 FTP-сессию.

38

Контроль доступа

38.1 Обзор контроля доступа

В данной главе описан контроль доступа к коммутатору.

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 147 Обзор контроля доступа

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

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

38.1.1 О чем рассказывается в этой главе

- Экран **Access Control** (разд. 38.2 на стр. 332) представляет собой главный экран для настройки управления доступом.
- С помощью экрана **SNMP** (разд. 38.3 на стр. 333) можно настроить параметры SNMP.
- С помощью экрана **Trap Group** (разд. 38.3.1 на стр. 334) можно выбрать типы ловушек SNMP, которые необходимо отправлять каждому из менеджеров SNMP.
- С помощью экрана **User Information** (разд. 38.3.3 на стр. 337) можно создавать пользователей SNMP для аутентификации с менеджерами с использованием SNMP v3 и ассоциировать их с группами SNMP.
- С помощью экранов **Logins** (разд. 38.4 на стр. 338) можно указать пользователей, которым разрешен доступ к коммутатору через web-конфигуратор в любой момент времени.
- С помощью экрана **Service Access Control** (разд. 38.5 на стр. 340) можно выбрать службы, с помощью которых разрешается обращаться к коммутатору.
- С помощью экрана **Remote Management** (разд. 38.6 на стр. 341) можно указать группу, включающую в себя один или несколько «доверенных компьютеров», с которых администратор может управлять коммутатором посредством определенной службы.

38.2 Главный экран контроля доступа

Перейдите на главный экран.

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

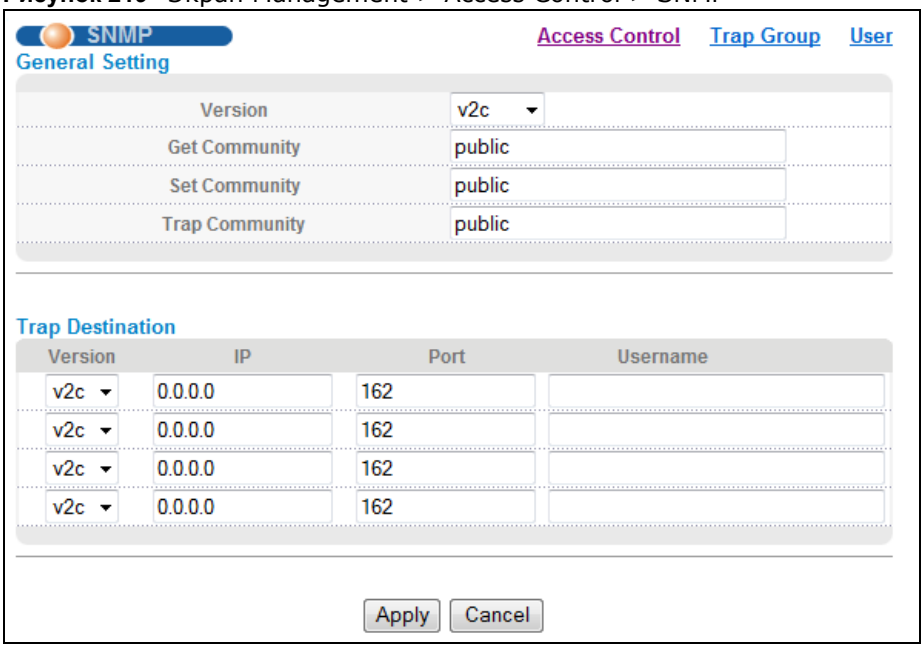
Рисунок 218 Экран Management > Access Control

38.3 Настройка SNMP

Настройка SNMP осуществляется на этом экране.

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

Рисунок 219 Экран Management > Access Control > SNMP



Поля экрана описаны в следующей таблице.

Таблица 148 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**). SNMP версии 2c обратно совместим с SNMP версии 1.

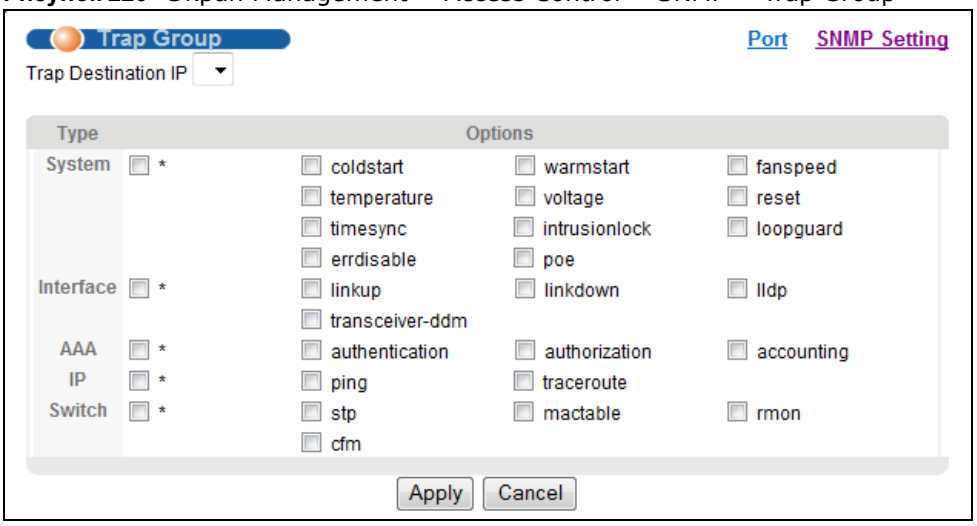
Таблица 148 Экран Management > Access Control > SNMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
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 ловушка SNMP коммутатором.
Version	Укажите версию SNMP для отправки сообщений Trap.
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. Данное имя пользователя должно соответствовать существующей учетной записи на коммутаторе (настраивается на экране **Management** > **Access Control** > **Logins**).
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.

38.3.1 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 220 Экран Management > Access Control > SNMP > Trap Group



Поля экрана описаны в следующей таблице.

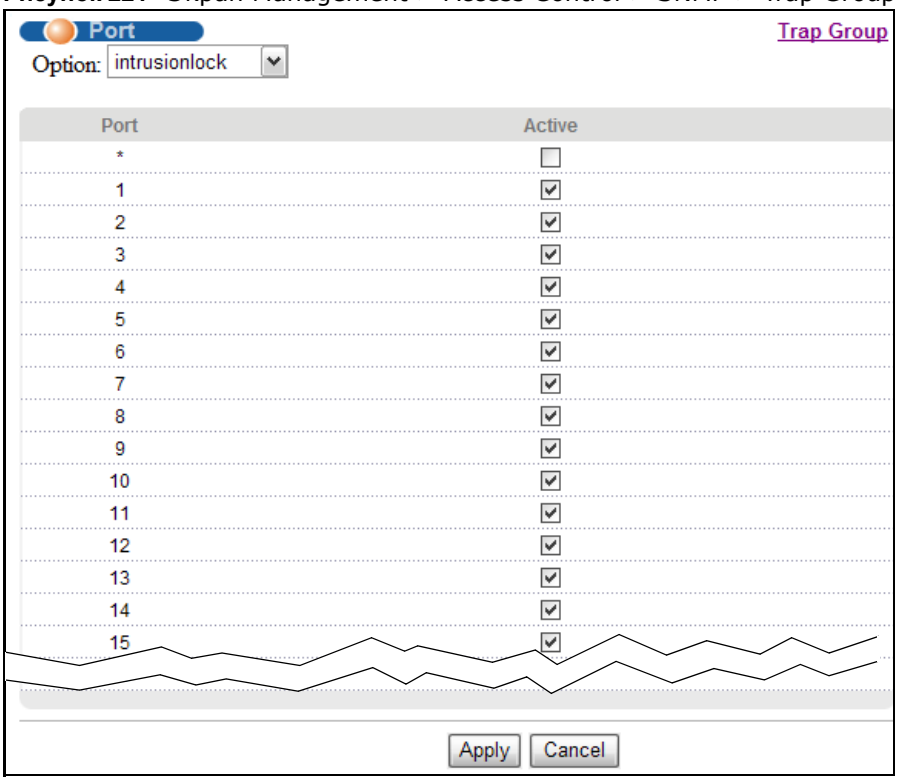
Таблица 149 Экран Management > Access Control > SNMP > Trap Group

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 «Команды Trap протокола SNMP» на стр. 344. 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).
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.

38.3.2 Включение/отключение отправки ловушек SNMP на определенном порту

На экране **SNMP > Trap Group** перейдите по ссылке **Port**, чтобы открыть экран, изображенный на рисунке ниже. С помощью этого экрана можно указать, следует ли отправлять ловушку, полученную через указанный порт (или порты), указанному менеджеру SNMP.

Рисунок 221 Экран Management > Access Control > SNMP > Trap Group > Port



Поля экрана описаны в следующей таблице.

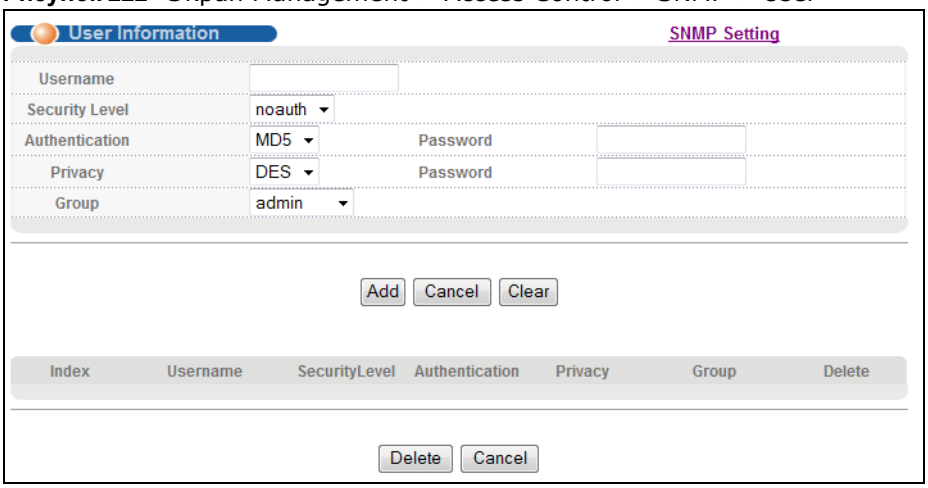
Таблица 150 Экран Management > Access Control > SNMP > Trap Group > Port

ПОЛЕ	ОПИСАНИЕ
Option	Выберите тип ловушки, который требуется настроить.
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. Изменения в данной строке сразу же копируются на все порты.
Active	Установите этот переключатель, чтобы включить данный тип ловушки для ловушек SNMP на данном порту. Снимите выделение с этого переключателя, чтобы отключить отправку ловушек SNMP на этом порту.
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.

38.3.3 Настройка пользователей SNMP

На экране **SNMP** перейдите по ссылке **User**, чтобы открыть экран, изображенный на рисунке ниже. С помощью экрана **User** можно создать пользователей для аутентификации с менеджерами с использованием SNMP v3 и ассоциировать их с группами SNMP. Пользователь SNMP является менеджером SNMP.

Рисунок 222 Экран Management > Access Control > SNMP > User



Поля экрана описаны в следующей таблице.

Таблица 151 Экран Management > Access Control > SNMP > User

ПОЛЕ	ОПИСАНИЕ
User Information	Примечание: Для создания учетных записей на менеджере SNMP v3 используйте имена пользователей и пароли, указанные на этом экране.
Username	Укажите 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 хеширования **MD5** (Message Digest 5) и **SHA** (Secure Hash Algorithm). Аутентификация SHA считается более стойкой по сравнению с MD5, но более медленной.
Password	Введите пароль для аутентификации пользователя SNMP (не более 32 ASCII-символов).

Таблица 151 Экран Management > Access Control > SNMP > User (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.
Password	Введите пароль для шифрования пакетов SNMP (не более 32 ASCII-символов).
Group	SNMP v3 использует концепцию групп в рамках модели управления доступом на основе видов (View-based Access Control Model, VACM). Менеджеры SNMP в пределах одной группы имеют одинаковые права доступа к базам MIB. Укажите, в какую группу SNMP следует включить данного пользователя. **admin** – Участники этой группы могут выполнять любые виды системных настроек, включая управление учетными записями администраторов. **readwrite** – Участники этой группы имеют права на чтение и запись, то есть пользователи из этой группы могут создавать и изменять базы MIB на коммутаторе, за исключением учетных записей пользователей и конфигурации AAA. **readonly** – Участники этой группы имеют права только на чтение, то есть пользователи из этой группы могут собирать информацию с коммутатора.
Add	Нажмите эту кнопку, чтобы создать новую или изменить существующую запись. Это действие позволяет сохранить изменения настроек 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	Нажмите **Clear**, чтобы вернуться к заводским настройкам.
Index	Порядковый номер (только для чтения) учетной записи на коммутаторе. Щелкните на порядковом номере, чтобы отобразить более подробную информацию и изменить параметры существующей учетной записи.
Username	В этом поле отображается имя пользователя для учетной записи на коммутаторе.
Security Level	Это поле указывает на то, необходимо ли использовать аутентификацию и/или шифрование в сессиях SNMP с данным пользователем.
Authentication	Это поле показывает алгоритм аутентификации, используемый в сессиях SNMP с данным пользователем.
Privacy	Это поле показывает метод шифрования, используемый в сессиях SNMP с данным пользователем.
Group	Это поле отображает группу SNMP, в которую входит данный пользователь.
Delete	Нажмите **Delete**, чтобы удалить выбранную запись из итоговой таблицы.
Cancel	Нажмите **Cancel**, чтобы начать настройку на этом экране заново.

38.4 Настройка учетных записей пользователей

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

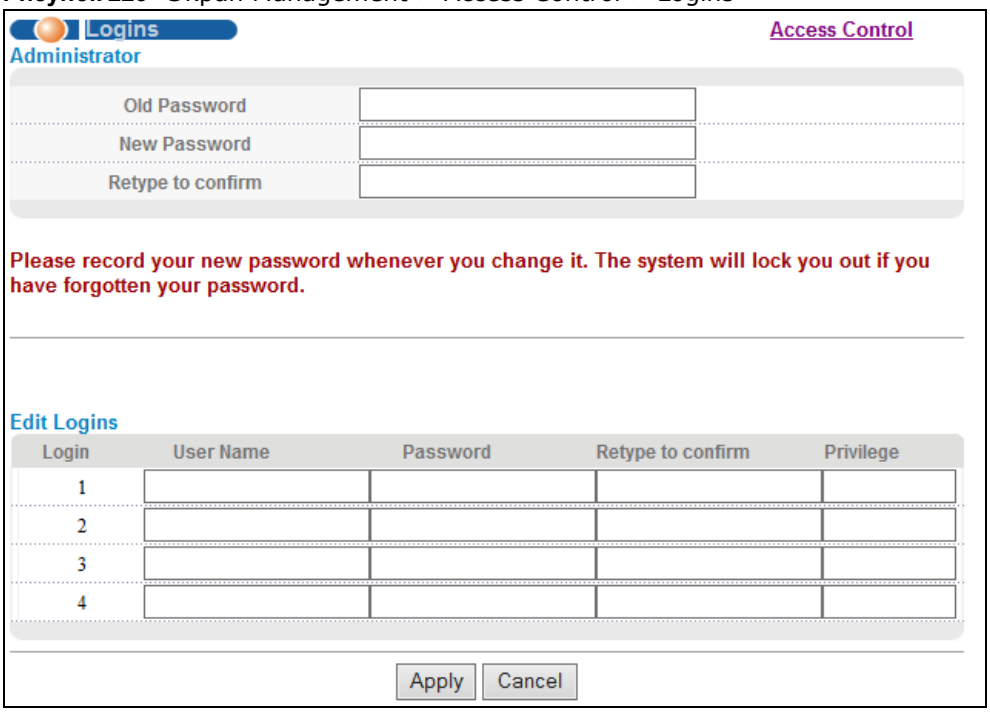
- Администратор – это пользователь, который может как просматривать, так и вносить изменения в настройки коммутатора. Имя пользователя для администратора не может быть изменено – это всегда **admin**. Пароль по умолчанию – **1234**.

Примечание: 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 223 Экран Management > Access Control > Logins



Поля экрана описаны в следующей таблице.

Таблица 152 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 о назначении уровней привилегий можно найти в Справочном руководстве по интерфейсу командной строки.	

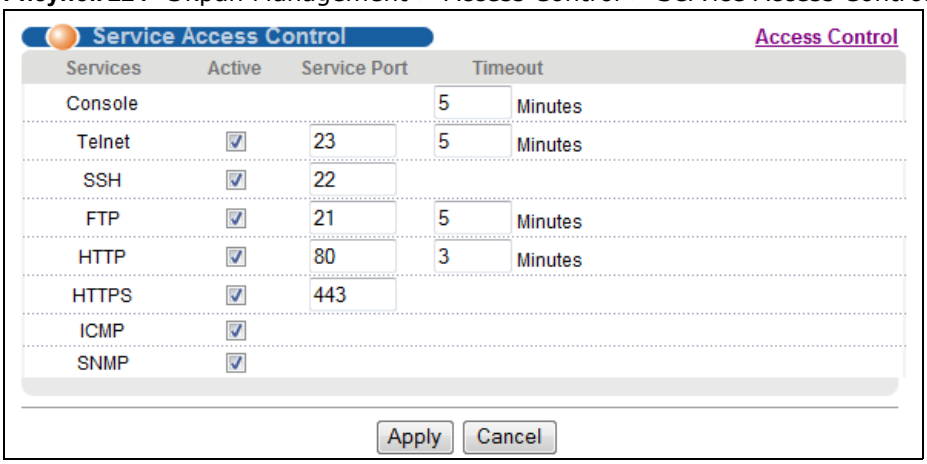
Таблица 152 Экран Management > Access Control > Logins (продолжение)

ПОЛЕ	ОПИСАНИЕ
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.
Privilege	Укажите уровень привилегий для данного пользователя. На момент написания этого документа пользователи могли иметь уровень привилегий 0, 3, 13 или 14. Каждое из этих чисел соответствует определенному набору прав доступа, описание которых приведено ниже. • 0 – Получение основных сведений о системе. • 3 – Получение сведений о конфигурации и статусе. • 13 – Настройка различных функций, за исключением учетных записей для входа на устройство, учетных записей SNMP, настроек последовательности методов аутентификации и авторизации, настройки нескольких учетных записей для входа на устройство, учетных записей администратора, активации паролей и отображения сведений о конфигурации. • 14 – Права на создание учетных записей для входа на устройство, учетных записей SNMP, настройку последовательности методов аутентификации и авторизации, настройку нескольких учетных записей для входа на устройство, настройку учетных записей администратора, активацию паролей и отображение сведений о конфигурации. Пользователи могут использовать интерфейс командной строки, если уровень привилегий данной сессии больше или равен уровню привилегий данной команды. Уровень привилегий сессии изначально определяется по уровню привилегий учетной записи. Например, если данный пользователь имеет уровень привилегий 5, то он может запускать команды, которые требуют уровня привилегий не выше 5.
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.

38.5 Контроль доступа к службам

Контроль доступа к службам позволяет определить, каким службам разрешен доступ к коммутатору. Также имеется возможность изменить номер порта по умолчанию для службы 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 224 Экран Management > Access Control > Service Access Control



Поля экрана описаны в следующей таблице.

Таблица 153 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 **Service 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 (от 1 до 255 минут), 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.

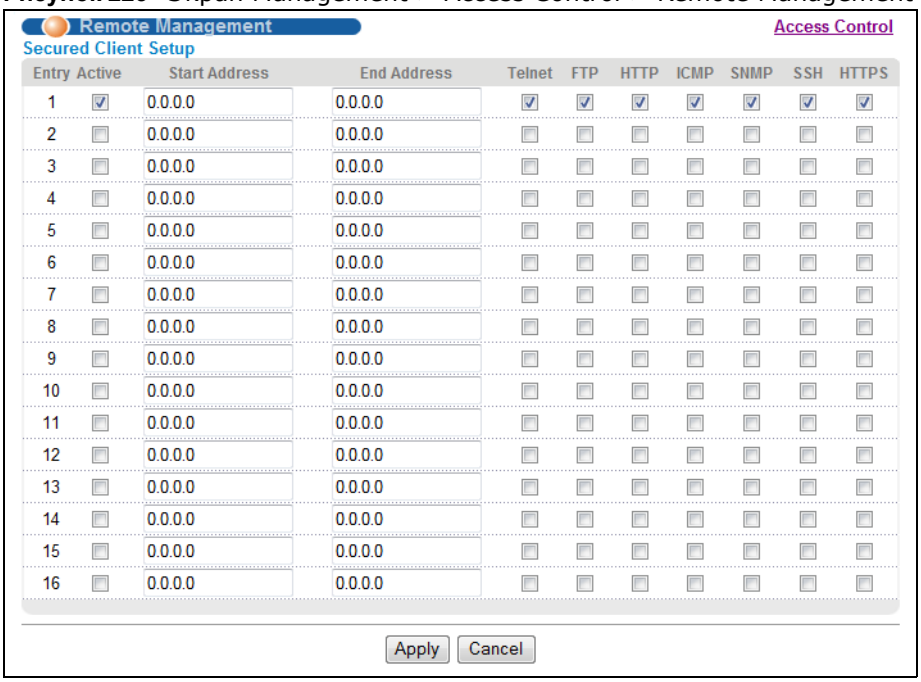
38.6 Удаленное управление

С помощью этого экрана можно определить группу из одного или нескольких «доверенных компьютеров», с которых администратор может управлять коммутатором через определенные службы.

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

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 225 Экран Management > Access Control > Remote Management



Поля экрана описаны в следующей таблице.

Таблица 154 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.

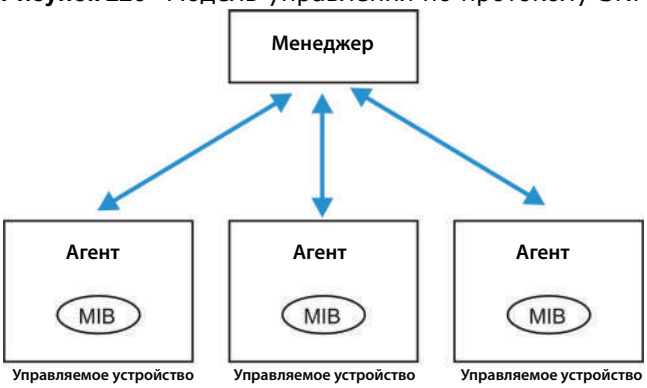
38.7 Справочная техническая информация

Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

38.7.1 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 коммутатором и осуществлять мониторинг его работы 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 226 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 155 Команды протокола SNMP

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

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.

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

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

Таблица 156 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	zyHwMonitorFanSpeedOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.1	Эта команда Trap отправляется при понижении или повышении скорости вентилятора так, что она выходит из нормального рабочего диапазона.
	zyHwMonitorFANSpeedOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.26.2.6	Эта команда Trap отправляется при возвращении скорости вентилятора в нормальный рабочий диапазон.
poe (Только для моделей с поддержкой PoE)	zyPoePowerPortOverload	1.3.6.1.4.1.890.1.15.3.59.4.1	Эта команда Trap отправляется при отключении подачи питания через порт в связи с перегрузкой.
	zyPoePowerPortShortCircuit	1.3.6.1.4.1.890.1.15.3.59.4.2	Эта команда Trap отправляется при отключении подачи питания через порт в связи с коротким замыканием.
	zyPoePowerPortOverSystemBudget	1.3.6.1.4.1.890.1.15.3.59.4.3	Эта команда Trap отправляется при отключении подачи питания через порт в связи с тем, что запрошенная мощность превысит совокупный бюджет мощности для PoE коммутатора.
	zyPoePowerPortOverloadRecovered	1.3.6.1.4.1.890.1.15.3.59.4.5	Эта команда Trap отправляется при включении подачи питания через порт в связи с прекращением перегрузки.
	zyPoePowerPortShortCircuitRecovered	1.3.6.1.4.1.890.1.15.3.59.4.6	Эта команда Trap отправляется при включении подачи питания через порт в связи с прекращением короткого замыкания.
	zyPoePowerPortOverSystemBudgetRecovered	1.3.6.1.4.1.890.1.15.3.59.4.7	Эта команда Trap отправляется при включении подачи питания через порт в связи с прекращением превышения бюджета мощности системы.
temperature	zyHwMonitorTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.2	Эта команда Trap отправляется при понижении или повышении температуры так, что она выходит из нормального рабочего диапазона.
	zyHwMonitorTemperatureOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.26.2.7	Эта команда Trap отправляется при возвращении температуры в нормальный рабочий диапазон.
voltage	zyHwMonitorPowerSupplyVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.3	Эта команда Trap отправляется при понижении или повышении напряжения так, что оно выходит из нормального рабочего диапазона.
	zyHwMonitorPowerSupplyVoltageOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.26.2.8	Эта команда Trap отправляется при возвращении напряжения питания в нормальный рабочий диапазон.

Таблица 156 Системные команды Trap протокола SNMP (System) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
reset	zySysMgmtUncontrolledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.1	Эта команда Trap отправляется при автоматическом сбросе коммутатора.
	zySysMgmtControlledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.2	Эта команда Trap отправляется при сбросе коммутатора администратором через интерфейс управления.
	zySysMgmtBootImageInconsistence	1.3.6.1.4.1.890.1.15.3.49.2.3	Эта команда Trap отправляется в том случае, если номер образа, загружаемого при запуске коммутатора, отличается от указанного через интерфейс командной строки.
	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	zyDateTimeTrapTimeServerNotReachable	1.3.6.1.4.1.890.1.15.3.82.3.1	Эта команда Trap отправляется в том случае, если дата и время не были установлены на коммутаторе вручную и указанный сервер времени оказался недоступен.
	zyDateTimeTrapTimeServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.82.3.2	Эта команда Trap отправляется при синхронизации часов реального времени на коммутаторе.
intrusionlock	zyPortIntrusionLock	1.3.6.1.4.1.890.1.15.3.61.3.2	Эта команда Trap отправляется при блокировке порта для защиты от вторжения.
loopguard	zyLoopGuardLoopDetect	1.3.6.1.4.1.890.1.15.3.45.2.1	Эта команда Trap отправляется при блокировке порта функцией защиты от образования петель.
errdisable	zyErrdisableDetect	1.3.6.1.4.1.890.1.15.3.24.4.1	Эта команда Trap отправляется при обнаружении ошибки на порту, такой как петля или превышение лимита скорости для определенных управляющих пакетов.
	zyErrdisableRecovery	1.3.6.1.4.1.890.1.15.3.24.4.2	Эта команда Trap отправляется после того, как коммутатор прекращает принимать меры, активированные на определенном порту, такие как отключение порта или отбрасывание пакетов на порту, по прошествии указанного интервала восстановления.

Таблица 157 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.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	Эта команда Trap отправляется при разрыве Ethernet-соединения.

Таблица 157 Интерфейсные команды Trap протокола SNMP (Interface) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
autonegotiation	zyPortAutonegotiationFailed	1.3.6.1.4.1.890.1.15.3.61.3.1	Эта команда Trap отправляется в случае, когда интерфейсу Ethernet не удается автоматически согласовать параметры соединения с другим интерфейсом Ethernet.
	zyPortAutonegotiationFailedRecovered	1.3.6.1.4.1.890.1.15.3.61.3.3	Эта команда Trap отправляется в случае, когда на интерфейсе Ethernet устраняется ситуация с невозможностью автоматически согласовать параметры соединения с другим интерфейсом Ethernet.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	Эта команда Trap отправляется при любых изменениях записей в удаленной базе данных. Протокол обнаружения канального уровня (Link Layer Discovery Protocol, LLDP), описанный в стандарте IEEE 802.1ab, позволяет устройствам локальной сети, поддерживающим LLDP, обмениваться информацией о настройках. Это помогает избавиться от проблем, вызванных несоответствием настроек.

Таблица 157 Интерфейсные команды Trap протокола SNMP (Interface) (продолжение)

ОПЦИЯ	МЕТКА ОБЪЕКТА	ИДЕНТИФИКАТОР ОБЪЕКТА	ОПИСАНИЕ
transceiver-ddm	zyTransceiverDdmiTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.1	Эта команда Trap отправляется при понижении или повышении температуры трансивера так, что она выходит из нормального рабочего диапазона.
	zyTransceiverDdmiTxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.2	Эта команда Trap отправляется при понижении или повышении оптической мощности передатчика так, что она выходит из нормального рабочего диапазона.
	zyTransceiverDdmiRxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.3	Эта команда Trap отправляется при понижении или повышении уровня оптической мощности на приемнике так, что она выходит из нормального рабочего диапазона.
	zyTransceiverDdmiVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.4	Эта команда Trap отправляется при понижении или повышении напряжения питания трансивера так, что оно выходит из нормального рабочего диапазона.
	zyTransceiverDdmiTxBiasOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.5	Эта команда Trap отправляется при понижении или повышении тока смещения лазера передатчика так, что он выходит из нормального рабочего диапазона.
	zyTransceiverDdmiTemperatureOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.6	Эта команда Trap отправляется при возвращении температуры трансивера в нормальный рабочий диапазон.
	zyTransceiverDdmiTxPowerOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.7	Эта команда Trap отправляется при возвращении оптической мощности передатчика в нормальный рабочий диапазон.
	zyTransceiverDdmiRxPowerOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.8	Эта команда Trap отправляется при возвращении оптической мощности на приемнике в нормальный рабочий диапазон.
	zyTransceiverDdmiVoltageOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.9	Эта команда Trap отправляется при возвращении напряжения питания трансивера в нормальный рабочий диапазон.
	zyTransceiverDdmiTxBiasOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.10	Эта команда Trap отправляется при возвращении тока смещения лазера передатчика в нормальный рабочий диапазон.

Таблица 158 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.
	zyAaaAuthenticationFailure	1.3.6.1.4.1.890.1.15.3.8.3.1	Эта команда Trap отправляется при невозможности аутентификации из-за неправильного имени пользователя и/или пароля.
	zyRadiusServerAuthenticationServerNotReachable	1.3.6.1.4.1.890.1.15.3.71.2.1	Эта команда Trap отправляется при отсутствии ответа от сервера аутентификации RADIUS.
	zyTacacsServerAuthenticationServerUnreachable	1.3.6.1.4.1.890.1.15.3.83.2.1	Эта команда Trap отправляется при отсутствии ответа от сервера аутентификации TACACS+.
	zyRadiusServerAuthenticationServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.71.2.3	Эта команда Trap отправляется при получении ответа от ранее недоступного сервера аутентификации RADIUS.
	zyTacacsServerAuthenticationServerUnreachableRecovered	1.3.6.1.4.1.890.1.15.3.83.2.3	Эта команда Trap отправляется при получении ответа от ранее недоступного сервера аутентификации TACACS+.
authorization	zyAaaAuthorizationFailure	1.3.6.1.4.1.890.1.15.3.8.3.2	Эта команда Trap отправляется при неудачной авторизации через подключение для управления.
accounting	zyRadiusServerAccountingServerNotReachable	1.3.6.1.4.1.890.1.15.3.71.2.2	Эта команда Trap отправляется при отсутствии ответа от сервера учета RADIUS.
	zyTacacsServerAccountingServerUnreachable	1.3.6.1.4.1.890.1.15.3.83.2.2	Эта команда Trap отправляется при отсутствии ответа от сервера учета TACACS+.
	zyRadiusServerAccountingServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.71.2.4	Эта команда Trap отправляется при получении ответа от ранее недоступного сервера учета RADIUS.
	zyTacacsServerAccountingServerUnreachableRecovered	1.3.6.1.4.1.890.1.15.3.83.2.4	Эта команда Trap отправляется при получении ответа от ранее недоступного сервера учета TACACS+.

Таблица 159 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.

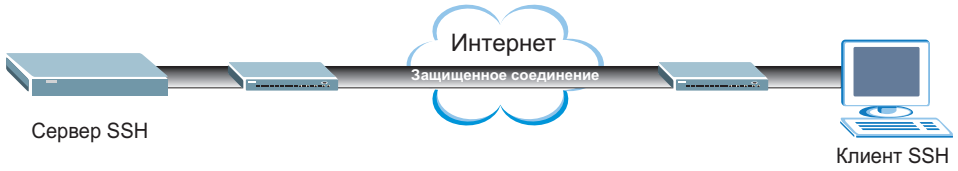
Таблица 160 Команды Trap протокола SNMP для коммутатора (Switch)

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.
	zyMrstpNewRoot	1.3.6.1.4.1.890.1.15.3.52.3.1	Эта команда Trap отправляется при изменении корневого коммутатора MRSTP.
	zyMstpNewRoot	1.3.6.1.4.1.890.1.15.3.53.3.1	Эта команда Trap отправляется при изменении топологии MSTP.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	Эта команда Trap отправляется при изменении топологии STP.
	zyMrstpTopologyChange	1.3.6.1.4.1.890.1.15.3.52.3.2	Эта команда Trap отправляется при изменении топологии MRSTP.
	zyMstpTopologyChange	1.3.6.1.4.1.890.1.15.3.53.3.2	Эта команда Trap отправляется при изменении топологии MSTP.
mactable	zyMacForwardingTableFull	1.3.6.1.4.1.890.1.15.3.48.2.1	Эта команда Trap отправляется при использовании более 99% таблицы MAC-адресов.
	zyMacForwardingTableFullRecovered	1.3.6.1.4.1.890.1.15.3.48.2.2	Эта команда Trap отправляется при возврате таблицы MAC-адресов из переполненного состояния в обычное.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	Эта команда Trap отправляется при выходе переменной за пределы верхнего порогового значения RMON.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	Эта команда Trap отправляется при выходе переменной за пределы нижнего порогового значения RMON.
cfm	dot1agCfmFaultAlarm	1.3.111.2.802.1.1.8.0.1	Эта команда Trap отправляется при обнаружении коммутатором сбоя соединения.

38.7.2 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 227 Пример связи по протоколу SSH



38.7.2.1 Как работает протокол SSH

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

Рисунок 228 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).

38.7.2.2 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.

38.7.2.3 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).

38.7.3 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.

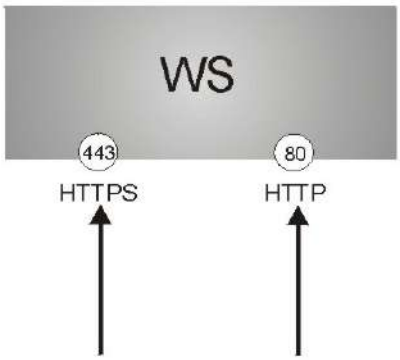
Протокол HTTPS на коммутаторе используется для получения защищенного доступа к коммутатору через Web-конфигуратор. Протокол SSL предусматривает, что SSL-сервер (коммутатор) должен всегда предоставлять свою аутентификационную информацию SSL-клиенту (компьютеру, который запрашивает HTTPS-соединение с коммутатором), 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 229 Реализация протокола HTTPS



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

38.7.3.1 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.

Предупреждения от Internet Explorer

Internet Explorer 6

При попытке получить доступ к устройству коммутатор через HTTPS-сервер появится диалоговое окно Windows с вопросом о доверии к сертификату сервера.

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.

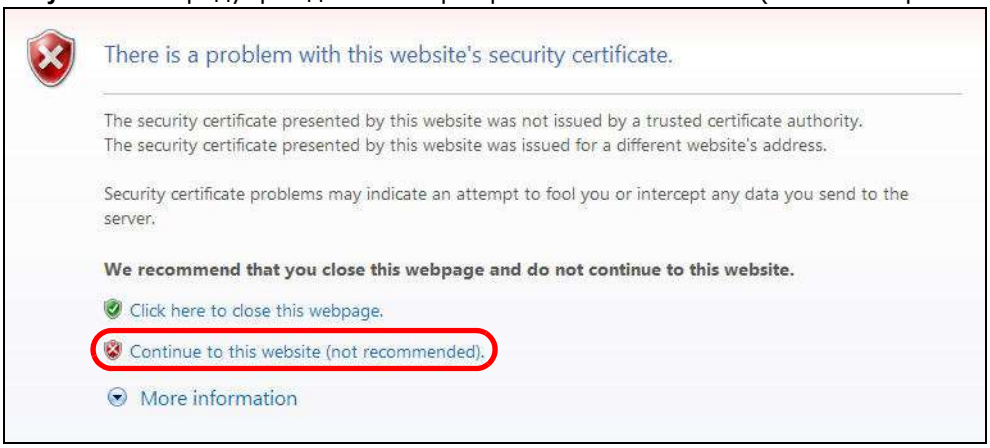
Рисунок 230 Диалоговое окно Security Alert (Internet Explorer 6)

Internet Explorer 7 и 8

При попытке обратиться к HTTPS-серверу коммутатора может появиться экран с сообщением «There is a problem with this website's security certificate.» («Имеется проблема с сертификатом безопасности данного веб-сайта»). При появлении такого сообщения перейдите по ссылке

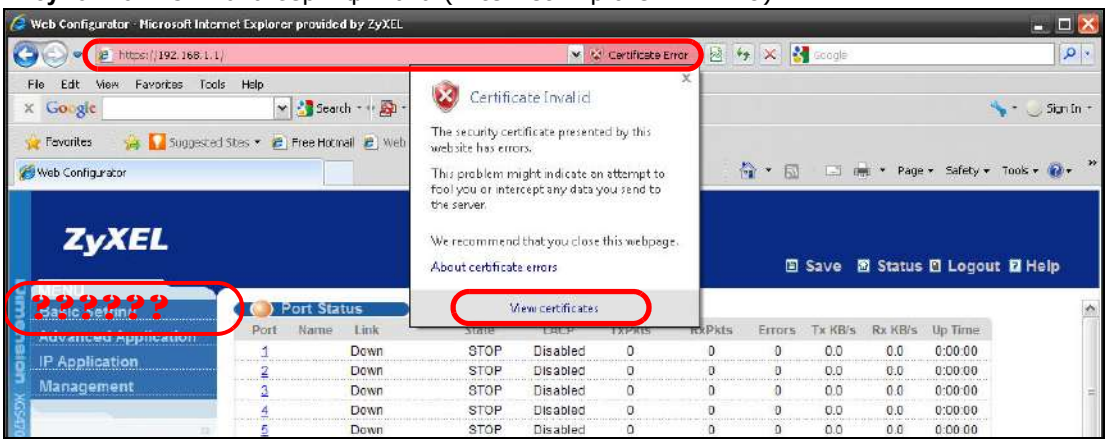
Continue to this website (not recommended) [Все равно открыть этот веб-сайт (не рекомендуется)], чтобы открыть страницу входа в Web-конфигуратор.

Рисунок 231 Предупреждение о сертификате безопасности (Internet Explorer 7 или 8)



После входа в web-конфигуратор появится красная строка адреса с сообщением **Certificate Error** (Ошибка сертификата). Щелкните по сообщению **Certificate Error** рядом со строкой адреса и нажмите кнопку **View certificates**.

Рисунок 232 Ошибка сертификата (Internet Explorer 7 или 8)



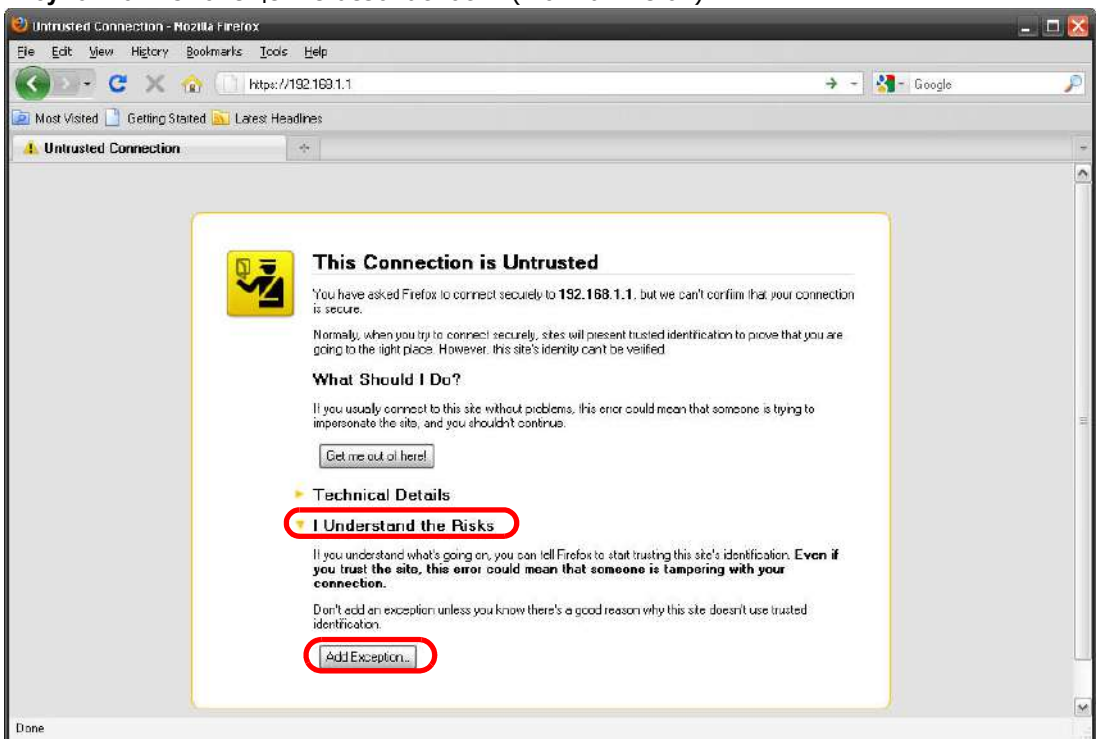
Нажмите кнопку **Install Certificate...** и установите этот сертификат в браузере, следуя инструкциям на экране.

Рисунок 233 Сертификат (Internet Explorer 7 или 8)

Предупредительные сообщения в Mozilla Firefox

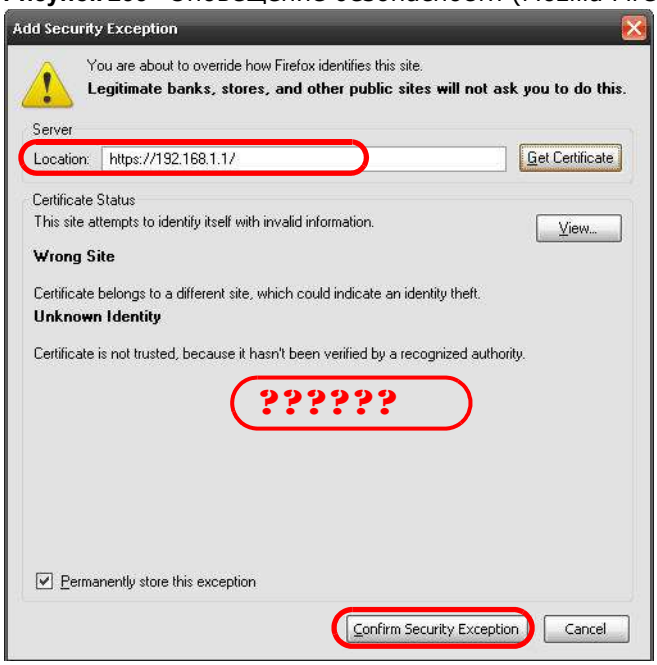
При попытке обратиться к HTTPS-серверу коммутатора может появиться экран с сообщением **This Connection is Unstructed**. Если это произошло, нажмите кнопку **I Understand the Risks**, а затем кнопку **Add Exception...**.

Рисунок 234 Оповещение безопасности (Mozilla Firefox)



Проверьте правильность адреса HTTPS-сервера. Нажмите кнопку **Confirm Security Exception**, чтобы перейти на страницу входа в Web-конфигуратор.

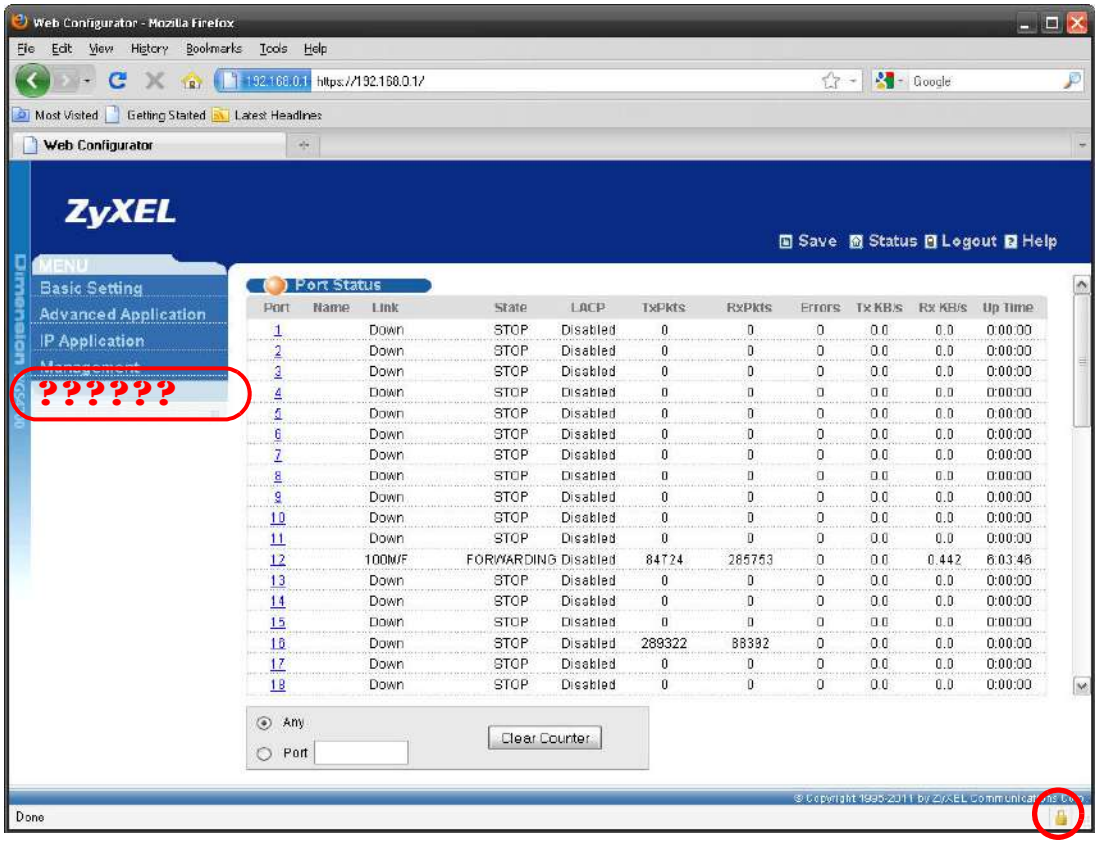
Рисунок 235 Оповещение безопасности (Mozilla Firefox)



38.7.3.2 Основной экран

После того, как был принят сертификат и введены имя пользователя и пароль, появится основной экран коммутатора. Значок замка, который появляется справа снизу в строке состояния браузера (в Internet Explorer 6 или Mozilla Firefox) или рядом с адресной строкой (в Internet Explorer 7 или 8) указывает на защищенное соединение.

Рисунок 236 Пример: значок замка для защищенного соединения



39

Диагностика

39.1 Обзор

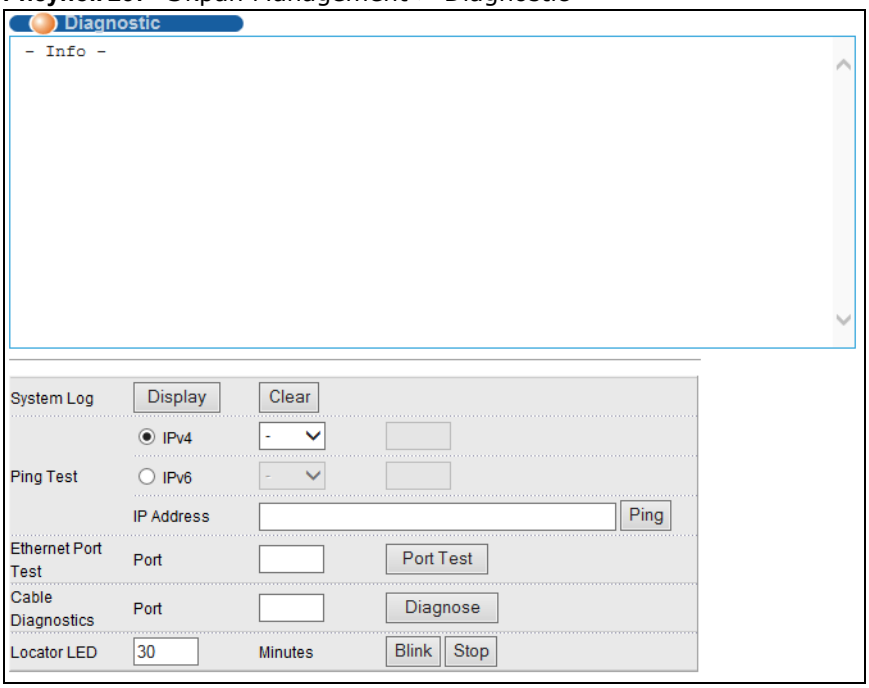
В данной главе описан экран диагностики **Diagnostic**.

С помощью экрана **Diagnostic** (разд. 39.2 на стр. 358) можно просмотреть системные журналы, проверить IP-адреса при помощи эхо-пакетов и протестировать порты.

39.2 Экран Diagnostic

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

Рисунок 237 Экран Management > Diagnostic



Поля экрана описаны в следующей таблице.

Таблица 161 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.
Ping Test	
IPv4	Выберите эту опцию, чтобы отправить эхо-запрос на адрес IPv4 и укажите, какой поток трафика (внутриполосный **in-band** или внеполосный **out-of-band**) должен использовать коммутатор для отправки кадров ping. При выборе опции **in-band** коммутатор будет посылать указанные кадры на все порты, за исключением порта управления (отмеченный надписью **MGMT**). При выборе опции **out-of-band** коммутатор будет посылать указанные кадры на порт управления (отмеченный надписью **MGMT**).
IPv6	Выберите эту опцию, если необходимо отправить эхо-запрос на адрес IPv6. Кроме того, потребуется выбрать тип интерфейса IPv6 и указать идентификатор интерфейса, через который коммутатор будет отправлять кадры ping.
IP Address	Введите IP-адрес устройства, на которое необходимо направлять эхо-запросы для проверки соединения. Нажмите **Ping**, чтобы коммутатор направил эхо-запрос на IP-адрес (введенный в поле слева).
Ethernet Port Test	Введите номер порта и нажмите **Port Test** для выполнения теста внутренней обратной петли.
Cable Diagnostics	Введите номер порта и нажмите кнопку **Diagnose**, чтобы выполнить физическую проверку проводной пары соединений Ethernet на указанном порту (или портах). В процессе диагностики порта на экране появятся следующие поля.
Port	Это поле показывает номер физического порта Ethernet на коммутаторе.
Channel	Кабель Ethernet обычно состоит из четырех проводных пар. Порты 10BASE-T или 100BASE-TX используют и позволяют протестировать только две пары, тогда как порту 1000BASE-T для работы необходимы все четыре пары. Это поле отображает имя-описание данной проводной пары в кабеле.
Pair status	**Ok**: Физическое соединение между проводной парой в нормальном состоянии. **Open**: Отсутствует физическое соединение (обнаружен разрыв цепи) между проводной парой. **Short**: Обнаружено короткое замыкание между проводной парой. **Unknown**: Данному коммутатору не удалось выполнить диагностику кабеля, подключенного к данному порту. **Unsupported**: Это порт является оптическим или не активен.
Cable length	Это поле показывает длину кабеля Ethernet, подключенного к данному порту, если значение поля **Pair status** равно **Ok** и чипсет коммутатора поддерживает данную функцию. Это поле отображает значение **N/A**, если значение поля **Pair status** равно **Open** или **Short**. Проверьте значение в поле **Distance to fault**. Это поле отображает значение **Unsupported**, если чипсет коммутатора не поддерживает отображение длины кабеля.

Таблица 161 Экран Management > Diagnostic (продолжение)

ПОЛЕ	ОПИСАНИЕ
Distance to fault	Это поле показывает расстояние от порта до точки, где обнаружен разрыв кабеля или короткое замыкание. Это поле отображает значение **N/A**, если значение поля **Pair status** равно **Ok**. Это поле отображает значение **Unsupported**, если чипсет коммутатора не поддерживает отображение длины кабеля.
Locator LED	Укажите интервал времени (в минутах) и нажмите кнопку **Blink**, чтобы показать реальное местоположение коммутатора между несколькими устройствами в стойке. Интервал времени по умолчанию равен 30 минутам. Нажмите кнопку **Stop**, чтобы прекратить мигание индикатора местоположения коммутатора.

40

Системный журнал Syslog

40.1 Обзор Syslog

В данной главе описаны экраны системного журнала 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 162 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	Warning: системой сгенерировано предупреждение.
5	Уведомление: нормальное, но важное состояние в системе.
6	Информация: информационное сообщение в журнале syslog.
7	Отладка: сообщение предназначено для отладки.

40.1.1 О чем рассказывается в этой главе

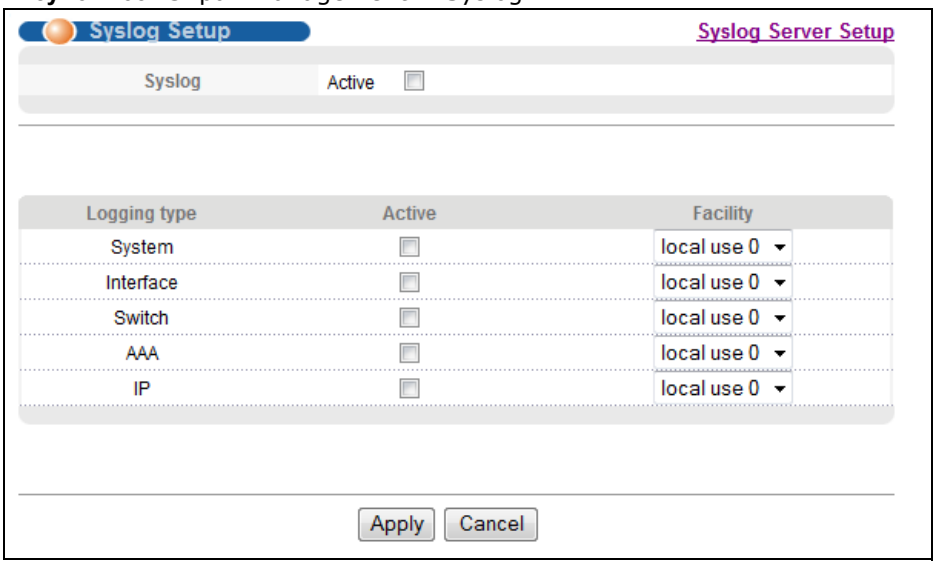
- С помощью экрана **Syslog Setup** (разд. 40.2 на стр. 361) можно настроить параметры системного журнала устройства.
- С помощью экрана **Syslog Server Setup** (разд. 40.3 на стр. 362) можно составить список внешних серверов syslog.

40.2 Настройка Syslog

На этом экране можно настроить параметры ведения системного журнала устройства.

Чтобы отобразить показанный ниже экран, выберите в навигационной панели **Management** > **Syslog**. Функция syslog позволяет передавать записи системных журналов на внешний сервер syslog.

Рисунок 238 Экран Management > Syslog



Поля экрана описаны в следующей таблице.

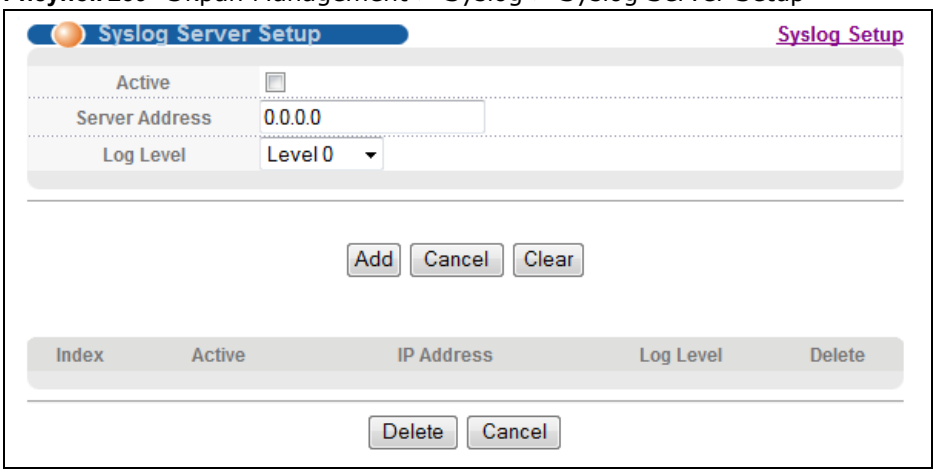
Таблица 163 Экран Management > Syslog

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.

40.3 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 239 Экран Management > Syslog > Syslog Server Setup



Поля экрана описаны в следующей таблице.

Таблица 164 Экран Management > Syslog > 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.

41

Управление кластерами

41.1 Обзор управления кластерами

В данной главе описано управление кластерами.

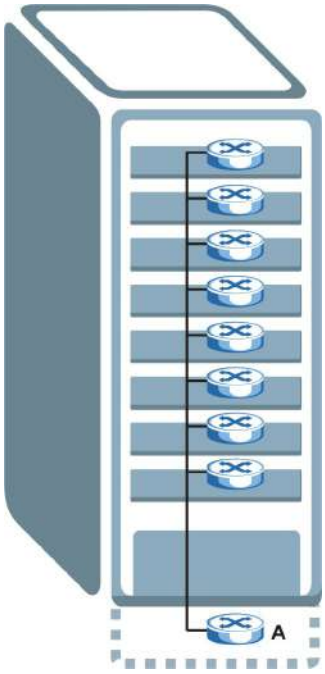
Функция управления кластером (Cluster Management) позволяет управлять несколькими коммутаторами с помощью одного коммутатора, который называется менеджером кластера. Чтобы коммутаторы могли взаимодействовать друг с другом, они должны быть подключены напрямую и принадлежать к одной группе VLAN.

Таблица 165 Спецификации управления кластерами ZyXEL

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

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

Рисунок 240 Пример реализации кластера



41.1.1 О чем рассказывается в этой главе

- С помощью экрана **Cluster Management** (разд. 41.2 на стр. 365) можно увидеть роль коммутатора в кластере и получить доступ к web-конфигуратору коммутаторов, являющихся членами кластера.
- С помощью экрана **Clustering Management Configuration** (разд. 41.1 на стр. 364) можно настроить параметры управления кластером.

41.2 Состояние управления кластером

С помощью этого экрана можно увидеть роль коммутатора в кластере и получить доступ к web-конфигуратору коммутаторов, являющихся членами кластера.

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

Примечание: У кластера может быть только один менеджер.

Рисунок 241 Экран Management > Cluster Management: Status

Поля экрана описаны в следующей таблице.

Таблица 166 Экран Management > Cluster Management: Status

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** представляет собой гиперссылку на web-конфигуратор коммутатора, являющегося членом кластера (см. рис. 243 на стр. 368).
MacAddr	В этом поле отображается аппаратный MAC-адрес коммутатора-члена кластера.
Name	Системное имя (**System Name**) члена кластера.

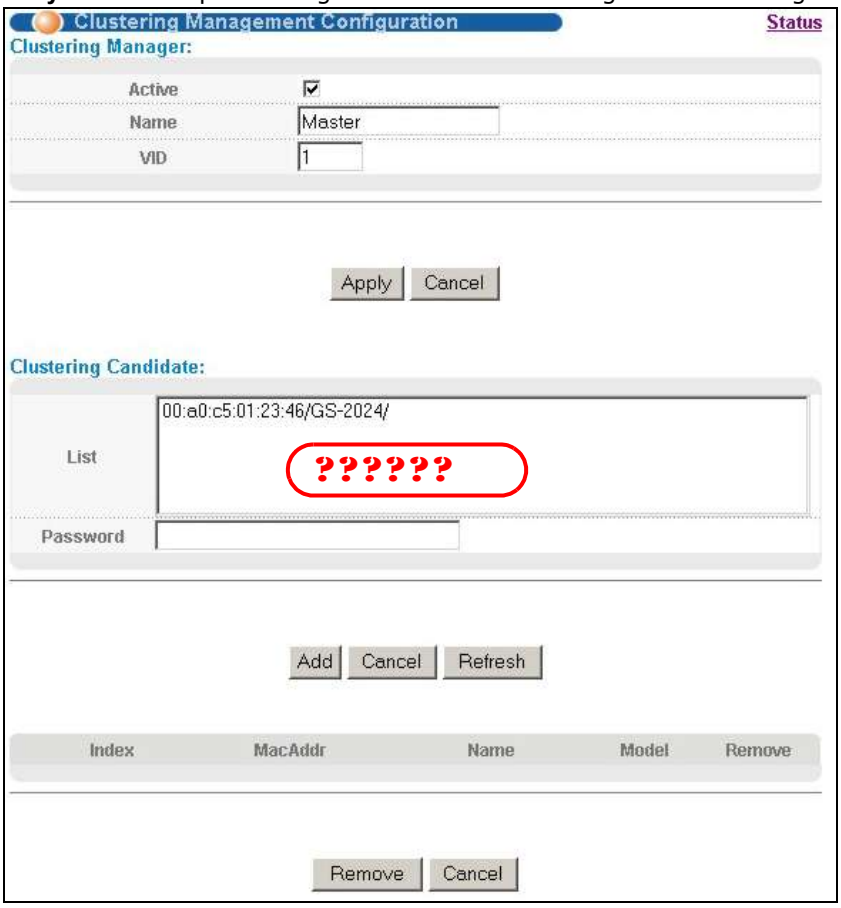
Таблица 166 Экран Management > Cluster Management: Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
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)

41.3 Настройка управления кластерами

Данный экран используется для настройки управления кластерами. Чтобы открыть приведенный ниже экран, нажмите **Management** > **Cluster Management** > **Configuration**.

Рисунок 242 Экран Management > Cluster Management > Configuration



Поля экрана описаны в следующей таблице.

Таблица 167 Экран Management > Cluster 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 (⚠).
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.	

Таблица 167 Экран Management > Cluster Management > Configuration (продолжение)

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

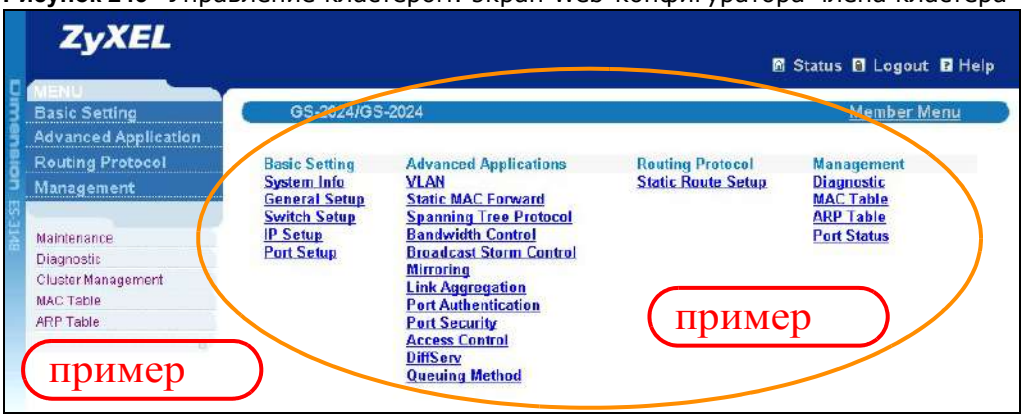
41.4 Справочная техническая информация

Это раздел содержит дополнительную техническую информацию по вопросам, обсуждаемым в текущей главе.

41.4.1 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 243 Управление кластером: экран Web-конфигуратора члена кластера



41.4.1.1 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 244 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 410AAHW0.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 168 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.
`410AAHW0.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.

42

Таблица MAC-адресов

42.1 Обзор таблицы MAC-адресов

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

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**).

42.1.1 О чем рассказывается в этой главе

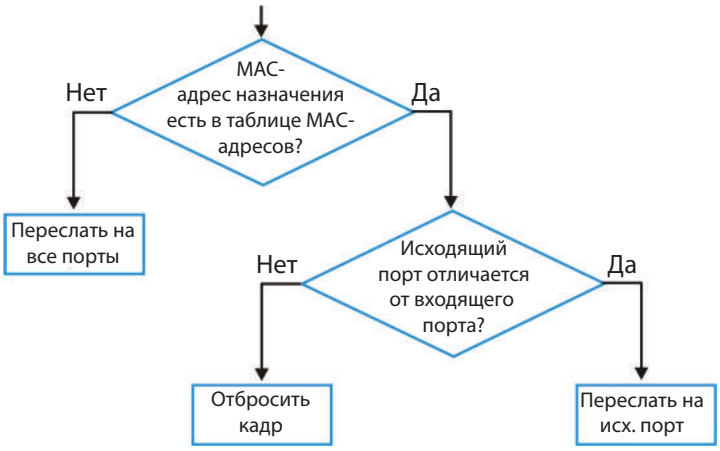
С помощью экрана **MAC Table** (разд. 42.2 на стр. 371) можно проверить, является ли определенный MAC-адрес динамическим или статическим.

42.1.2 Что необходимо знать

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 245 Схема работы таблицы MAC-адресов

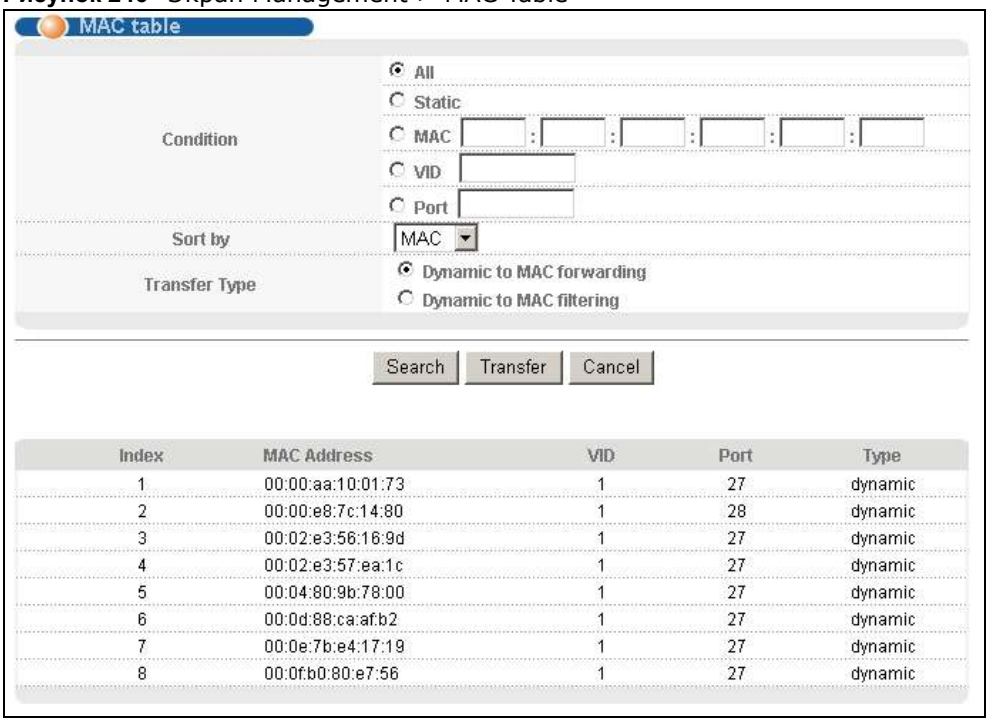


42.2 Просмотр таблицы MAC-адресов

С помощью этого экрана можно проверить, является ли данный MAC-адрес динамическим или статическим.

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

Рисунок 246 Экран Management > MAC Table



Поля экрана описаны в следующей таблице.

Таблица 169 Экран Management > MAC Table

ПОЛЕ	ОПИСАНИЕ
Condition	Установите один из радиопереключателей и нажмите кнопку **Search**, чтобы отобразить только те данные, которые соответствуют указанным критериям. Выберите опцию **All**, чтобы показать любую запись в таблице MAC-адресов коммутатора. Выберите опцию **Static**, чтобы показать записи MAC-адресов, созданные вручную на коммутаторе. Выберите опцию **MAC** и введите в соответствующем поле MAC-адрес, чтобы отобразить запись для указанного MAC-адреса. Выберите опцию **VID** и введите в соответствующем поле идентификатор сети VLAN, чтобы отобразить записи для MAC-адресов, принадлежащих указанной сети VLAN. Выберите опцию **Port** и введите в соответствующем поле номер порта, чтобы отобразить MAC-адреса, пересылаемые на указанный порт.
Sort by	Выберите, каким образом коммутатор должен отобразить и упорядочить данные в сводной таблице, приведенной ниже. Выберите опцию **MAC**, чтобы отобразить и упорядочить данные по MAC-адресу. Выберите опцию **VID**, чтобы отобразить и упорядочить данные по принадлежности к группе VLAN. Выберите опцию **PORT**, чтобы отобразить и упорядочить данные по номеру порта.
Transfer Type	Выберите опцию **Dynamic to MAC forwarding** и нажмите кнопку **Transfer**, чтобы сделать все динамически полученные записи MAC-адресов, присутствующие в сводной таблице ниже, статическими. Эти записи появятся на экране **Static MAC Forwarding**. Выберите опцию **Dynamic to MAC filtering** и нажмите кнопку **Transfer**, чтобы перенести все динамически полученные записи MAC-адресов, присутствующие в сводной таблице ниже, в записи фильтрации по MAC-адресам. Эти записи будут отображаться только на экране **Filtering**, и действием фильтрации по умолчанию для них будет **Discard source**.
Cancel	Нажмите **Cancel**, чтобы вернуться к сохраненным значениям полей.
Index	Порядковый номер входящего кадра.
MAC Address	MAC-адрес устройства, с которого прибыл входящий кадр.
VID	Группа VLAN, которой принадлежит данный кадр.
Port	Это поле отображает порт, на который пересылается 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**).

43

Таблица ARP

43.1 Обзор

В данной главе описана таблица протокола разрешения адресов (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.

43.1.1 О чем рассказывается в этой главе

С помощью экрана **ARP Table** (разд. 43.2 на стр. 373) можно ознакомиться с таблицей соответствия между IP-адресами и MAC-адресами.

43.1.2 Что необходимо знать

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.

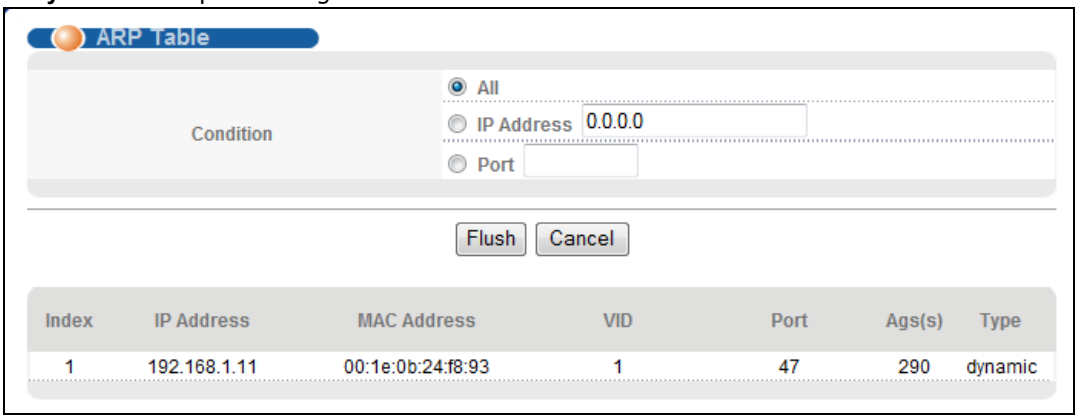
Если для IP-адреса не найдено записи, протокол ARP направляет широковещательный запрос всем устройствам в локальной сети. Данный коммутатор заполняет поля его собственных MAC-адреса и IP-адреса в адресе отправителя, а затем вносит известный IP-адрес получателя в соответствующем поле. Кроме того, коммутатор 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.

43.2 Просмотр таблицы ARP

С помощью таблицы ARP можно ознакомиться с соответствиями между IP-адресами и MAC-адресами и удалить конкретные динамические записи ARP.

Выберите в навигационной панели **Management > ARP Table**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 247 Экран Management > ARP Table



Поля экрана описаны в следующей таблице.

Таблица 170 Экран Management > ARP Table

ПОЛЕ	ОПИСАНИЕ
Condition	Выберите способ, с помощью которого коммутатор должен удалять записи ARP при нажатии кнопки **Flush**. Выберите опцию **All**, чтобы удалить все динамические записи из таблицы ARP. Выберите опцию **IP Address** и введите IP-адрес, чтобы удалить все динамические полученные записи, содержащие указанный IP-адрес. Выберите опцию **Port** и введите номер порта, чтобы удалить динамические записи, полученные через указанный порт.
Flush	Нажмите кнопку **Flush**, чтобы удалить записи ARP в соответствии с указанными условиями.
Cancel	Нажмите кнопку **Cancel**, чтобы вернуть значения в полях к заводским настройкам по умолчанию.
Index	Порядковый номер записи в таблице ARP.
IP Address	Это поле содержит IP-адрес устройства, подключенного к порту коммутатора с соответствующим MAC-адресом, указанным ниже.
MAC Address	MAC-адрес устройства с соответствующим ему IP-адресом.
VID	Это поле показывает идентификатор сети VLAN, которой принадлежит данное устройство.
Port	Это поле показывает порт, к которому подключается устройство. Значение **CPU** означает, что этот IP-адрес является IP-адресом управления коммутатора.
Age(s)	Это поле показывает, сколько времени (в секундах) запись может оставаться в таблице ARP, пока она не устареет и не потребует обновления. Значение **0** в этом поле соответствует статической записи.
Type	Это поле указывает на тип IP-адреса – динамический (получен коммутатором) или статический (создан вручную на экране **Basic Setting > IP Setup** или на экране **IP Application > ARP Setup > Static ARP**).

44

Таблица MTU путей

44.1 Обзор таблицы MTU путей

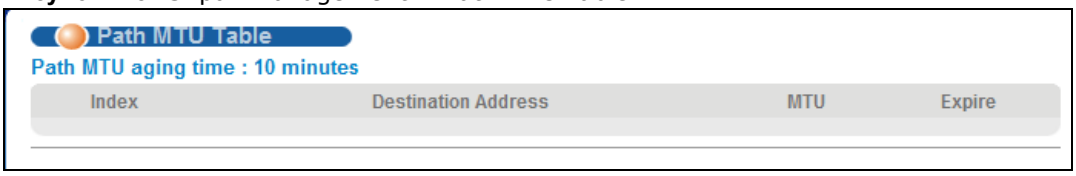
В этой главе описана таблица MTU путей IPv6.

Максимальный размер пакета (в байтах), который может быть передан по каналу данных, называется Maximum Transmission Unit (MTU). Данный коммутатор использует протокол Path MTU Discovery для обнаружения MTU путей, то есть минимального MTU из всех каналов на пути к узлу назначения. Если после отправки пакета коммутатор получает сообщение об ошибке ICMPv6 Packet Too Big, то он фрагментирует следующий пакет в соответствии со значением MTU, указанным в сообщении об ошибке.

44.2 Просмотр таблицы MTU путей

С помощью этого экрана можно просмотреть информацию об MTU путей IPv6 на коммутаторе. Выберите в навигационной панели **Management** > **Path MTU Table**, чтобы открыть экран, изображенный на экране ниже.

Рисунок 248 Экран Management > Path MTU Table



Поля экрана описаны в следующей таблице.

Таблица 171 Экран Management > Path MTU Table

ПОЛЕ	ОПИСАНИЕ
Path MTU aging time	Это поле показывает, сколько времени в секундах запись может оставаться в таблице MTU путей, пока она не устареет и не потребует обновления.
Index	Это поле отображает порядковый номер записи в таблице.
Destination Address	Это поле показывает адрес назначения IPv6 для каждого пути/каждой записи.
MTU	Это поле показывает значение MTU для каналов на пути.
Expire	Это поле показывает, сколько времени (в минутах) запись может оставаться в таблице MTU путей, пока она не устареет и не потребует обновления.

45

Настройка клонирования

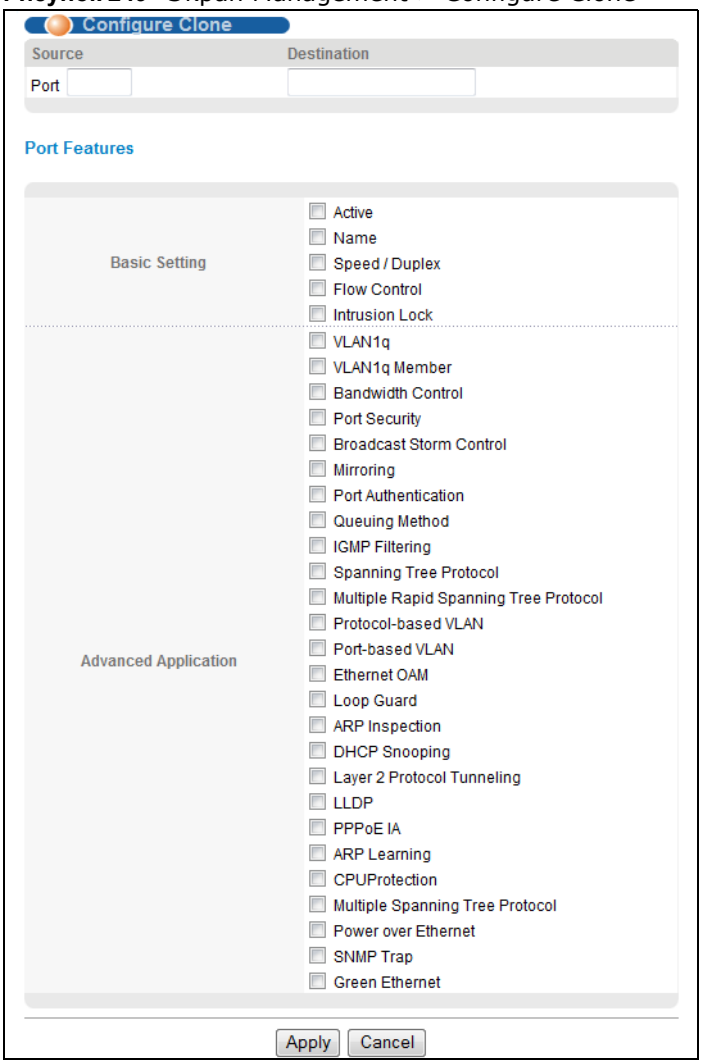
45.1 Обзор

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

45.2 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 249 Экран Management > Configure Clone



Поля экрана описаны в следующей таблице.

Таблица 172 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.

Таблица 172 Экран Management > Configure Clone (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.

46

Таблица соседних устройств

46.1 Обзор таблицы соседних устройств IPv6

В этой главе рассказывается о таблице соседних устройств IPv6.

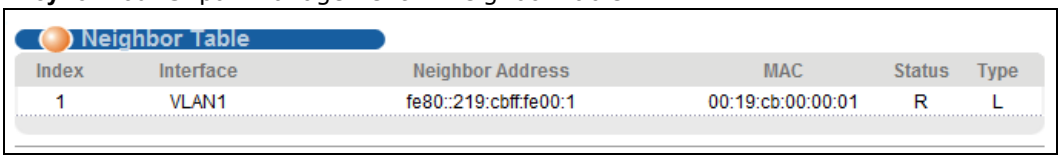
Каждый хост IPv6 должен иметь таблицу соседних устройств. При наличии адреса, который надо разрешить или верифицировать, коммутатор отправляет сообщение типа «Запрос доступных соседей». При получении сообщения типа «Ответ соседа» коммутатор сохраняет адрес канального уровня соседнего устройства в таблице соседних устройств. Кроме того, в таблице соседних устройств можно создать статическую запись о соседнем устройстве IPv6 вручную с помощью экрана **Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup**.

Если коммутатору необходимо отправить пакет, то он в первую очередь обращается к другой таблице, чтобы определить следующий переход. После определения адреса IPv6 следующего перехода коммутатор ищет в таблице соседних устройств соответствующий адрес канального уровня и отправляет пакет, когда соседнее устройство становится досягаемым. Если коммутатор не может найти нужной записи в таблице соседних устройств, или требуемое соседнее устройство недоступно, то коммутатор начинает процесс разрешения адреса. Это помогает уменьшить число IPv6-сообщений типа «Запрос...» и «Ответ...».

46.2 Просмотр таблицы соседних устройств IPv6

С помощью этого экрана можно просмотреть информацию о соседних устройствах IPv6 коммутатора. Выберите в навигационной панели **Management** > **Neighbor Table**, чтобы открыть экран, изображенный на рисунке ниже.

Рисунок 250 Экран Management > Neighbor Table



Поля экрана описаны в следующей таблице.

Таблица 173 Экран Management > Neighbor Table

ПОЛЕ	ОПИСАНИЕ
Index	Это поле отображает порядковый номер записи в таблице.
Interface	Это поле показывает идентификатор интерфейса IPv6, на котором создан данный адрес IPv6 или через который доступно соседнее устройство.
Neighbor Address	Это поле показывает адрес IPv6 коммутатора или соседнего устройства.

Таблица 173 Экран Management > Neighbor Table (продолжение)

ПОЛЕ	ОПИСАНИЕ
MAC	Это поле показывает MAC-адрес интерфейса IPv6, на котором создан данный адрес IPv6, или MAC-адрес соседнего устройства.
Status	Это поле показывает, является ли интерфейс IPv6 соседнего устройства досягаемым. Для протокола IPv6 понятие «досягаемый» означает, что пакет IPv6 можно корректно переслать на соседний узел (хост или маршрутизатор), а соседнее устройство может успешно получить и обработать пакет. Это поле может содержать следующие значения: • reachable (R): Интерфейс соседнего устройства является досягаемым (коммутатор получил ответ на начальный запрос). • stale (S): Последний интервал досягаемости истек, и коммутатор ожидает ответа на новый начальный запрос. Поле отображает это значение и в том случае, если коммутатор получает ответ от интерфейса соседнего устройства при отсутствии начального запроса. • delay (D): С соседним устройством недавно происходил обмен трафиком, но в настоящий момент интерфейс соседнего устройства является недосягаемым; коммутатор откладывает отправку пакетов с запросом на небольшое время, чтобы дать возможность протоколам верхнего уровня определить досягаемость. • probe (P): коммутатор посылает пакеты с запросом и ожидает ответа от соседнего устройства. • invalid (IV): Адрес соседнего устройства не является допустимым адресом IPv6. • unknown (?): Статус интерфейса соседнего устройства не удается определить по каким-либо причинам. • incomplete (I): Выполняется процесс разрешения адреса, но адрес канального уровня соседнего устройства еще не определен. Полный ответ от интерфейса соседнего устройства не получен.
Type	Это поле указывает на тип соответствия адресов для интерфейса соседнего устройства. Это поле может содержать следующие значения: • other (O): ни один из следующих типов. • local (L): Интерфейс коммутатора использует данный адрес. • dynamic (D): Соответствие между IP-адресом и MAC-адресом можно успешно разрешить с помощью протокола IPv6 Neighbor Discovery. Этот протокол аналогичен протоколу ARP (Address Resolution protocol) для IPv4. • static (S): Для данного интерфейса указан статический адрес.

47

Устранение неполадок

В данной главе описаны некоторые способы разрешения проблем, с которыми можно столкнуться при эксплуатации устройства. Возможные проблемы разделены по следующим категориям:

- Проблемы с питанием, подключения к устройству и индикаторы
- Проблемы с доступом к коммутатору и входом в систему
- Настройки коммутатора

47.1 Проблемы с питанием, подключения к устройству и индикаторы

Не включается коммутатор. Ни один из индикаторов не горит.

1. Убедитесь, что с коммутатором используются адаптер питания или шнур питания из комплекта поставки.
2. Убедитесь, что адаптер питания или шнур подключены к коммутатору и к соответствующему источнику питания. Убедитесь, что источник питания включен и работает.
3. Отсоедините и вновь присоедините адаптер питания или шнур к коммутатору.
4. Если проблема сохраняется, обратитесь к поставщику.

Горит индикатор **ALM**.

1. Отсоедините и вновь присоедините адаптер питания или шнур к коммутатору.
2. Если проблема сохраняется, обратитесь к поставщику.

Показания одного из индикаторов отличаются от обычного.

1 Проверьте, какими именно должны быть показания индикатора в нормальном режиме. См. разд. 3.3 на стр. 30.

2 Проверьте подключения к устройству. См. разд. 47.1 на стр. 381.

3 Осмотрите кабели на предмет повреждений. Обратитесь к поставщику для замены всех поврежденных кабелей.

4 Отсоедините и вновь присоедините адаптер питания или шнур к коммутатору.

5 Если проблема сохраняется, обратитесь к поставщику.

47.2 Проблемы с доступом к коммутатору и входом в систему

Забыт IP-адрес коммутатора.

1 По умолчанию используется IP-адрес **192.168.1.1**.

2 Воспользуйтесь консольным портом для входа на коммутатор.

3 Если это не помогает, можно сбросить устройство к заводским настройкам по умолчанию. См. разд. 4.6 на стр. 39.

Забыто имя пользователя и/или пароль.

1 Имя пользователя по умолчанию – **admin**, а соответствующий ему пароль по умолчанию – **1234**.

2 Если это не помогает, можно сбросить устройство к заводским настройкам по умолчанию. См. разд. 4.6 на стр. 39.

Невозможно получить доступ к экрану **Login** Web-конфигуратора.

1 Убедитесь, что используется правильный IP-адрес.

- По умолчанию используется IP-адрес 192.168.1.1.

- Если IP-адрес был изменен, используйте новый IP-адрес.
- Если IP-адрес был изменен, но невозможно узнать, на какой именно, обратитесь к рекомендациям раздела Забыт IP-адрес коммутатора.

2 Проверьте подключения к устройству и убедитесь, что показания индикаторов соответствуют нормальным. См. разд. 3.3 на стр. 30.

3 Убедитесь, что в браузере не включена блокировка всплывающих окон и включены JavaScripts и Java.

4 Убедитесь, что компьютер находится в той же подсети, что и коммутатор. (Если точно известно, что подключение компьютера к коммутатору осуществляется через маршрутизатор, пропустите данный шаг).

5 Выполните сброс устройства к заводским настройкам по умолчанию и попытайтесь получить доступ к коммутатору с использованием IP-адреса по умолчанию. См. разд. 4.6 на стр. 39.

6 Если проблема сохраняется, обратитесь к поставщику или попытайтесь воспользоваться одной из дополнительных рекомендаций.

Дополнительные рекомендации

- Попробуйте получить доступ к коммутатору с использованием другой службы, например, Telnet. В случае успешного доступа к коммутатору проверьте настройки удаленного управления, чтобы выяснить, почему коммутатор не отвечает на подключения через HTTP.

Экран **Login** появляется, но выполнить вход на коммутатор не удается.

1 Убедитесь, что имя пользователя и пароль вводятся правильно. Имя пользователя по умолчанию – **admin**, а соответствующий ему пароль по умолчанию – **1234**. Данные значения чувствительны к регистру, поэтому убедитесь, что [Caps Lock] не включен.

2 Возможно, превышено допустимое количество одновременных сессий Telnet. Завершите другие сессии Telnet и попробуйте подключиться еще раз.

Убедитесь, что доступ через HTTP или Telnet разрешен. 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.

3 Отсоедините и вновь присоедините шнур питания к коммутатору.

4 Если это не помогает, можно сбросить устройство к заводским настройкам по умолчанию. См. разд. 4.6 на стр. 39.

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).

Я не вижу некоторые из меню нижнего уровня **Advanced Application** в нижней части навигационной панели.

Рекомендованное разрешение экрана – 1024 на 768 пикселей. Отрегулируйте разрешение экрана на компьютере, что позволит увидеть остальные меню нижнего уровня **Advanced Application** в нижней части навигационной панели.

К коммутатору осуществляется несанкционированный доступ по протоколам telnet, HTTP и SSH.

Нажмите кнопку **Display** в поле **System Log** на экране **Management** > **Diagnostic**, чтобы выявить попытки несанкционированного доступа к коммутатору. Чтобы исключить возможность несанкционированного доступа, настройте параметры безопасного клиентского доступа на экране **Management** > **Access Control** > **Remote Management** для протоколов telnet, HTTP и SSH (см. разд. 38.6 на стр. 341). Компьютеры, не принадлежащие к числу безопасных клиентов, не смогут получить доступ к коммутатору.

47.3 Настройки коммутатора

После перезагрузки коммутатора пропали настройки конфигурации.

Обязательно сохраняйте конфигурацию в постоянной памяти коммутатора каждый раз, когда вносите какие-либо изменения. Нажмите **Save** в правом верхнем углу Web-конфигуратора, чтобы сохранить конфигурацию на постоянной основе. Более подробную информацию о том, как сохранить конфигурацию, можно найти в разд. 37.5 на стр. 327.

A

Часто используемые службы

В приведенной ниже таблице перечислен ряд наиболее часто используемых служб, с указанием соответствующих протоколов и номеров портов. Полный перечень номеров портов, кодов/типов ICMP и служб можно найти на сайте IANA (уполномоченной организации по распределению нумерации в сети Интернет).

- **Наименование**: Краткое описательное имя службы. Можно использовать это имя или создать другое, при желании.
- **Протокол**: Тип IP-протокола, используемого службой. Если в этом столбце указано **TCP/UDP**, данной службой используются одинаковые номера портов как для TCP, так и для UDP. Если в этом столбце указано **ОПРЕДЕЛЯЕТСЯ ПОЛЬЗОВАТЕЛЕМ**, в столбце **Порт(ы)** указывается номер протокола IP, а не номер порта.
- **Порты(ы)**: Значение в данном столбце зависит от значения в столбце **Протокол**. Более подробную информацию о номерах портов можно найти в RFC 1700.
  - Если в столбце **Протокол** указано **TCP**, **UDP** или **TCP/UDP**, в данном столбце указывается номер порта IP.
  - Если в столбце **Протокол** стоит **ОПРЕДЕЛЯЕТСЯ ПОЛЬЗОВАТЕЛЕМ**, в данном столбце указывается номер протокола IP.
- **Описание**: Краткое описание приложений, которые используют службу, или ситуаций, в которых используется служба.

Таблица 174 Часто используемые службы

НАИМЕНОВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	Определяется пользователем	51	Данная служба используется протоколом туннелирования IPSEC AH (заголовок аутентификации).
AIM/New-ICQ	TCP	5190	Служба Интернет-сообщений AOL. Также используется как порт прослушивания ICQ.
AUTH	TCP	113	Протокол аутентификации, используемый некоторыми серверами.
BGP	TCP	179	Протокол пограничной маршрутизации.
BOOTP_CLIENT	UDP	68	Клиент DHCP.
BOOTP_SERVER	UDP	67	Сервер DHCP.
CU-SEEME	TCP UDP	7648 24032	Популярное решение для видеоконференций от White Pines Software.
DNS	TCP/UDP	53	Сервер доменных имен, служба, определяющая соответствие между именами в Интернете (такими как www.zyxel.com) и IP-адресами.
ESP (IPSEC_TUNNEL)	Определяется пользователем	50	Данная служба используется протоколом туннелирования IPSEC ESP (Encapsulation Security Protocol).

Таблица 174 Часто используемые службы (продолжение)

НАИМЕНОВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
FINGER	TCP	79	Finger – команда в UNIX или в Интернете, используемая для поиска зарегистрированных в системе пользователей.
FTP	TCP TCP	20 21	Программа передачи файлов, программа, обеспечивающая быструю передачу файлов, в том числе файлов большого размера, которые не всегда возможно передать по электронной почте.
H.323	TCP	1720	Данный протокол используется программой NetMeeting.
HTTP	TCP	80	Протокол передачи гипертекста – протокол клиент/сервер для сети World Wide Web.
HTTPS	TCP	443	HTTPS – защищенные сессии http, часто используемые в электронной коммерции.
ICMP	Определяется пользователем	1	Межсетевой протокол контрольных сообщений часто используется для диагностики или маршрутизации.
ICQ	UDP	4000	Популярная программа для Интернет-чата.
IGMP (MULTICAST)	Определяется пользователем	2	Межсетевой протокол управления группами многоадресной рассылки используется при отправке пакетов определенной группе хостов.
IKE	UDP	500	Алгоритм обмена ключами в Интернете используется для распространения ключей и управления ключами.
IRC	TCP/UDP	6667	Еще одна популярная программа Интернет-чата.
MSN Messenger	TCP	1863	Данный протокол используется службой сообщений Microsoft Networks.
NEW-ICQ	TCP	5190	Программа Интернет-чата.
NEWS	TCP	144	Протокол новостных групп.
NFS	UDP	2049	Сетевая файловая система NFS – распределенная файловая служба клиент/сервер, обеспечивающая прозрачный доступ к совместному использованию файлов в сети.
NNTP	TCP	119	Сетевой протокол передачи новостей представляет собой механизм доставки для службы новостей USENET.
PING	Определяется пользователем	1	Packet INternet Groper – протокол, рассылающий эхо-запросы ICMP для проверки доступности удаленного хоста.
POP3	TCP	110	Почтовый протокол Post Office Protocol версии 3 позволяет клиентским компьютерам получать электронную почту с сервера POP3 с использованием временного подключения (TCP/IP или другого).
PPTP	TCP	1723	Протокол туннелирования «точка-точка» обеспечивает защищенную передачу данных через общедоступные сети. Этот порт используется для управляющего канал.
PPTP_TUNNEL (GRE)	Определяется пользователем	47	Протокол туннелирования «точка-точка» PPTP обеспечивает защищенную передачу данных через общедоступные сети. Этот порт используется для канала передачи данных.

Таблица 174 Часто используемые службы (продолжение)

НАИМЕНОВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
RCMD	TCP	512	Служба удаленных команд.
REAL_AUDIO	TCP	7070	Служба потоковой передачи аудио обеспечивает трансляцию звука через Интернет в реальном времени.
REXEC	TCP	514	Процесс (daemon) удаленного исполнения.
RLOGIN	TCP	513	Удаленный вход в систему.
RTELNET	TCP	107	Удаленный Telnet.
RTSP	TCP/UDP	554	Протокол потоковой передачи реального времени (управления средой передачи) RTSP обеспечивает удаленное управление потоками мультимедиа в Интернете.
SFTP	TCP	115	Простой протокол передачи файлов.
SMTP	TCP	25	Простой протокол пересылки почты представляет собой стандарт обмена сообщениями через Интернет. SMTP позволяет передавать сообщения с одного сервера электронной почты на другой.
SNMP	TCP/UDP	161	Простой протокол сетевого управления.
SNMP-TRAPS	TCP/UDP	162	«Ловушки», используемые в протоколе SNMP (RFC:1215).
SQL-NET	TCP	1521	Язык структурированных запросов SQL – интерфейс доступа к данным в различных системах баз данных, в том числе на мейнфреймах, системах среднего уровня, UNIX-системах и сетевых серверах.
SSH	TCP/UDP	22	Программа удаленного входа в систему через защищенную оболочку.
STRM WORKS	UDP	1558	Протокол Stream Works.
SYSLOG	UDP	514	Syslog обеспечивает передачу системных контрольных журналов на сервер UNIX.
TACACS	UDP	49	Протокол входа в систему, используемый для систем TACACS (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet – протокол входа в систему и эмуляции терминала, часто используемый в Интернете и UNIX-системах. Работает в сетях TCP/IP. Основное назначение данного протокола – удаленный вход пользователей на хост-системы.
TFTP	UDP	69	Тривиальный протокол передачи файлов – сходный с FTP протокол передачи файлов в Интернете, отличается от FTP использованием протокола UDP (User Datagram Protocol) вместо TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Еще одно решение для видеоконференций.

B

IPv6

Обзор

IPv6 (версия 6 протокола IP, Internet Protocol) была разработана с целью увеличения размера и функциональности IP-адресов. Увеличение размера адреса IPv6 до 128 битов (по сравнению с 32-битными адресами IPv4) позволяет увеличить количество доступных IP-адресов до 3,4 x 10^{38}.

Адресация IPv6

128-разрядный адрес IPv6 записывается в виде восьми 16-битных шестнадцатеричных блоков, разделенных двоеточием (:). Вот пример адреса IPv6:
`2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

Адреса IPv6 можно сокращать двумя способами:

- Ведущие нули в блоках можно опускать. Например, адрес `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` можно записать в виде `2001:db8:1a2b:15:0:0:1a2f:0`.
- Любое число последовательных блоков, состоящих из нулей, можно заменить двойным двоеточием. Двойное двоеточие можно использовать при написании адреса IPv6 только один раз. Соответственно, адрес `2001:0db8:0000:0000:1a2f:0000:0000:0015` можно записать как `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` или `2001:db8:0:0:1a2f::15`.

Префикс и его длина

По аналогии с маской подсети для IPv4 протокол IPv6 использует адресный префикс для указания на адрес сети. Длина префикс IPv6 говорит о том, сколько наиболее значимых битов адреса, если отсчитывать слева, составляют адрес сети. Длина префикса записывается в формате «/x», где x – это число. Например,

```
запись 2001:db8:1a2b:15::1a2f:0/32
```

означает, что первые 32 бита (`2001:db8`) являются адресом подсети.

Адрес Link-local

Адрес link-local уникальным образом идентифицирует устройство в локальной сети. Он аналогичен «частному IP-адресу» протокола IPv4. Один и тот же адрес link-local может быть назначен двум и более интерфейсам одного устройства. Однонаправленный адрес link-local имеет предопределенный префикс fe80::/10. Формат однонаправленного адреса link-local выглядит следующим образом.

Таблица 175 Формат однонаправленного адреса link-local

1111 1110 10	0	Идентификатор интерфейса
10 битов	54 бита	64 бита

Глобальный адрес

Глобальный адрес уникальным образом идентифицирует устройство в сети Интернет. Он аналогичен «внешнему IP-адресу» протокола IPv4. Глобальный однонаправленный адрес начинается с 2 или 3.

Неуказанный адрес

Неуказанный адрес (0:0:0:0:0:0:0:0 или ::) используется в качестве адреса источника в том случае, если устройство не имеет собственного адреса. Он аналогичен адресу «0.0.0.0» протокола IPv4.

Адрес обратной петли

Адрес обратной петли (0:0:0:0:0:0:0:1 или ::1) дает хосту возможность отправлять пакеты самому себе. Этот тип адреса аналогичен адресу «127.0.0.1» протокола IPv4.

Адрес для многоадресной рассылки

Адреса для многоадресной рассылки протокола IPv6 выполняют ту же функцию, что и широковещательные адреса протокола IPv4. Протокол IPv6 не поддерживает широковещательные рассылки. Адрес для многоадресной рассылки позволяет хосту рассылать пакеты всем хостам, входящим в группу многоадресной рассылки.

Масштаб многоадресной рассылки позволяет определять размер группы многоадресной рассылки. Адрес для многоадресной рассылки имеет предопределенный префикс ff00::/8. В таблице ниже приведено описание некоторых предопределенных адресов для многоадресной рассылки.

Таблица 176 Предопределенные адреса для многоадресной рассылки

АДРЕС ДЛЯ МНОГОАДРЕСНОЙ РАССЫЛКИ	ОПИСАНИЕ
FF01:0:0:0:0:0:0:1	Все хосты на локальном узле.
FF01:0:0:0:0:0:0:2	Все маршрутизаторы на локальном узле.
FF02:0:0:0:0:0:0:1	Все хосты на локально подключенном соединении.
FF02:0:0:0:0:0:0:2	Все маршрутизаторы на локально подключенном соединении.
FF05:0:0:0:0:0:0:2	Все маршрутизаторы на локальной площадке.
FF05:0:0:0:0:0:1:3	Все DHCP-серверы на локальной площадке.

В таблице ниже приведен список зарезервированных адресов для многоадресной рассылки, которые нельзя назначить группе многоадресной рассылки.

Таблица 177 Зарезервированные адреса для многоадресной рассылки

АДРЕС ДЛЯ МНОГОАДРЕСНОЙ РАССЫЛКИ
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Маски подсети

И адрес IPv6, и маска подсети IPv6 состоят из 128-битных цифр, которые разбиты на восемь 16-битных блоков и записаны в шестнадцатеричной нотации. Шестнадцатеричная нотация использует четыре бита под каждый символ (1 ~ 10, A ~ F). 16 битов каждого блока затем представляются в виде четырех шестнадцатеричных символов. Например, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Идентификатор интерфейса

В протоколе IPv6 идентификатор интерфейса – это 64-битное число. Он идентифицирует физический интерфейс (например, порт Ethernet) или виртуальный интерфейс (например, IP-адрес управления для сети VLAN). Каждый интерфейс должен иметь уникальный идентификатор.

EUI-64

Расширенный уникальный идентификатор EUI-64 (Extended Unique Identifier), разработанный институтом IEEE (Institute of Electrical and Electronics Engineers), – это формат идентификатора интерфейса, адаптированный для протокола IPv6. Как показано ниже, он является производным от 48-битного (6-байтового) MAC-адреса Ethernet. EUI-64 вставляет шестнадцатеричные цифры fffe между третьим и четвертым байтами MAC-адреса и дополняет седьмой бит первого байта MAC-адреса. Пример приводится ниже.

Таблица 178

MAC	00	:	13	:	49 : 12	:	34	:	56

Таблица 179

EUI-64	02	:	13	:	49	:	FF	:	FE	: 12	:	34	:	56

Автоматическая настройка без сохранения состояния

Функция автоматической настройки без сохранения состояния для IPv6 позволяет автоматически генерировать уникальные адреса. В отличие от DHCPv6 (Dynamic Host Configuration Protocol версии шесть), который используется для автоматической настройки IPv6 с сохранением состояния, в данном случае DHCP-сервер не должен хранить сведения о владельце и состоянии адресов. Каждое устройство IPv6 может сгенерировать собственный, уникальный IP-адрес автоматически, если на данном интерфейсе включена поддержка IPv6. Полный адрес IPv6 формируется из префикса и идентификатора интерфейса (сгенерированного на основе собственного MAC-адреса Ethernet, см. Идентификатор интерфейса и EUI-64).

Если на устройстве включена поддержка IPv6, то его интерфейс автоматически генерирует адрес link-local (начинающийся с префикса fe80).

Если этот интерфейс подключен к сети с маршрутизатором, а настройки коммутатор предусматривают автоматическое получение сетевого префикса IPv6 для данного интерфейса с маршрутизатора, то он генерирует еще один адрес, сочетающий в себе идентификатор интерфейса, информацию о глобальной сети и информацию о подсети, полученную от маршрутизатора[3]. Это будет маршрутизируемый, глобальный IP-адрес.

DHCPv6

Протокол DHCPv6 (Dynamic Host Configuration Protocol for IPv6, протокол динамической конфигурации хостов для IPv6, RFC 3315) – это клиент-серверный протокол, который позволяет DHCP-серверу назначать и передавать сетевые адреса, префиксы и другие сведения о конфигурации IPv6 DHCP-клиентам. Серверы и клиенты DHCPv6 обмениваются сообщениями DHCP с использованием протокола UDP.

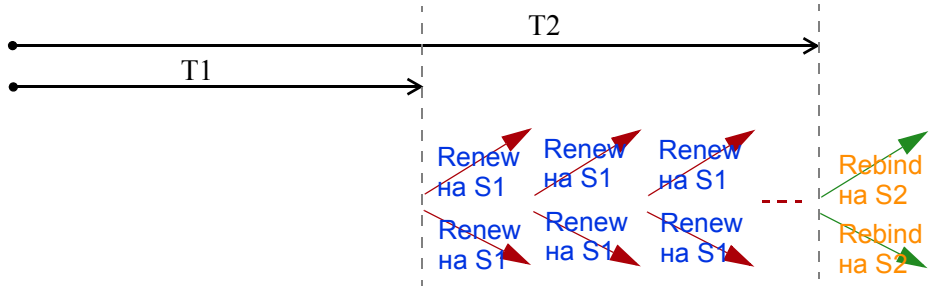
Каждый DHCP-клиент и DHCP-сервер имеет уникальный идентификатор DHCP (DHCP Unique IDentifier, DUID), который используется для идентификации при обмене сообщениями DHCPv6. DUID генерируется на основе MAC-адреса, времен, идентификатора, назначенного поставщиком, и/или частного корпоративного номера поставщика, зарегистрированного в IANA. DUID не должен меняться со временем, даже после перезагрузки устройства.

Ассоциация идентификаторов

Ассоциация идентификаторов (Identity Association, IA) – это коллекция адресов, назначенных DHCP-клиенту, посредством которой сервер и клиент могут управлять группой связанных IP-адресов. Каждая ассоциация IA должна быть ассоциирована только с одним интерфейсом. DHCP-клиент использует ассоциацию IA, назначенную данному интерфейсу, для получения настроек для данного интерфейса с DHCP-сервера. Каждая ассоциация IA включает в себя уникальный идентификатор IAID и связанную с ним информацию протокола IP.
Тип IA – это тип адреса в IA. Каждая ассоциация IA хранит адреса одного типа. IA_NA означает ассоциацию идентификаторов для постоянных адресов, а IA_TA – ассоциацию идентификаторов для временных адресов. Опция IA_NA содержит поля T1 и T2, а опция IA_TA – нет. Сервер DHCPv6 использует поля T1 и T2 для управления временем обращения клиента к

3. Протокол IPv6 допускает привязку двух и более адресов к любому сетевому интерфейсу.

серверу с целью заблаговременного продления сроков жизни любых адресов, входящих в ассоциацию IA_NA. При наступлении момента времени T1 клиент отправляет серверу (**S1**), от которого были получены адреса, содержащиеся в ассоциации IA_NA, сообщение Renew. Если уже наступил момент времени T2, а сервер не отвечает, то клиент отправляет сообщение Rebind любому доступному серверу (**S2**). В случае ассоциации IA_TA клиент может посылать сообщения Renew или Rebind по собственному усмотрению.



Агент ретрансляции DHCP

Агент ретрансляции DHCP находится в одной сети с DHCP-клиентами и помогает пересылать сообщения между DHCP-сервером и DHCP-клиентами. Если клиент не может использовать собственный адрес link-local и хорошо известный адрес для многоадресной рассылки для поиска DHCP-сервера в своей сети, то ему нужен агент ретрансляции DHCP для отправки сообщения DHCP-серверу, находящемуся в другой сети.

Агент ретрансляции DHCP может добавлять опцию удаленной идентификации (remote-ID) и опцию идентификации интерфейса (interface-ID) в сообщения Relay-Forward протокола DHCPv6. Опция remote-ID содержит строку, заданную пользователем, например, имя системы. Опция interface-ID передает серверу DHCPv6 сведения о номере слота, информация о портах и идентификатор VLAN. Опция remote-ID (если она есть) удаляется из сообщений Relay-Reply до момента отправки пакетов агентом ретрансляции клиентам. DHCP-сервер копирует опцию interface-ID из сообщения Relay-Forward в сообщение Relay-Reply и отправляет его агенту ретрансляции. Значение interface-ID не должно меняться даже после перезапуска агента ретрансляции.

Делегирование префикса

Функция делегирования префикса позволяет маршрутизатору IPv6 использовать префикс IPv6 (сетевой адрес), полученный от провайдера услуг Интернет (или агрегирующего маршрутизатора), для локальной сети. Устройство коммутатор использует полученный префикс IPv6 (например, 2001:db2::/48) для генерации собственного IP-адреса в локальной сети. Устройство коммутатор передает информацию о префиксе IPv6 хостам в локальной сети посредством регулярной многоадресной рассылки анонсов маршрутизатора (Router Advertisements, RA). После получения сведений о префиксе хосты могут использовать его для генерации собственных адресов IPv6.

ICMPv6

Протокол ICMPv6 (Internet Control Message Protocol for IPv6 или ICMP for IPv6) описан в документе RFC 4443. Для ICMPv6 значение поля Next Header равно 58 – это отличается от значения, используемого для идентификации ICMP for IPv4. ICMPv6 является неотъемлемой частью IPv6. Узлы IPv6 используют ICMPv6 для информирования об ошибках, которые

встретились при обработке пакетов, и выполнения других диагностических функций, таких, как «ping».

Neighbor Discovery Protocol (NDP)

Протокол NDP (Neighbor Discovery Protocol, протокол обнаружения соседей) – это протокол, используемый для обнаружения других устройств IPv6 и отслеживания их досягаемости в сети. Устройство IPv6 использует следующие типы сообщений ICMPv6:

- Запрос доступных соседей (Neighbor solicitation): Запрос от хоста с целью узнать адрес канального уровня (MAC-адрес) соседнего устройства и определить, остается ли оно досягаемым. Соседнее устройство считается «досягаемым», если оно отвечает на сообщение типа «Запрос доступных соседей», поступившее от хоста, сообщением типа «Ответ соседа».
- Ответ соседа (Neighbor advertisement): Ответ от узла с целью анонса его адреса канального уровня.
- Запрос на доступность маршрутизаторов (Router solicitation): Запрос от хоста с целью поиска маршрутизатора, который может выступать в качестве маршрутизатора по умолчанию и пересылать пакеты.
- Ответ маршрутизатора (Router advertisement): Ответ на сообщение типа «Запрос на доступность маршрутизаторов» или периодический широковещательный анонс от маршрутизатора, информирующий о его присутствии и содержащий сведения о ряде его параметров.

Кэш IPv6

Хост IPv6 обязательно должен иметь кэш соседских узлов, кэш узлов назначения, список префиксов и список маршрутизаторов по умолчанию. Устройство коммутатор постоянно обслуживает и обновляет кэши IPv6 на основе информации, получаемой в сообщениях-ответах. В соответствии с протоколом IPv6 устройство коммутатор автоматически выполняет настройку адреса link-local, а затем отправляет сообщение типа «Запрос доступных соседей» для проверки уникальности адреса. При наличии адреса, который надо разрешить или верифицировать, устройство коммутатор также отправляет сообщение типа «Запрос доступных соседей». При получении сообщения типа «Ответ соседа» устройство коммутатор сохраняет адрес канального уровня соседнего устройства в кэше соседних узлов. При получении в ответ на сообщение типа «Запрос на доступность маршрутизаторов» сообщения типа «Ответ маршрутизатора» устройство коммутатор добавляет сведения о маршрутизаторе в кэш соседних узлов, список префиксов и кэш узлов назначения. Если данный маршрутизатор можно использовать в качестве маршрутизатора по умолчанию, то устройство коммутатор создает запись в списке маршрутизаторов по умолчанию.

Если устройству коммутатор необходимо отправить пакет, то оно вначале обращается к кэшу узлов назначения, чтобы определить следующий переход. Если соответствующей записи в кэше узлов назначения нет, устройство коммутатор с помощью списка префиксов определяет, доступен ли данный адрес назначения, и можно ли связаться с ним напрямую, в обход маршрутизатора. В случае доступности этот адрес выбирается в качестве следующего перехода. В противном случае устройство коммутатор выбирает следующий переход из списка маршрутизаторов по умолчанию или из таблицы маршрутизации. Если IP-адрес следующего перехода известен, устройство коммутатор ищет в кэше соседних узлов соответствующий адрес канального уровня и отправляет пакет, когда соседний узел становится досягаемым. Если устройство коммутатор не может найти нужной записи в кэше соседних узлов, или соседний узел недоступен, то оно начинает процесс разрешения адреса. Это помогает уменьшить число IPv6-сообщений типа «Запрос...» и «Ответ...».

Пример – Включение поддержки протокола IPv6 в операционных системах Windows XP/2003/Vista

По умолчанию операционные системы Windows XP и Windows 2003 поддерживают протокол IPv6. Этот пример иллюстрирует процесс включения поддержки протокола IPv6 в операционных системах Windows XP/2003 с помощью команды `ipv6 install`. Кроме того, здесь рассматривается применение команды `ipconfig` для просмотра автоматически сгенерированных IP-адресов.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.1.1.46
        Subnet Mask . . . . . . . . . . . :255.255.255.0
        IP Address. . . . . . . . . . . . : fe80::2d0:59ff:feb8:103c%4
        Default Gateway . . . . . . . . . :10.1.1.254
```

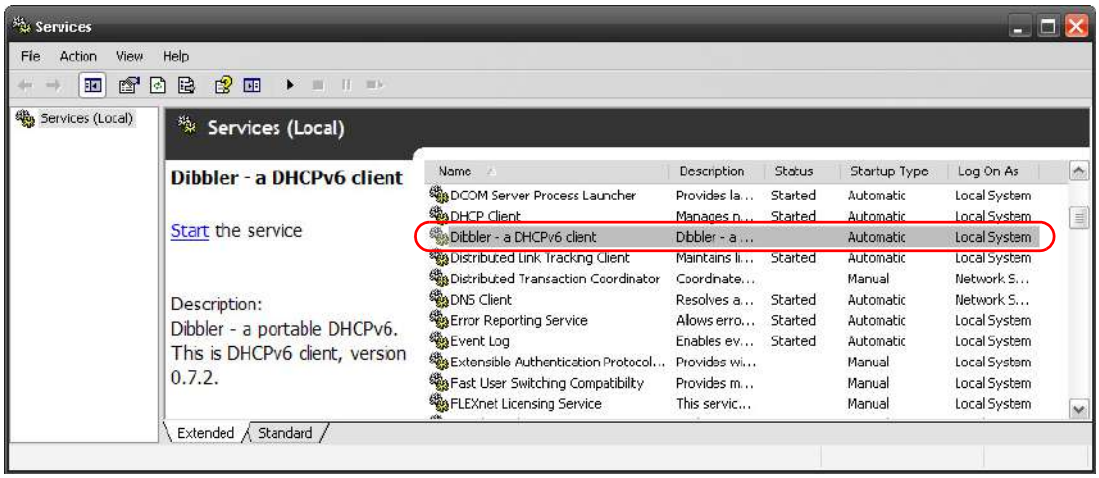
Протокол IPv6 установлен и включен по умолчанию в операционной системе Windows Vista. Воспользуйтесь командой `ipconfig` для просмотра автоматически назначенного адреса IPv6. Для данного интерфейса на компьютере должен отображаться как минимум один доступный адрес IPv6.

Пример – Включение поддержки DHCPv6 в операционной системе Windows XP

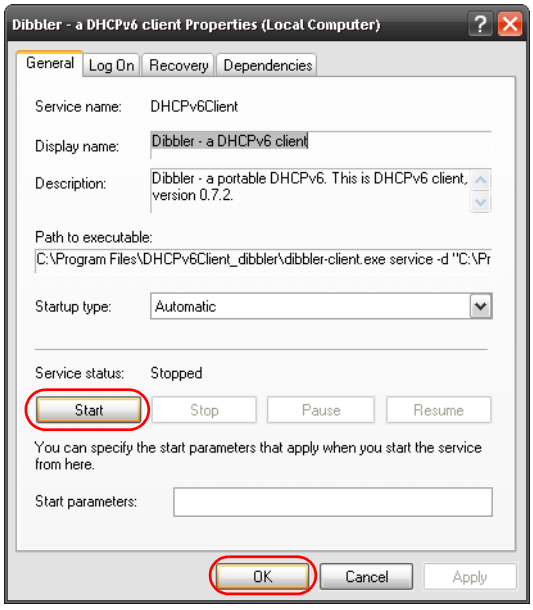
Windows XP не поддерживает DHCPv6. Если в сети для назначения IP-адресов используется протокол DHCPv6, необходимо установить клиентское программное обеспечение DHCPv6 в операционной системе Windows XP. (Примечание: Если для назначения адресов IPv6 в сети используются статические IP-адреса или анонсы маршрутизаторов (Router Advertisement), этот раздел можно пропустить).

В этом примере в качестве клиента DHCPv6 используется Dibbler. Чтобы включить клиент DHCPv6 на компьютере:

1. Установите на компьютер Dibbler и выберите опцию «клиент DHCPv6».
2. После завершения установки выберите в меню **Start** > **All Programs** > **Dibbler-DHCPv6** > **Client Install as service**.
3. Выберите **Start** > **Control Panel** > **Administrative Tools** > **Services**.
4. Дважды щелкните мышью по строке **Dibbler – a DHCPv6 client**.



5 Нажмите кнопку **Start**, затем кнопку **OK**.



6 Теперь компьютер сможет получать адрес IPv6 от сервера DHCPv6.

Пример – Включение поддержки IPv6 в операционной системе Windows 7

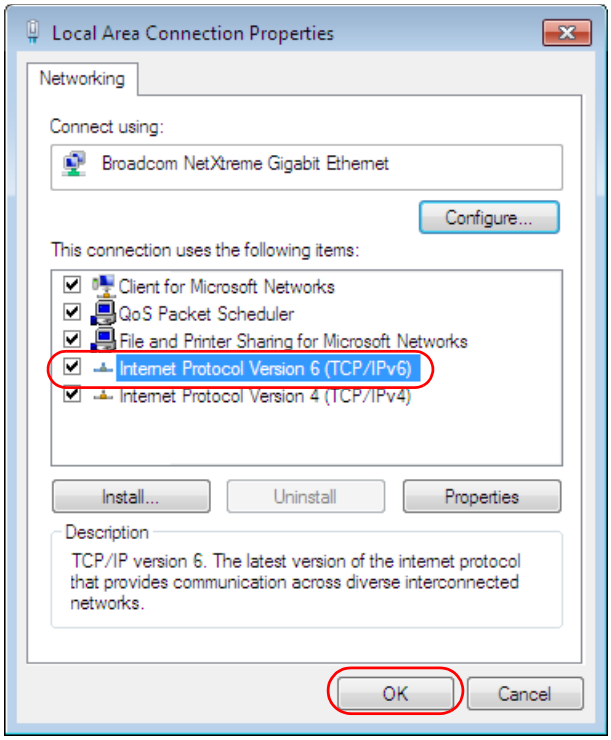
По умолчанию операционная система Windows 7 поддерживает IPv6. Включение поддержки IPv6 на компьютере, работающем под управлением Windows 7, автоматически включает поддержку DHCPv6.

Чтобы включить поддержку IPv6 в операционной системе Windows 7:

1 Выберите в меню **Control Panel** > **Network and Sharing Center** > **Local Area Connection**.

2 Установите переключатель **Internet Protocol Version 6 (TCP/IPv6)**, чтобы включить поддержку протокола IPv6.

3 Нажмите кнопку **OK**, чтобы сохранить изменения.



4 Нажмите кнопку **Close**, чтобы закрыть экран **Local Area Connection Status**.

5 Выберите в меню **Start** > **All Programs** > **Accessories** > **Command Prompt**.

6 Воспользуйтесь командой `ipconfig` для просмотра динамического адреса IPv6. В этом примере показан глобальный адрес (2001:b021:2d::1000), полученный от DHCP-сервера.

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b021:2d::1000
   Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
   IPv4 Address. . . . . . . . . . . :172.16.100.61
   Subnet Mask . . . . . . . . . . . :255.255.255.0
   Default Gateway . . . . . . . . . : fe80::213:49ff:feaa:7125%11
                                       172.16.100.254
```

Предупреждения по безопасности

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

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

- Внимание: В случае установки батареи неправильного типа (на материнской плате) существует опасность взрыва. Соблюдайте указания по утилизации использованных батарей. Сдавайте использованные батареи в пункты утилизации электрических и электронных компонентов. Подробную информацию об утилизации данного изделия можно получить в местном муниципалитете, службе утилизации бытовых отходов или в магазине, где оно было приобретено.
- НЕ заслоняйте вентиляционные отверстия устройства, так как ограниченный приток воздуха может послужить причиной повреждения устройства.
- Устройства, поддерживающие подачу или получение питания по витой паре (PoE), а также подключенные к ним кабели Ethernet должны располагаться целиком внутри помещений.
- Длина зачищенного (оголенного) силового провода не должна превышать 7 мм.
- Устройства укомплектованные силовым кабелем питания имеющим гнездо заземления, относятся к классу электробезопасности 1, обязаны быть заземлены.”

Данное изделие подлежит утилизации. Соблюдайте надлежащие требования по утилизации.