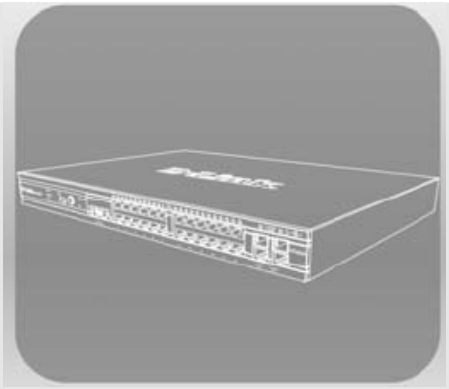
D-Link®
Building Networks for People



XSTACK

Руководство пользователя

Коммутаторы серии DES-3800 xStack™
Управляемые стекируемые коммутаторы
Fast Ethernet 3 уровня
Release 3

Содержание

Предисловие

Руководство пользователя для коммутаторов ***серии DES-3800*** xStack состоит из нескольких разделов, в которых приводятся инструкции по настройке и примеры конфигурации. Ниже приводится краткий обзор разделов:

Раздел 1, Введение - Описание коммутатора и его свойств.

Раздел 2, Установка- Помогает осуществить установку коммутатора, а также содержит описание передней, задней панелей и индикаторов коммутатора. Также в этом раздел содержатся инструкции, как подключить питание постоянного тока к Коммутатору DES-3828DC.

Раздел 3, Подключение коммутатора - Описывает, как подключить коммутатор к сети Ethernet/Fast Ethernet.

Раздел 4, Введение в управление коммутатором - Вводная информация по управлению коммутатором, включая функции защиты паролем, настройки SNMP, назначения IP-адреса и подключение устройств к коммутатору.

Раздел 5, Настройка Коммутатора через Web-интерфейс - Рассматривается управление устройством с помощью Web-интерфейса.

Раздел 6, Настройка Коммутатора - Детально рассматриваются настройки основных функций коммутатора, включая доступ к информации коммутатора, использование утилит коммутатора и настроек сетевых конфигураций, таких как назначение IP-адреса, настройки портов, учетные записи пользователей, зеркалирование портов, настройки системного журнала, SNTP, TFTP, Ping Test, SNMP, управление через единый IP-адрес, продвижение и фильтрация пакетов.

Раздел 7, Управление – Обсуждаются предусмотренные на Коммутаторе функции безопасности, включая задание безопасных IP-адресов, учетные записи пользователей, управление аутентификацией доступа и SNMP.

Раздел 8, Мониторинг - Обсуждаются графические интерфейсы, используемые для управления свойствами и пакетами коммутатора.

Раздел 9, Техническая эксплуатация – Приводится информация по таким функциям Коммутатора, как TFTP-сервисы, журнал коммутатора, Ping Test, сохранение изменений и перезагрузка коммутатора.

Раздел 10, Технология Single IP Management – Обсуждается функция Single IP Management (Управление через единый IP-адрес), включая пользовательский интерфейс на основе Java и утилиты функции SIM.

Приложение A, Техническая спецификация – Техническая спецификация для коммутаторов серии DES-3500.

Приложение B, Кабели и коннекторы - Описание гнезд RJ-45 /коннекторов, прямых и кроссовых кабелей и стандартного распределения контактов.

Приложение C, Записи в системном журнале – Приводится пояснение для записей в системном журнале.

Приложение D, Распределение PIN-разъемов в консольном кабеле

Приложение E, Длина кабелей - Информация о типах кабеля и их максимальной длине.

Глоссарий - Список терминов и сокращений, использованных в этом документе.

Предполагаемые читатели

Руководство пользователя для коммутаторов ***серии DES-3800*** содержит необходимую информацию для настройки и управления коммутатором. Это руководство предназначено преимущественно для администраторов сети, знающих принципы сетевого управления и терминологию.

Условные обозначения

Обозначение	Описание
[ ]	В квадратных скобках в командной строке указываются данные, которые вводить необязательно, но их ввод предоставляет определенные дополнительные опции. Например: фрагмент [copy filename] в командной строке означает, что существует возможность напечатать копию, сопровождаемую названием файла. При вводе команды скобки не печатаются.
Полужирный шрифт	Таким шрифтом указывается кнопка, иконка панели инструментов, меню или пункт меню. Например: Откройте меню **File** и выберите **Cancel**. Таким образом, достигается визуальное выделение информации. Этим шрифтом могут также указываться сообщения системы или сообщения, появляющиеся на экране. Например: **You have mail** (Имеется почта). Полужирный шрифт используется для обозначения имен файлов, названий программ и команд. Например: **use the copy command.**
Жирный шрифт печатной машинки	Указывает, что команда или информация в строке приглашения должны быть напечатаны именно в таком стиле, как напечатано в руководстве.
Начальная заглавная буква	Название окон и клавиш на клавиатуре, имеющих заглавные буквы, печатается с заглавной буквы. Например: Нажмите на **Enter**.
Курсив	Курсивом указывается название окна или области, а также переменные или параметры, которые необходимо заменить соответствующим словом или строкой. Например: фраза «напечатайте *имя файла»* означает, что необходимо напечатать фактическое имя файла, а не саму фразу («имя файла»), обозначенную курсивом.
Menu Name > Menu Option	**Menu Name > Menu Option** показывает структуру меню. Например, **Device > Port > Port Properties** означает, что опция **Port Properties** (свойства порта) находится в разделе **Port** меню **Device**.

Замечания, предупреждения и предостережения

ЗАМЕЧАНИЕ содержит важные указания, помогающие наиболее эффективно использовать устройство.

ПРЕДУПРЕЖДЕНИЕ содержит указание на возможность повреждения оборудования или риск потери данных, а также указывает на способы избежать проблемы.

ПРЕДОСТЕРЕЖЕНИЕ содержит указание на возможность нанесения вреда человеку, повреждения или выхода из строя устройства.

Инструкция по безопасности

Соблюдение приводимых ниже инструкций по безопасности позволяет обеспечить персональную безопасность, а также защитить систему от возможного повреждения. При чтении данного раздела особое внимание следует обратить на значки (⚠). Рядом с ними приводится информация по мерам предосторожности, которым необходимо следовать при работе с устройством.

⚠ Предостережения безопасности

Для снижения риска нанесения физического вреда, поражения электрическим током и ожогов человека, а также выхода из строя оборудования, необходимо соблюдать следующие меры предосторожности:

- Твердо придерживайтесь указаний маркировки.
  - Не обслуживайте устройство при отсутствии документации на него.
  - Вскрытие или снятие покрытий, которые отмечены треугольным символом с молнией, может привести к поражению человека электрическим током.
  - Только обученный сервисный специалист может обслуживать внутренние компоненты устройства.
- При возникновении любого из следующих условий необходимо отключить устройство от электрической розетки, заменить вышедший из строя модуль или связаться с сервисной службой:
  - Повреждение кабеля электропитания, удлинителя или штепселя.
  - Попадание постороннего предмета внутрь устройства.
  - Устройство было подвержено действию воды.
  - Повреждение или падение устройства.
  - Устройство работает некорректно при точном соблюдении инструкций по эксплуатации.
- Держите систему вдали от радиаторов и источников тепла, а также избегайте перекрытия вентиляционных отверстий, предназначенных для охлаждения.
- Не проливайте пищу или жидкости на компоненты системы, и никогда не работайте с устройством во влажной окружающей среде. Если система была подвергнута воздействию влаги, то необходимо обратиться к соответствующему разделу в Руководстве по устранению неисправностей или связаться со специалистом службы сервиса.
- Не помещайте никаких предметов в отверстия системы. Это может привести к возгоранию или электрическому разряду в связи с замыканием внутренних компонентов системы.
- Используйте данное устройство только совместно с сертифицированным оборудованием.
- Прежде чем снять корпус устройства или прикоснуться к его внутренним компонентам, необходимо дать устройству достаточно времени на охлаждение.
- Не используйте устройство с источниками питания, характеристики которых отличны от обозначенных на ярлыке с электрическими параметрами. Если информация о требуемых характеристиках источника питания отсутствует, проконсультируйтесь с провайдером или энергетической компанией.
- Во избежание повреждения системы, убедитесь, что переключатель напряжения (если он предусмотрен) на блоке электропитания соответствует нужной мощности:
  - 115 Вт (V)/60 Гц (Hz) используется в большинстве стран Северной и Южной Америки и некоторых дальневосточных странах, например, Южной Корее и Тайване.
  - 100 Вт/50 Гц - в восточной Японии и 100 Вт/60 Гц - в западной Японии
  - 230 Вт/50 Гц - в большинстве стран Европы, Ближнего Востока и Дальнего Востока

- Убедитесь, что характеристики питания подключаемых устройств соответствуют нормам, действующим в данной местности.
- Используйте только подходящие силовые кабели. Если нужный кабель не входил в комплект поставки, то приобретите силовой кабель, который одобрен для использования в вашей стране. Силовой кабель должен соответствовать характеристикам напряжения и тока, необходимым для данного устройства. Характеристики напряжения и тока кабеля должны быть больше, чем мощность, указанная на устройстве.

• Чтобы избежать удара электрическим током, при работе с устройством пользуйтесь заземленными должным образом электрическими розетками и кабелями.
• Соблюдайте характеристики кабеля-удлинителя и шины питания. Удостоверьтесь, что общий номинальный ток всех устройств, подключенных к кабелю-удлинителю или шине питания, не превышает лимит 80% номинального тока кабеля-удлинителя или шины питания.
• Для обеспечения защиты системы от внезапных кратковременных скачков электропитания используйте ограничитель напряжения, формирователь линии или источник бесперебойного питания (UPS).
• Кабели, используемые для подключения устройства, необходимо размещать таким образом, чтобы на них не наступали и не спотыкались об них. Убедитесь также, что на кабелях ничего не лежит.
• Не заменяйте используемые кабели питания или штепсели, не проконсультировавшись у квалифицированного электрика или в энергетической компании. Всегда следуйте существующим в стране нормам по прокладке кабелей.
• При подключении или отключении от сети в «горячем» режиме источника питания, рекомендуемого для использования с данным устройством, соблюдайте следующие указания:

- Установите источник питания до подключения к нему силового кабеля.
- Отключите силовой кабель перед извлечением источника питания.
- Если система имеет множество блоков питания, отключите питание системы, отсоединив все силовые кабели от блоков питания.

• При перемещении устройства соблюдайте осторожность; убедитесь, что все ролики и/или стабилизаторы надежно прикреплены к системе. Избегайте внезапных остановок и неровных поверхностей.

Общие меры безопасности для устройств, устанавливаемых в стойку

Соблюдайте следующие меры предосторожности, обеспечивающие устойчивость и безопасность коммутационных стоек. Дополнительные инструкции и предостережения приведены в документации по установке коммутационной стойки.

• В качестве «компонента» стойки может рассматриваться как система в целом, так и различные периферийные или дополнительные аппаратные средства.

ПРЕДОСТЕРЕЖЕНИЕ: Перед монтажом компонентов в стойку сначала установите стабилизаторы, поскольку в противном случае возможно опрокидывание стойки, что может, при определенных обстоятельствах, привести к телесным повреждениям человека. После установки системы/компонентов в стойку, никогда не извлекайте более одного компонента из нее. Большой вес компонента может опрокинуть стойку, что приведет к серьезным повреждениям.

• Перед началом работы убедитесь, что стабилизаторы прикреплены к стойке и что стойка устойчиво упирается в пол. Установите передний и боковой стабилизаторы на стойку или только передний стабилизатор для соединения нескольких стоек.
• Всегда загружайте оборудование в стойку снизу вверх, начиная с самого тяжелого.
• Перед добавлением компонента в стойку, убедитесь, что стойка устойчива.

• Соблюдайте осторожность, передвигая компоненты стойки по удерживающим рельсам, - рельсы могут защемить пальцы
• После того, как компонент вставлен в стойку, аккуратно удлините рельс в положение захвата, и тогда поместите компонент в стойку
• Не перегружайте ветвь питания переменного тока распределительной сети, обеспечивающей электропитание стойки. Стойка при полной загрузке не должна потреблять более 80% мощности, доступной для данной ветви распределительной сети.

• Удостоверьтесь, что компонентам в стойке обеспечивается надлежащая циркуляция воздуха.

• Обслуживая одни компоненты стойки, не наступайте на другие компоненты.

ЗАМЕЧАНИЕ: Подключение питания постоянного тока и защитного заземления должно выполняться силами квалифицированного электрика. Все электрические соединения должны выполняться в соответствии с местными и государственными нормами и правилами эксплуатации.

ПРЕДОСТЕРЕЖЕНИЕ: При необходимости заменить заземляющий провод или

работающее оборудование нужно обеспечить наличие другого заземляющего провода. Свяжитесь с соответствующей инспекцией или электриком, если сомневаетесь, что подходящее заземляющее устройство имеется в наличии.

ПРЕДОСТЕРЕЖЕНИЕ: Системный блок должен быть непосредственно заземлен на корпус стойки. Не пытайтесь подключить силовой кабель к системе до тех пор, пока не организовано надлежащее заземление. Полная мощность и безопасность заземляющего провода должна быть проверена квалифицированным специалистом. Это очень опасно, если кабель заземления отсутствует или не подключен.

Защита от электростатического разряда

Статическое электричество может нанести ущерб компонентам системы. Для предотвращения статических повреждений, обеспечьте защиту тела до того, как прикоснуться к электронным компонентам, таким как микропроцессор. Для этого можно периодически прикасаться к металлической поверхности блока.
Можно также принять следующие шаги для предотвращения получения ущерба от электростатических разрядов (ESD):

1. При распаковке компонента, чувствительного к статическому электричеству, из картонной коробки, не стоит снимать с него антистатический упаковочный материал, не подготовившись к установке компонента в систему. Перед развертыванием антистатической упаковки убедитесь, что с тела снято статическое электричество.
2. При транспортировке чувствительного к статическому электричеству компонента сначала поместите его в антистатический контейнер или упаковку.
3. Работайте со всеми чувствительными компонентами в статически-безопасной зоне. По возможности, используйте антистатический коврик на полу и на рабочем месте оператора, а также антистатический ремень для запястья.

Раздел 1 – Введение

Коммутаторы серии xStack DES-3800

Коммутаторы серии DES-3800 относятся к семейству стекируемых коммутаторов D-Link xStack, которое включает в себя как коммутаторы, работающие на скоростях 10/100 Мбит/с, так и гигабитные решения. Коммутаторы семейства xStack обладают конкурентоспособными характеристиками, необходимой отказоустойчивостью, масштабируемостью, безопасностью и возможностью взаимодействия с продукцией других поставщиков.
Данное руководство описывает установку, эксплуатацию и настройку коммутаторов серии DES-3800, включающей в себя DES-3828, DES-3828P, DES-3828DC и DES-3852. Эти четыре коммутатора идентичны в настройках (за исключением настройки функции питания по Ethernet (PoE) для коммутатора DES-3828P и различного количества портов) и очень схожи по основным аппаратным средствам, соответственно большая часть информации в данном руководстве будет универсальной для всей группы коммутаторов. Соответствующие изображения на экране, возникающие при настройке через Web-интерфейс, будут представлены для одного из коммутаторов серии, однако пользователь без труда сможет выполнить аналогичные настройки и для других коммутаторов.
Также в данном руководстве будут даны примеры, разъяснения и состав оборудования для коммутаторов серии DES-3800.

Технология Gigabit Ethernet

Gigabit Ethernet – это расширение стандарта IEEE 802.3 Ethernet, использующее такую же структуру и формат пакета. Gigabit Ethernet поддерживает протокол CSMA/CD, режим полного дуплекса, управление потоком и объекты управления, но характеризуется десятикратным увеличением теоретической пропускной способности по сравнению с Fast Ethernet (100Мб/с) и стократным увеличением по сравнению с Ethernet (10 Мб/с). При этом переход от технологии Ethernet/Fast Ethernet к Gigabit Ethernet не требует дополнительных инвестиций в аппаратные средства, программное обеспечение и подготовку кадров.
Увеличенная скорость и расширенная пропускная способность, предоставляемые технологией Gigabit Ethernet, необходимы для пользователей, использующих более скоростные приложения, генерирующие большое количество трафика. Совершенствование основных компонентов, таких как магистраль и серверы, до Gigabit Ethernet может значительно улучшить производительность сети, а также увеличить скорость передачи данных между подсетями.
Применение Gigabit Ethernet позволяет реализовывать скоростные соединения по оптическому волокну для поддержки видеоконференции, систем формирования изображений и приложений, генерирующих большое количество трафика. Поскольку передача данных происходит в 10 раз быстрее, чем в технологии Fast Ethernet, серверы должны быть снабжены сетевыми адаптерами Gigabit Ethernet, которые способны выполнять в 10 раз больше операций за тот же период времени.

К тому же существенная полоса пропускания, предоставляемая Gigabit Ethernet, является экономически эффективным методом использования преимуществ данной технологии в рамках быстро развивающихся на сегодняшний день технологий коммутации и маршрутизации сетей.

Описание коммутатора

Коммутаторы серии DES-3800 снабжены портами под неэкранированную витую пару (UTP), обеспечивающими выделенную полосу пропускания 10 или 100 Мбит/с. Коммутатор оснащен 24 (для DES-3828, DES-3828P и DES-3828DC) или 48 (для DES-3852) портами 10/100Base-TX, поддерживающими автоматическое определение полярности MDI-X/MDI-II. Эти порты применяются для подключения ПК, принтеров, серверов, концентраторов, маршрутизаторов, коммутаторов и другого сетевого оборудования. Они могут быть использованы для подключения ПК, принтеров, серверов, концентраторов, маршрутизаторов, коммутаторов и другого сетевого оборудования. Данные порты на основе стандартной витой пары идеально подходят для сегментирования сетей на малые подсети для получения улучшенных характеристик. Каждый порт 10/100 Мбит/с может обеспечить пропускную способность до 200 Мбит/с в полнодуплексном режиме.
Кроме того, коммутатор снабжен двумя комбо-портами 1000Base-T/SFP, расположенными на передней панели устройства, и двумя портами 1000Base-T на задней панели. Гигабитные комбо-порты идеально подходят для подключения к серверу или магистрали сети. С различиями между гигабитными комбо-портами и портами, расположенными на задней панели, можно ознакомиться в главе «Порты».
Данный коммутатор позволяет реализовывать в сети некоторые из наиболее распространенных мультимедийных и видео приложений одновременно с другими пользовательскими приложениями без создания, так называемых, «узких мест». Встроенный интерфейс командной строки может быть использован для настройки приоритезации очередей, виртуальных локальных сетей (VLAN), групп агрегированных каналов, мониторинга по портам и скорости по портам.

Технические характеристики

- Агрегирование портов (LACP) согласно IEEE 802.3ad
- Управление доступом IEEE 802.1x на основе портов и MAC-адресов
- Поддержка VLAN IEEE 802.1Q
- Поддержка протоколов IEEE 802.1D Spanning Tree, IEEE 802.1W Rapid Spanning Tree and IEEE 802.1s
- Списки управления доступом (ACL)
- Управление через единый IP-адрес (SIM)
- Аутентификация с помощью TACACS, XTACACS and TACACS+
- Поддержка двух копий ПО (Dual Image)
- Протокол SNTP
- MAC Notification
- Асимметричные VLAN
- Просмотр использования системы и портов
- Журнал регистраций
- Настройки на базе портов
- Размер таблицы MAC-адресов 16K
- Буфер пакетов 32 Мбайт
- Группы VLAN на основе портов
- Гибкое агрегирование портов
- IGMP Snooping
- SNMP
- Secure Sockets Layer (SSL) и Secure Shell (SSH)
- Зеркалирование портов

• Управление доступом на основе Web
• Управление доступом на основе MAC-адресов
• Базы управляющей информации MIB для:
• RFC1213 MIB II
• RFC1493 Bridge
• RFC2819 RMON
• RFC2665 Ether-like MIB
• RFC2863 Interface MIB
• Private MIB
• RFC2674 for 802.1p
• IEEE 802.1x MIB
• Управление потоком в полнодуплексном режиме согласно IEEE 802.3x
• Приоритезация очередей IEEE 802.1p
• IEEE 802.3u 100BASE-TX
• Консольный порт RS-232 DCE для управления коммутатором
• Индикаторы, отображающие статус каждого порта
• IEEE 802.3 10BASE-T
• Высокопроизводительная коммутация, позволяющая осуществлять продвижение и фильтрацию пакетов со скоростью, соответствующей среде передачи: максимум 14 881 пакетов/с для каждого порта Ethernet 10Мбит/с, максимум 148 810 пакетов/с для каждого порта 100Мбит/с Fast Ethernet.
• Поддержка режимов полного и полудуплекса для соединений 10 и 100Мбит/с. В режиме полного дуплекса порт коммутатора может одновременно передавать и принимать данные. Этот режим используется для соединения с конечными станциями и коммутаторами, поддерживающими данный режим. Соединение с концентраторами должны осуществляться в режиме полудуплекса.
• Поддержка управления широковещательным штормом:
• Неблокирующая схема коммутации store and forward с автоматическим выбором скорости и протокола.
• Поддержка управления входящей / исходящей скоростью на основе портов.
• Эффективный механизм распознавания адресов и создания таблицы адресов

Порты

Коммутаторы оснащены 24 (для DES-3828, DES-3828P и DES-3828DC) или 48 (для DES-3852) портами 10/100Base-TX. Эти порты соответствуют следующим стандартам:

- IEEE 802.3
- IEEE 802.3u
- Поддержка полудуплексного/дуплексного режимов работ
- Все порты поддерживают автоматическое определение полярности MDI-X/MDI-II
- Метод «обратного давления» для управления потоком в полудуплексном режиме работы
- Управления потоком IEEE 802.3x в дуплексном режиме работы.

Примечание: Помимо указанных характеристик, все 24 порта 10/100BASE-TX коммутатора DES-3828P поддерживают также стандарт PoE (IEEE 802.3af).

Все коммутаторы серии DES-3800 снабжены двумя комбо-портами 1000Base-T/SFP на передней панели, которые поддерживают следующие стандарты:

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- Поддержка дуплексного режима работы

- Управление потоком IEEE 802.3x в дуплексном режиме работы.
- IEEE 802.3z

В SFP-порты коммутаторов данной серии могут быть установлены следующие трансиверы:

- DEM-310GT (1000 Base-LX)
- DEM-311GT (1000 Base-SX)
- DEM-314GT (1000 Base-LH)
- DEM-315GT (1000 Base-ZX)

На задней панели коммутатора расположены два порта 1000Base-T, которые выполнены в соответствии со следующими стандартами:

- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- Поддержка дуплексного режима работы
- Поддержка управления потоком IEEE 802.3x в дуплексном режиме работы

Примечание: Комбо-порты SFP нельзя одновременно использовать с соответствующими 1000Base-T портами. Если подключены оба порта (например, 25-й SFP-порт и 25-й порт 1000Base-T), SFP-порты будут иметь приоритет, и соответствующий порт 1000Base-T перейдет в неактивное состояние.

Компоненты передней панели

На передней панели коммутатора в моделях DES-3828, DES-3828P и DES-3828DC размещены 24 порта 10/100 Base-TX, в модели DES-3852 – 48 портов 10/100 Base-TX, два комбо-порта 1000 Base-T/SFP и консольный порт RS-232 (только для моделей DES-3828, DES-3828P и DES-3828DC). На коммутаторе DES-3828P также есть кнопка выбора режима Link/Act/State или PoE.

Рисунок 1.1 – Передняя панель коммутатора DES-3828

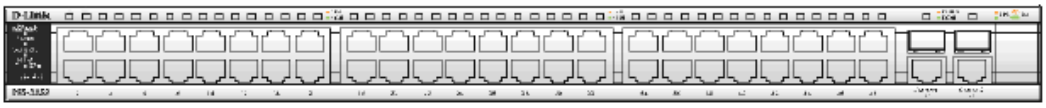


Рисунок 1.2 – Передняя панель коммутатора DES-3852

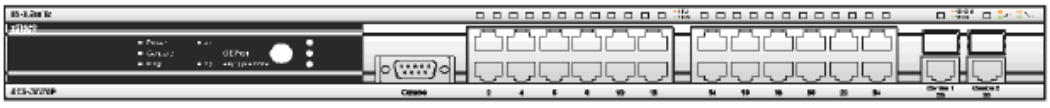


Рисунок 1.3 – Передняя панель коммутатора DES-3828P

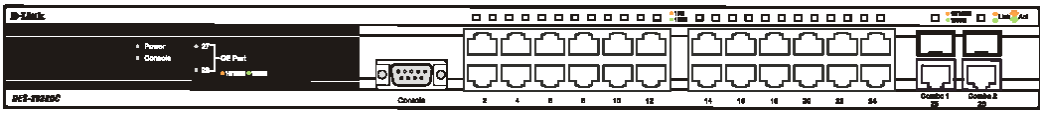


Рисунок 1.4 – Передняя панель коммутатора DES-3828DC

Светодиодные индикаторы коммутатора DES-3828P

Светодиодные индикаторы отображают состояние коммутатора и сети. На передней панели DES-3828P расположены светодиодные индикаторы питания, консоли, резервного блока питания RPS, 27-го и 28-го портов Gigabit Ethernet (GE), размещенных на задней панели, Link/Act/Speed, PoE, 24-х портов Ethernet 10/100 Мбит/с и двух комбо-портов 1000Base-T/SFP.

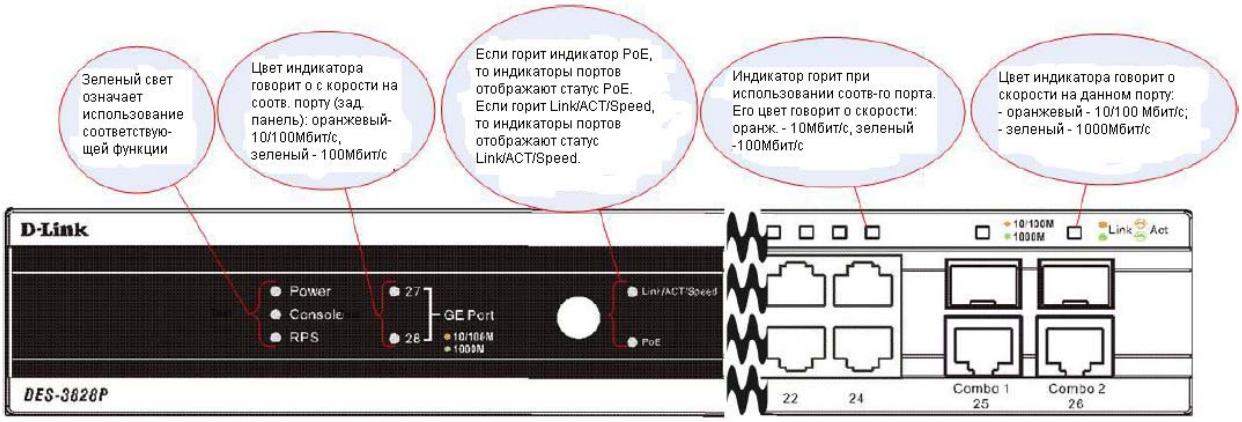


Рисунок 1.5 – Вид передней панели коммутатора DES-3828P

Светодиодные индикаторы коммутаторов DES-3828/DES-3828DC

На передней панели коммутаторов DES-3828/DES-3828DC есть светодиодные индикаторы питания, консоли, резервного блока питания RPS (только для модели DES-3828), 27-го и 28-го портов Gigabit Ethernet (GE), размещенных на задней панели, 24-х Ethernet портов 10/100 Мбит/с и двух комбо-портов 1000Base-T/SFP.

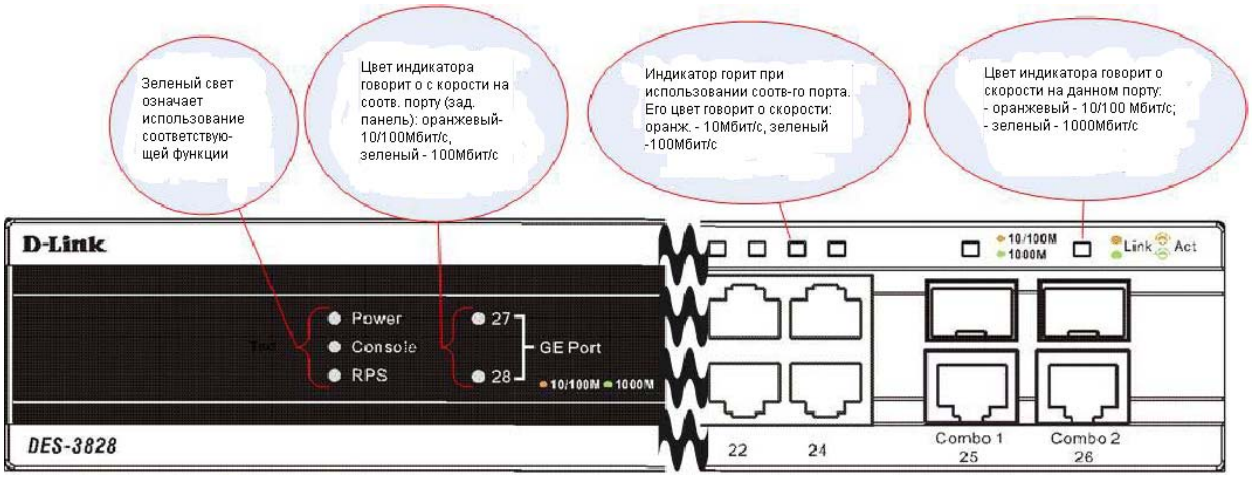


Рисунок 1.6 – Вид передней панели коммутатора DES-3828DC

Светодиодные индикаторы коммутатора DES-3852

На передней панели коммутаторов DES-3852 расположены светодиодные индикаторы питания, консоли, резервного блока питания RPS, 51-го и 52-го портов Gigabit Ethernet (GE), размещенных на задней панели, 48-ми портов Ethernet 10/100 Мбит/с и двух комбо-портов 1000Base-T/SFP.

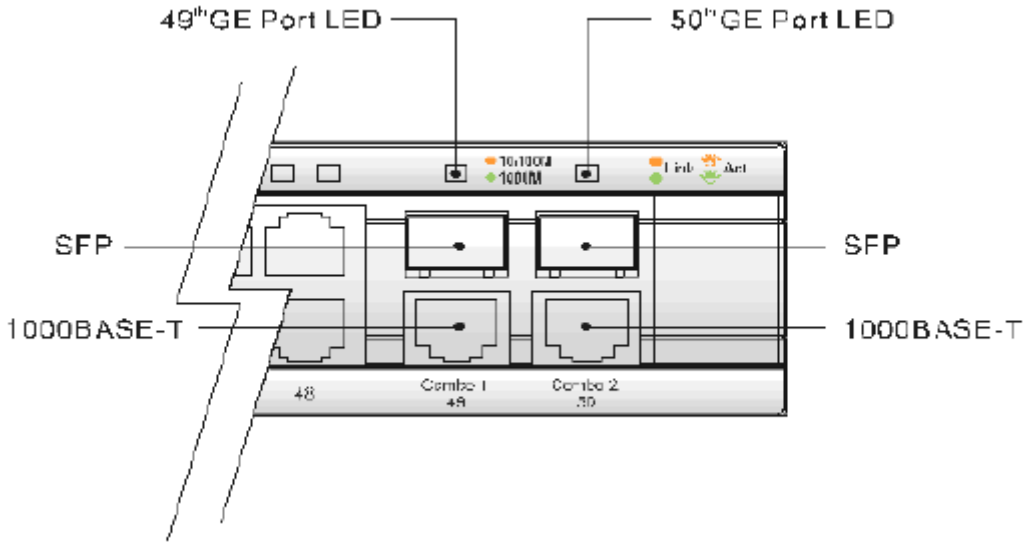


Рисунок 1.7 – Светодиодные индикаторы коммутатора DES-3852

В представленной ниже таблице дается описание индикаторов DES-3828/DES-3828P/DES-3828DC/DES-3852:

Светодиодный индикатор	**Описание**
Power	*Не горит* – питание отключено. *Постоянный зеленый свет* – питание включено.
Console	*Постоянный зеленый свет* – Индикатор будет гореть постоянным зеленым цветом в случае удаленного либо местного управления коммутатором через консольный порт RS-232 с помощью «прямого» последовательного кабеля. *Мигающий зеленый свет* – коммутатор находится в процессе самотестирования при включении питания Power-On Self Test (POST).
RPS (за исключением модели DES-3828DC)	*Не горит* – резервный блок питания отключен. *Постоянный зеленый цвет* – резервный блок питания включен.
27-й, 28-й порты GE (DES-3828/DES-3828P/DES-3828DC) **51-й, 52-й порты GE (DES-3852)**	Порты 27 и 28 (51 и 52) 1000Base-T расположены на задней панели коммутатора, значение индикации приводится ниже: ▪ *Постоянный зеленый свет* – соединение на скорости 1000 Мбит/с ▪ *Мигающий зеленый свет* – передача данных на скорости 1000 Мбит/с ▪ *Постоянный желтый свет* – соединение на скорости 100 Мбит/с ▪ *Мигающий желтый свет* – передача данных на скорости 1000 Мбит/с ▪ *Не горит* – отсутствие соединения.
Link/Act/Speed и PoE (только для модели DES-3828P)	Для того чтобы изменить режим работы светодиодного индикатора из состояния Link/Act/Speed в PoE и наоборот, нажмите кнопку LED Mode Select. Индикатор Link/Act/Speed будет гореть зеленым светом при включении данного режима и не гореть при выборе PoE. Точно так же при выборе Link/Act/Speed индикатор PoE гореть не будет, а будет гореть зеленым светом индикатор Link/Act/Speed.

Порты 1-24 (1-48)	Над каждым портом передней панели коммутатора располагается по индикатору, который отображает следующую информацию: Для режима Link/Act/Speed: ▪ *Постоянный зеленый свет* – соединение на скорости 100 Мбит/с ▪ *Мигающий зеленый свет* – передача данных на скорости 100 Мбит/с ▪ *Постоянный желтый свет* – соединение на скорости 10 Мбит/с ▪ *Мигающий желтый свет* – передача данных на скорости 10 Мбит/с ▪ *Не горит* – отсутствие соединения. *Для режима PoE (только для модели DES-3828P):* ▪ *Постоянный зеленый свет* – питание PoE (Обнаружено устройство PoE, совместимое с 802.3af) ▪ *Мигающий желтый свет* – может означать одно из следующих состояний: ошибка на порту PoE (обнаружено устройство, несовместимое со стандартом, поддерживающее старые спецификации; состояние недогрузки или перегрузки в соответствии со стандартом 802.3 af (ток меньше минимального тока I min или больше максимального I cut); проблемы в программном обеспечении; недостаточный запас питания; обнаружено короткое замыкание на порту питания; превышена допустимая температура на порту; последовательность состояний недогрузки и перегрузки может быть причиной отключения порта и т.д.) ▪ *Не горит* – отсутствие питания (устройство, поддерживающее PoE, не обнаружено, или отсутствует соединение)
25-й, 26-й комбо-порты GE (DES-3828/DES3828P/DES-3828DC) **49-й, 50-й комбо-порты GE (DES-3852)**	Порты 25 и 26 (49,50) являются комбо-портами 1000Base-T/SFP и располагаются на передней панели коммутатора. Соответствующие им индикаторы отображают следующую информацию: ▪ *Постоянный зеленый свет* – соединение на скорости 1000 Мбит/с ▪ *Мигающий зеленый свет* – передача данных на скорости 1000 Мбит/с ▪ *Постоянный желтый свет* – соединение на скорости 100 Мбит/с ▪ *Мигающий желтый свет* – передача данных на скорости 100 Мбит/с ▪ *Не горит* – отсутствие соединения.

Описание задней панели

Ниже приводится описание задних панелей каждой из моделей серии: DES-3828, DES-3828DC, DES-3828P и DES-3852.

DES-3828

На задней панели коммутатора DES-3828 находятся 27-й и 28-й порты 1000Base-T, разъем питания переменного тока и разъем для подключения внешнего резервного источника питания.

Рисунок 1.8 – Вид задней панели коммутатора DES-3828

Для получения более подробной информации по портам 27 и 28 обратитесь к главе «Порты», приведенной выше. На задней панели располагается разъем для подключения внешнего резервного источника питания (RPS). В случае пропадания питания немедленно заработает резервный источник питания. Разъем питания переменного тока представляет собой стандартный трехконтактный разъем под шнур питания. В данный разъем поместите один конец шнура питания с разъемом типа «мама», другой конец с разъемом типа «папа» вставьте в розетку. Коммутатор автоматически отрегулирует настройки питания под потребляемое напряжение в диапазоне 100 ~ 240 В переменного тока с частотой 50 ~ 60 Гц.

DES-3828P

На задней панели коммутатора DES-3828P находятся 27-й и 28-й порты 1000Base-T, теплоотвод, разъем питания переменного тока и разъем для подключения внешнего резервного источника питания.

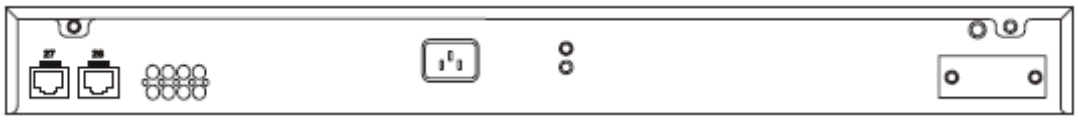


Рисунок 1.9 – Вид задней панели коммутатора DES-3828P

На задней панели расположены вентиляционные отверстия для системного вентилятора, который используется для рассеивания тепла. Не закрывайте эти отверстия и оставьте по 6 дюймов (1 дюйм = 2,54 см, 6 дюймов = 15,24 см) свободного пространства вокруг задней панели коммутатора. Без правильно организованного рассеивания тепла и циркуляции воздуха, системные компоненты могут перегреться, что, в свою очередь, может привести к нарушению работы устройства. На задней панели устройства также располагается разъем для внешнего резервного источника питания. В случае пропадания питания немедленно заработает резервный источник питания. Разъем питания переменного тока представляет собой стандартный трехконтактный разъем под шнур питания. В данный разъем поместите один конец шнура питания с разъемом типа «мама», другой конец с разъемом типа «папа» вставьте в розетку. Коммутатор автоматически отрегулирует настройки питания под потребляемое напряжение в диапазоне 100 ~ 240 В переменного тока с частотой 50 ~ 60 Гц. Максимальная мощность нагрузки для питания поверх Ethernet (PoE) 370 Вт. Установленная по умолчанию мощность PoE - 15,4 Вт на порт. Эта настройка может быть изменена в диапазоне от 1 Вт до 16,8 Вт на порт. Для изменений настроек PoE обратитесь к инструкциям в разделе 6.

DES-3828DC

Рисунок 1.10 – Вид задней панели коммутатора DES-3828DC

На задней панели коммутатора DES-3828DC находятся 27-й и 28-й порты 1000Base-T. Помимо этого на задней панели также располагаются клеммы, позволяющие подключить питание постоянного тока. Для получения более подробной информации по установке обратитесь к разделу 2.

DES-3852

На задней панели коммутатора DES-3852 находятся 51-й и 52-й порты 1000Base-TX, разъем питания переменного тока, консольный порт RS-232 и разъем для подключения внешнего резервного источника питания.

Рисунок 1.11 – Вид задней панели коммутатора DES-3852

Описание боковых панелей

На правой и левой боковых панелях коммутатора находятся вентилятор и вентиляционные отверстия. Вентиляторы используются для рассеивания тепла. Не закрывайте эти отверстия и оставьте по 6 дюймов (1 дюйм = 2,54 см, 6 дюймов = 15,24 см) свободного пространства вокруг задней и боковых панелей коммутатора. Напоминаем, что без правильно организованного теплового рассеивания и циркуляции воздуха, системные компоненты могут перегреться, что, в свою очередь, может привести к нарушению работы устройства.

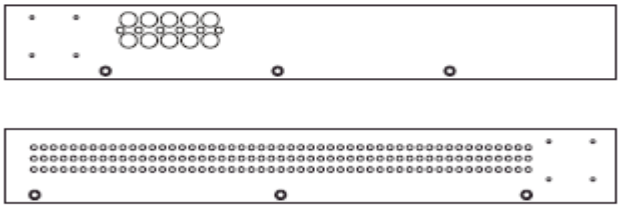


Рисунок 1.12 – Вид боковых панелей

Гигабитные порты

В дополнение к 24 портам (48 портам в модели DES-3852) 10/100 Мбит/с коммутатор также оснащен двумя гигабитными комбо-портами 1000Base-T/SFP, расположенными на передней панели, и двумя портами 1000BASE-T, выполненными под медную витую пару и расположенными на задней панели. На представленном ниже рисунке показаны 25-й и 26-й (49-й

и 50-й) гигабитные порты в правой части передней панели. 27-й и 28-й (51-й и 52-й)гигабитные порты располагаются в левой части задней панели. Пожалуйста, обратите внимание, что гигабитные порты не поддерживают PoE.

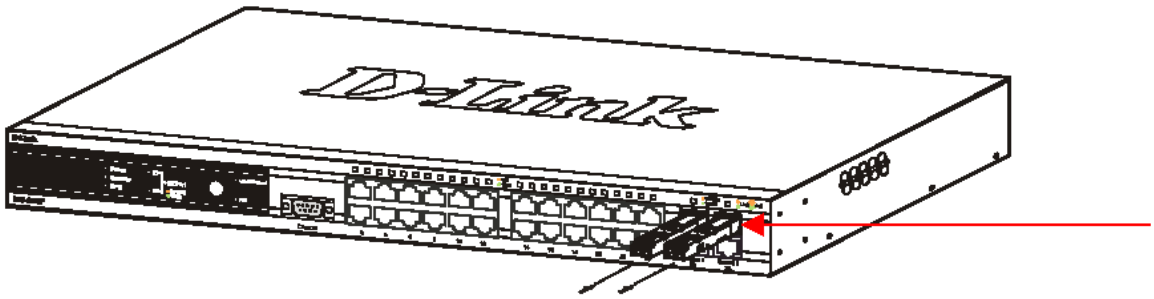


Рисунок 1.13 – Порты Mini-GBIC (SFP) на передней панели

Раздел 2 - Установка

Комплект поставки

Откройте коробку, в которой поставляется коммутатор, и аккуратно распакуйте содержимое. В коробке должно быть следующее:

- Один автономный коммутатор
- Один шнур питания переменного тока (за исключением модели DES-3828DC)
- Данное руководство пользователя на CD-диске
- Набор для крепления в стойку (петли и винты)
- Четыре резиновые «ножки» с одной клейкой стороной
- RS-232 консольный шнур

Если какая-либо из перечисленных составляющих повреждена или отсутствует, пожалуйста, свяжитесь с партнером D-Link для замены.

Перед началом работы

Местоположение коммутатора может значительно влиять на его характеристики. Пожалуйста, при установке коммутатора следуйте данным рекомендациям.

- Установите коммутатор на прочную горизонтальную поверхность, которая может выдержать, по крайней мере, 4,24 кг для моделей DES-3828/DES-3828DC/DES-3852 или 6,02 кг для модели DES-3828P. Не помещайте тяжелые предметы на коммутатор.
- Электрическая розетка должна быть не далее 1,82 м от коммутатора.
- Визуально осмотрите шнур питания и проверьте, чтобы он был плотно закреплен в разъеме питания переменного/постоянного тока.
- Убедитесь, что существует надлежащий теплоотвод и соответствующая вентиляция вокруг коммутатора. Оставьте по 10 см свободного пространства перед передней и задней панелью коммутатора.
- Установите коммутатор в довольно прохладном и сухом месте с допустимым рабочим диапазоном температур и влажности.
- Установите коммутатор таким образом, чтобы избежать воздействия на устройство источников сильного электромагнитного поля, вибрации, пыли и прямых солнечных лучей.
- Когда будете устанавливать коммутатор на горизонтальную поверхность, прикрепите прилагаемые резиновые «ножки» на основание устройства. Резиновые «ножки» коммутатора предохранят корпус от царапин.

Настольное размещение коммутатора

Прежде чем установить коммутатор на стол или полку, прикрепите прилагающиеся к коммутатору резиновые амортизационные «ножки» на каждый угол основания устройства. Обеспечьте устройству надлежащий теплоотвод.

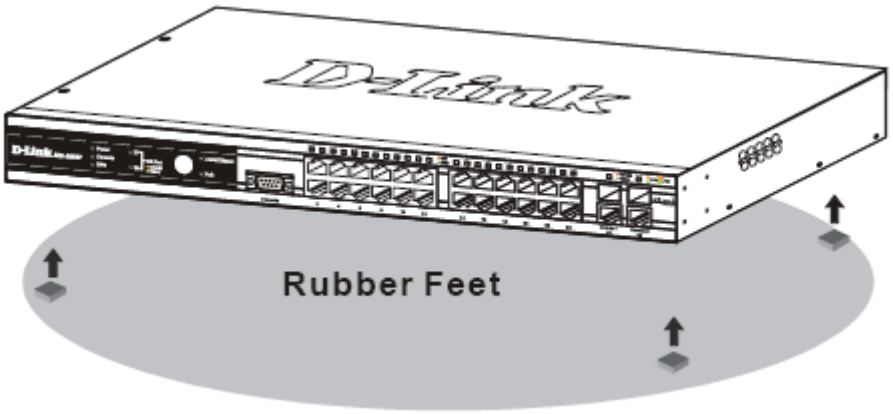


Рисунок 2.1 – Подготовка коммутатора к установке на стол или полку

Монтаж коммутатора в стойку

Кроме настольного размещения, рассмотренного в предыдущей главе Руководства, коммутатор может также устанавливаться в стандартную 19'' стойку. Используйте следующие рисунки в качестве руководства.

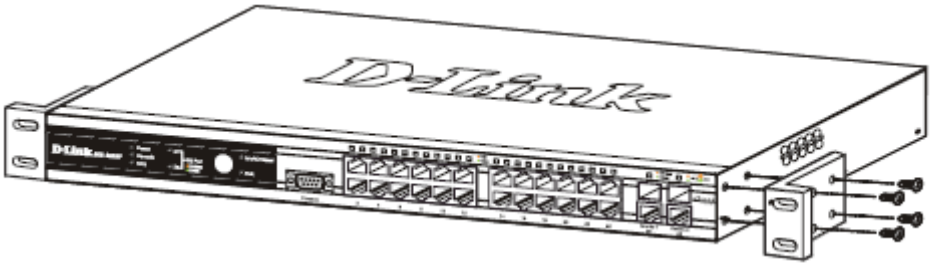


Рисунок 2.2 – Прикрепление петлей к коммутатору

Прикрепите петли к коммутатору с помощью прилагающихся винтов. Прикрепив входящие в комплект поставки петли, установите коммутатор в стандартную стойку, как это показано ниже на рисунке 2.3.

Монтаж коммутатора в стандартную 19'' стойку

Предупреждение: Установка оборудования в стойку без передних и боковых стабилизаторов может привести к опрокидыванию стойки, что в свою очередь может закончиться, при определенных обстоятельствах, телесными повреждениями. Таким образом, всегда устанавливайте стабилизаторы до инсталляции устройств в стойку. После установки оборудования в стойку не вынимайте из стойки более одного устройства, поскольку это может привести к опрокидыванию стойки и нанесению телесных повреждений.

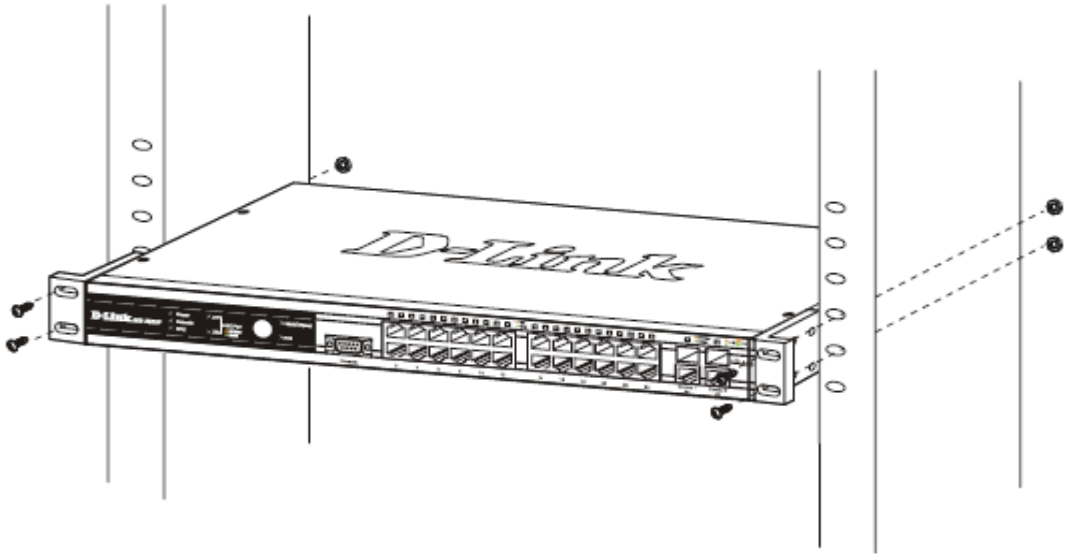


Рисунок 2.3 – Монтаж коммутатора в стойку

Включение электропитания переменным током

Один конец шнура питания вставьте в разъем питания коммутатора, а другой конец в гнездо ближайшей розетки. Сразу же после включения коммутатора замигают светодиодные индикаторы. Подобное мигание означает установку системы в исходное состояние.

Отключение электричества

В целях с блока питания переменного тока, в случае отключения электричества, отключите коммутатор от сети. Когда питание будет возобновлено, снова подключите коммутатор.

Подключение DES-3828DC к источнику постоянного тока

Для подключения DES-3828DC к источнику постоянного тока, следуйте приведенным ниже рекомендациям.

Рисунок 2.4 – Подключение коммутатора к источнику постоянного тока

1. Подключите внешний блок питания постоянного тока к коммутатору, как показано на рисунке 2.4.
   - Отрицательный полюс (-) подключается к контакту **-48V.**
   - Положительный полюс (+) подключается к контакту **-48V Return.**
   - Заземление может быть подключено к центральной клемме.
2. Убедитесь, что винты плотно затянуты.

Установка резервного источника питания

Для подключения резервного источника питания к коммутатору следуйте приведенным ниже рекомендациям (DPS-200 к моделям DES-3828/DES-3852 или DPS-600 к DES-3828P). Резервный источник питания DPS-200 соответствует всем требованиям по напряжению для перечисленных моделей коммутаторов DES-3828/DES-3852. DPS-200 можно установить в шасси для резервных источников питания DPS-900 или DPS-800.

Предупреждение: Прежде чем приступить к установке DPS-200, шнур питания переменного тока нужно отсоединить.

DPS-900

DPS-900 – это шасси стандартного размера для монтирования в стойку (5U в высоту), предназначенное для размещения 8 резервных источников питания DPS-200.

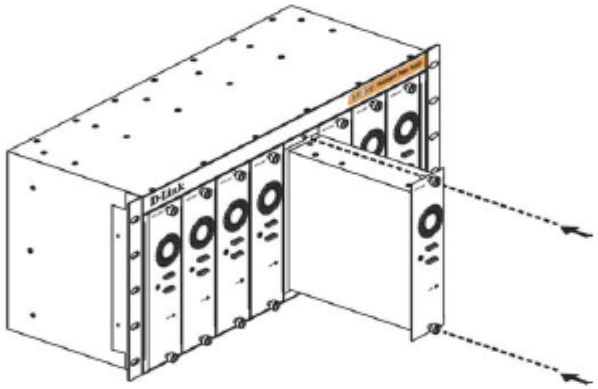


Рисунок 2.5 – Установка DPS-200 в шасси DPS-900

Для монтирования шасси для резервных источников питания в стандартную 19” стойку воспользуйтесь следующими рисунками:

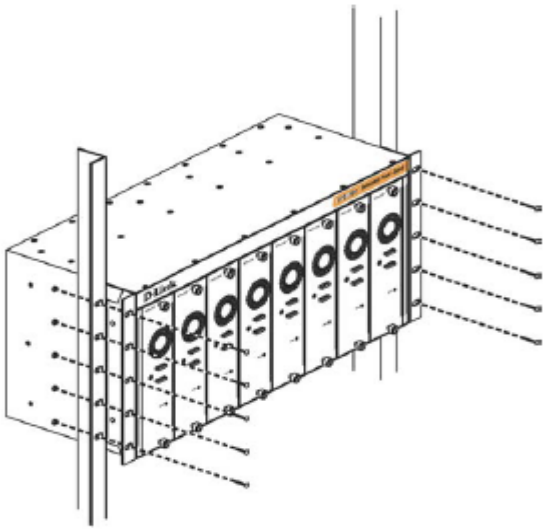


Рисунок 2.6 – Установка DPS-900 в стойку

Предупреждение: Установка оборудования в стойку без передних и боковых стабилизаторов может привести к опрокидыванию стойки, что в свою очередь может закончиться, при определенных обстоятельствах, телесными повреждениями. Таким образом, всегда устанавливайте стабилизаторы до инсталляции устройств в стойку. После установки оборудования в стойку, не вынимайте из стойки более одного устройства, поскольку это может привести к опрокидыванию стойки и нанесению повреждений.

DPS-800

DPS-800 – это шасси стандартного размера для монтирования в стойку (1U в высоту), предназначенное для размещения двух резервных источников питания DPS-200.

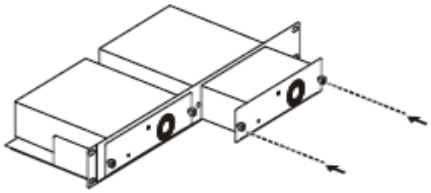


Рисунок 2.7 – Установка DPS-200 в шасси DPS-800

Для монтирования шасси для резервных источников питания в стандартную 19” стойку воспользуйтесь следующими рисунками:

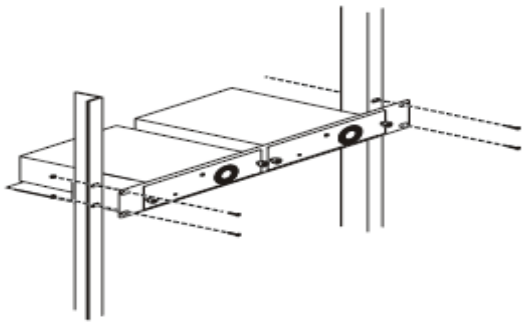


Рисунок 2.6 – Установка DPS-800 в стойку

Подключение к резервному источнику питания

Резервный источник питания DPS-200 подключается к коммутатору-мастеру с помощью 14-ти контактного кабеля питания постоянного тока. Обычно подключение резервного источника питания к основному источнику электропитания осуществляется с помощью трехконтактного кабеля питания переменного тока.

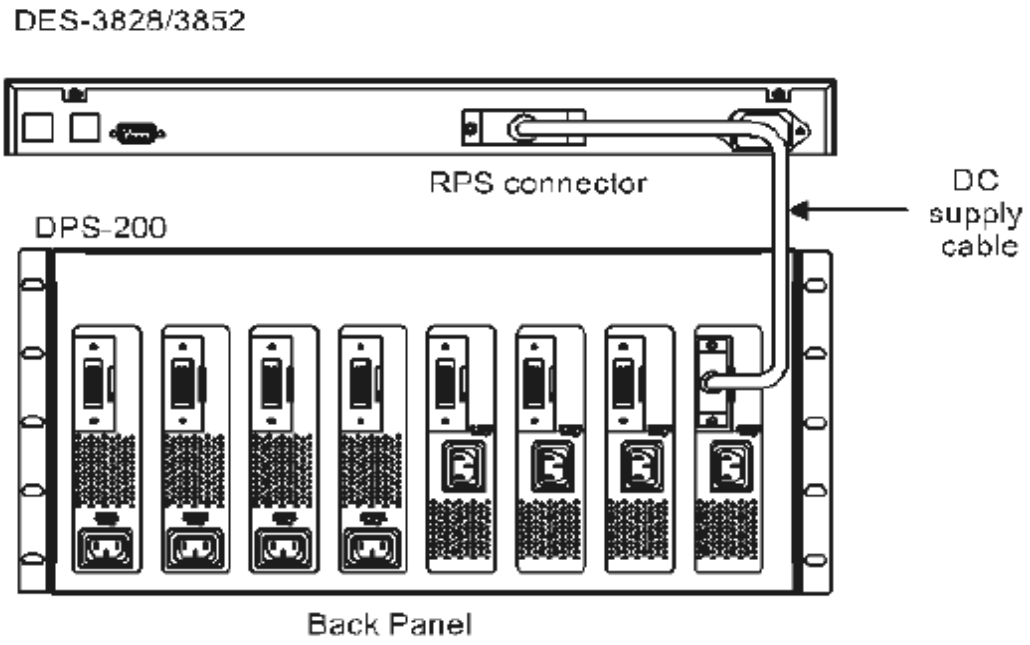


Рисунок 2.9 – Коммутатор DES-3828, подключенный к резервному источнику питания

1. Вставьте один конец 14-ти контактного кабеля в гнездо на коммутаторе, другой - в резервный источник питания.

2. Используйте стандартный кабель питания переменного тока для подключения резервного источника питания к основному источнику электропитания переменного тока. Горящий зеленый светодиодный индикатор на передней панели DPS-200 будет свидетельствовать об успешном подключении.

3. Переподключите коммутатор к источнику питания переменного тока. На определенных коммутаторах, таких как DES-3828, светодиодный индикатор будет отображать, что резервный источник питания находится в работе.

4. Для данной установки не требуется внесения изменений в настройках коммутатора.

Примечание: Для получения более подробной информации обратитесь к документации DPS-200.

Предупреждение: Не используйте коммутатор с иными резервными источниками питания, кроме DPS-200 или DPS-600.

DPS-600

Коммутатор DES-3828P может работать с внешним резервным источником питания DPS-600.

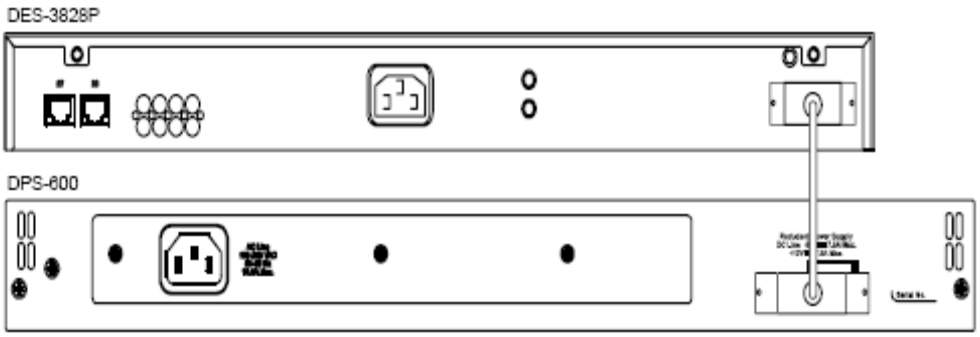


Рисунок 2.10 – Коммутатор DES-3828P, подключенный к внешнему резервному источнику питания DPS-600

Раздел 3 – Подключение коммутатора

Подключение коммутатора к конечному узлу

Подключение коммутатора к концентратору или коммутатору

Подключение коммутатора к магистрали сети или серверу

Примечание: Все 24 (48 для DES-3852) высокопроизводительных порта NWay Ethernet могут поддерживать как MDI-II, так и MDI-X соединения.

Подключение коммутатора к конечному узлу

Под конечным узлом подразумевается персональный компьютер ПК (PC) с 10, 100 или 1000 Мбит/с с сетевыми адаптерами Ethernet/Fast Ethernet с разъемом RJ-45, а также большинство маршрутизаторов. Конечный узел может быть подключен к любому порту коммутатора по витой паре категории 3, 4 или 5 UTP/STP-кабеля.

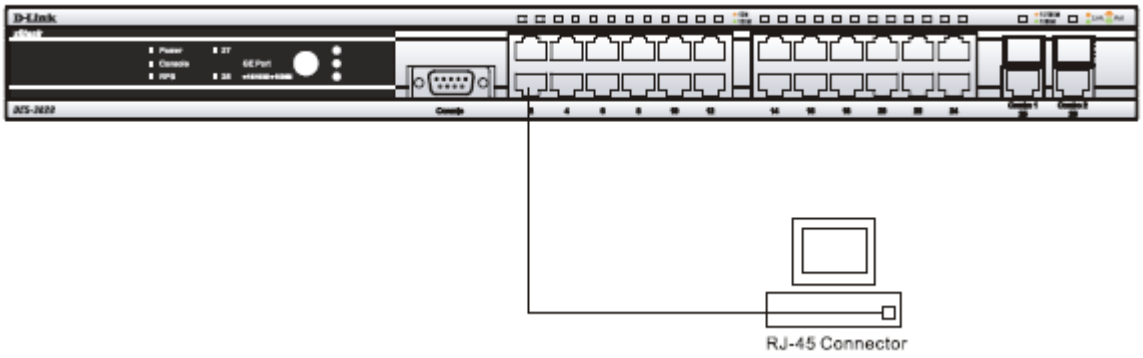


Рисунок 3.1 – Подключение коммутатора к конечному узлу

Светодиодный индикатор Link/Act для каждого UTP порта в случае надежного соединения будет гореть зеленым или желтым светом. Мигающие светодиоды свидетельствуют об активности на порту.

Подключение коммутатора к концентратору или коммутатору

Данные подключения могут быть выполнены различными способами с помощью обыкновенного кабеля.

- 10Base-T концентратор или коммутатор может быть подключен к коммутатору по витой паре категории 3, 4 или 5 неэкранированного/экранированного (UTP/STP) кабеля.
- 100Base-TX концентратор или коммутатор может быть подключен к коммутатору по витой паре 5 категории неэкранированного/экранированного (UTP/STP) кабеля.
- 1000Base-T коммутатор может быть подключен к коммутатору по витой паре категории 5e неэкранированного/экранированного (UTP/STP) кабеля.
- Коммутатор, поддерживающий организацию волоконно-оптического высокоскоростного канала, можно подключить к порту SFP соответственно по волоконно-оптическому кабелю.

- У коммутатора можно изменить режим питания на PoE, используя кнопку выбора режима Mode Select. В режиме питания PoE коммутатор DES-3828P будет работать со всеми устройствами D-Link, работающими по стандарту 802.3af . Коммутатор может также работать в режиме PoE со всем оборудованием D-Link, не совместимым с 802.3af, беспроводными точками доступа, IP-камерами и IP-телефонами через DWL-P50.

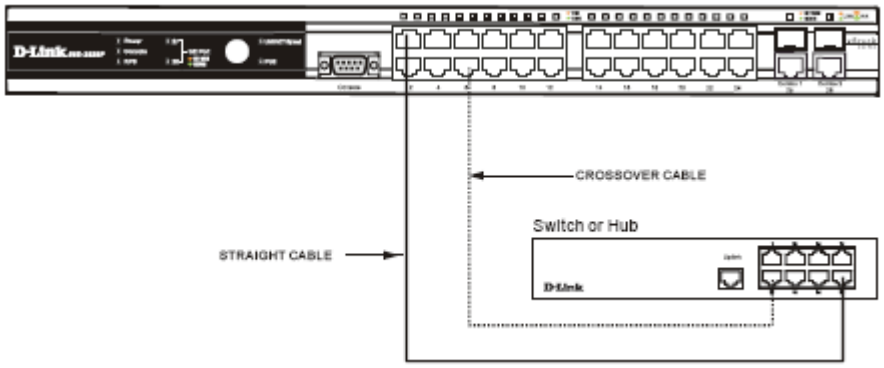


Рисунок 3.2 – Коммутатор, подключенный к обыкновенному (не Uplink) порту концентратора или коммутатора с помощью прямого или кроссового кабеля

Предупреждение: Когда SFP передатчик установит соединение, связанный с ним порт 10/100/1000Base-T отключится.

Подключение коммутатора к магистрали сети или серверу

Два комбо-порта Mini–GBIC идеально подходят для uplink-подключения к магистрали сети или серверу. Медные порты работают на скоростях 1000, 100 или 10 Мбит/с в дуплексном режиме. Порты, выполненные под волоконно-оптический кабель, могут работать на скорости 1000 Мбит/с в дуплексном режиме. Подключения к портам Gigabit Ethernet осуществляются в зависимости от типа порта по волоконно-оптическому кабелю или по медному кабелю категории 5. Свечение индикатора Link свидетельствует о правильном подключении.

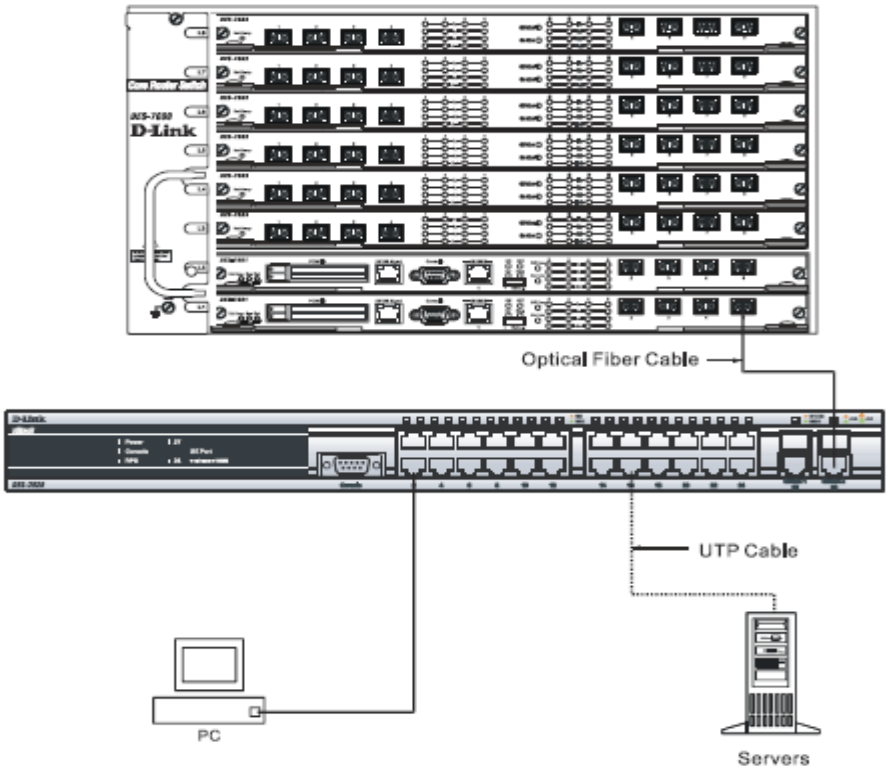


Рисунок 3.3 – Организация uplink – подключения коммутатора к серверу, PC или к стеку коммутаторов.

Раздел 4 - Введение в управление коммутатором

Функции управления

Коммутатором можно управлять удаленно через консольный порт на передней панели, либо локально, используя Telnet. Пользователь также может управлять коммутатором через Web-интерфейс посредством Web-браузера.

Web-интерфейс управления

После успешной установки коммутатора, вы можете настраивать его, проверять по светодиодам на панели и графически отображать статистику, используя Web-браузер, например, Netscape Navigator (версии 6.2 и выше) или Microsoft Internet Explorer (версия 5.0).

Управление через SNMP- протокол

Вы также управлять коммутатором с помощью консольной программы, совместимой с SNMP-протоколом. Коммутатор поддерживает SNMP версии 1.0, 2.0 и 3.0. SNMP-агент декодирует входящие SNMP-сообщения и отвечает на запросы объектов базы управляющей информацией MIB, сохраненных в базе данных. SNMP-агент обновляет объекты MIB для формирования статистики и счетчиков.

Подключение к консольному порту коммутатора (RS-232 DCE)

Коммутатор снабжен последовательным RS-232 портом, с помощью которого можно осуществить подключение к компьютеру или терминалу для контроля и настройки коммутатора. Данный порт – это коннектор DB-9 типа «мама», выполненный для подключения терминального оборудования (DTE – Data Terminal Equipment).

Для использования консольного порта вам понадобится следующее оборудование:

- Терминал или компьютер с двумя последовательными портами и возможностью эмуляции терминала.
- Нуль-модем или кроссовый кабель RS-232 с коннектором DB-9 типа «мама» для консольного порта коммутатора.

Для подключения терминала к консольному порту:

1. Подключите кабель RS-232 с коннектором типа «мама» к консольному порту коммутатора и плотно закрутите винты.
2. Подключите другой конец кабеля к терминалу или последовательному порту компьютера. Установите программное обеспечение эмулятора терминала следующим образом:

3. Выберите подходящий последовательный порт (COM порт 1 или COM порт 2).
4. Установите скорость передачи данных 9600 бод.
5. Установите формат данных: 8 бит данных; 1 стоповый бит и отсутствие контроля по четности.
6. Установите отсутствие управление потоком.
7. В свойствах выберите VT 100 (for Emulation mode) для запуска эмуляционного режима.
8. Выберите клавиши терминала для Function, Arrow и Ctrl клавиш. Необходимо обеспечить выбор клавиш терминала (а не клавиш Windows).

Примечание: Когда вы будете использовать HyperTerminal с операционной системой Microsoft® Windows® 2000, убедитесь, пожалуйста, что у вас установлен Windows 2000 Service Pack 2 или более поздняя версия. Windows 2000 Service Pack 2 позволяет использовать клавиши со стрелками в эмуляторе HyperTerminal VT100. Зайдите на сайт www.microsoft.com для получения информации по Windows 2000 Service Pack.

9. После того, как вы правильно установили терминал, вставьте шнур питания в гнездо питания на задней панели коммутатора. На терминале отобразится начальная последовательность загрузки.
10. После того, как завершится загрузка последовательности, появится окно console login.
11. Если вы еще не зарегистрировались в программе интерфейса командной строки (CLI), нажмите клавишу Enter в полях имя пользователя (User name) и пароль (Password), т.к. они не заданы по умолчанию. Администратор, прежде всего, должен создать имя пользователя и пароль. Если вы ранее установили учетные записи пользователей, зарегистрируйтесь и продолжайте настраивать коммутатор.
12. Введите команды для выполнения требуемых задач. Многие команды требуют привилегии доступа уровня администратора. Прочитайте следующий раздел для получения информации по настройке учетных записей пользователей. В документации на CD-диске просмотрите ***Справочное руководство по интерфейсу командной строки CLI для коммутаторов серии xStack DES-3800***, где приведен список всех команд и дополнительная информация по использованию CLI.
13. После того, как вы выполните ваши задачи, закройте сессию с помощью команды завершения сеанса или закройте программу эмулятора.
14. Убедитесь, что терминал или ПК, который вы используете для подключения, настроен в соответствии с данными настройками.

Если у вас возникли проблемы с созданием данного соединения на ПК, проверьте правильность установки в свойствах VT-100.

Вы можете установить режим эмуляции, нажав в окне Hyper Terminal **File ⇨ Properties ⇨ Settings ⇨ Emulation.** Если вы не заметили никаких изменений, попытайтесь перезапустить коммутатор, отключив питание.

После подключения к консоли появится представленный ниже экран. В нем пользователь будет вводить команды для выполнения всех доступных функций управления. Коммутатор попросит пользователя ввести имя пользователя и пароль. При первоначальном соединении нет имени пользователя и пароля, таким образом, для доступа к интерфейсу типа командной строки необходимо будет дважды нажать Enter.

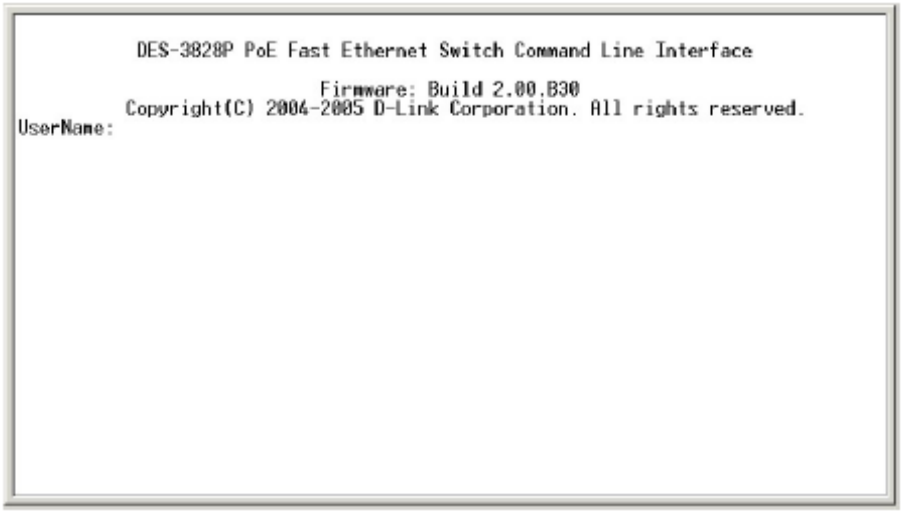


Рисунок 4.1 – Исходный экран при первом соединении

Первое подключение к коммутатору

Коммутатор обеспечивает безопасность, основанную на имени пользователя, что позволяет предотвратить доступ неавторизованных пользователей к коммутатору и изменению его настроек. В данном пункте описывается, как зарегистрироваться на коммутаторе.

Примечание: Пароли, используемые для доступа к коммутатору, зависят от регистра клавиатуры, таким образом, знак «S» не является идентичным знаку «s».

Во время первого подключения к коммутатору появится регистрационное окно.

Примечание: Нажмите Ctrl+R для обновления экрана. Данная команда может быть использована в любое время для перезагрузки консольной программы в коммутаторе и обновления консольного экрана.

Нажмите Enter в обоих полях Username (Имя пользователя) и Password (Пароль). Вы получите доступ к командной строке **DES-3828:4#,** как это показано ниже.

Начального имени пользователя или пароля нет. Оставьте поля Username (Имя пользователя) и Password (Пароль) пустыми.

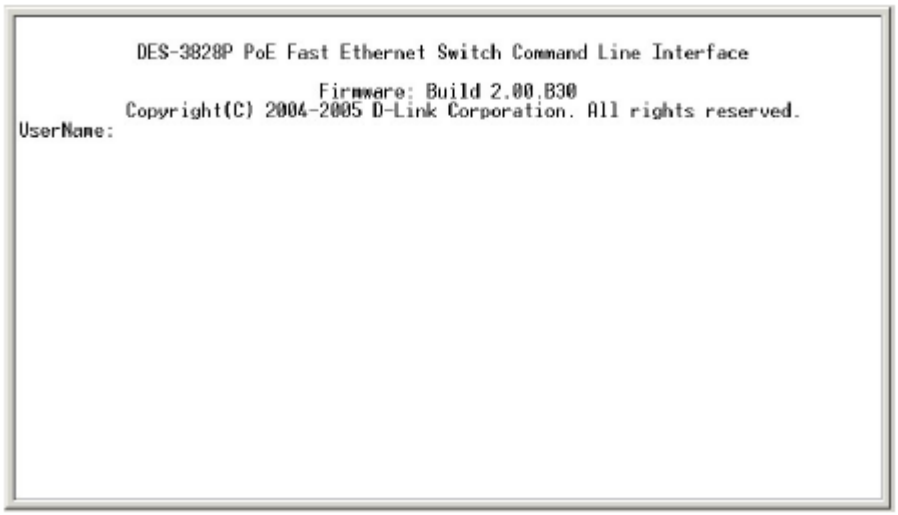


Рисунок 4.2 – Командная строка

Примечание: Первый пользователь автоматически получает права уровня администратора. Рекомендуется создать одну учетную запись пользователя уровня администратора для коммутатора.

Защита паролем

Коммутатор не имеет по умолчанию имени пользователя и пароля. Одной из первых задач при настройке коммутатора является создание учетных записей пользователей. Если вы зарегистрировались, используя предписанное имя пользователя уровня администратора, то у вас будет привилегированный доступ к программному обеспечению коммутатора.
После первоначальной регистрации создайте новые пароли для каждого имени пользователя для предотвращения доступа к коммутатору неавторизованных пользователей и запишите пароли.

Для создания в коммутаторе учетной записи уровня администратора, выполните следующее:

- В командной строке CLI введите **create account admin**, после чего укажите имя пользователя <*user name*> и нажмите клавишу Enter.
- Вас попросят ввести пароль. Введите <*password*> , использованный для созданной учетной записи администратора, и нажмите клавишу Enter.
- Для подтверждения пароля вас попросят ввести его еще раз. Введите тот же пароль и нажмите клавишу Enter.
- Удачное создание новой учетной записи администратора будет подтверждено сообщением **Success**.

Примечание: Пароли зависят от положения регистра. Длина имени пользователя и пароля может быть до 15 символов.

Ниже приведенный пример иллюстрирует удачное создание новой учетной записи уровня администратора с именем пользователя «newmanager».

```
DES-3800:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:********
Enter the new password again for confirmation:********

Success.

DES-3800:4#
```

Примечание: Изменение настроек коммутатора при помощи CLI лишь модифицирует текущую конфигурацию и не сохраняет ее при перезагрузке коммутатора. Для того чтобы настройки не терялись при перезагрузке коммутатора, используйте команду **Save,** сохраняющую текущую конфигурацию в энергонезависимой памяти.

Настройки SNMP

Простой протокол сетевого управления Simple Network Management Protocol (SNMP) – протокол седьмого уровня (уровень приложений) семиуровневой модели OSI, созданный специально для управления и контроля сетевого оборудования. SNMP дает возможность станциям управления сетью читать и изменять настройки шлюзов, маршрутизаторов, коммутаторов и других сетевых устройств. Используйте SNMP для настройки системных характеристик для правильной работы, контроля характеристик и обнаружения потенциальных проблем в коммутаторе, группе коммутаторов или сети.

Управляемые устройства поддерживают программное обеспечение SNMP (называемое агентом), работающее локально на оборудовании. Определенный набор управляемых объектов обслуживается SNMP и используется для управления устройством. Эти объекты определены в базе данных управляющей информации MIB (Management Information Base), которая обеспечивает стандартное представление информации, контролируемое встроенным SNMP-агентом. Протокол SNMP определяет оба формата спецификаций MIB и используется для доступа к информации по сети.

Коммутаторы серии DES-3800 поддерживают протокол SNMP версий: 1, 2c и 3. Можно указать, какую версию SNMP использовать для контроля и управления коммутатором. Три версии SNMP протокола различаются в уровне обеспечиваемой безопасности между управляющей станцией и сетевым оборудованием.

В SNMP версиях v.1 и v.2 аутентификация пользователей осуществляется при помощи так называемой «строки сообщества» («community string»), данная функция похожа на пароли. Удаленный пользователь приложения SNMP и коммутатора должен использовать одну и ту же community string. Пакеты SNMP от станций, не прошедших аутентификацию будут игнорироваться (удаляться).

По умолчанию community strings для коммутатора, использующего версии v.1 и v.2 протокола SNMP, следующие:

- **public –** позволяет авторизованным станциям управления извлекать объекты MIB.
- **private –** позволяет авторизованным станциям управления извлекать и изменять объекты MIB.

SNMP версии v.3 использует более сложный процесс, который подразделяется на два этапа. Первая часть – это сохранение списка пользователей и их свойств, которые позволяют работать SNMP-менеджеру. Вторая часть описывает, что каждый пользователь из списка может делать в качестве SNMP-менеджера.

Коммутатор разрешает заносить в список и настраивать группы пользователей с определенным набором привилегий. Можно также устанавливать различные версии SNMP для занесенной в список группы SNMP-менеджеров. Таким образом, можно создать группу SNMP-менеджеров, которым разрешено просматривать информацию только в режиме чтения или получать запросы, используя SNMP v.1, в то время как другой группе можно назначить более высокий уровень безопасности и дать привилегию чтения/записи, используя SNMP v3.
Индивидуальным пользователям и группам SNMP-менеджеров, использующим SNMP v.3, может быть разрешено или ограничено выполнение определенных функций управления SNMP. Функции «разрешено» или «запрещено» определяются идентификатором объекта (OID – Object Identifier), связанного со специальной базой MIB. Дополнительный уровень безопасности доступен в SNMP v.3, в данной версии SNMP сообщения могут быть зашифрованы. Для получения дополнительной информации по настройке SNMP v.3 в коммутаторе, прочитайте раздел под названием Управление.

Traps

«Traps» - это аварийные сообщения, сообщающие о событиях, происходящих в коммутаторе. События могут быть такими серьезными, как перезапуск (кто-нибудь случайно выключил коммутатор) или менее, как например, изменение статуса порта. Коммутатор создает сообщения «traps» и отправляет их к «trap» получателю (или сетевому менеджеру). Обычные «traps» содержат сообщение об ошибке аутентификации Authentication Failure, изменении топологии сети Topology Change и широковещательном шторме Broadcast\Multicast Storm.

Базы управляющей информации MIB

Коммутатор хранит в базе управляющей информации MIB управляющую информацию и значения счетчика. Коммутатор использует стандартный модуль MIB-II. В результате, значения объектов MIB могут быть извлечены из любого сетевого управляющего программного обеспечения, основанного на проколе SNMP. Помимо стандартной базы MIB-II, коммутатор также поддерживает свою собственную базу MIB, в качестве расширенной базы данных управляющей информации. Определив идентификатор объекта MIB, можно также извлечь собственную базу данных MIB. Значения MIB можно либо только читать, либо читать-записывать.

Назначение IP-адреса

Каждому коммутатору должен быть назначен свой собственный IP-адрес, который используется для связи с сетевым менеджером SNMP или другим приложением TCP/IP (например, BOOTP, TFTP). IP-адрес коммутатора по умолчанию 10.90.90.90.
Коммутатору также назначен уникальный заводской MAC-адрес. Данный MAC-адрес не может быть изменен, посмотреть его можно с помощью ввода команды «show switch» через интерфейс командной строки, как это показано ниже:

Рисунок 4.3 – Демонстрация команды

MAC-адрес коммутатора можно также найти через управляющую Web-программу в окне **Switch Information (Basic Settings)** в меню **Configuration.**
IP-адрес коммутатора должен быть установлен до момента управления коммутатором с помощью web-менеджера. IP-адрес коммутатора можно автоматически установить, используя BOOTP или DHCP протоколы, в данном случае должен быть известен текущий адрес, назначенный коммутатору. IP-адрес можно также установить, используя интерфейс командной строки CLI по консольному последовательному порту, следующим образом:

В командной строке введите команду:

config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy,

где

x – IP-адрес;

y – маска подсети.

Вы также можете ввести команду: **config ipif System ipaddress xxx.xxx.xxx.xxx/z. ,**

где

x – IP-адрес;

z – количество подсетей

Таким образом, x представляет собой IP-адрес, назначенный IP-интерфейсу, называемому System и z – префикс сети в системе обозначений CIDR.
IP-интерфейсу, называемому System, может быть назначен как IP- адрес, так и как подсети для обеспечения подключения управляющей станции к коммутатору по протоколу Telnet или к Web-интерфейсу управления.

Рисунок 4.4 – Назначение IP-адреса коммутатору

В приведенном выше примере коммутатору назначен IP-адрес 10.53.13.52 с маской подсети 255.0.0.0. Пользователь может установить адрес в CIDR-сети (10.53.13.52/8). Системное сообщение **Success** свидетельствует о том, что команда успешно выполнена. Коммутатор можно настроить и управлять через Telnet и CLI или через Web-интерфейс управления.

Раздел 5 - Настройка коммутатора через Web-интерфейс

Введение

Все программные функции коммутатора могут управляться, настраиваться и контролироваться через встроенный Web-интерфейс управления (HTML). Коммутатором можно управлять с удаленных станций сети через стандартный браузер, такой как Opera, Netscape Navigator/Communicator или Microsoft Internet Explorer. Браузер работает как универсальное средство доступа и может соединяться с коммутатором напрямую через HTTP протокол.
Модуль управления через Web-интерфейс и консольная программа (Telnet) – это различные способы для доступа к одному и тому же внутреннему коммутирующему программному обеспечению и его настройки. Таким образом, все настройки, встречающиеся в Web-интерфейсе идентичны тем, которые представлены в консольной программе.

Подключение к Web-интерфейсу

Для того чтобы начать настройку вашего коммутатора, просто запустите браузер, установленный на вашем компьютере, и укажите IP-адрес, который вы определили для устройства. URL в адресной строке должен выглядеть на подобие этого: http://123.123.123.123, где числа 123 представляют IP-адрес коммутатора.

Примечание: Заводской IP-адрес коммутатора по умолчанию 10.90.90.90.

Откроется окно аутентификации пользователя, как показано ниже:

Рисунок 5.1 – Окно «Enter Network Password»

Оставьте поля Имя пользователя и Пароль незаполненными и нажмите **ОК**. Это позволит открыть пользовательский Web-интерфейс. Возможности по управлению коммутатором, доступные в web-менеджере, поясняются ниже.

Пользовательский Web-интерфейс

Web-интерфейс обеспечивает доступ к различным настройкам коммутатора и окнам управления, позволяет видеть статистические данные и графически контролировать состояние системы.

Поля интерфейса пользователя

Рисунок, представленный ниже, демонстрирует пользовательский интерфейс, он делится на три отдельные области, как это и описывается далее в таблице.

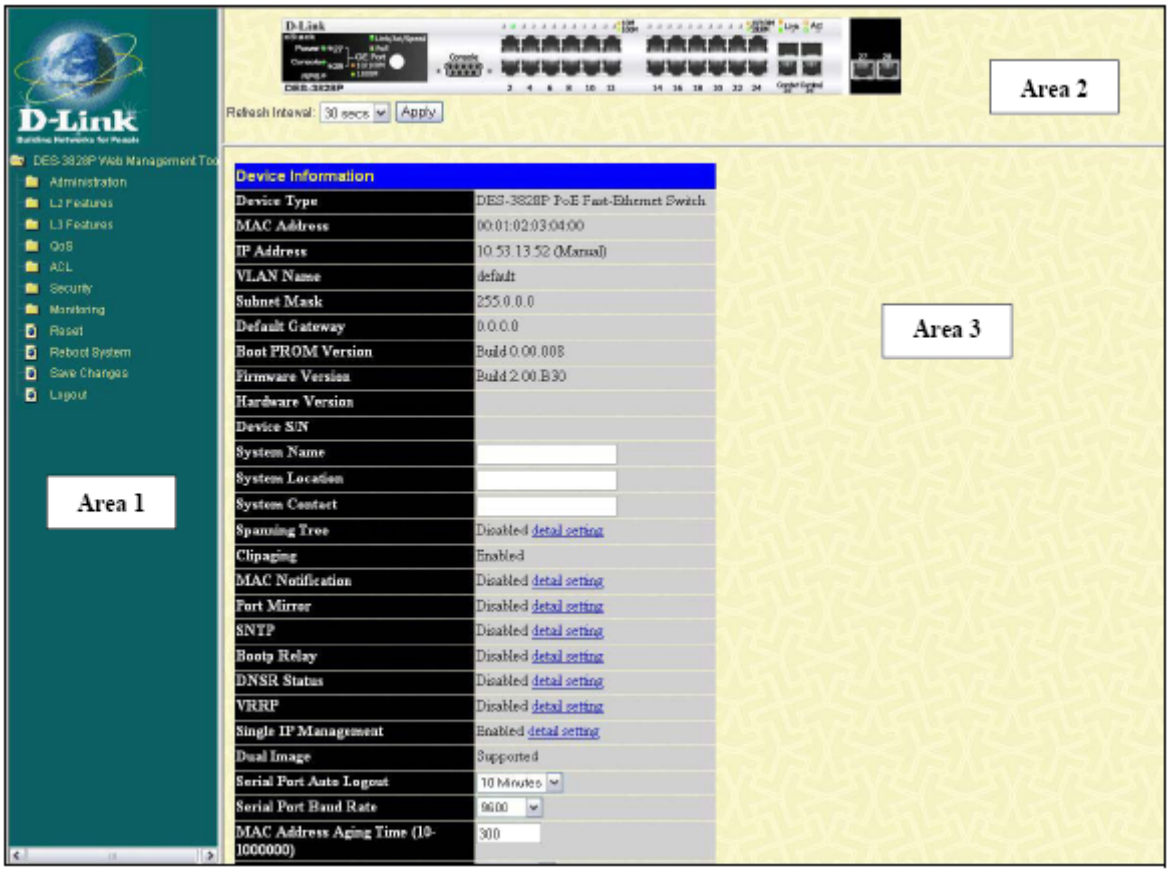


Рисунок 5.2 – Главная страница Web-менеджера

Область	Функция
Area 1	Выберите в меню интересующую вас папку и щелкните по ней для открытия. При открытии папок отображаются меню гипертекстовых ссылок, а также содержащиеся в них папки нижележащего уровня. Для посещения сайта D-Link нажмите на соответствующий логотип.
Area 2	Отображает графическое представление передней панели коммутатора почти в реальном масштабе времени. Данная область демонстрирует порты коммутатора, модули расширения, светодиодную индикацию, дуплексный

	режим, контроль потока, зависящие от выбранного режима. Можно выбирать различные области для рассмотрения различных функций управления, включая конфигурацию портов.
Area 3	В данной области отображается информация по настройке данных

Примечание: Любые изменения, произведенные в настройках коммутатора во время текущей сессии должны быть сохранены в Web-меню (описанном ниже) Save Changes или использовать команду сохранить Save через интерфейс командной строки CLI.

Web-страницы

Когда вы подключитесь к режиму управления коммутатора через Web-браузер, появится окно регистрации. Введите имя пользователя и пароль для доступа к режиму управления коммутатором.

Ниже приведен список и описание основных папок, доступных через Web-интерфейс:

Administration – Содержит опции, позволяющие настроить IP-адрес, конфигурацию порта, конфигурацию PoE (для DES-3828), учетные записи пользователей, зеркалирование портов, системный журнал System Log, System Severity, SNTP, MAC-уведомление, сервисы TFTP, сервисы Mulitple Image, сервисы Dual Configurations, Ping-тест, SNMP Manager и Single IP Management .
Layer 2 Features – Содержит опции, позволяющие настроить VLAN, Trunking, IGMP Snooping, Spanning Tree, и Forwarding.
Layer 3 Features – Содержит опции, позволяющие настроить IP Interfaces, настройки MD5 Key, Route Redistribution, Static/Default Route, Route Preference, Static ARP, RIP, OSPF, DHCP/BOOTP Relay, DNS Relay, VRRP и IP Multicast Routing.
QoS – Содержит опции, позволяющие настроить контроль полосы пропускания, QoS Scheduling Mechanism, QoS Output Scheduling, 802.1P Default Priority, приоритеты пользователей 802.1P и настройки WRED.
ACL – Содержит опции, позволяющие настроить таблицы профилей доступа и CPU-интерфейс фильтрации.
Security – Содержит опции, позволяющие настроить контроль трафика, безопасность порта, Port Lock Entries, 802.1x, Trusted Host, контроль доступа, сегментацию трафика, SSL, SSH, IP-MAC привязки, широковещательный диапазон Limited IP, конфигурацию WAC и средства безопасности.
Monitoring – Содержит опции, позволяющие настроить статус устройства, использование CPU, состояние средств безопасности, использование порта, пакеты, ошибки, размер пакетов, просмотр порта маршрутизатора, контроль доступа к портам, таблицы MAC-адресов , таблицы IP-адресов, просмотр таблицы маршрутизации, просмотр ARP-таблицы, просмотра таблицы IP Mulitcast Forwarding, группы IGMP Snooping, IGMP Snooping Forwarding, просмотр таблицы IGMP Group, DVMRP-мониторинг, OSPF-мониторинг, просмотр состояния PoE, просмотр настроек WRED и журнал коммутатора Switch Log.

Примечание: Прежде чем подключить коммутатор к сети убедитесь, что в меню учетных записей пользователя сконфигурировано имя пользователя и пароль.

Раздел 6 - Настройка коммутатора

Информация об устройстве
IP-адрес
Конфигурация порта
Конфигурация PoE
Учетные записи пользователей
Зеркалирование портов
Настройки системного журнала System Log
Настройки System Severity
Настройки SNTP
Настройки MAC-уведомления
Сервисы TFTP
Настройки Mulitple Image
Сервисы Dual Configurations
Ping-тест
SNMP-менеджер
Настройки Single IP Management

Информация о коммутаторе

В окне **«Device Information»,** которое появится автоматически после входа в систему, содержатся основные настройки главных функций коммутатора. Для возвращения к окну **«Device Information»,** щелкните по папке **DES-3800 Web Management Tool.** В окне **«Device Information»** отображается MAC-адрес (заводской и несменный), версия **Boot PROM**, версия прошивки и аппаратная версия. Данная информация полезна для отслеживания обновлений PROM и версий программного обеспечения и получения, в случае необходимости, информации о MAC-адресе коммутатора для заполнения адресной таблицы сетевых устройств.

Пользователь по своему предпочтению может также ввести **System Name, System Location** и **System Contact** для полного определения коммутатора. Кроме этого в окне отображается статус опций коммутатора для быстрого доступа к их текущему глобальному статусу. Некоторые опции имеют гиперссылки к соответствующим окнам настроек для более простого доступа из окна **«Device Information».**

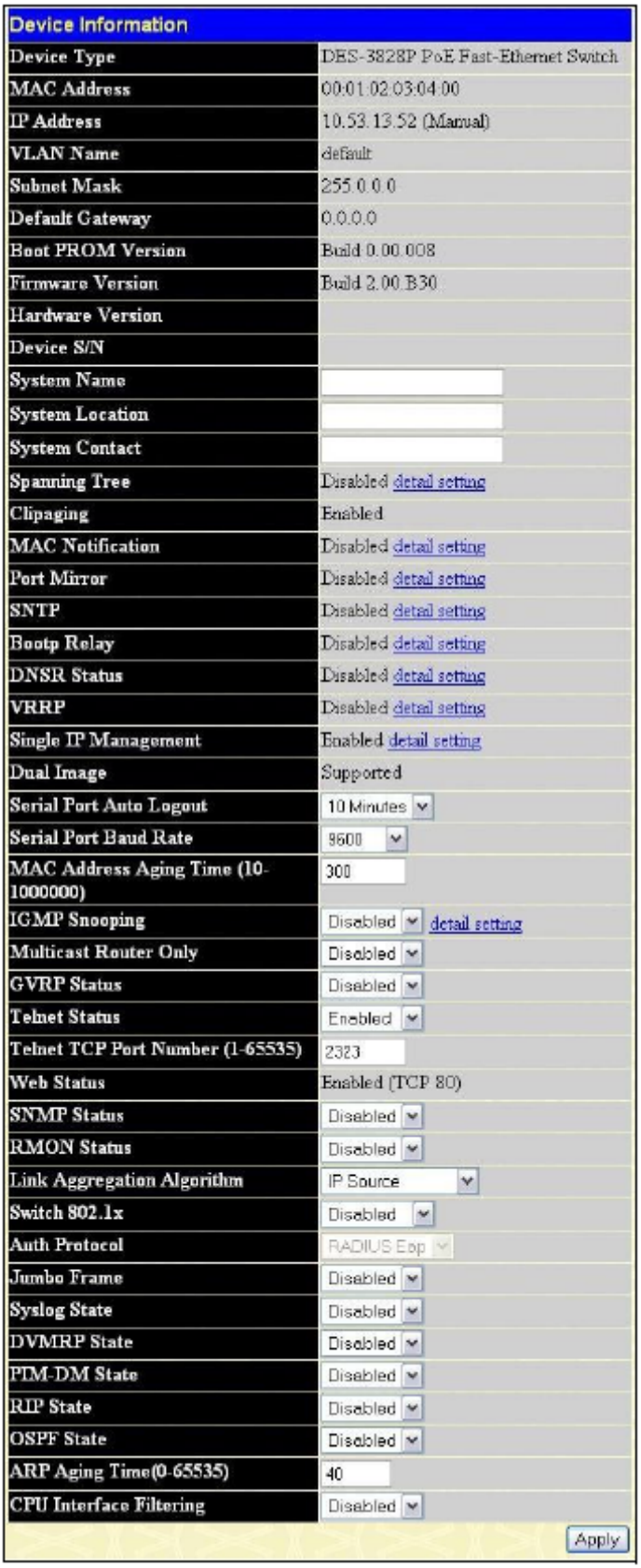


Рисунок 6.1 – Окно «Device Information»

Описание полей, подлежащих настройке, приводится ниже:

Параметр	Описание
System Name	По желанию, можете ввести имя коммутатора. Данное имя будет определять коммутатор в сети.
System Location	По желанию, можете ввести расположение коммутатора.
System Contact	По желанию, можете ввести имя контакта
Dual Image	Коммутатором поддерживается Dual Image, т.е. способность коммутатора сохранять более одного кода прошивки.
Serial Port Auto Logout Time	Выберите время завершения сеанса работы через консольный интерфейс. После истечения определенного вами времени, произойдет автоматический выход из системы. Может быть установлено следующее время *2 мин., 5 мин., 15 мин.* или *никогда.*
Serial Baud Rate	В данном поле определяется в Бодах скорость передачи последовательного порта. Существует возможность выбрать одну из четырех возможных скоростей передачи последовательного порта коммутатора: *9600, 19200, 38400* и *115200*. Для подключения к коммутатору через интерфейс CLI, скорость передачи должна быть установлена *9600*, что соответствует настройкам по умолчанию.
MAC Address Aging Time	Это поле определяет величину времени, в течение которого записанный MAC-адрес будет находиться в таблице коммутации без обновления. Внесите необходимое значение времени обновления таблицы коммутации в секундах. Значение времени обновления таблицы коммутации может составлять от 10 до 1 000 000 секунд, и по умолчанию составляет 300 секунд.
IGMP Snooping	Для использования в полном объеме функций IGMP Snooping выберите вариант *Enabled.* По умолчанию IGMP Snooping находится в состоянии *Disabled* (отключен). Включение IGMP Snooping подразумевает включение этой функции в широковещательном режиме(см. ниже). Для настройки IGMP Snooping для отдельных VLAN используйте функцию **IGMP Snooping**, расположенную в папке **IGMP Snooping,** содержащейся в свою очередь в папке **L2 Features**.
Multicast Router Only	Если эта функция подключена (*Enabled*), то предполагается, что коммутатор будет обмениваться широковещательным трафиком только с маршрутизаторами, поддерживающими данную функцию. В противном случае, маршрутизатор будет пересылать весь широковещательный трафик на любой IP-маршрутизатор. По умолчанию эта функция отключена (*Disabled*).
GVRP Status	Используйте выпадающее меню для подключения или отключения GVRP на коммутаторе.
Telnet Status	Опция настройки через Telnet включена *Enabled* по умолчанию. Если вы не хотите разрешать настройку коммутатора через Telnet, выберите *Disabled.*
Tenet TCP Port Number (1-65535)	Номер TCP порта. TCP порты нумеруются от 1 до 65535. Общеизвестно, что TCP порт протокола Telnet 23.
Web Status	Управление через Web-интерфейс по умолчанию включено *Enabled*. Если вы отключите данную опцию *Disabled*, то потеряете возможность настройки устройства через Web-интерфейс, как только настройки будут применены.
SNMP Status	Простой протокол сетевого управления (SNMP) можно включить и отключить в данном поле. По умолчанию опция отключена *Disabled.*
RMON Status	Удаленный мониторинг (RMON) коммутатора можно включить *Enabled* или отключить *Disabled*.
Link Aggregation Algorithm	Применяемый в коммутаторе алгоритм для распределения нагрузки между портами, которые объединены в агрегированный канал, описывается в этом разделе. Выберите *MAC Source, MAC Destination, MAC Src & Dest, IP Source, IP Destination, IP Src & Dest* (смотри раздел Агрегация каналов этого руководства)

802.1x Status	MAC-адрес может подключаться через порт или функцию коммутатора 802.1x. По умолчанию эта функция отключена. Это поле должно быть включено, чтобы просмотреть и настроить определенные окна под протокол 802.1x. Больше информации по протоколу 802.1x, его реализации и функциям можно будет найти в этом разделе под заголовком **Port Access Entity.** Стандарт 802.1x на базе порта определяет, что порты, настроенные для 802.1x, определяются только по номеру порта и являются основой для настройки любого параметра авторизации. Стандарт 802.1x на базе MAC-адреса определяет, что порты, настроенные для 802.1x, определяются и по номеру порта, и по MAC-адресу и являются основой для настройки любого параметра авторизации.
Auth Protocol	Протокол аутентификации 802.1x устанавливается на RADIUS Eap и не подлежит изменениям.
Jumbo Frame	В данном поле вы можете включить либо отключить функцию «jumbo»-кадров на коммутаторе. По умолчанию данная настройка отключена *Disabled.* В том случае, когда эта опция включена, «jumbo»-кадры (кадры, превышающие размер стандартных Ethernet кадров 1518 байт) вплоть до 9 кбайт (9004 байт с учетом меток) могут передаваться коммутатором.
Syslog State	**Syslog State** может быть включен (*Enabled*) или выключен (*Disabled*, по умолчанию)
DVMRP State	Пользователь имеет возможность глобально подключать или отключать функцию Distance Vector Multicast Routing Protocol (DVMRP) с помощью выпадающего меню.
PIM-DM State	Пользователь имеет возможность глобально подключать или отключать функцию Protocol Independent Multicast- Dense Mode с помощью выпадающего меню
RIP State	Пользователь имеет возможность глобально подключать или отключать функцию Distance Vector Multicast Routing Protocol (DVMRP) с помощью выпадающего меню
OSPF State	Пользователь имеет возможность глобально подключать или отключать функцию Open Shortest Path First(OSPF) с помощью выпадающего меню
ARP Aging Time	Пользователь может глобально устанавливать максимальное время в минутах, в течение которого данные Address Resolution Protocol(ARP) могут оставаться в ARP-таблице коммутатора, прежде чем они будут удалены. Данное значение может варьироваться от 0 до 65535 минут и по умолчанию составляет 20 минут.
CPU Interface Filtering	Пользователь имеет возможность глобально подключать или отключать функцию CPU Interface Filtering с помощью выпадающего меню

Нажмите **Apply**, для того чтобы настройки вступили в силу.

IP-адрес

IP-адрес может быть первоначально установлен через консольный интерфейс, подсоединившись к нему через Ethernet.
Если IP-адрес коммутатора еще не меняли, прочитайте введение к руководству по интерфейсу командной строки коммутаторов серии ***xStack DES-3800*** или вернитесь к разделу 4 данного руководства для получения более полной информации.
Для того чтобы настроить IP-адрес коммутатора:
Откройте папку **Administration** и нажмите в меню **IP Address**. Web-менеджер отобразит текущие IP настройки в меню настроек IP, как показано ниже.

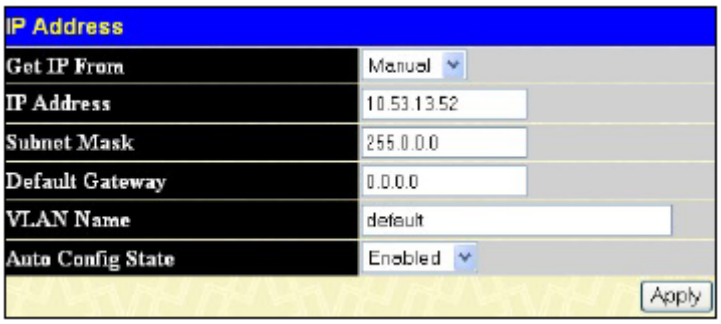


Рисунок 6.2 – Окно « IP Address Settings »

Для того чтобы вручную назначить коммутатору IP-адрес, маску подсети и адрес шлюза по умолчанию:

1. Выберите *Manual* из выпадающего меню в Get IP From.
2. Введите соответствующий IP-адрес и маску подсети.
3. Если вы хотите получить доступ к коммутатору из различных подсетей, введите IP-адрес шлюза по умолчанию. Если вы будете управлять коммутатором из подсети, в которой он установлен, вы можете оставить в поле IP-адрес по умолчанию (0.0.0.0).
4. Если на коммутаторе не было ранее настроенных VLAN, вы можете использовать имя VLAN по умолчанию. VLAN по умолчанию включает в себя все порты коммутатора. Если VLAN ранее настраивались на данном коммутаторе, вам необходимо будет ввести VLAN ID той виртуальной локальной сети, которая включает в себя порт, подключенный к управляющему устройству, которое и будет иметь доступ к коммутатору.

Коммутатор будет разрешать доступ к управлению устройствам с таким же VID, занесенным в список.

Примечание: Заводской IP-адрес по умолчанию 10.90.90, маска подсети 255.0.0.0 и IP-адрес шлюза по умолчанию 0.0.0.0.

Для того, чтобы использовать BOOTP или DHCP протоколы, необходимо назначить коммутатору IP-адрес, маску подсети и адрес шлюза по умолчанию. В Get IP From из выпадающего меню выберите *BOOTP* или *DHCP*, что определит, каким образом после перезагрузки коммутатору будет назначен IP-адрес.

Примечание: Если вы запустите **Auto Config**, в **Get IP From** будет автоматически прописан DHCP.

Описание настроек дается ниже:

Параметр	Описание
BOOTP	Коммутатор будет высылать BOOTP широковещательный запрос, когда этот параметр подключен. BOOTP протокол позволяет IP-адресам, сетевым маскам и шлюзам по умолчанию быть присвоенными к центральному BOOTP серверу, чтобы обеспечить его этой информацией до использования настроек по умолчанию или предустановленных настроек.
DHCP	Коммутатор отправляет широковещательный запрос DHCP, если включено питание. DHCP протокол позволяет получать IP-адрес, маску сети и шлюза по умолчанию от DHCP-сервера. Если установить данную опцию, коммутатор будет сначала искать DHCP-сервер для получения данной информации прежде чем использовать настройки по умолчанию или ранее произведенные настройки.
Manual	Позволяет вручную вводить IP-адрес, маску подсети и IP-адрес шлюза по умолчанию для коммутатора. Данные поля должны заполняться согласно

	образцу xxx.xxx.xxx.xxx, где xxx – это число, представленное в десятичной системе счисление), от 0 до 255. Данный адрес должен быть уникальным адресом в сети, назначенным для использования администратором сети.
Subnet Mask	Бит-маска определяет часть подсети, к которой подключается коммутатор. При этом маска подсети имеет следующий вид xxx.xxx.xxx.xxx, где xxx – это число, представленное в десятичной системе счисление), от 0 до 255. Для сетей класса A маска подсети принимает значение 255.0.0.0, для сетей класса B – 255.255.0.0, для сетей класса C – 255.255.255.0, но разрешаются и другие маски подсети.
Default Gateway	IP-адрес, который определяет куда нужно отправлять пакеты с адресом назначения за пределами текущей подсети. Обычно это адрес маршрутизатора или рабочей станции, работающей в качестве IP-шлюза. Если ваша сеть не является частью интранета или вы не хотите, чтобы коммутатор был доступен за пределами сети, то оставьте данное поле неизменным.
VLAN Name	Этот параметр позволяет присвоить VLAN имя, используя которое управляющая станция сможет управлять коммутатором через TCP/IP протокол(или локально через Web менеджер или Telnet). Управляющие станции, которые не знают введенное имя VLAN, не смогут управлять данным коммутатором, если их IP-адреса не введены в Security IP-management menu. Если виртуальные локальные сети VLAN еще не настроены в коммутаторе, то по умолчанию VLAN включает в себя все порты коммутатора. По умолчанию также нет записей в Security IP-management таблице. Таким образом, любая управляющая станция, которая имеет доступ к коммутатору до тех пор, пока не задано имя VLAN или не введены IP-адреса управляющих станций в соответствующую таблицу.
Auto Config State	Когда этот параметр подключен, коммутатор получает задание создать конфигурационный файл с помощью TFTP и автоматически становится DHCP-клиентом. Конфигурационный файл будет загружен перед начальной загрузкой. В случае использования Auto Config, DHCP-сервер должен быть настроен так, чтобы доставлять на TFTP-сервер информацию по IP-адресам и имени конфигурационного файла в ответном DHCP-пакете. Когда приходит запрос от коммутатора, TFTP-сервер должен запускать и иметь требуемый конфигурационный файл, который хранится в его корневом каталоге. Для получения информации по загрузке конфигурационного файла обращайтесь к Инструкциям по программному обеспечению для DHCP-сервера и/или TFTP-сервера, применяемые клиентами. Если коммутатор не способен завершить процесс автоконфигурирования, будет загружен последний сохраненный в памяти коммутатора файл конфигурации.

Для того чтобы настройки вступили в силу, нажмите **Apply**.

Назначение IP-адреса коммутатору через консольный интерфейс

Каждому коммутатору должен быть назначен свой собственный IP-адрес, который используется для связи с сетевым менеджером протокола SNMP или другими TCP/IP приложениями (например, BOOTP, TFTP). IP-адрес коммутатора по умолчанию 10.90.90.90, вы можете его изменить для удовлетворения спецификации плана сетевых адресов.

IP-адрес должен быть назначен коммутатору прежде, чем он будет управляться через web-менеджер. IP-адрес может быть автоматически установлен, используя протокол BOOTP или DHCP, в данном случае должен быть известен действующий адрес. IP-адрес может быть установлен через интерфейс командной строки (CLI) через консольный последовательный порт следующим образом:

- Введите команду **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy,** где x – IP-адрес; y – соответствующая маска подсети.
- В качестве альтернативы, вы можете ввести **config ipif System ipaddress xxx.xxx.xxx.xxx/z,** где x - IP-адрес; z – префикс подсети для случая бесклассовой междоменной маршрутизации (CIDR).

Через IP-интерфейс, называемый System, коммутатору можно назначить IP-адрес и маску подсети, которые можно использовать в дальнейшем для подключения к управляющей станции Telnet.

Системное сообщение **Success** свидетельствует о том, что команда успешно выполнена. Теперь коммутатор может быть настроен и управляться через Telnet и CLI или с помощью агента управления через Web-интерфейс, используя IP-адрес для подключения к коммутатору.

Настройка портов

Данный раздел содержит информацию для настройки различных функций и свойств индивидуально для каждого физического порта, включая скорость на порту и управление потоком.

Port Settings

Для открытия окна нажмите: **Administration ⇨ Port Configuration ⇨ Port Settings.**

Для настройки портов коммутатора:

Для настройки портов коммутатора:

1. Выберите порт или последовательный диапазон портов, используя From…To… (от ….до…) из выпадающего меню.
2. Используйте выпадающие меню для настройки параметров, описанных ниже.

Нажмите **Apply**, чтобы измененные настройки вступили в силу на коммутаторе.

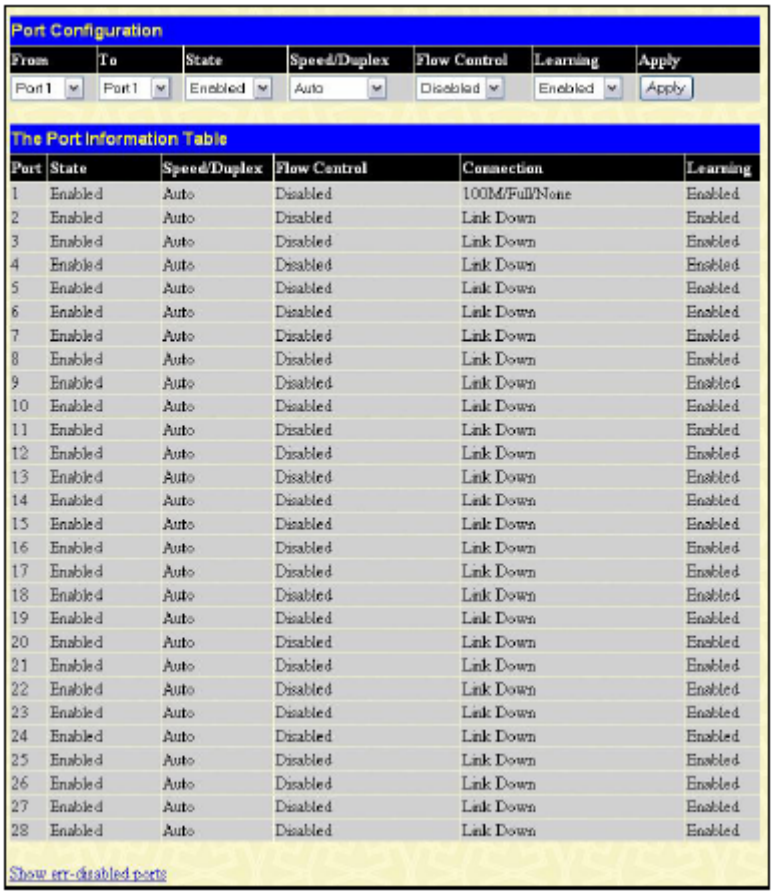


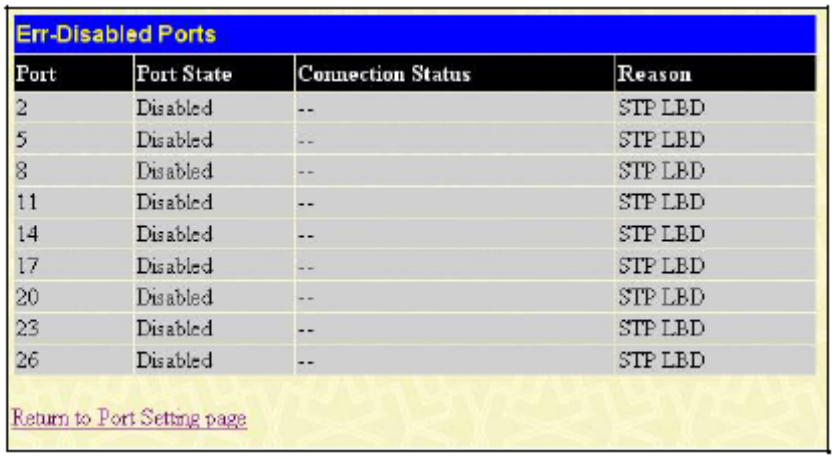
Рисунок 6.3 – Окно «Port Configuration»

Можно настроить следующие параметры:

Параметр	Описание
From …To	Для настройки портов с помощью выпадающего меню выберите номер порта или диапазон портов.
State	В данном поле можно включать или выключать выбранный порт или группу портов.
Speed/Duplex	В данном поле вы можете выбрать скорость и дуплексный/полудуплексный режим передачи порта. *Auto* режим обеспечивает согласование устройств на скоростях от 10 до 100 Мбит/с как дуплексном, так и полудуплексном режимах. Настройки Auto позволяют автоматически определять на порту самую высокую скорость подключения и использовать ее. Кроме Auto возможны следующие режимы работы: 10M/Half, 10M/Full, 100M/Half, 100M/Full и 1000M/Full, однако они не обеспечивают автоматическую регулировку настроек.
Flow Control	В данном поле отображается алгоритм управления потоком, используемый при различных настройках порта. Порты, настроенные на работу в полнодуплексном режиме, используют управление потоком 802.3x, полудуплексные порты используют метод обратного давления, для режима

	Auto осуществляется автоматический выбор управления потоком. По умолчанию, опция управления потоком отключена
Learning	В данном поле можно включать или отключать запоминание MAC-адресов для выбранных портов. В случае подключения опции *Enabled* MAC-адрес источника и получателя будут автоматически заноситься в адресную таблицу. Это делается для обеспечения безопасности и эффективности работы. Для внесения MAC-адреса в адресную таблицу, обратитесь к пункту Forwarding/Filtering. По умолчанию данная настройка отключена.

Для того чтобы настройки вступили в силу, нажмите **Apply**.
В нижней части окна «Port Configuration» есть гиперссылка Show err-disabled ports, при открытии которой будет представлена информация о портах, которые в данный момент являются отключены по причинам обнаружения петли при работе протокола STP или физически не подключены. Нажмите данную гиперссылку для открытия следующего окна:


Err-Disabled Ports

Port	Port State	Connection Status	Reason
2	Disabled	--	STP LBD
5	Disabled	--	STP LBD
8	Disabled	--	STP LBD
11	Disabled	--	STP LBD
14	Disabled	--	STP LBD
17	Disabled	--	STP LBD
20	Disabled	--	STP LBD
23	Disabled	--	STP LBD
26	Disabled	--	STP LBD

Return to Port Setting page

Рисунок 6.4 – Окно «Err-disabled ports»

Описание портов

Коммутатор поддерживает функцию описания порта, при которой пользователь может давать имена различным портам коммутатора. Для того, чтобы назначить имена различным портам, нажмите**: Administration ⇨ Port Configuration ⇨ Port Description.**

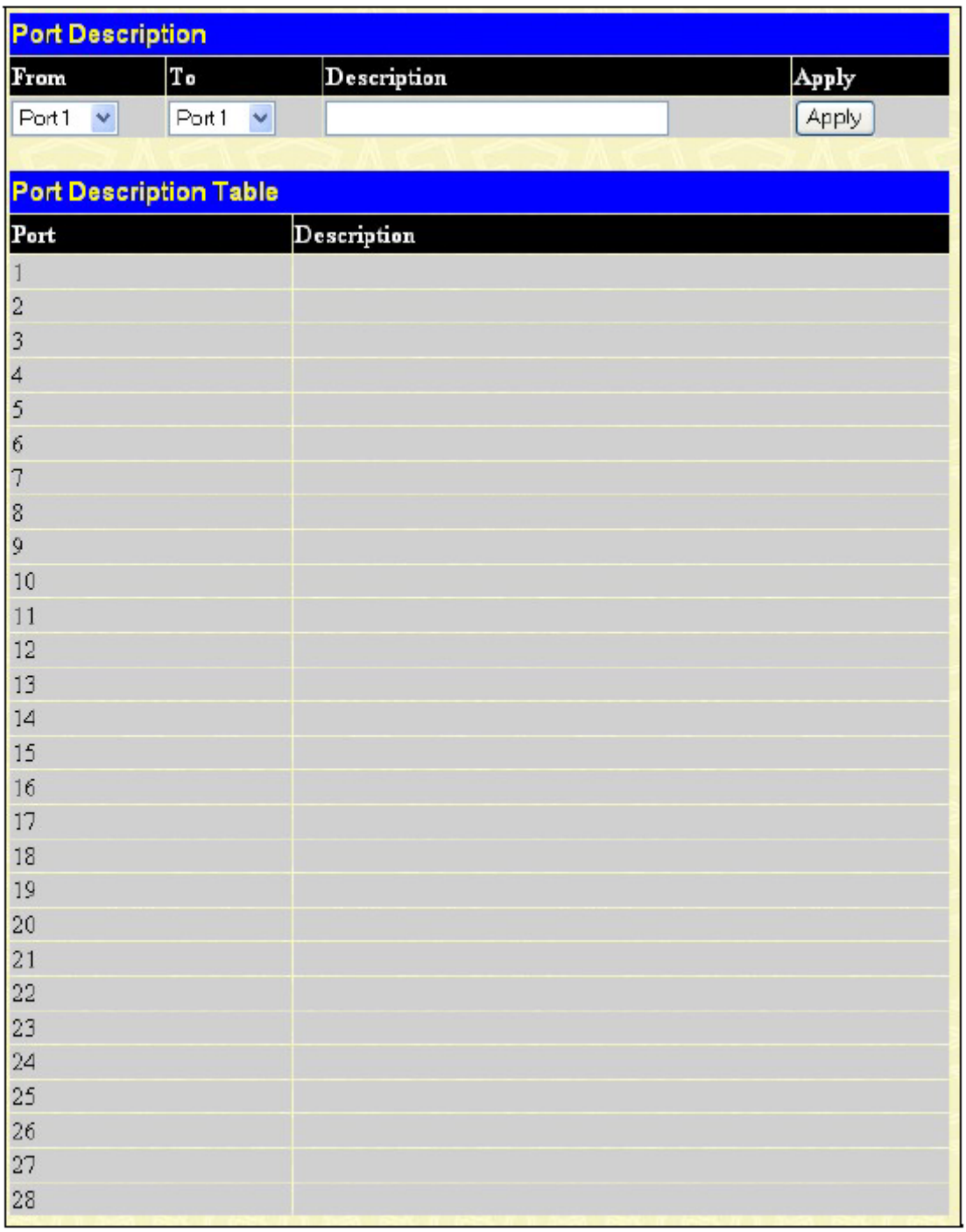


Рисунок 6.5 – Окно «Port Description Setting»

Для выбора порта или диапазона портов для описания используйте выпадающее меню **From** и **To**, также введите описание порта (ов).
Нажмите **Apply** для размещения описания в таблице описания порта **Port Description Table.**

Настройка питания по Ethernet PoE

Коммутатор DES-3828P поддерживает питание по сети Ethernet (Power over Ethernet, PoE) согласно спецификации IEEE 802.3af. К портам 1-24 можно подать питание 48 В постоянного тока от устройства питания (Power Devices, PDs) по витой паре категории 5 или 3. DES-3828P работает согласно стандарту PSE (Power Source over Ethernet) с разводкой выводов Alternative A, в соответствие с которым питание подается на контакты 1, 2 и 6. Коммутатор DES-3828P работает со всеми устройствами D-Link, совместимыми с 802.3af, он также поддерживает режим питания PoE со всеми устройствами D-Link, такими как точки доступа, IP камеры, IP телефоны, не совместимыми с 802.3af, через DWL-P50.
Коммутатор DES-3828P обладает следующими PoE характеристиками:

- Автоматическое определение подключения устройства питания PD и автоматическая подача питания
- Автоматическое отключение данной опции может произойти в двух случаях: если общее потребление мощности превысит установленный лимит или, если потребление мощности на порту превысит установленный лимит мощности на порт.
- Активная схема защиты автоматически отключит порт в случае короткого замыкания, остальные порты будут работать.

Класс	Максимальная мощность, потребляемая PD
0	От 0,44 до 12,95 Вт
1	От 0,44 до 3,84 Вт
2	От 3,84 до 6,49 Вт
3	От 6,49 до 12,95 Вт

Класс	Максимальная мощность, потребляемая PSE
0	15,4 Вт
1	4,0 Вт
2	7,0 Вт
3	15,4 Вт

Для настройки питания по Ethernet, нажмите **Administration ⇨ PoE Configuration.** Окно **« PoE System»** используется для ограничения мощности и отключения питания для всей PoE системы. Для настройки ограничения мощности Power Limit введите в поле Power Limit значение от 37 Вт и 370 Вт. Когда общая потребляемая мощность превысит установленный лимит, контроллер PoE (находящийся в PSE) отключит питание для предотвращения перегрузки источника питания.
Для настройки PoE питания коммутатора, нажмите **Administration ⇨ PoE Configuration** для обновления следующего окна:

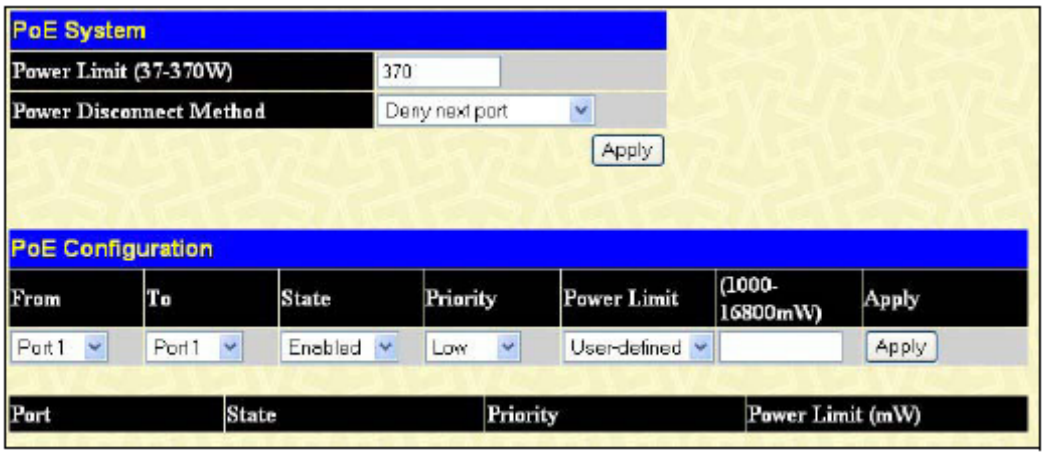


Рисунок 6.6 – Окно «PoE Configuration»

Окно «PoE Configuration» содержит следующие поля для настройки питания по Ethernet:

Параметр	Описание
PoE System	
Power Limit	Устанавливается лимит по мощности, используемой источником питания коммутатора для PoE портов. Пользователь может настроить ограничение мощности от 37 до 370Вт.
Power	Контроллер PoE использует две опции **Deny next port** или **Deny low priority port**

Disconnect Method	для компенсации мощности, превышающей установленный лимит и поддержании питания коммутатора на необходимом уровне. Используйте выпадающее меню для выбора способа отключения питания, по умолчанию установлен Deny next port. Оба способа описываются ниже: **Deny next port** – после превышения установленного лимита по мощности, попытка следующего порта получить питание будет отменена независимо от его приоритета. **Deny low priority port -** после превышения установленного лимита по мощности, попытка следующего порта получить питание, приведет к тому, что порт с наименьшим приоритетом будет закрыт, позволяя тем самым подачу питания на порты с более высоким приоритетом.
PoE Configuration	
From…To	С помощью выпадающего меню выберите диапазон портов для включения или отключения питания по Ethernet.
State	Используйте выпадающее меню для включения или отключения портов с питанием по Ethernet.
Priority	С помощью выпадающего меню выберите приоритезацию для портов с PoE.
Power Limit	Установите ограничение по мощности для порта с питанием по Ethernet. Таким образом, в случае достижения мощностью установленного лимита, будет происходить отключение питания, как это описывалось выше. Пользователь может установить ограничение по мощности от 1000 до 16800 мВт.

Для того чтобы произведенные изменения по настройке питания по Ethernet вступили в силу, нажмите **Apply**. Состояние всех портов, настроенных на питание по Ethernet, отображается в нижней части таблицы, представленной в окне выше.

Учетные записи пользователей

Используйте окно **«User Account Management»** для управления привилегиями пользователя. Для просмотра существующих учетных записей пользователей откройте папку **Administration** и нажмите **User Accounts.** Это позволит открыть окно **«User Account Management»**, показанное ниже.

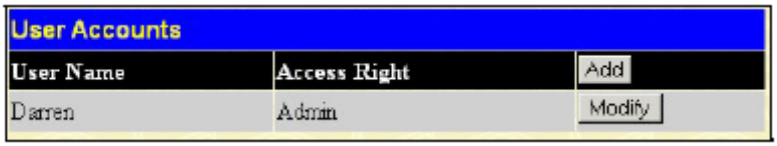


Рисунок 6.7 – Окно «User Accounts»

Для добавления нового пользователя, нажмите кнопку **Add.** Для изменения и удаления существующего пользователя, нажмите на кнопку **Modify** напротив соответствующего пользователя.

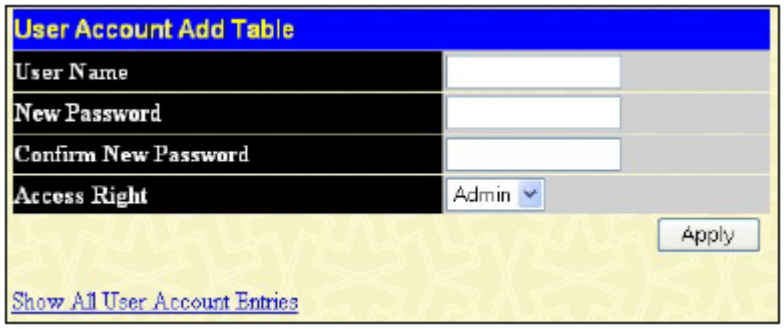


Рисунок 6.8 – Таблица «User Accounts Add»

Для добавления нового пользователя, наберите имя пользователя и пароль в полях *User Name* и *New Password*, подтвердите новый пароль в поле *Confirm New Password*. Из выпадающего меню в поле *Access Right* выберите уровень привилегий (*Admin* или *User*).

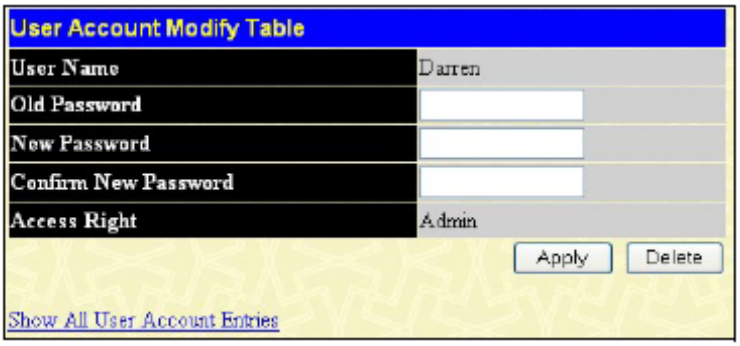


Рисунок 6.9 –Таблица «User Accounts Modify»

Для изменения или удаления существующей учетной записи пользователя в таблице **User Accounts Modify** нажмите кнопку **Delete.** Для изменения пароля введите в поле *New Password* новый пароль, далее подтвердите его в поле *Confirm New Password*. Уровень привилегий (*Admin* или *User*) Из выпадающего меню в поле **Access Right.**

Зеркалирование портов

Благодаря зеркалированию портов вы сможете копировать переданные и полученные кадры на порту и перенаправлять копии на другой порт. Вы также можете подключить контролирующее устройство, такое как сниффер (анализатор пакетов) или устройство для удаленного мониторинга RMON, к порту, на который происходит зеркалирование, для просмотра информации о проходящих через порт пакетах. Данная функция полезна для мониторинга сети и поиска неисправностей. Для просмотра окна **Port Mirroring,** нажмите **Administration ⇨ Port Mirroring.**

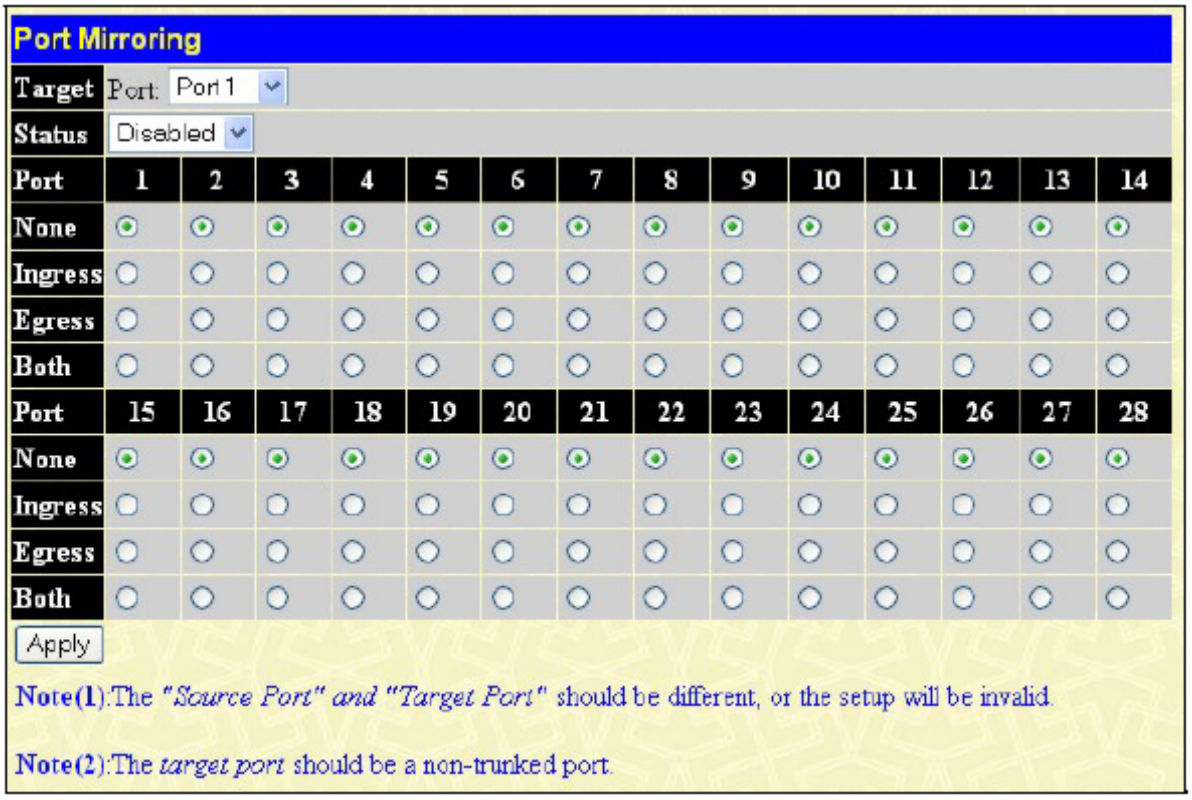


Рисунок 6.10 – Окно «Port Mirroring»

Для настройки зеркального порта:

1. Выберите порт-источник Source Port, с которого вы хотите копировать кадры и порт, на который будете производить зеркалирование, - Target Port, т.е. тот, который будет получать копии с порта-источника.
2. Выберите направление источника, вход Ingress, выход Egress или оба и измените статус Status с помощью выпадающего меню на включено (*Enabled).*

.

3. Нажмите **Apply**, чтобы измененные настройки вступили в силу.

Настройки Системного журнала (System Log)

С помощью **System Log Server** коммутатор может отправлять сообщения **Syslog** до четырех назначенным серверам. Для просмотра окна, представленного ниже нажмите: **Administration ⇨ System Log Settings.**

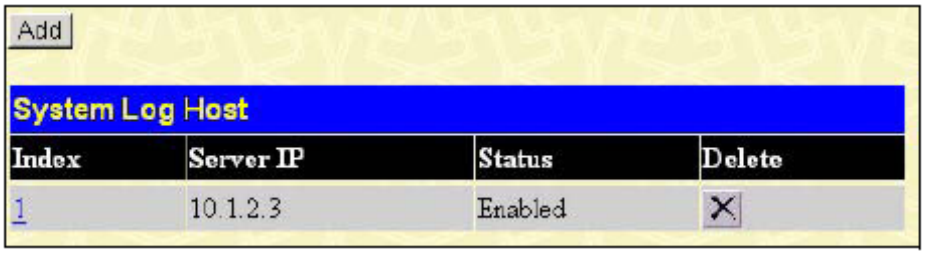


Рисунок 6.11 – Окно «System Log Host»

Настраиваемые параметры для добавления и редактирования **System Log Server** такие же.

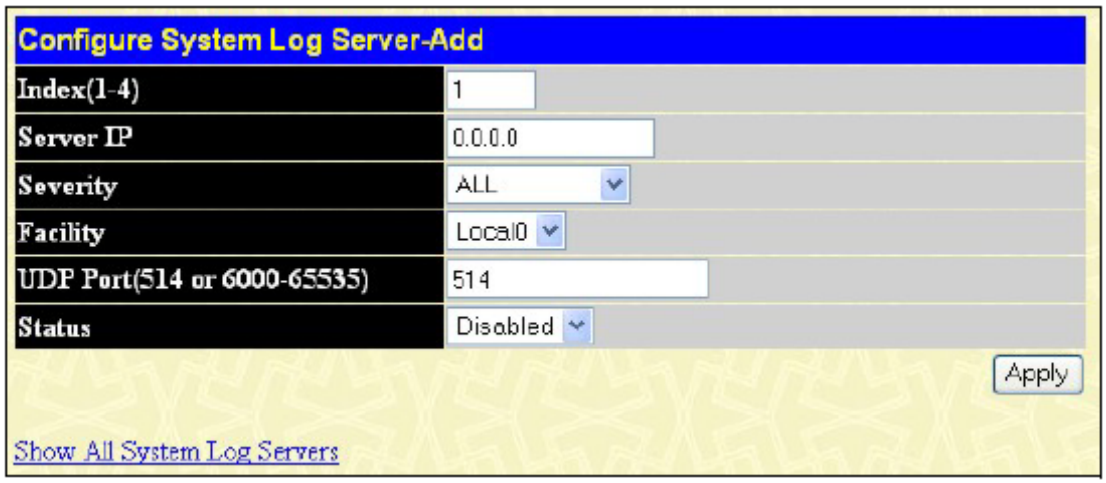


Рисунок 6.12 – Окно «Configure System Log Server-Add»

Могут быть установлены следующие параметры:

Параметр	Описание
Index	Индекс настройки Syslog-сервера (1-4).
Server IP	IP-адрес Syslog-сервера.
Severity	В выпадающем меню выберите тип отсылаемых сообщений: *Warning* (предупреждающее), *Informational* (информационное) и *All* (все типы).
Facility	Некоторые процессы и демоны можно определить при помощи значения Facility Values. Процессы и демоны, которые не определены явно, имеют значение Facility Values «Сообщения пользовательского уровня» или «Локальное использование». Ниже показаны присвоенные различным Facility Values обозначения. Жирным шрифтом показаны **Facility Values**, в которых коммутатор задействован непосредственно: 0- сообщения ядра 1- сообщения пользовательского уровня 2- почтовая система 3- системные демоны 4- сообщения безопасности/авторизации 5- сообщения, генерируемые внутри системы подсистемой syslog line printer 7- подсистема сетевых новостей 8- UUCP подсистема 9- демон часов 10- сообщения безопасности/авторизации

	11- FTP-демон 12- NTP подсистема 13- Аудит журнала регистрации 14- Предупреждение журнала регистрации 15- демон часов **16- локальное использование 0(local0)** **17- локальное использование 1(local1)** **18- локальное использование 2(local2)** **19- локальное использование 3(local3)** **20- локальное использование 4(local4)** **21- локальное использование 5(local5)** **22- локальное использование 6(local6)** **23- локальное использование 7(local7)**
UDP Port (514 или 6000- 65535)	Введите номер UDP порта, который используется для передачи сообщений Syslog.
Status	Для активации/деактивации выберите *Enabled/Disabled*

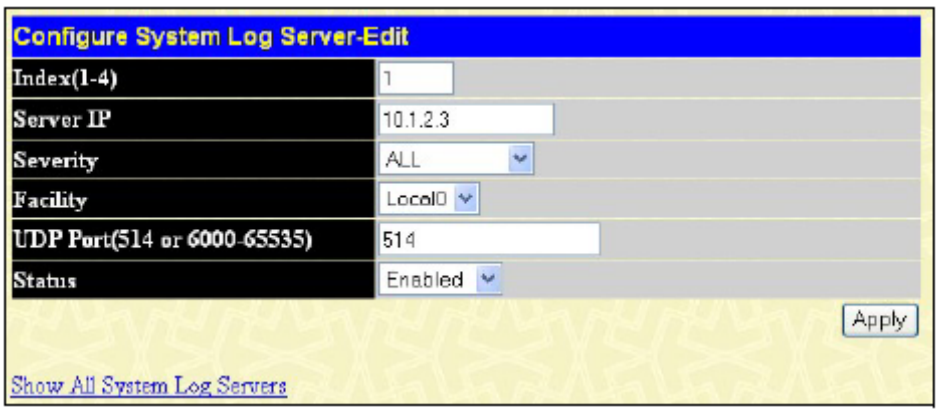


Рисунок 6.13 – Окно «Configure System Log Server-Edit»

Для установки System Log конфигурации сервера нажмите **Apply.** Чтобы отменить ввод из окна **System Log Host** нажмите соответствующий знак для изменения ввода на удаление. Для возвращения в окно **System Log Host** нажмите Show All System Log Server link .

ЗАМЕЧАНИЕ. Нельзя зеркалировать порт с большей скоростью на порт с меньшей скоростью. При попытке отображения трафика с порта 100 Мбит/с на порт 10Мбит/с могут возникнуть проблемы с пропускной способностью канала. Порт, с которого копируются кадры должен всегда поддерживать меньшую или равную скорость по сравнению с портом, на который отсылаются копии. Кроме того, Target Port не может быть членом группы агрегированных каналов. А также Target Port и Source Port не могут быть одним и тем же портом.

Настройки системных сигналов (System Severity)

Коммутатор может быть настроен таким образом, чтобы предупреждения либо записывались в журнал, либо передавались в виде трапов в SNMP-агент, либо и то, и другое одновременно. Воспользуйтесь меню System Severity System для установки условий предупреждений. Текущие настройки отображаются под Settings menu. Войдя в папку **Administration**, нажмите **System Severity Settings**, на экране появится следующее окно:

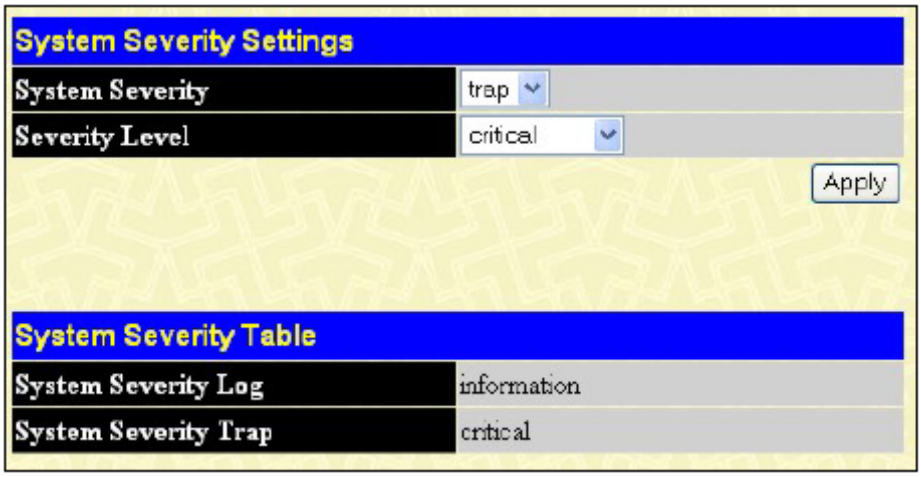


Рисунок 6-14 System Severity Settings

Используйте выпадающие меню, чтобы настроить параметры, указанные ниже:

Параметр	Описание
System Severity	Выберите в выпадающем меню настройки предупреждений. Выберите *log*, чтобы посылать предупреждения в журнал регистрации коммутатора для анализа. Выберите *trap* для отправки предупреждений в SNMP-агент для анализа. Выберите *all* для отправки выбранного типа предупреждения и в журнал регистрации, и в SNMP-агент для анализа.
Severity Level	Выберите уровень предупреждений, при котором будет инициирована передача поступившей записи или трап-сообщений (в зависимости от настроек Severity Name). Выберите *critical*- для пересылки только критических событий в журнал регистрации коммутатора или на SNMP-агент, *warning* - для отправки критических событий и предупреждений; *information* – для отправки информационных сигналов, предупреждений и критических событий.

Нажмите **Apply**, чтобы измененные настройки вступили в силу.

Настройка SNTP. Установка времени

Для настройки параметров времени для коммутатора откройте папку **Administration,** а затем папку **SNTP Settings** и нажмите на вкладку **Time Settings,** воспроизводящую следующее окно для выполнения пользователем соответствующих настроек.

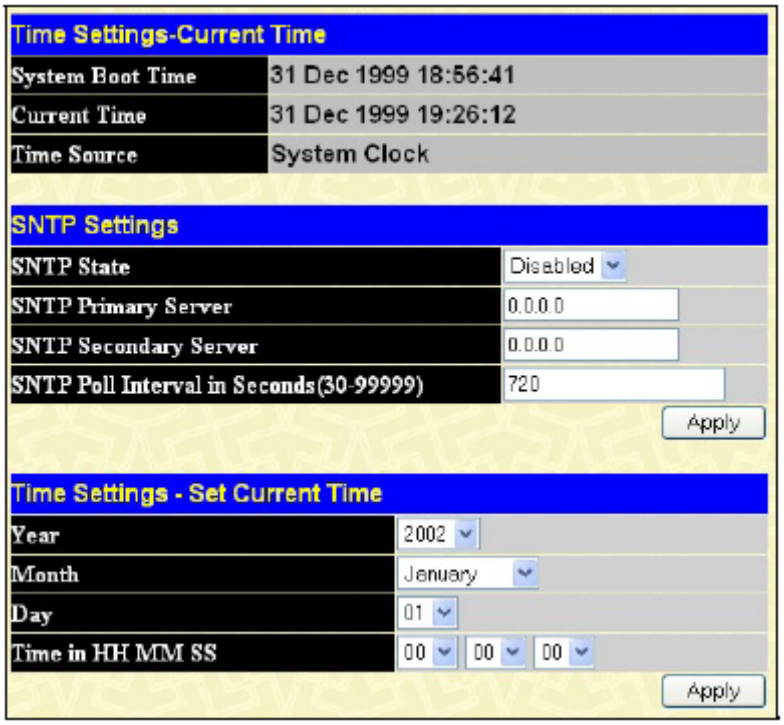


Рисунок 6.15 – Окно «Time Settings»

Параметр	**Описание**
System Boot Time	Отображает время, когда коммутатором была начата эта сессия.
Current Time	Отображает текущее время, которое установлено на коммутаторе.
Time Source	Отображает время источника.
SNTP Settings	
SNTP State	При помощи нисходящего меню подключайте (Enabled) или отключайте (Disabled) SNTP
SNTP Primary Server	В этом поле указывается IP-адрес первичного сервера, на который будет передаваться SNTP-информация
SNTP Secondary Server	В этом поле указывается IP-адрес вторичного сервера, на который будет передаваться SNTP-информация
SNYP Poll Interval in Seconds (30-99999)	Интервал времени в секундах между запросами на обновление SNTP-информации
Set Current Time	
Year	Введите текущий год, если вы хотели бы обновить системные часы.
Month	Введите текущий месяц, если вы хотели бы обновить системные часы.
Day	Введите текущий день, если вы хотели бы обновить системные часы.
Time in HH MM SS	Введите текущее время в часах, минутах и секундах.

Нажмите **Apply** для того, чтобы настройки вступили в силу.

Часовые пояса и DST

Представленные ниже окна используются для настройки часовых поясов и для перевода времени на зимнее и летнее время, для их открытия нажмите **Administration ⇨ SNTP Settings ⇨ Time Zone and DST.**

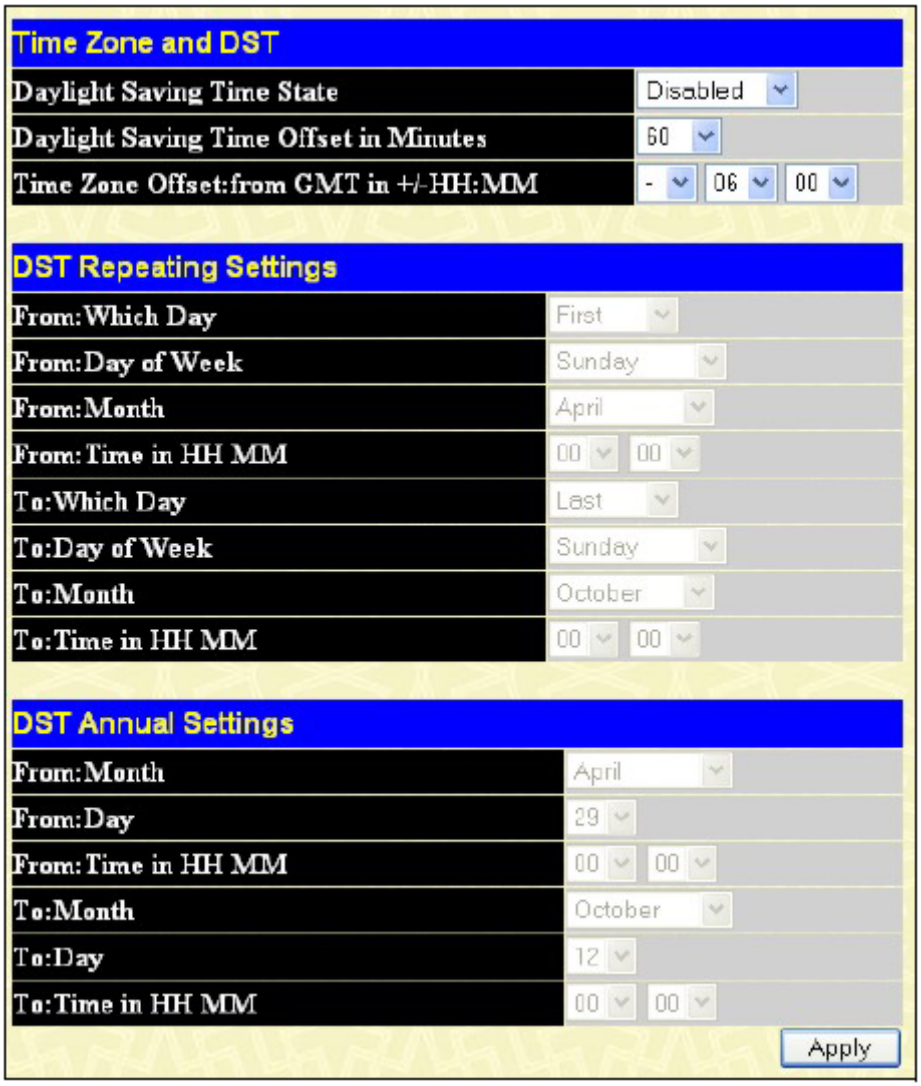


Рисунок 6.16 – Окно «Time Zone and DST Settings»

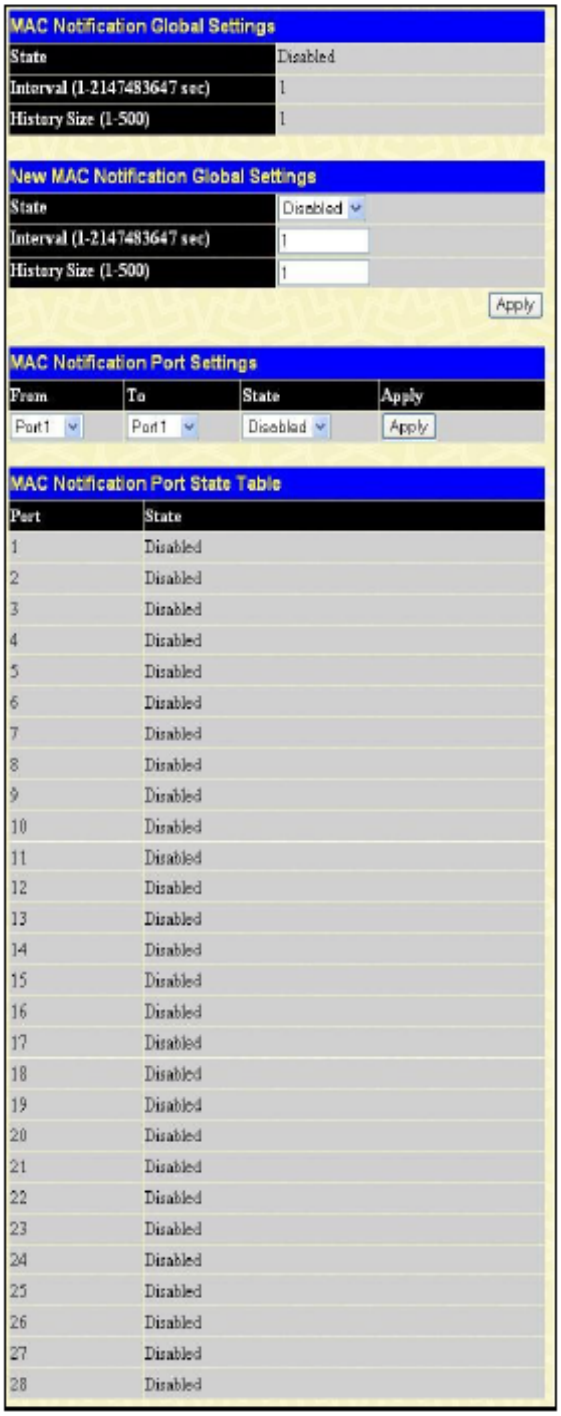
Можно установить следующие параметры:

Параметр	Описание
Часовой пояс и DST	
Daylight Saving Time State	Используйте выпадающее меню для включения или отключения настроек DST.
Daylight Saving Time Offset in Minutes	Данное выпадающее меню используется для задания смещения во времени для летнего времени – 30, 60, 90 или 120 минут.
Time Zone Offset from GMT in +/- PP:MM	Данное выпадающее меню используется для задания временного смещения относительно Гринвича (Greenwich Mean Time (GMT)).
DST Repeating Settings	
Использование режима повтора позволяет отрегулировать сезонные времена. Режим повтора требует, чтобы начало и конец летнего времени были установлены по формуле. Например, определено, что летнее время начинается в первую субботу апреля и заканчивается в последнюю неделю октября.	

From: Which Day	Введите неделю месяца, когда должен осуществиться перевод времени.
From: Day of Week	Введите день недели, когда должен осуществиться перевод времени.
From: Month	Введите месяц, когда должен осуществиться перевод времени.
From: Time in HH:MM	Введите время (часы и минуты), во сколько должен осуществиться перевод времени.
To: Which Day	Введите неделю месяца, когда должен быть произведен обратный перевод времени.
To: Day of Week	Введите день недели, когда должен быть произведен обратный перевод времени.
To: Month	Введите месяц, когда должен быть произведен обратный перевод времени.
To: Time in HH:MM	Введите время (часы и минуты), когда должен быть произведен обратный перевод времени.
DST Annual Settings Использование ежегодного режима позволяет отрегулировать установку сезонного времени. Данный режим требует точного определения начала и конца действия сезонного времени. Например, установите перевод времени на летнее время на 3 апреля, а перевод на зимнее - на 14 октября.	
From: Month	Введите месяц, когда должен осуществляться перевод времени каждый год.
From: Day	Введите день недели, когда должен осуществляться перевод времени каждый год.
From: Time in HH:MM	Введите время (часы и минуты), когда должен осуществляться перевод времени каждый год.
To: Month	Введите месяц, когда должен быть произведен обратный перевод времени каждый день.
To: Day	Введите день недели, когда должен быть произведен обратный перевод времени каждый день.
To: Time in HH:MM	Введите время (часы и минуты), когда должен быть произведен обратный перевод времени каждый день.

Для того чтобы изменения вступили в силу, нажмите **Apply**.

Настройки MAC Notification (MAC-уведомления)



MAC Notification (MAC-уведомление) используется для изучения MAC-адресов и занесения в таблицу MAC-адресов. Для глобальной установки MAC Notification на коммутаторе, откройте следующее окно , нажав на ссылку **MAC Notification Settings** в папке **Administration**.

Глобальные настройки

Следующие параметры доступны для просмотра и изменения:

Параметр	Описание
State	Выбор-отмена MAC notification на Коммутаторе.
Interval (sec)	Временной интервал в секундах между уведомлениями.
History size	Максимальный размер истории уведомлений. Может быть определено до 500 элементов.

Настройка MAC Notification на порту

Для изменения настроек MAC Notification на порту или группе портов коммутатора, необходимо настроить следующие параметры:

Параметр	Описание
From…To	Выбор порта или группы портов, для которых разрешено MAC-уведомление.
State	Установка MAC-уведомления для выбранного порта.

Нажмите **Apply** для сохранения сделанных изменений.

Сервисы TFTP

Простейший протокол передачи данных (Trivial File Transfer Protocol ,TFTP) позволяет обновлять программно-аппаратные средства (прошивки) коммутатора посредством перемещения файла с новой прошивкой с TFTP-сервера на коммутатор. Конфигурационный файл можно загрузить в коммутаторе с TFTP-сервера. Настройки коммутатора можно сохранить на TFTP- сервере, а историю регистрационных записей загружать с коммутатора на TFTP-сервер.

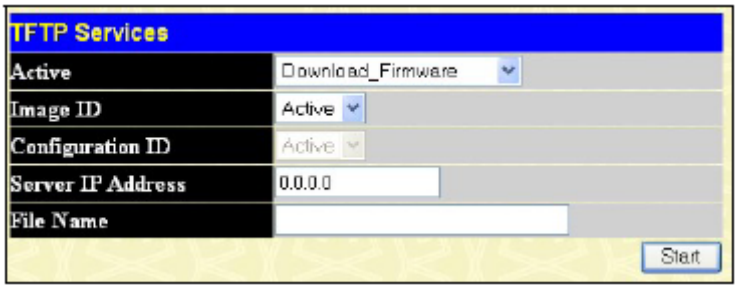


Рисунок 6.18 – Окно «TFTP Server»

Программное обеспечение сервера представляет собой часть нескольких пакетов программ сетевого управления, таких как NetSight, ПО можно также получить в качестве отдельной программы. Для обновления прошивки коммутатора или конфигурационного файла, откройте: **Administration ⇨ TFTP Services.**

Можно настроить следующие параметры:

Параметры	Описание
Active	Из выпадающего меню выберите нужную вам опцию: ▪ **Download Firmware** – Введите IP-адрес TFTP-сервера и укажите местонахождение (путь) новой прошивки на TFTP-сервере. Для записи IP-адреса TFTP-сервера и передачи файла нажмите **Start**. ▪ **Download Configuration** – Введите IP-адрес TFTP-сервера, укажите путь и имя конфигурационного файла на TFTP-сервере. Для записи IP-адреса TFTP-сервера и передачи файла нажмите **Start**. ▪ **Upload Configuration** – Введите IP-адрес TFTP-сервера, укажите путь и имя файла для настроек коммутатора на TFTP-сервере. Для записи IP-адреса TFTP-сервера и передачи файла нажмите **Start**. ▪ **Upload Log** - Введите IP-адрес TFTP-сервера, укажите путь и имя файла историей регистрационных записей на TFTP-сервере. Для записи IP-адреса TFTP-сервера и передачи файла нажмите **Start**.
Image ID	Выберите образ прошивки **Image ID**. В памяти коммутатора может храниться два образа прошивок. Первый образ прошивки Image ID 1 будет использоваться при запуске коммутатора до тех пор, пока пользователь не определит другой. Если выбрать в данном поле значение **Active,** при запуске коммутатора будет загружаться в зависимости от настроек пользователя соответствующий образ прошивки Image ID Информацию по настройке образа прошивки Image ID можно найти в данном разделе в пункте **Multiple Image Services**.
Configuration ID	Для загрузки конфигурационных файлов на коммутатор выберите **Configuration ID**. Подобно образам, коммутатор может хранить два конфигурационных файла

	При выборе значения **Active** при запуске коммутатора будет загружаться Configuration ID в зависимости от настроек пользователя.
Server IP Address	Введите IP-адрес сервера, с которого будете скачивать прошивку или конфигурационные файлы.
File Name	Укажите путь и имя файла прошивки или конфигурационного файла, который вы хотите загрузить или скачать.

Сервисы Multiple Image

Папка **Multiple Image Services** позволяет администраторам коммутатора настраивать и просматривать информацию о прошивке на коммутаторе. В памяти коммутатора может храниться два образа прошивок, причем любой из них может быть настроен в качестве основной, используемой при загрузке коммутатора. Для получения информации о прошивке коммутатора, откройте **Firmware Information.** В настройках по умолчанию прошивка, используемая при запуске коммутатора, хранится в первом образе Image 1, однако пользователь может настроить другую прошивку в качестве основной, воспользовавшись окнами с настройками в папке **Dual Configurations Services.**

Информация о прошивке

Следующий экран позволит пользователю просмотреть информацию о текущей прошивке на коммутаторе. Для открытия данного экрана нажмите **Administration ⇨ Multiple Image Services.**

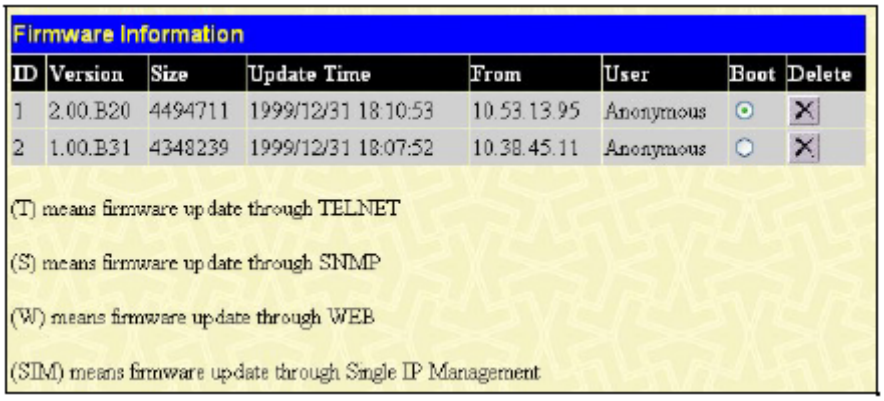


Рисунок 6.19 – Окно «Firmware Information»

Параметр	Описание
ID	Номер образа прошивки Image ID в памяти коммутатора. В коммутаторе может храниться два образа прошивки. Первый образ прошивки Image ID 1 будет использоваться при запуске коммутатора по умолчанию до тех пор, пока пользователь не настроит другой.
Version	Текущая версия прошивки.
Size	Размер соответствующей прошивки, в байтах.
Update Time	Время, через которое должна быть скачена новая версия прошивки.
From	IP-адрес устройства, с которого взята прошивка. Существует пять способов скачивания прошивки. ▪ **T** – Если в IP-адресе будет добавлена буква T, то команда на обновление прошивки была дана через Telnet. ▪ **S** – Если в IP-адресе будет добавлена буква S, то команда на обновление прошивки была дана через простой протокол сетевого управления SNMP (Simple Network Management Protocol). ▪ **W** – Если в IP-адресе будет добавлена буква W, то команда на обновление прошивки была дана через Web-интерфейс управления. ▪ **SIM** – Если в IP-адресе будет добавлена буквы SIM, то команда на обновление прошивки была дана через Single IP Management.
User	Имя пользователя, который скачивал прошивку. Для пользователей, которые были не идентифицированы, в данном поле может быть написано «Anonymous» или «Unknown»

Dual Configuration Services

Ниже приведенное окно используется для конфигурирования информации о прошивке, установленной в коммутаторе. У коммутаторов серии DES-3800 есть возможность хранить два образа прошивок. Для просмотра этого окна, откройте: **Administration ⇨ Dual Configuration.**

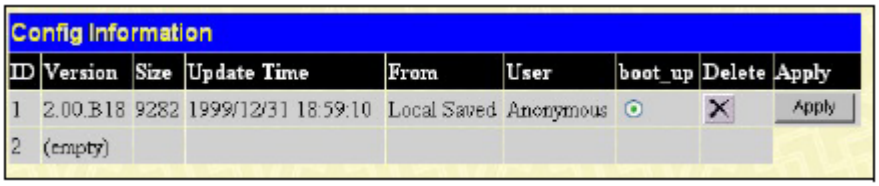


Рисунок 6.20 – Окно «Config Information»

Параметр	Описание
ID	Номер образа прошивки Image ID в памяти коммутатора. В коммутаторе может храниться два образа прошивки. Первый образ прошивки Image ID 1 будет использоваться при запуске коммутатора по умолчанию до тех пор, пока пользователь не настроит другой.
Version	Текущая версия прошивки.
Size	Размер конфигурационного файла в байтах.
Update Time	Время, через которое должен быть скачен обновленный конфигурационный файл.
From	Местонахождение источника, с которого был загружен конфигурационный файл.
User	Имя пользователя (устройства), который обновлял конфигурационный файл. Неизвестный пользователь будет отображаться как «Anonymous».
Boot Up	В данном поле нажмите кнопку для использования конфигурационного файла, который будет использоваться во время следующего запуска коммутатора в качестве основного.
Delete	Нажмите **X** в данной колонке для удаления конфигурационного файла из памяти коммутатора
Apply	Нажмите **Apply** для того, чтобы внесенные к настройкам конфигурационного файла изменения вступили в силу.

Ping-тест

Ping – это небольшая программа, отправляющая эхо-пакеты ICMP по заданному вами IP-адресу. Узел назначения отвечает или отражает «эхо»-пакеты. Данная процедура бывает очень полезна для проверки соединения между коммутатором и другими узлами сети.

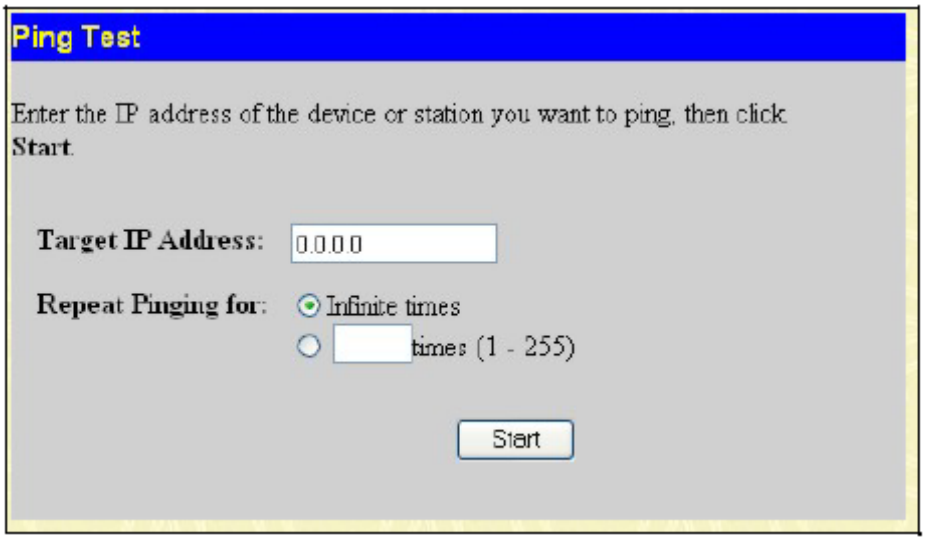


Рисунок 6.21 – Окно «Ping Test»

Пользователь может использовать функцию Infinite times в поле **Repeat Pinging for**, которая позволит отправлять ICMP эхо-пакеты на определенный IP-адрес до остановки программы. Пользователь также может задать определенное число раз для осуществления пинга указанного IP-адреса, путем ввода числа от 1 до 255. Нажмите **Start** для начала запуска программы пинг.

SNMP-менеджер

Настройка протокола SNMP

Простой протокол сетевого управления Simple Network Management Protocol (SNMP) – протокол седьмого уровня (уровень приложений) семиуровневой модели OSI, созданный специально для управления и контроля сетевого оборудования. SNMP дает возможность станциям управления сетью читать и изменять настройки шлюзов, маршрутизаторов, коммутаторов и других сетевых устройств. Используйте SNMP для настройки системных характеристик для обеспечения правильной работы, контроля характеристик и обнаружения потенциальных проблем в коммутаторе, группе коммутаторов или сети.

Управляемые устройства поддерживают SNMP программное обеспечение (называемое агентом), работающее локально на оборудовании. Определенный набор управляемых объектов обслуживается SNMP протоколом и используется для управления устройством. Эти объекты определены в базе данных управляющей информации MIB (Management Information Base), которая обеспечивает стандартное представление информации, контролируемое встроенным SNMP-агентом. Протокол SNMP определяет оба формата спецификаций MIB и используется для доступа к информации по сети.

Коммутаторы серии DES-3800 поддерживают протокол SNMP версий: 1, 2c и 3. Вы можете указать, какую версию SNMP вы хотите использовать для контроля и управления коммутатором. Три версии SNMP-протокола различаются в уровне обеспечиваемой безопасности между станцией управления и сетевым оборудованием.

В SNMP версий v.1 и v.2 аутентификация пользователей осуществляется при помощи так называемой «строки сообщества» («community string»), данная функция похожа на пароли. Удаленный пользователь SNMP-приложения и коммутатора должен использовать одну и ту же «community string». Пакеты SNMP от станций, не прошедших аутентификацию будут игнорироваться (удаляться).

По умолчанию «community strings» для коммутатора, использующего версии v.1 и v.2 протокола SNMP, следующие:

- **public –** позволяет авторизованным станциям управления извлекать объекты MIB.
- **private –** позволяет авторизованным станциям управления извлекать и изменять объекты MIB.

SNMP версии v.3 использует более сложный процесс, который подразделяется на два этапа. Первая часть – это сохранение списка пользователей и их свойств, которые позволяют работать SNMP-менеджеру. Вторая часть описывает, что каждый пользователь из списка может делать в качестве SNMP-менеджера.

Коммутатор разрешает заносить в список и настраивать группы пользователей с разделенным набором привилегий. Можно также устанавливать различные версии SNMP для занесенной в список группы SNMP-менеджеров. Таким образом, вы можете создать группу SNMP-менеджеров, которым разрешено только читать просматриваемую информацию или получать запросы, используя SNMP v.1, в то время как другой группе можно назначить более высокий уровень безопасности с разрешением чтения/записи, используя SNMP v3.

Индивидуальным пользователям и группам SNMP-менеджеров, использующим SNMP v.3, может быть разрешено выполнение или ограничено выполнение определенных функций управления SNMP. Функции «разрешено» или «запрещено» определяются идентификатором объекта (OID – Object Identifier), связанного со специальной базой MIB. Дополнительный уровень безопасности доступен в SNMP v.3, в данной версии SNMP сообщения могут быть зашифрованы. Для получения большей информации по настройке SNMP v.3 в коммутаторе, прочитайте следующий раздел.

Traps

«Traps» - это аварийные сообщения, сообщающие о событиях, происходящих в коммутаторе. События могут быть такими серьезными, как перезапуск (кто-нибудь случайно

выключил коммутатор) или менее, как например, изменение статуса порта. Коммутатор создает сообщения «traps» и отправляет их к получателю «traps» (или сетевому менеджеру). Обычные «traps» содержат сообщение об ошибке аутентификации Authentication Failure, изменении топологии сети Topology Change и широковещательном шторме Broadcast\Multicast Storm.

Базы управляющей информации MIB

Коммутатор хранит в базе управляющей информации MIB управляющую информацию и значения счетчика. Коммутатор использует стандартный модуль MIB-II. В результате, значения объектов MIB могут быть извлечены из любого сетевого управляющего программного обеспечения, основанного на протоколе SNMP. Помимо стандартной базы MIB-II, коммутатор также поддерживает свою собственную базу MIB, в качестве расширенной базы данных управляющей информации. Определяя идентификатор объекта MIB, можно также извлечь собственную базу данных MIB. Значения MIB можно либо только читать, либо читать-записывать.

Коммутаторы серии xStack DES-3800 включают в себя удобное управление SNMP коммутирующим оборудованием. SNMP управление может быть выполнено исходя из потребностей сети и предпочтений сетевого администратора. Используйте меню SNMP V3 для выбора решения более сложных задач.

Коммутаторы серии DES-3800 поддерживают протокол SNMP версий: 1, 2c и 3. Администратор может выбрать версию SNMP протокола для контроля за работой коммутатора и управления им. Три версии SNMP протокола различаются в уровне обеспечиваемой безопасности между станцией управления и сетевым оборудованием. SNMP настройки производятся с помощью меню, расположенного в папке SNMP V3 web-менеджера. Рабочим станциям, которым был предоставлен привилегированный доступ к коммутатору, можно ограничить благодаря меню Management Station IP Address.

Таблица пользователей SNMP

Таблица «SNMP User Table» отображает всех сконфигурированных на коммутаторе пользователей SNMP, для открытия данной таблицы нажмите: **Administration ⇨ SNMP Manager ⇨ SNMP User Table.**

Рисунок 6.22 – Окно «SNMP User Table»

Для удаления существующей записи в таблице **SNMP User Table**, нажмите ***X*** под заголовком Delete напротив той записи, которую хотите удалить. Для отображения более подробной информации по представленным пользователям, нажмите гиперссылку имени пользователя, в результате откроется окно, как показано ниже:

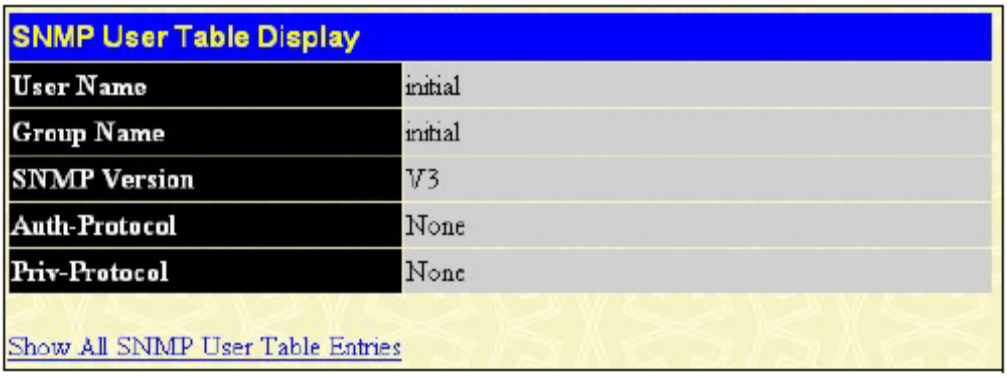


Рисунок 6.23 – Окно «SNMP User Table Display»

В окне отображаются следующие параметры:

Параметр	Описание
User Name	Имя пользователя может состоять из буквенно-цифровой последовательности длиной не более 32 символов, оно позволяет идентифицировать SNMP пользователей.
Group Name	Имя созданной SNMP-группы, которая может запрашивать SNMP-сообщения.
SNMP Version	*V1* – свидетельствует о том, что используется SNMP версии 1. *V2* – свидетельствует о том, что используется SNMP версии 2. *V3* – свидетельствует о том, что используется SNMP версии 3.
Auth-Protocol	*None* – свидетельствует о том, что протокол авторизации не используется. *MD5* – свидетельствует о том, что будет использоваться уровень аутентификации HMAC-MD5-96. *SHA* – свидетельствует о том, что будет использоваться протокол HMAC-SHA.
Priv-Protocol	*None* – свидетельствует о том, что протокол авторизации не используется. *DES* – свидетельствует о том, что будет использоваться 56-битное шифрование. DES на основе стандарта CBC-DES (DES-56).

Для возвращения к таблице SNMP User Table, нажмите Show All SNMP User Table Entries. Для добавления новой записи нажмите кнопку **Add** в окне **SNMP User Table Configuration.**

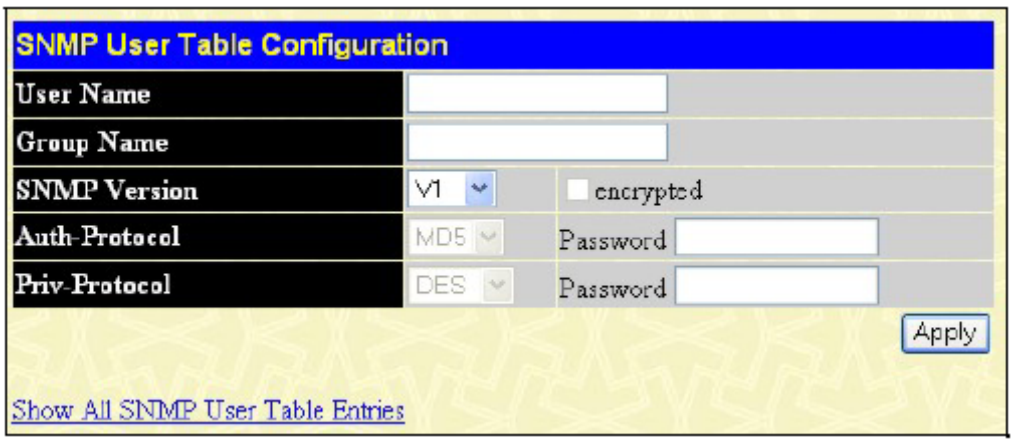


Рисунок 6.24 – Окно «SNMP User Table Configuration»

Можно установить следующие параметры:

Параметр	Описание
User Name	Имя пользователя может состоять из буквенно-цифровой последовательности длиной не более 32 символов, оно позволяет идентифицировать SNMP пользователей.
Group Name	Имя созданной SNMP-группы, которая может запрашивать SNMP-сообщения.
SNMP Version	*V1* – свидетельствует о том, что используется SNMP версии 1. *V2* – свидетельствует о том, что используется SNMP версии 2. *V3* – свидетельствует о том, что используется SNMP версии 3.
Auth-Protocol	*MD5* – свидетельствует о том, что будет использоваться уровень аутентификации HMAC-MD5-96. Данное поле доступно, когда в поле SNMP Version выбрана версия *V3* и подключено шифрование в поле Encryption, пользователя попросят ввести пароль. *SHA* – свидетельствует о том, что будет использоваться протокол HMAC-SHA. Данное поле доступно, когда в поле SNMP Version выбрана версия *V3* и подключено шифрование в поле Encryption, пользователя попросят ввести пароль.

Для того чтобы изменения вступили в силу, нажмите **Apply**. Для возвращения к таблице «SNMP User Table», нажмите Show All SNMP User Table Entries.

SNMP View Table

Таблица «SNMP View Table» используется для просмотра «community strings», которые определяют к каким объектам MIB можно получить доступ удаленным SNMP менеджером. Для просмотра окна нажмите: **Administration ⇨ SNMP Manager ⇨ SNMP View Table.**

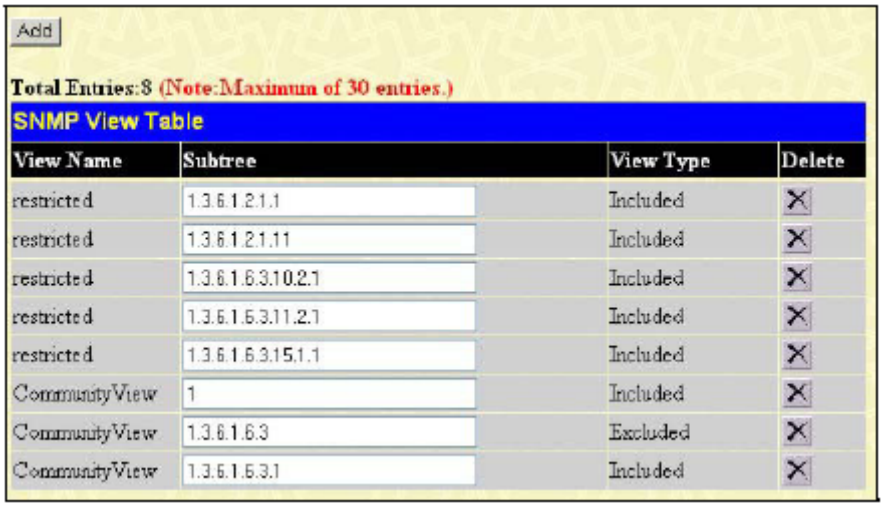


Рисунок 6.25 - Окно «SNMP View Table»

Для удаления существующей записи, нажмите ***X*** в колонке Delete напротив той записи, которую хотите удалить. Для создания новой записи нажмите кнопку **Add,** после чего появится окно.

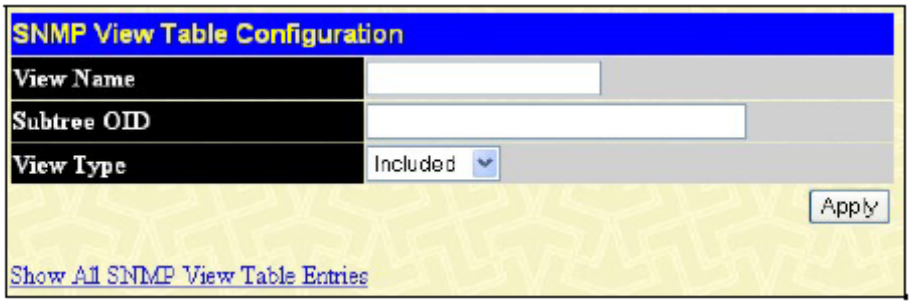


Рисунок 6.26 – Окно «SNMP View Table Configuration»

SNMP-группа, созданная в этой таблице, заносит SNMP-пользователей (определённых в таблице SNMP-пользователей (SNMP User Table)) в отображаемые элементы, созданные в предыдущем меню.

Могут быть установлены следующие параметры:

Параметр	Описание
View Name	Введите имя пользователя, которое может состоять из буквенно-цифровой последовательности длиной не более 32 символов. Параметр используется для идентификации нового SNMP объекта.
Subtree OID	Введите Object Identifier Subtree (OID) для объекта. OID идентифицирует объект MIB tree, который будет включён или исключён SNMP-менеджером
View Type	Отметьте (Included) в списке объектов те, к которым SNMP-менеджер сможет получать доступ. Отметьте (Excluded) в списке объектов те, к которым SNMP-менеджер не сможет получать доступ.

Для того чтобы новые настройки вступили в силу, нажмите **Apply**. Для возвращения к таблице **SNMP View Table**, нажмите Show All SNMP View Table Entries.

SNMP Group Table

SNMP-группа, созданная в этой таблице, заносит SNMP-пользователей (определённых в таблице SNMP-пользователей (SNMP User Table)) в отображаемые элементы, созданные в предыдущем меню.
Для просмотра окна нажмите: **Administration ⇨ SNMP Manager ⇨ SNMP Group Table.** Появится следующее окно:

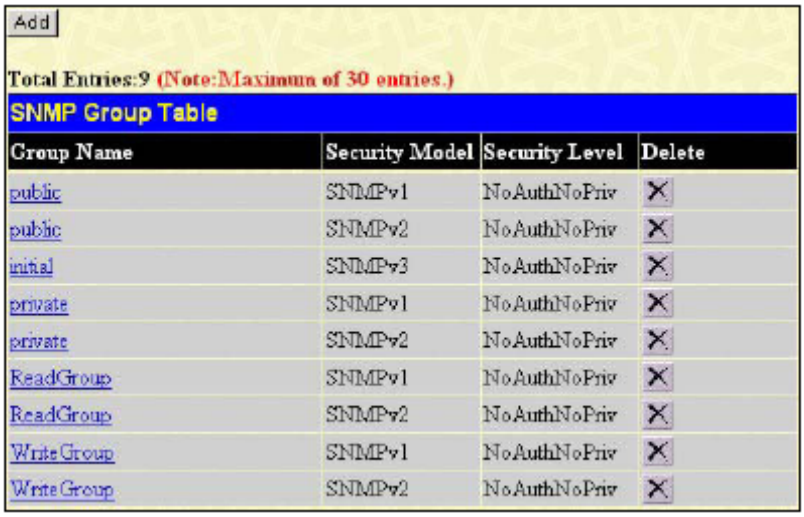


Рисунок 6.27 – Окно «SNMP Group Table»

Для удаления существующей записи в SNMP Group Table, нажмите ***X*** под заголовком Delete. Для отображения текущих настроек существующей записи в **SNMP Group Table**, нажмите гиперссылку записи под заголовком **Group Name**.

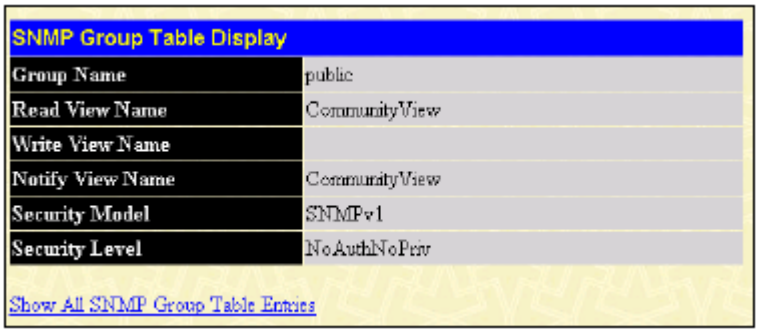


Рисунок 6.28 – Окно «SNMP Group Table Display»

Для добавления новой записи в таблицу SNMP Group Table, нажмите кнопку **Add** в верхнем левом углу окна **SNMP Group Table,** после чего откроется окно **SNMP Group Table Configuration,** показанное ниже:

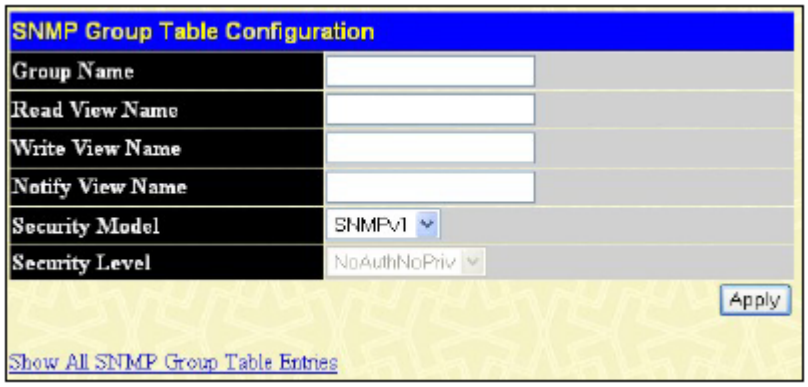


Рисунок 7.35 – Окно «SNMP Group Table Configuration»

Можно установить следующие параметры:

Параметр	Описание
Group Name	Введите имя группы, которое может состоять из буквенно-цифровой последовательности длиной не более 32 символов. Оно используется для идентификации новой SNMP группы SNMP пользователей.
Read View Name	Данное имя используется для определения созданной SNMP группы, которая может запрашивать SNMP сообщения.
Write View Name	Определите имя SNMP группы пользователей, которым разрешены права записи на SNMP агент коммутатора.
Notify View Name	Определите имя SNMP группы пользователей, которые могут получать SNMP «trap» сообщения, создаваемые SNMP агентом коммутатора.
Security Model	*SNMP v1* – свидетельствует о том, что будет использоваться SNMP версии 1. *SNMP v2* – свидетельствует о том, что будет использоваться SNMP версии 2. SNMP v.2 поддерживает централизованную и распределенную модели сетевого управления. В данной версии есть улучшения в структуре информации для управления сетью (Structure of Management Information, SMI), а также добавлены некоторые функции безопасности. *SNMP v3* – свидетельствует о том, что будет использоваться SNMP версии 3. SNMP v3 обеспечивает безопасный доступ к оборудованию, благодаря сочетанию аутентификации и шифрования пакетов, передаваемых по сети.
Security Level	Настройки уровня безопасности применимы только для SNMP v.3. *NoAuthNoPriv* – свидетельствует о том, что будет отсутствовать авторизация, а также шифрование пакетов, отправляемых между коммутатором и удаленным SNMP менеджером. *AuthNoPriv* – свидетельствует о том, что будет затребована авторизация, но будет отсутствовать шифрование пакетов, отправляемых между коммутатором и удаленным SNMP менеджером. *AuthPriv* – свидетельствует о том, что будет затребована авторизация и пакеты, пересылаемые между коммутатором и удаленным SNMP менеджером, будут шифроваться.

Для того чтобы новые настройки вступили в силу, нажмите **Apply**. Для возвращения к таблице SNMP Group Table, нажмите ссылку Show All SNMP Group Table Entries.

Таблица конфигурации SNMP Community

Используйте данную таблицу для создания SNMP «community string», для определения связей между SNMP менеджером и агентом. «Community string» работают по типу паролей, разрешающих доступ к агенту на коммутаторе. Одна или несколько следующих характеристик может быть связана с «community string»:

- Список IP-адресов SNMP менеджеров, которым разрешено использовать «community string» для получения доступа к SNMP агенту коммутатора.
- Любой MIB, который определяет подмножество всех объектов MIB, будет доступен через SNMP community.
- Разрешение чтения/записи или только чтения доступны SNMP community для объектов MIB.

Для настройки записей SNMP Community, откройте окно: **Administration ⇨ SNMP Manager ⇨ SNMP Community Table.**

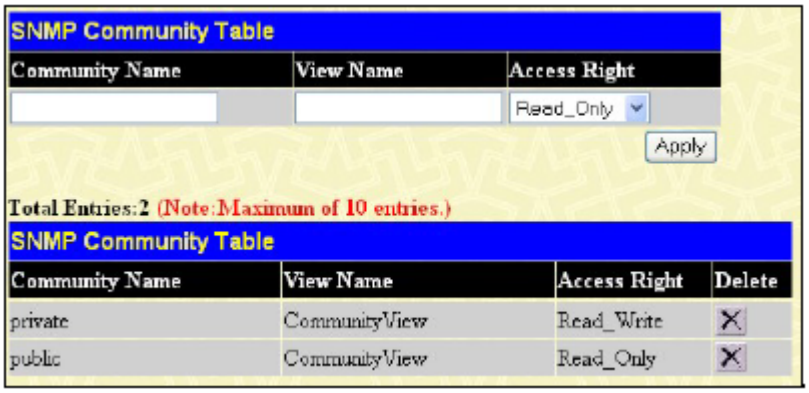


Рисунок 6.30 – Окно «SNMP Community Table Configuration»

Можно установить следующие параметры:

Параметр	Описание
Community Name	Введите имя, которое может состоять из буквенно-цифровой последовательности длиной не более 33 символов. Данный параметр используется как пароль для получения доступа к объектам MIB в SNMP-агентах коммутатора удаленными SNMP-менеджерами для идентификации членов SNMP «сообщества».
View Name	Введите имя, которое может состоять из буквенно-цифровой последовательности длиной не более 32 символов, используемое для идентификации группы объектов MIB, что позволяет SNMP менеджеру получать доступ к коммутатору. Имя «View Name» должно присутствовать в SNMP View Table.
Access Right	Read Only – свидетельствует о том, что члены «SNMP community», использующие созданную «community string», могут только читать содержимое баз MIB коммутатора. Read Write – свидетельствует о том, что члены «SNMP community», использующие созданную «community string», могут читать и записывать в содержимое баз MIB коммутатора.

Для выполнения новых настроек, нажмите **Apply**. Для удаления существующей записи из **SNMP Community Table**, нажмите ***X*** в колонке Delete напротив той записи, которую хотите удалить.

Таблица SNMP Host

Используйте окно **SNMP Host Table** для установки получателя SNMP-сообщений (SNMP trap). Откройте окно **SNMP Host Table,** для этого нажмите: **Administration ⇨ SNMP Manager ⇨ SNMP Host Table Configuration ⇨ SNMP Host Table.**

Для удаления существующей записи из SNMP Host Table, нажмите ***X*** в колонке Delete напротив той записи, которую хотите удалить. Для отображения текущих настроек существующей записи **SNMP Group Table,** нажмите ссылку под заголовком Host IP Address.

Для добавления новой записи к таблице SNMP Host Table, нажмите кнопку **Add** в верхнем левом углу окна – это откроет окно, показанное ниже, **SNMP Host Table Configuration.**

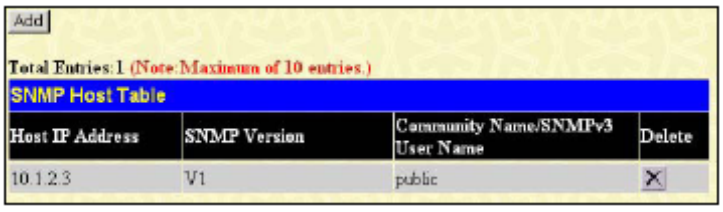


Рисунок 6.31 – Окно «SNMP Host Table»

Рисунок 6.32 – Окно «SNMP Host Table Configuration»

Можно установить следующие параметры:

Параметр	Описание
Host IP Address	Наберите IP-адрес удаленной станции управления, которая будет служить SNMP сервером коммутатора.
SNMP Version	*V1* – свидетельствует о том, что будет использоваться SNMP версии 1. *V2* – свидетельствует о том, что будет использоваться SNMP версии 2. *V3-NoAuth-NoPriv*– свидетельствует о том, что будет использоваться SNMP версии 3 с уровнем безопасности NoAuth-NoPriv. *V3-Auth-NoPriv* – свидетельствует о том, что будет использоваться SNMP версии 3 с уровнем безопасности Auth-NoPriv. *V3-Auth-Priv* – свидетельствует, что будет использоваться SNMP версии 3 с уровнем безопасности Auth-Priv.
Community String/SNMP V3 User Name	Введите в «community string» или SNMP V3 назначенное имя пользователя.

Для применения новых настроек, нажмите **Apply**. Для возвращения к **SNMP Host Table**, нажмите Show All SNMP Host Table Entries.

SNMP Engine ID

Engine ID – это уникальный идентификатор, используемый для реализации SNMP v3. Это буквенно-цифровая последовательность для идентификации механизма SNMP на коммутаторе. Для отображения SNMP Engine ID Коммутатора, откройте **Administration ⇨ SNMP Manger ⇨ SNMP Engine ID,** что позволит открыть окно **SNMP Engine ID Configuration,** показанное ниже.

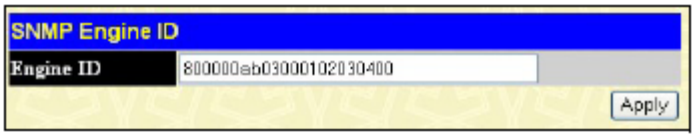


Рисунок 6.33 – Окно «SNMP Engine ID Configuration»

Для изменения Engine ID введите новый Engine ID в нужном поле и нажмите кнопку **Apply**.

D-Link Single IP Management

Обзор технологии Single IP Management (SIM)

D-Link Single IP Management (управление через единый IP-адрес) – технология, которая позволяет объединять коммутаторы в стек поверх Ethernet без стекирующих портов или модулей стекирования. Существуют следующие преимущества в работе с функцией «Single IP Management»:

1. SIM может упростить процесс управления небольшой рабочей группой или коммутационным отсеком, вычисляя размеры сети для увеличения полосы пропускания.
2. SIM может сократить число необходимых в Вашей сети IP-адресов.
3. SIM может исключить использование специализированных кабелей для соединения в стек и преодолеть барьеры расстояния, которые ограничивают возможности топологии при задействовании других технологий стекирования.

Коммутаторы, использующие функцию D-Link Single IP Management (SIM), должны подчиняться следующим правилам:

- SIM – это дополнительная функция коммутатора, которая может быть легко включена или отключена через интерфейс командной строки или Web-интерфейс. Стекирование коммутаторов по технологии SIM не будет влиять на стандартную работу коммутатора в сети пользователя.
- Существует три классификации для коммутаторов, использующих функцию SIM. ***Commander Switch (CS)*** – это управляющий коммутатор в группе, ***Member Switch (MS)*** – это коммутатор, который опознается управляющим коммутатором CS в качестве члена SIM-группы и ***Candidate Switch (CaS)*** – коммутатор, имеющий физическое соединение с SIM-группой, но не распознаваемый мастером CS в качестве члена SIM-группы.
- SIM-группа может иметь только один управляющий коммутатор Commander Switch (CS).
- Все коммутаторы в отдельной SIM-группе должны быть в одной IP-подсети (широковещательном домене). Члены SIM-группы не маршрутизируются.
- В SIM-группе может быть до 33 коммутаторов (нумерация от 0 до 32), включая управляющий коммутатор (нумерованный 0).

Нет ограничений на количество SIM-групп в одной IP-подсети (широковещательном домене), однако один коммутатор может принадлежать только одной группе.

Если настроено большое количество VLAN, SIM-группа будет использовать на любом коммутаторе только VLAN по умолчанию.

Технология SIM может использоваться в сетях, содержащих устройства, не поддерживающие SIM. Это позволяет пользователю контролировать работу коммутаторов, которые находятся на расстоянии более одного hop (скачка) от управляющего коммутатора CS.

SIM-группа – это группа коммутаторов, которые управляются, как единый объект. Коммутаторы могут выполнять три различные функции:

1. **Commander Switch (CS) –** Это коммутатор, настраиваемый вручную в качестве управляющего устройства и обладающий следующими свойствами:
   - Имеет IP-адрес.
   - Не является управляющим коммутатором CS или членом другой SIM-группы.
   - Подключен к другим коммутаторам, являющимися членами группы, через управляющую виртуальную локальную сеть VLAN.
2. **Member Switch (MS) –** Это коммутатор, который является членом SIM-группы и, к которому возможен доступ с управляющего коммутатора CS, он обладает следующими свойствами:
   - Не является управляющим коммутатором или членом другой IP-группы.
   - Подключен к CS через управляющую виртуальную локальную сеть VLAN управляющего коммутатора.
3. **Candidate Switch (CaS) –** это коммутатор, который готов стать членом SIM-группы, но не являющийся еще таковым. При помощи ручной настройки коммутатор Candidate Switch

может стать членом SIM-группы. Коммутатор, настроенный в качестве CaS, который не является членом SIM-группы и обладает следующими свойствами:

- Не является управляющим коммутатором или членом другой IP-группы.
- Подключен к CS через управляющую виртуальную локальную сеть VLAN управляющего коммутатора.

После настройки одного коммутатора в качестве управляющего SIM-группы, другие коммутаторы могут стать членами группы через непосредственное подключение к управляющему коммутатору. Только управляющий коммутатор может обращаться к CaS, он является своеобразной точкой доступа к членам группы. IP-адрес управляющего коммутатора станет адресом для всех членов группы, управление же доступом ко всем членам группы будет осуществляться через пароль администратора CS и/или аутентификацию.

Когда SIM-функция включена, приложения управляющего коммутатора будут перенаправлять пакеты вместо их выполнения.

Приложения будут декодировать пакет от администратора, видоизменять некоторые данные и затем отправлять его членам группы. После выполнения этих действий управляющий коммутатор может получить ответный пакет, который закодирует и отправит обратно администратору.

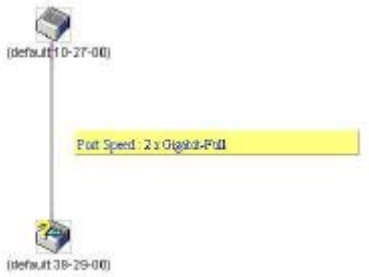
После того, как управляющий коммутатор станет обыкновенным членом SIM-группы, он будет членом первой SNMP-группы (включая права чтения/записи и права только чтения), к которой принадлежит управляющий коммутатор. Однако если у коммутатора MS есть свой собственный IP-адрес, то он может принадлежать к SNMP-группе, в которой другие коммутаторы SIM-группы не состоят.

The Upgrade to v1.50

В целях улучшения работы SIM, коммутаторы серии xStack DES-3800 вышли с обновленной версией SIM 1.50. Главными отличительными особенностями данной версии являются:

1. Управляющий коммутатор CS имеет возможность автоматически определять количество коммутаторов, которые находились в SIM-группе даже в случае перезагрузки или неправильной работы Web. Данную опцию усовершенствовали благодаря использованию пакетов Discover и Maintain, которые в прежней версии члены SIM-группы отбрасывали после перезагрузки коммутатора. При использовании данной версии SIM MAC-адреса и пароли всех членов SIM группы хранятся в базе данных управляющего коммутатора CS. Если происходит перезапуск одного из членов SIM группы, то управляющий коммутатор CS сохраняет соответствующую запись в своей базе данных и при повторном включении члена SIM группы автоматически включает его в SIM-дерево. Таким образом, нет необходимости выполнять какие-либо дополнительные настройки для переобнаружения этого члена SIM группы.
   Есть несколько случаев, когда предварительно сохраненные члены SIM-группы не обнаруживаются управляющим коммутатором. Например, если так и не подключено питание коммутатора, если он все еще остается членом другой SIM-группы или он настроен в качестве управляющего коммутатора CS, то процесс переобнаружения коммутатора не происходит.

2. Топология сети имеет новые возможности для подключения членов группы, теперь будут отображаться скорость и количество Ethernet соединений, создающих группу агрегированных каналов на порту, как это показано на рисунке



3. В этой версии поддерживается Multiple switch upload и download (множественная загрузка) для прошивок, конфигурационных файлов и лог файлов, а именно:

- Прошивка. –Теперь коммутатор поддерживает для членов SIM группы MS множественную загрузку прошивок с TFTP-сервера.

- Конфигурационные файлы. –Теперь коммутатор поддерживает множественную загрузку конфигурационных файлов к(для восстановления конфигурации)/от (для создания резервной копии конфигурации) члену SIM группы MS .

- log-файлы. –Теперь коммутатор поддерживает для членов SIM-группы MS множественную загрузку log-файлов на TFTP-сервер.

4. Теперь пользователь может увеличивать и уменьшать масштаб окна Topology window с целью получить лучшее и четкое отображение.

Подключение функции SIM через Web-интерфейс

Все коммутаторы установлены в качестве коммутаторов CaS согласно заводским настройкам по умолчанию, и функция Single IP Management будет отключена. Для того чтобы подключить функцию SIM через Web-интерфейс, нажмите: **Administration ⇨ Single IP Management ⇨ SIM Settings,** после чего появится следующее окно.

Рисунок 6.34 – Окно «SIM Settings» (disabled – отключено)

Измените SIM состояние **SIM State** на *Enabled* (подключено) при помощи выпадающего меню и нажмите **Apply**, после чего окно обновится и будет выглядеть следующим образом:

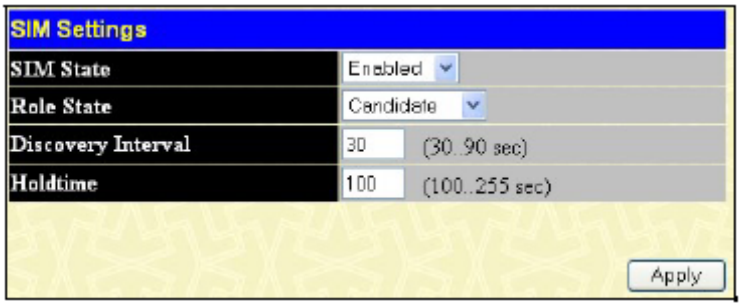


Рисунок 6.35 – Окно «SIM Settings» (enabled – включено)

Если администратор захочет настроить коммутатор в качестве управляющего, необходимо выбрать Commander в поле **Role State** и нажмите **Apply.** Окно еще раз обновится и примет следующий вид:

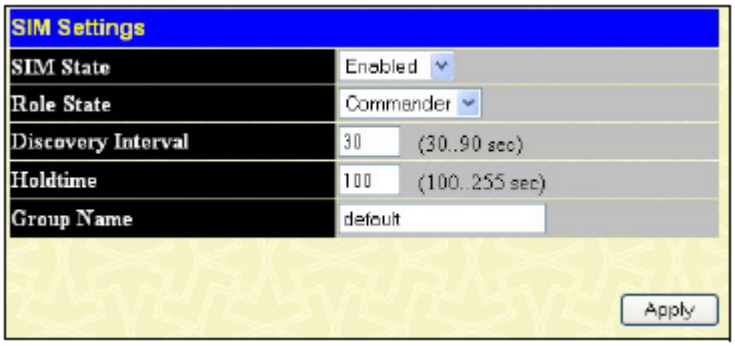


Рисунок 10.2 – Окно «SIM Settings» (Commander enabled)

Можно настроить следующие параметры:

Параметр	Описание
SIM State	Используйте выпадающее меню для изменения SIM-состояния коммутатора. *Disabled* переведет все SIM функции коммутаторе в нерабочее состояние.
Role State	Используйте выпадающее меню для изменения роли коммутатора в SIM-группе. Возможно два варианта: *Candidate* – Candidate Switch (CaS) не является членом SIM-группы, но подключен к управляющему коммутатору Commander Switch (CS). Данная роль коммутатора в SIM-группе является настройкой по умолчанию. *Commander* – Выберите данный вариант, чтобы коммутатор выполнял роль управляющего CS. Пользователь может подключить другие коммутаторы к управляющему поверх Ethernet, чтобы они стали членами этой SIM-группы. Выбирая данную роль для коммутатора, становится возможным настройка SIM.
Discovery Interval	Пользователь может установить интервал посылки в секундах Коммутатором обнаруживающих пакетов (discovery packets).

	Возвращающаяся к коммутатору CS информация будет содержать информацию о других коммутаторах, подключенных к нему (например, MS, CaS). Пользователь может установить Descovery Interval от 30 до 90 секунд.
Holdtime	Коммутатор будет хранить информацию, отправленную с других коммутаторов, в течение данного интервала времени. Пользователь может установить holdtime равным от *100* до *255* секунд.
Group Name	Администратор может назначить имя SIM-группы, в которой коммутатор является управляющим. Имя группы по умолчанию default.

Для того чтобы настройки вступили в силу нажмите **Apply**.
После включения коммутатора в качестве управляющего CS, в папке **Single IP Management** для помощи пользователю в настройке SIM через Web-интерфейс появятся три ссылки: **Topology, Firmware Upgrade** и **Configuration Backup/Restore** и **Upload Log File.**

Топология сети

Окно **Topology** используется для настройки и управления коммутатором без SIM-группы и требует наличие Java-скрипта для правильного функционирования на вашем компьютере.

Java Runtime Environment на Вашем сервере будет установлено, что приведет вас к окну Topology, показанному ниже.

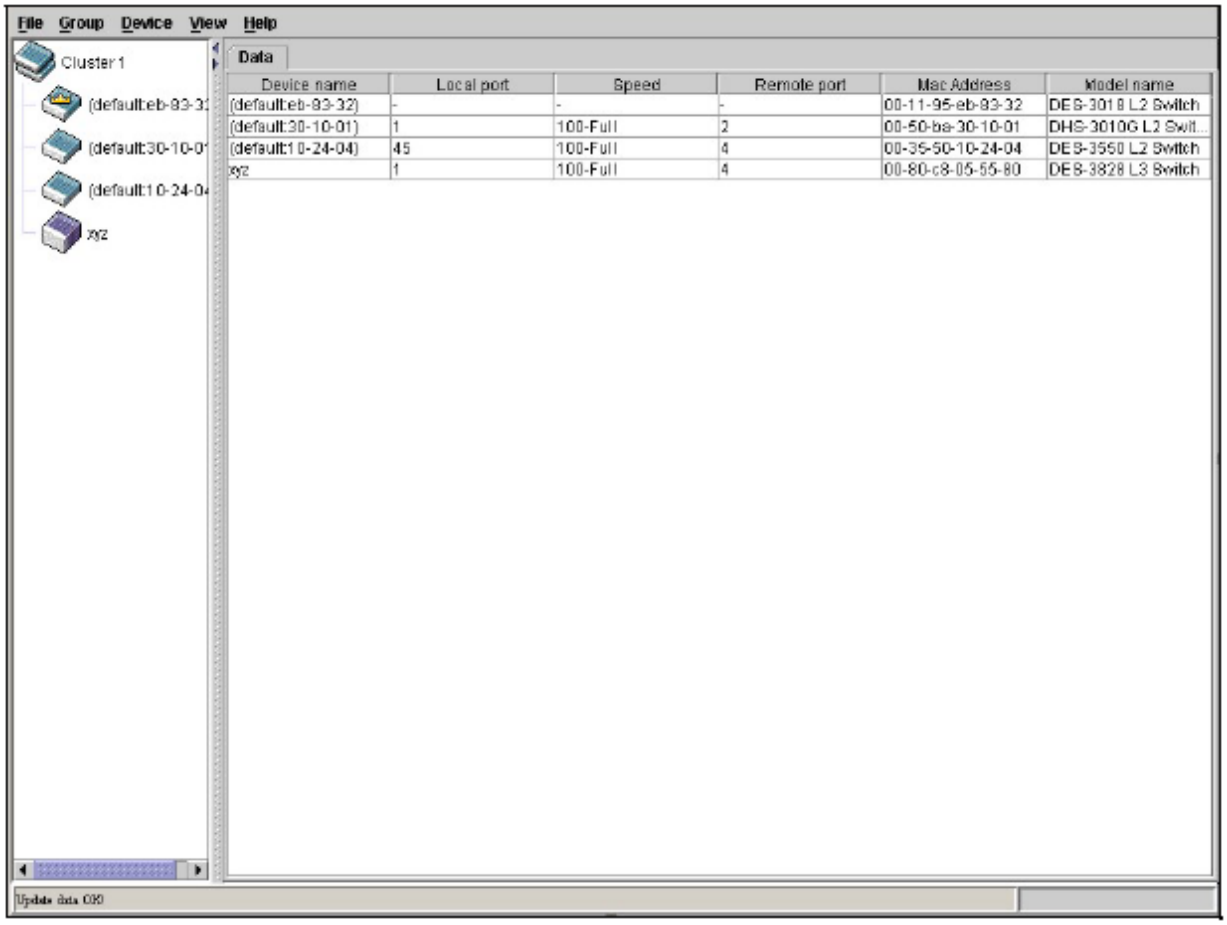


Рисунок 6.37 – Окно «Single IP Management – Tree View»

Окно «Tree View» содержит следующую информацию:

Параметр	Описание
Device Name	Данное поле будет отображать имена устройств, т.е. коммутаторов, в SIM-группе, настроенные пользователем. Если имя устройства не задано, то для идентификации оборудования будет присвоено имя по умолчанию (default), к которому добавляют шесть последних цифр MAC-адреса.
Local Port	Отображает номер физического порта на управляющем коммутаторе CS, к которому подключен MS или CaS. У управляющего коммутатора не будет записи в данном поле.
Speed	Отображает скорость соединения между управляющим коммутатором и MS или CaS.
Remote Port	Отображает номер физического порта на коммутаторе MS или CaS, который подключен к управляющему коммутатору. У управляющего коммутатора не будет записи в данном поле.
MAC Address	Отображает MAC-адрес соответствующего коммутатора.
Model Name	Отображает полное название модели соответствующего коммутатора.

Для просмотра топологии сети **Topology Map**, нажмите **View ⇨ Topology**, в результате чего откроется следующее окно. **Topology View** периодически обновляется (через 20 сек. по умолчанию).

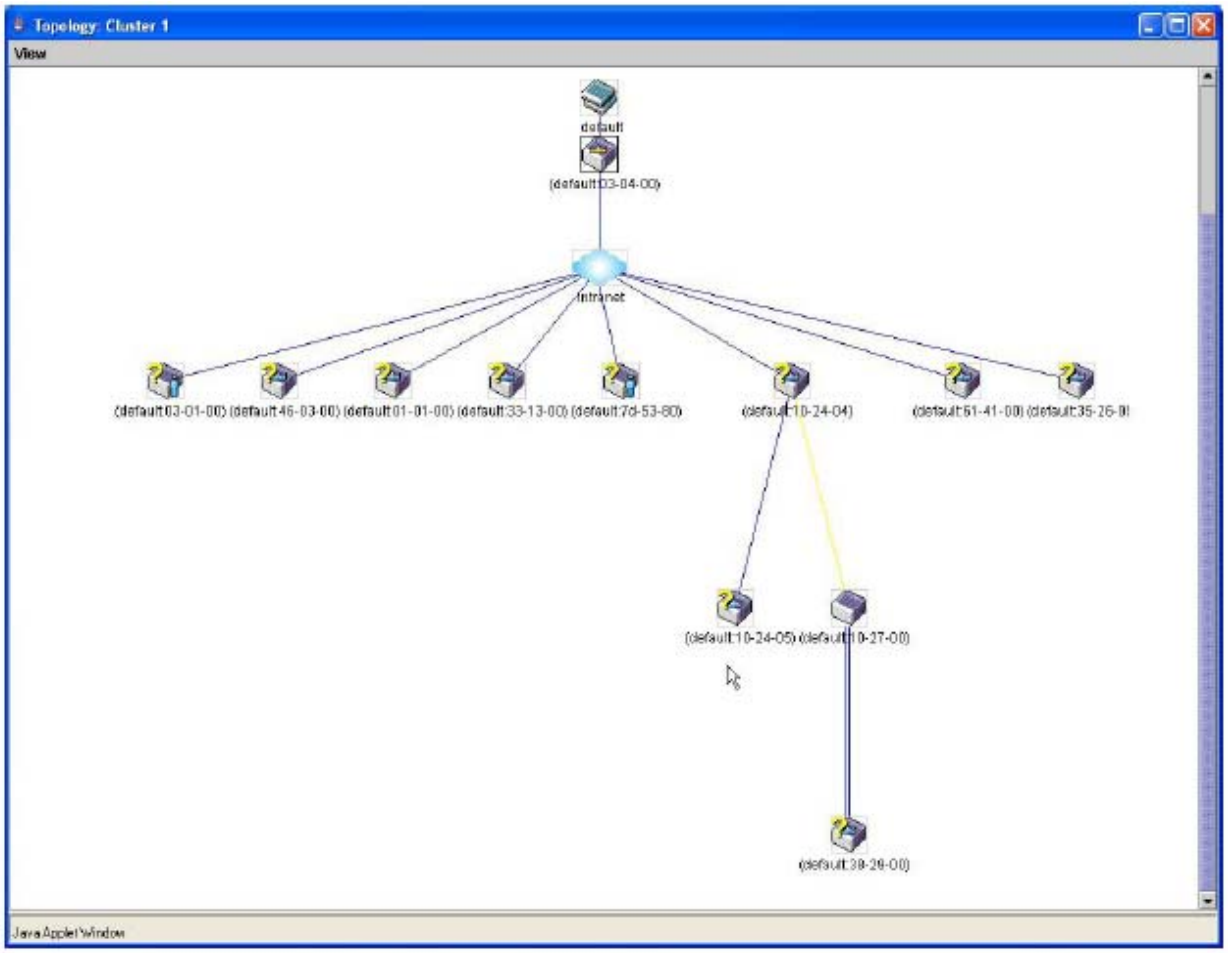


Рисунок 6.38 – Окно «Topology View»

Данное окно покажет, каким образом устройства из группы Single IP Management подключены к другим группам и устройствам. В этом окне могут встретиться следующие значки:

Значок	Описание
	Группа
	Управляющий коммутатор второго уровня
	Управляющий коммутатор третьего уровня
	Управляющий коммутатор CS другой группы
	Коммутатор MS второго уровня
	Коммутатор MS третьего уровня
	Коммутатор MS, который является членом другой группы
	Коммутатор CaS второго уровня
	Коммутатор CaS третьего уровня
	Неизвестное устройство

	Устройство, не поддерживающее SIM-технологию.

Tool Tips

В окне **Topology view** мышка играет важную роль в настройке и просмотре информации об устройстве. Подведите курсор мышки к интересующему вас устройству, изображенному на топологии, после чего появится информация о данном устройстве. В качестве примера просмотрите окно, которое приведено ниже.

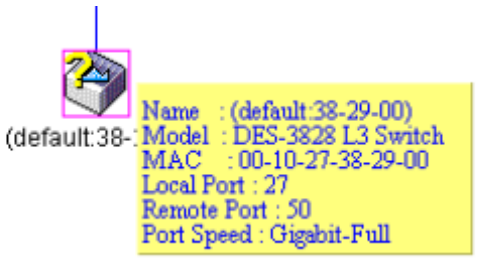


Рисунок 6.39 – Получение информации об устройстве, используя Tool Tips

Установите курсор мышки над линией, соединяющей два устройства, и появится сообщение о скорости соединения между ними, как это показано на рисунке ниже.

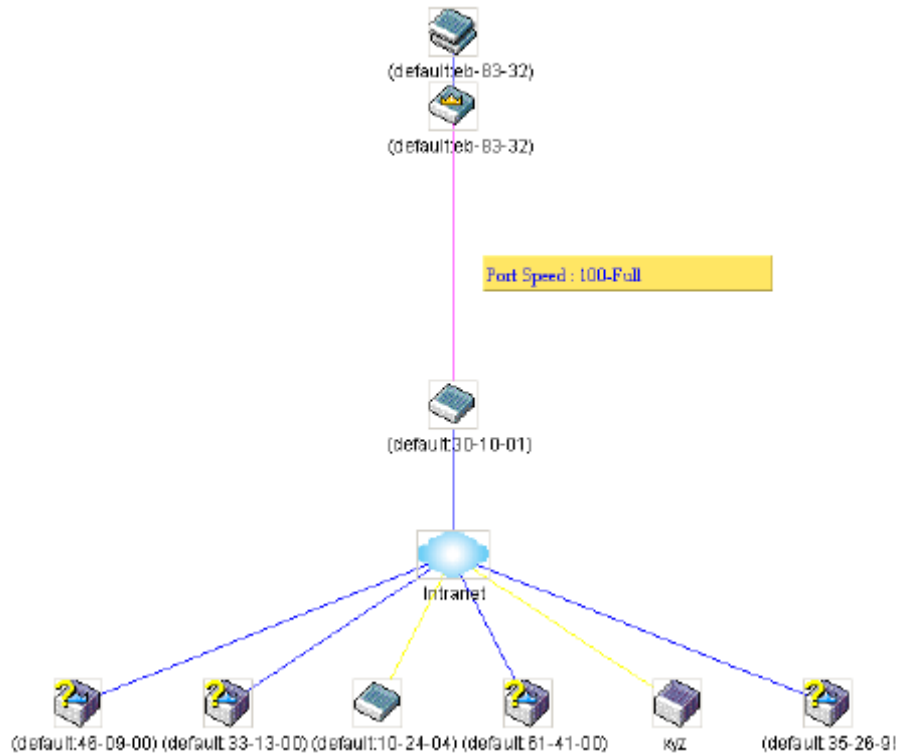


Рисунок 6.40 – Получение информации о скорости порта, используя Tool Tip

Правый клик мышью

Нажатие правой кнопки мышки на устройстве позволит пользователю работать с различными функциями, зависящими от роли коммутатора в SIM-группе.

Пиктограмма группы

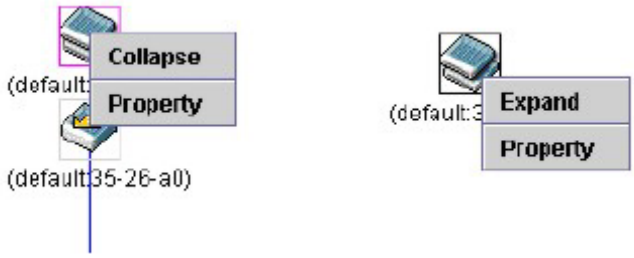


Рисунок 6.41 – Правый клик на пиктограмме группы

Следующие опции могут быть доступны пользователю при настройке:

- **Collapse** – свернуть группу, чтобы она была представлена одним значком.
- **Expand** – развернуть SIM-группу для детального рассмотрения.
- **Property** – показать на экране информацию о группе.

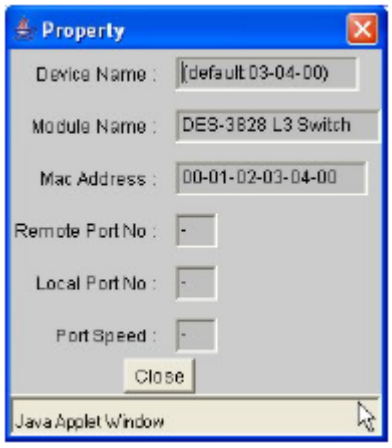


Рисунок 6.42 – Окно «Property»

Пиктограмма управляющего коммутатора

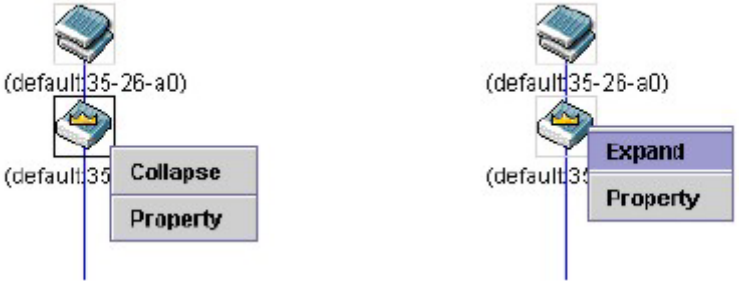


Рисунок 6.43 – Правый клик мыши по пиктограмме управляющего коммутатора

Следующие опции могут быть доступны пользователю при настройке:

- **Collapse** – свернуть группу, чтобы она была представлена одним значком.
- **Expand** – развернуть SIM-группу для детального рассмотрения.
- **Property** – показать на экране информацию о группе.

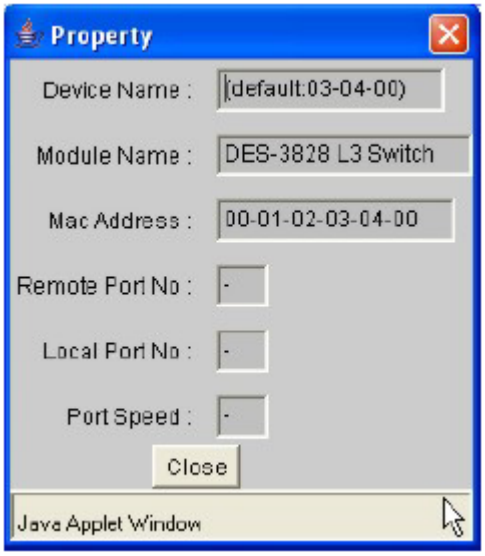


Рисунок 6.44 – Окно «Property»

Пиктограмма Member Switch

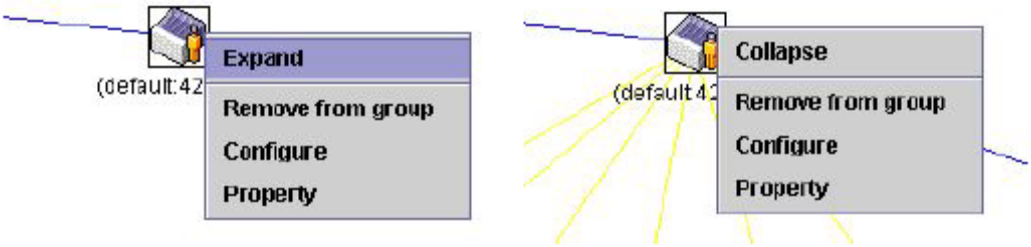


Рисунок 6.45 – Правый клик мышью на пиктограмме Member

Следующие опции могут быть доступны пользователю при настройке:

- **Collapse** – свернуть группу, чтобы она была представлена одним значком.
- **Expand** – развернуть SIM-группу для детального рассмотрения.
- **Remove from group** – удалить коммутатор MS из SIM-группы.
- **Configure** – запустить Web-менеджер для настройки коммутатора.
- **Property** – показать на экране информацию о группе.

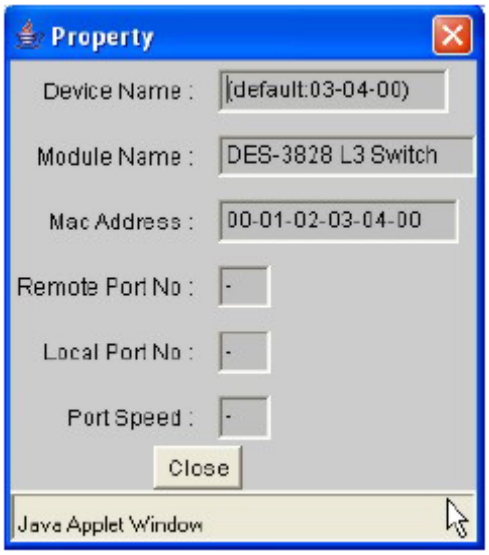


Рисунок 6.46 – Окно «Property»

Пиктограмма Candidate Switch

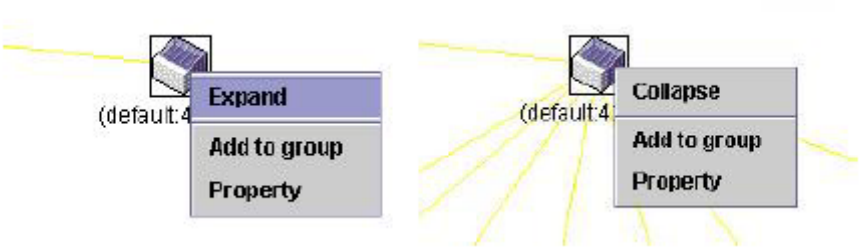


Рисунок 6.47 – Правый клик мышью на пиктограмме Candidate

Следующие опции могут быть доступны пользователю при настройке:

- **Collapse** – свернуть группу, чтобы она была представлена одним значком.
- **Expand** – развернуть SIM-группу для детального рассмотрения.
- **Add to group** – добавить к группе коммутатор CaS. При нажатии на данную ссылку появится диалоговое окно, где пользователю предложат ввести пароль аутентификации коммутатора CaS до его присоединения к SIM-группе, после чего нажмите **OK** для введения пароля или **Cancel** для закрытия окна.

Рисунок 6.48 – Диалоговое окно «Input password»

- **Property** – показать на экране информацию о группе.

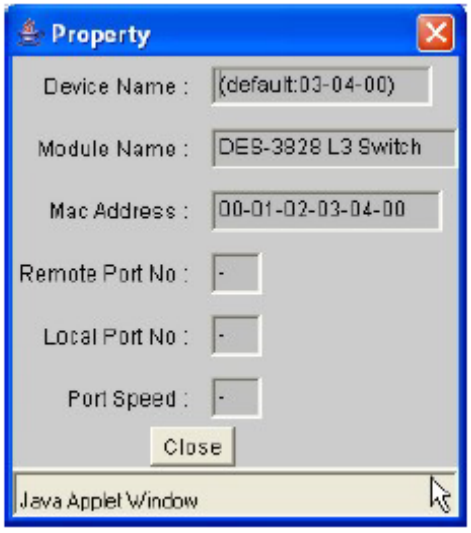


Рисунок 6.49 - Окно «Property»

Данное окно содержит следующую информацию:

Параметр	Описание
Device Name	Данное поле будет отображать имена устройств, т.е. коммутаторов, в SIM-группе, настроенные пользователем. Если имя устройства не задано, то для идентификации оборудования будет присвоено имя по умолчанию (default), к которому добавляют шесть последних цифр MAC-адреса.
Module Name	Отображает полное название модели соответствующего коммутатора, как при нажатии правой кнопки мышки.
MAC Address	Отображает MAC-адрес соответствующего коммутатора.
Remote Port No.	Отображает номер физического порта на коммутаторе MS или CaS, который подключен к управляющему коммутатору. У управляющего коммутатора не будет записи в данном поле.
Local Port No.	Отображает номер физического порта на управляющем коммутаторе CS, к которому подключен MS или CaS. У управляющего коммутатора не будет записи в данном поле.
Port Speed	Отображает скорость соединения между управляющим коммутатором и MS или CaS.

Для закрытия окна **«Property»,** нажмите **Close.**

Линейка меню

В окне «**Single IP Management**» для настройки устройств есть линейка меню, изображенная ниже:

Рисунок 10.17 – Линейка меню в окне «Topology View»

Содержание пяти пунктов меню описывается далее.

File

• **Print Setup** – просмотреть изображение перед печатью.
• **Print Topology** - напечатать топологию.
• **Preference** – показать свойства, такие как, интервал между опросами и варианты просмотра топологий во время запуска SIM.

Group

▪ **Add to group –** добавить к группе коммутатор CaS. При нажатии на **Add to group** появится диалоговое окно, в котором пользователя попросят ввести пароль для аутентификации CaS до его присоединения к SIM-группе, после чего нажмите **OK** для ввода пароля или **Cancel** для закрытия окна.

Рисунок 6.51 - Диалоговое окно «Input password»

▪ **Remove from Group** – удалить коммутатор MS из SIM-группы.

Device

▪ **Configure** – открыть web-менеджер для настройки устройства.

View

▪ **Refresh** – обновить окна просмотра.

▪ **Topology** – показать топологию (окно «Topology View»)

Help

▪ **About** – показать информацию о функции SIM, включая текущую версию SIM.

Примечание: В данной версии прошивки некоторые функции можно настроить только через интерфейс командной строки CLI (Command Line Interface). Для получения более полной информации о технологии SIM и ее настройках, обратитесь к ***DES-3800 Command Line Interface Reference Manual***

Обновление прошивки

Окно «Firmware Upgrade» используется для обновления прошивки на коммутаторе, являющемся членом SIM-группы, с управляющего коммутатора CS. Для доступа к этому окну нажмите: **Administration ⇨ Single IP Management Settings ⇨ Firmware Upgrade.** Коммутатор MS будет

занесен в таблицу и будет определен порт (порт на управляющем коммутаторе, к которому подключен MS), MAC-адрес, название модели и версия. Для того чтобы скачать прошивку на выбранный вами коммутатор, под заголовком **Port** нажмите на соответствующую кнопку, далее введите IP-адрес сервера, на котором она находится, и укажите путь и имя файла прошивки, после чего нажмите **Download**.

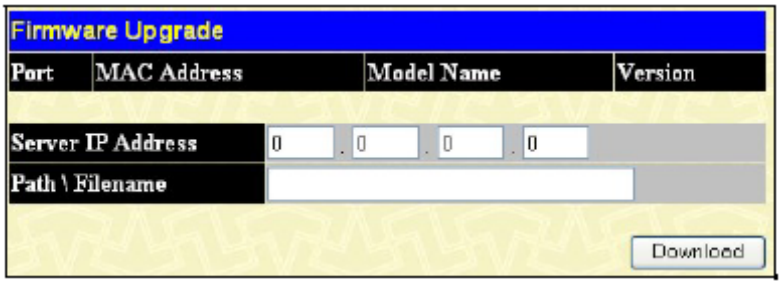


Рисунок 6.52 – Окно «Firmware Upgrade»

Сохранение резервной копии/восстановление конфигурационных файлов

Окно «Configuration File Backup/Restore» используется для обновления конфигурационных файлов на коммутаторе, являющемся членом SIM-группы, с управляющего коммутатора CS с помощью TFTP-сервера. Коммутатор MS будет занесен в таблицу и будет определен порт (порт на управляющем коммутаторе, к которому подключен MS), MAC-адрес, название модели и версия. Для того чтобы скачать конфигурационные файлы на выбранный вами коммутатор, под заголовком Port нажмите на соответствующую кнопку, далее введите IP-адрес сервера, на котором она находится, и укажите путь и имя конфигурационного файла, после чего нажмите **Download**. Нажмите **Upload** для создания резервной копии конфигурационного файла на TFTP-сервере. Для открытия окна «Configuration File Backup/Restore» нажмите: **Administration ⇨ Single IP Management Settings ⇨ Configuration Backup/Restore.**

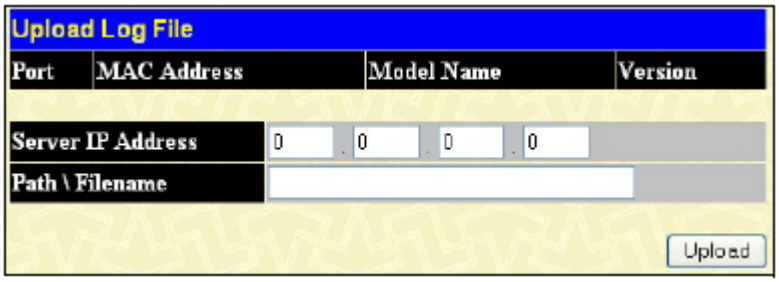


Рисунок 6.53 – Окно «Configuration File Backup/Restore»

Upload Log File

Окно «Upload Log File» используется для загрузки журнала событий с коммутатора, являющегося членом SIM-группы на выбранный компьютер. Для просмотра данного окна нажмите: **Administration ⇨ Single IP Management ⇨ Upload Log File.** Для загрузки журнала событий введите IP-адрес коммутатора, являющегося членом SIM-группы, затем укажите путь на Вашем компьютере, где бы Вы хотели сохранить файл. Для начала скачивания нажмите **Upload**.

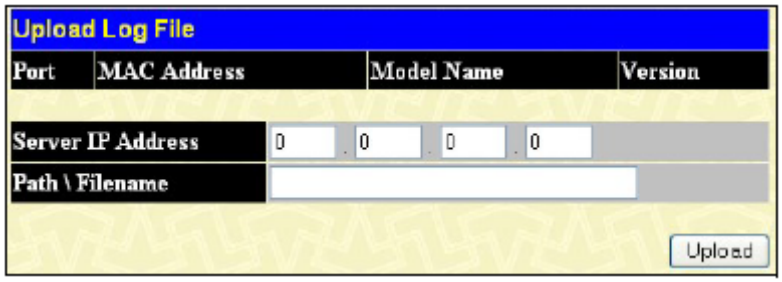


Рисунок 6.54 – Окно «Upload Log File»

Раздел 7 – Опции второго уровня

VLAN
Агрегирование каналов
IGMP Snooping
Spanning Tree
Forwarding

Данный раздел поможет пользователю произвести настройки функций безопасности на коммутаторе. Дается более подробное описание таких опций коммутатора, как VLAN, Trunking, IGMP Snooping, Spanning Tree и Forwarding.

Виртуальные локальные сети

Понятие приоритезации пакетов согласно протоколу IEEE 802.1p

Приоритезация пакетов на основе меток является функцией, определенной стандартом IEEE 802.1p, созданным для управления трафиком сети, в которой одновременно может передаваться большое количество различных типов данных. Приоритезация решает проблемы, связанные со временем доставки данных, чувствительных к задержке. На качество приложений, таких как, например, видео-конференция, может неблагоприятно влиять даже очень небольшие задержки времени. Сетевое оборудование, совместимое со стандартом IEEE 802.1p, имеет возможность определять уровень приоритета пакетов данных. Такие устройства могут также добавлять или извлекать метки из заголовков пакетов, именно в метках указываются степень срочности передачи пакетов и очередь, которая должна быть им назначена. Всего существует 8 очередей, т.е. значения тегов назначаются от 0 до 7, причем 0 – имеет низший приоритет данных, а 7 – наивысший. Седьмой наивысший приоритет обычно используется только для данных видео или аудио-приложений, которые чувствительны к малейшим задержкам времени, или для данных от определенных конечных пользователей, которые заключили особое соглашение на присвоение передаваемому трафику седьмого приоритета.
Коммутатор позволяет задавать пути прохождения маркированных пакетов по сети. Использование очередей для управления маркированными данными позволяет определять относительную приоритетность данных для вашей сети. Возможны случаи, когда было бы полезно сгруппировать два или более маркированных пакетов с различными приоритетами в одну очередь. Однако, обычно рекомендуется, чтобы за очередью с наивысшим приоритетом, Queue 7, были зарезервированы пакеты данных со значением приоритета 7. Пакеты с незаданным значением приоритета помещаются в нулевую очередь, Queue 0, и, таким образом, им присваивается самый низкий приоритет при доставке.
Существует две схемы обслуживания очередей: строгая очередь приоритетов и взвешенный циклический алгоритм, благодаря которым определяется соотношение, по которому в очередях удаляются пакеты. Соотношение, используемое для очистки очередей 4:1. Это означает, что из очереди с наивысшим приоритетом Queue 7, будет удаляться по 4 пакета на каждый удаленный пакет из нулевой очереди, Queue 0.
Помните, что настройки приоритетной очереди на коммутаторе действуют для всех портов и всех устройств, подключенных к нему. Данная система приоритетных очередей будет особенно полезна, если в сети работают коммутаторы с возможностью назначения приоритетных меток.

Описание виртуальных локальных сетей VLAN

Виртуальная локальная сеть (VLAN, Virtual Local Area Network) – топология сети, настроенная в соответствии скорее с логической схемой, чем с физическим размещением. Виртуальные

локальные сети можно использовать для объединения LAN сегментов в автономную пользовательскую группу, которая предстает в качестве одиночной локальной сети. Виртуальная локальная сеть представляет собой логический сегмент сети в различных широковещательных доменах, таким образом, пакеты направляются между портами внутри VLAN. Обычно VLAN соответствует какой-то подсети, но не обязательно. Виртуальные локальные сети могут улучшать характеристики путем сохранения полосы пропускания, улучшить параметры безопасности путем ограничения трафика на определенные домены. Виртуальная локальная сеть – это логическая группа конечных узлов. Конечные узлы, которые часто общаются друг с другом, объединяются в одну виртуальную сеть независимо от их физического расположения в сети. Логически, виртуальная локальная сеть подобна широковещательному домену, поскольку широковещательные пакеты отправляются только членам VLAN сети, в которой и были созданы.

ОТЛИЧИТЕЛЬНЫЕ ПРИЗНАКИ СЕТЕЙ VLAN, ПОСТРОЕННЫХ НА КОММУТАТОРАХ DES-3800

Неважно, по какому принципу происходит однозначная идентификация конечных узлов и объединение этих узлов в VLAN, пакеты не могут проходить через сети VLAN без сетевого устройства, выполняющего функции маршрутизации между сетями VLANs.
Коммутаторы DES-3800 серии поддерживают VLAN на основе стандарта IEEE 802.1Q и VLAN на базе портов. Функция «port untagging» используется для удаления тега 802.1Q из заголовка пакетов для поддержки совместимости с устройствами, не поддерживающими теги.
Настройки коммутатора по умолчанию предполагают назначение всех портов в состояние 802.1Q VLAN, именуемой «сетью по умолчанию».
По умолчанию VLAN имеет значение VID = 1.
Порты сетей VLAN на основе порта могут перекрываться, если это необходимо.

IEEE 802.1Q VLANs

Некоторые тематические термины:

- **Tagging –** добавление тега в заголовок пакета (802.1Q VLAN).
- **Untagging –** удаление тега из заголовка пакета (802.1Q VLAN).
- **Ingress port** – порт коммутатора, на который приходят пакеты, когда определена VLAN.
- **Egress port –** порт коммутатора, с которого уходят пакеты на другой коммутатор или станцию, производится тегирование.

На Коммутаторе применяется стандарт IEEE 802.1Q (tagged) VLANs. IEEE 802.1Q VLANs требует тегирования, которое позволит охватить всю сеть (считается, что все коммутаторы сети поддерживают IEEE 802.1Q).
VLAN позволяют сегментировать сеть для того, чтобы снизить размер широковещательных доменов. Все пакеты, пришедшие в VLAN пересылаются только на станции (через коммутаторы, поддерживающие IEEE 802.1Q), являющиеся членами данной VLAN, и это включает передачу broadcast, multicast и unicast-пакетов от неизвестных источников.
VLAN также обеспечивает дополнительный уровень защиты сети. IEEE 802.1Q VLANs доставляет пакеты только между станциями одной VLAN.
Любой порт может быть сконфигурирован как для поддержки tagging, так и для untagging. Функция untagging IEEE 802.1Q VLANs позволяет VLANs работать с коммутаторами, не поддерживающими распознавание VLAN тегов в заголовках пакетов. Функция tagging позволяет VLAN охватывать управляемые коммутаторы, поддерживающие 802.1Q, через одну физическую связь и разрешает Spanning Tree быть включённым на всех портах и нормально работать.
Стандарт IEEE 802.1Q ограничивает пересылку нетегированных пакетов на принимающий порт VLAN.
Основными характеристиками IEEE 802.1Q являются:

- Назначение пакетов на VLAN через фильтрацию.
- Наличие единственного глобального Spanning Tree.
- Использует явную схему одноуровнего тегирования.
- 802.1Q VLAN Packet Forwarding.
- Решение о пересылке пакетов основывается на следующих трёх правилах:
- Ingress rules – управляет классификацией принимаемых фреймов VLAN.

- Forwarding rules между портами – решает отбросить или переслать пакет.
- Egress rules – определяет, может ли пакет быть послан тегированным или нетегированным

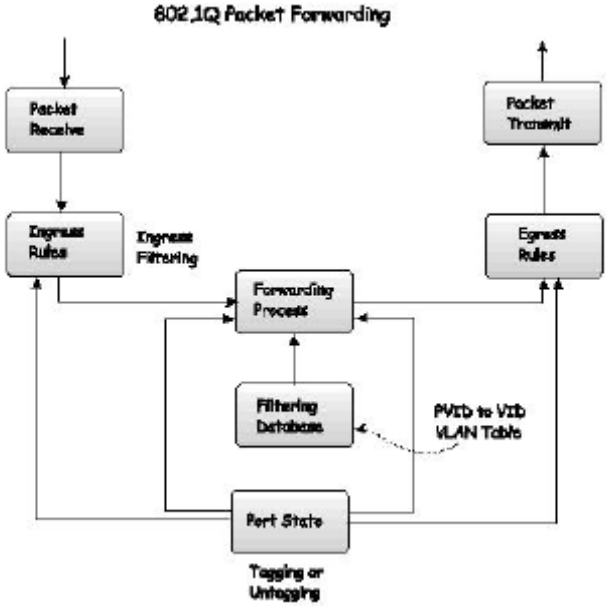


Рисунок 7.1 – Пересылка пакетов согласно IEEE 802.1Q

Метки 802.1Q VLAN

Рисунок, представленный ниже, показывает 802.1Q VLAN тег. Добавляются четыре байта после MAC-адреса источника. Их присутствие обозначено значение 0x8100 в поле EtherType. когда значение поля EtherType равно 0x8100, значит, в пакете присутствует IEEE 802.1Q/802.1p тег. Тег содержит следующие два байта и включает 3 бита приоритета пользователя, 1 бит Canonical Format Identifier (CFI – используется для инкапсуляции Token Ring пакетов с целью переноса их через Ethernet backbones), 12 битов VLAN ID (VID). 3 бита приоритета пользователя используются 802.1p. VID – идентификатор VLAN, используется стандартом 802.1Q. Т.к. длина VID 12 бит, то может адресоваться только 4094 различных VLAN.
Добавление тега в заголовок пакета делает пакет длиннее на 4 байта. Вся информация, первоначально содержащаяся в пакете, сохраняется дальше.

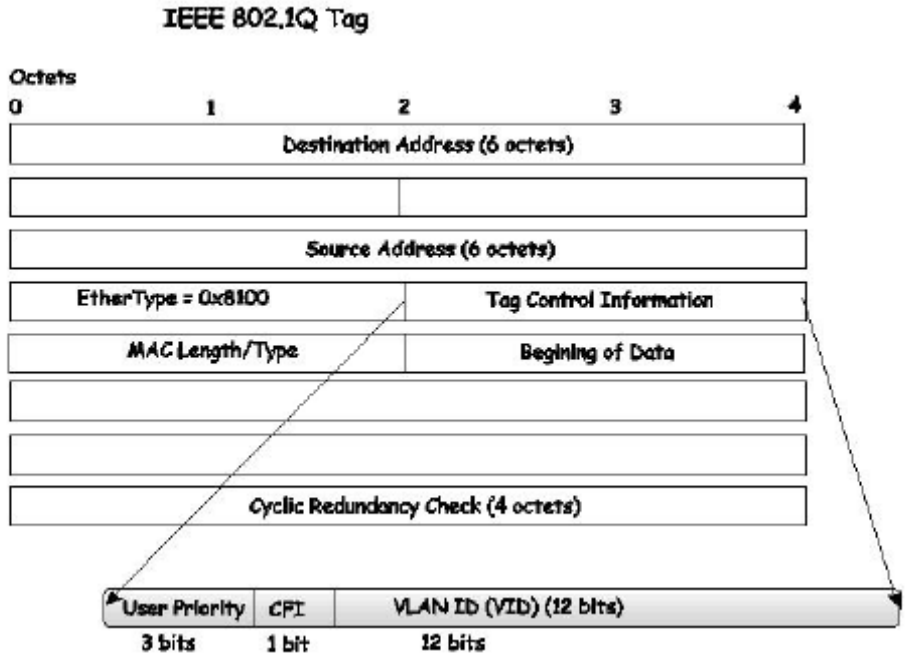
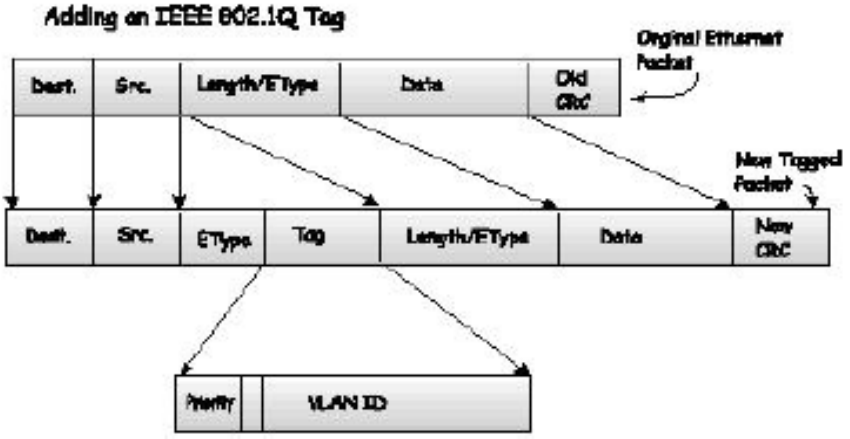


Рисунок 7.2 – Метка IEEE 802.1Q

EtherType и VLAN ID вставляются после MAC-адреса, но до EtherType/Length or Logical Link Control. Т.к. пакет теперь несколько длиннее, чем первоначально, Cyclic Redundancy Check (CRC) должен быть пересчитан.



Port VLAN ID

Тегированные пакеты (несущие информацию 802.1Q VID) могут быть переданы от одного устройства, поддерживающего 802.1Q, к другому. Это позволяет 802.1Q VLANs охватить сетевые устройства (и более того, всю сеть, если все устройства поддерживают 802.1Q).

К сожалению, не все устройства поддерживают 802.1Q. Эти устройства отнесены к tag-unaware. 802.1Q – устройства отнесены к tag-aware.

До принятия 802.1Q VLANs, VLAN на основе портов и MAC-адресов использовались совместно. Эти VLAN для пересылки пакетов использовали Port VLAN ID (PVID). Пакет, принятый на передающий порт, дополняется PVID, затем пересылается на соответствующий адрес порта (находящийся в таблице Коммутатора). Если PVID порта, который принял пакет, отличается от PVID порта, который передал пакет, Коммутатор отбросит пакет.

Внутри Коммутатора различные PVID означают различные VLAN (стоит помнить. что различные VLAN не коммутируются без внешнего маршрутизатора). Итак, идентификация VLAN, основанная на PVID не может создать VLANs, расширяющиеся через передающие коммутаторы (или стеки коммутаторов).

Каждый физический порт на Коммутаторе обладает своим PVID. Порты 802.1Q также связаны с PVID, для использования внутри Коммутатора. Если на Коммутаторе не задан VLAN, все порты будут связаны с VLAN по умолчанию с PVID, равным 1. Не тегированные пакеты связаны с PVID порта, на который они принимаются. Решение о пересылке принимается исходя из PVID на столько, на сколько это касается VLAN. Тегирование пакеты пересылаются, следуя содержащемуся в теге VID. Тегированные пакеты также связаны с PVID, но PVID не используется при пересылке.

Tag-aware коммутаторы должны хранить таблицу связи PVID внутри коммутатора с VID сети. Коммутатор сравнивает VID передаваемого пакета с VID порта, передающего пакет. Если эти два VID различны, то Коммутатор отбросит пакет. Т.к. существует PVID для нетегированных пакетов и VID для тегированный, tag-aware и tag-unaware устройства существуют в одной сети.

Порт коммутатора может содержать только один PVID, но может обладать таким количеством VID, какое сможет хранить Коммутатор в таблице VLAN.

Поскольку несколько устройств в сети могут быть tag-unaware, решение должно приниматься каждым портом tag-aware устройства до передачи пакетов – должен пакет быть послан или нет? Если передающий порт соединён с tag-unaware устройством, пакет будет нетегированным. Если передающий порт соединён с tag-aware устройством, пакет будет тегированным.

Тегирование и нетегирование

Каждый порт, поддерживающий 802.1Q, может быть сконфигурирован как тегирующий или нетегирующий.
Тегирующие порты добавляют VID, приоритет и другую VLAN-информацию в заголовки всех пакетов, проходящих через эти порты. Если в пакет уже был добавлен тег, то порт сохраняет VLAN информацию нетронутой. Остальные 802.1Q устройства, принимая решение о пересылке пакетов, используют эту VLAN-информацию.
Нетегирующий порт неспособен считывать тег 802.1Q из проходящих через него пакетов. Если у пакета нет тега802.1Q VLAN, порт не изменит пакет. Таким образом, пакеты, принятые или переданные через нетегирующий порт, не содержат информации802.1Q VLAN. (Следует помнить, что PVID используется только внутри Коммутатора). Нетегирование используется для посылки пакетов с устройств, поддерживающих 802.1Q, на сетевые устройства, не поддерживающие эту функцию.

Ingress фильтрация

Порт Коммутатора, на который приходят пакеты и при решениях, касающихся VLAN, этот порт называется входным портом. Если на порту установлен входной фильтр, то Коммутатор будет проверять VLAN-информацию в заголовке пакета и решать, стоит ли пересылать пакет или нет.
Если в пакете присутствует VLAN-информация, входной порт сначала проверит, является ли он членом VLAN, указанной в теге. Если нет, то пакет будет отброшен. Если входной порт является членом 802.1Q VLAN, то коммутатор определит, является ли порт назначения членом 802.1Q VLAN. Если нет, пакет будет отброшен.
Если порт назначения является членом 802.1Q VLAN, пакет будет передан и порт назначения перешлёт его дальше в сегмент сети, с которой он связан.
Если пакет не содержит VLAN-информацию, входной порт снабдит его своим собственным PVID как VID (если это тегирующий порт). Затем коммутатор определяет, является ли порт назначения членом той же самой VLAN (т.е. содержит такой же VID), что и входной порт. Если это не так, пакет отбрасывается. Если у порта назначения тот же самый VID, то пакет будет передан и порт назначения перешлёт его дальше в сегмент сети, с которой он связан.
Этот процесс называется входным фильтром и используется для сохранения полосы пропускания внутри Коммутатора путём отбрасывания пакетов, которые не относятся к тому же самому VLAN, что и входной порт.

VLAN по умолчанию

Коммутатор настраивает одну VLAN, VID = 1, называемую виртуальной локальной сетью по умолчанию. Заводские настройки по умолчанию «default» назначаются всем портам коммутатора. Как только будут настроены новые VLAN на основе портов, соответствующие номера портов будут удалены из настроек по умолчанию. Если члену одной VLAN необходимо связаться с членом другой VLAN, соединение должно осуществляться через внешний маршрутизатор.

Примечание: При отсутствии настроенных виртуальных локальных сетей на коммутаторе, все пакеты будут направляться на любой порт назначения. Пакеты с неизвестным адресом источника будут наполнять все порты. Широковещательные и многоадресные пакеты также будут наполнять все порты.

Пример представлен ниже:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Рисунок 7.4 – Пример VLAN – назначенные порты.

VLAN на базе портов

VLAN на основе портов ограничивают входящий и исходящий трафик на портах коммутатора. Таким образом, все устройства, соединённые с портом являются членами VLAN(s), которому относится данный порт, будь то отдельный компьютер или целый отдел.
В VLAN на основе портов сетевым информационным центрам (NICs) нет необходимости в идентификации тегов 802.1Q в заголовках пакетов. NICs посылают и принимают обычные Ethernet-пакеты. Если адрес назначения пакета лежит в том же самом сегменте, передача происходит по обычным Ethernet-протоколам. Когда адресом назначения пакета является порт другого коммутатора, решается должен ли пакет быть отброшен Коммутатором или доставлен.

Сегментация VLAN

Возьмём для примера пакет, переданный устройством на порт 1 (Port 1), который является членом VLAN 2. Если адрес назначения пакета – другой порт (найден в обычной таблице пересылки), тогда Коммутатор определяет, является ли другой порт (Port 10) членом VLAN 2 (значит может принимать пакеты VLAN 2). Если Port 10 не относится к VLAN 2, тогда пакет будет отброшен Коммутатором и не достигнет своего адреса назначения. Если Port 10 относится к VLAN 2, то пакет пройдёт. Это достигается путём накладывания VLANs. Это порты, которые принадлежат более чем одной VLAN-группе. Например для VLAN 1 установлены порты 1, 2, 3, и 4; для VLAN 2 – порты 1, 5, 6, и 7. Порт 1 принадлежит двум группам VLAN. Порты 8, 9, и 10 не сконфигурированы ни для одной VLAN-группы. Это означает, что порты 8, 9, и 10 находятся в одной VLAN-группе.

VLAN и группы агрегированных каналов

Члены группы агрегированных каналов обладают общими настройками VLAN. Любые настройки VLAN для члена группы будут распространены на остальные порты.

Примечание: Для того, чтобы использовать VLAN-сегментацию в сочетании с группой агрегированных каналов, сначала надо установить группу(ы) агрегированных каналов, после этого можно конфигурировать настройки VLAN. Если требуется изменить группировку в группах агрегированных каналов, при этом VLANs уже установлены, переконфигурировать VLANs не нужно, достаточно только изменить настройки групп агрегированных каналов. Настройки VLAN автоматически изменятся с изменением настроек групп агрегированных каналов.

Guest VLANs

802.1x необходим для обеспечения устройствам, не поддерживающим данный стандарт, или несовместимым с ним устройствам (как, например, компьютер, работающий с операционной системой Windows 98 или более ранними версиями операционной системы), ограниченного доступа к сети, а также для того, чтобы некоторые пользователи («гости») смогли получить доступ к сети без полной авторизации. С этой целью в коммутаторе сегодня применяются сети Guest 802.1x VLANs. Эти сети VLANs будут иметь ограниченные права доступа и характеристики, отличающиеся от других VLANs на сети. Для создания Guest 802.1x VLANs пользователь сначала должен создать VLAN на сети с ограниченными правами на сети и затем подключить ее как Guest 802.1x VLAN. Далее администратор должен создать учетные записи «гостей», подключающихся к коммутатору, чтобы они имели доступ в Guest VLAN при попытке подключения к коммутатору. При первом подключению к коммутатору желаемые клиентом услуги коммутатора должны быть аутентифицированы либо удаленным RADIUS сервером или локально на коммутаторе, чтобы подключиться к полноценной VLAN. Если аутентификация прошла успешно и аутентификатор принял информацию по размещению VLAN (VLAN placement information), то клиент может быть принят в полностью задействованную target VLAN (VLAN

назначения) с подключением стандартных функций коммутатора для клиента. Если аутентификатор не получил информацию по размещению в VLAN назначения, клиент будет возвращен в исходную VLAN. Если клиент не прошел аутентификацию у аутентификатора, он будет перемещен в Guest VLAN, где он будет иметь ограниченные доступ и права. Приводимый рисунок позволит лучше разобраться в процессах, происходящих в Guest VLAN.

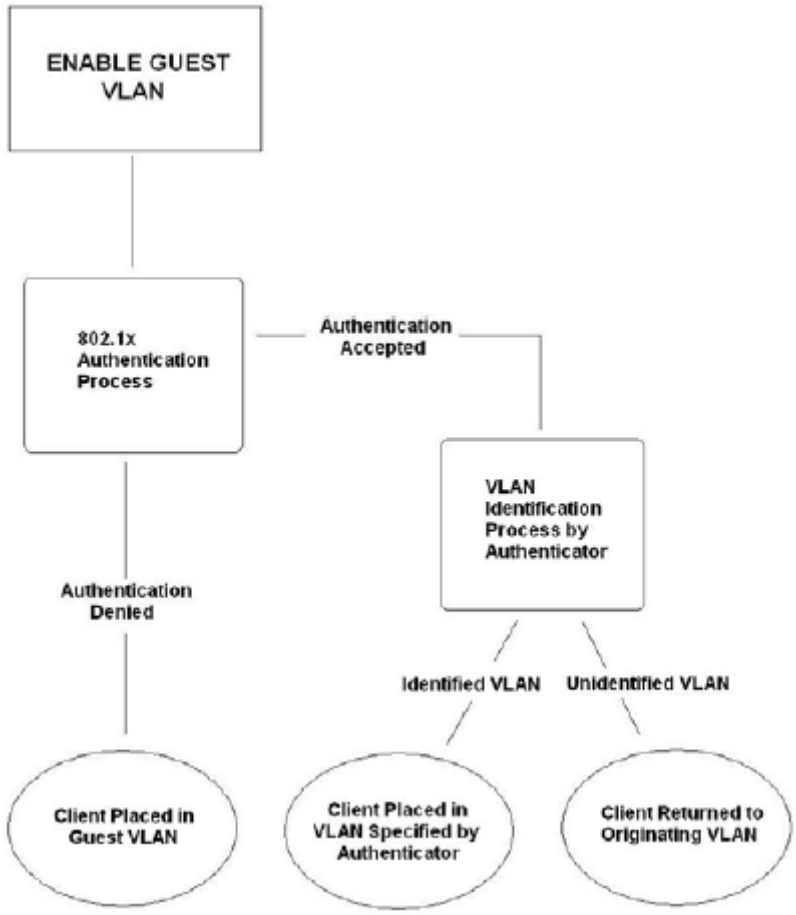


Рисунок 7.5. Процесс аутентификации Guest VLAN

Ограничения при использовании Guest VLAN

1. Guest VLANs поддерживаются только VLANs на базе портов. VLAN на базе MAC-адресов не могут поддерживать Guest VLANs.
2. Порты, поддерживающие Guest VLANs, не могут поддерживать GVRP и наоборот.
3. Порт не может быть членом Guest VLAN и Static VLAN(статичной VLAN) одновременно.
4. Если клиент подключен к Target VLAN , он уже не имеет доступа к Guest VLAN.
5. Если порт подключен к нескольким VLANs, он не может быть включен в Guest VLAN.

Double VLANs

Double или Q-in-Q VLANs позволяют сетевым провайдерам расширять конфигурации их VLAN, предоставляя заказчикам, наряду с обычной VLAN , также VLAN с большим функционалом, что приводит к добавлению дополнительного уровня в конфигурации VLAN. Это в основном позволяет крупным Интернет-провайдерам создать L2 Virtual Private Network (VPN, виртуальная частная сеть второго уровня), а также для их заказчиков- прозрачные сети VLANs, к которым будут подключаться две или больше LANs заказчика, созданных без дополнительных настроек на стороне пользователя. При этом появилась возможность иметь свыше 4000 VLANs, таким образом, мы имеем значительно расширяемую сеть, благодаря возможностям по поддержке пользователей множественных VLANs.

Double VLANs представляют собой обычные VLANs, тегированные, кроме обычного тега SPVID (Service Provider VLAN ID), при помощи TPID (Tagged Protocol ID) идентификатора, выраженного в шестнадцатиричном формате и вставляемого вместе с тегом VLAN в пакет. В результате пакет показывается как дважды тегированный и отделяется от других VLANs в сети, создавая таким образом иерархию сетей VLANs.

Ниже приведен образец Double VLAN тегированного пакета.

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload

Рассмотри приведенный ниже пример:

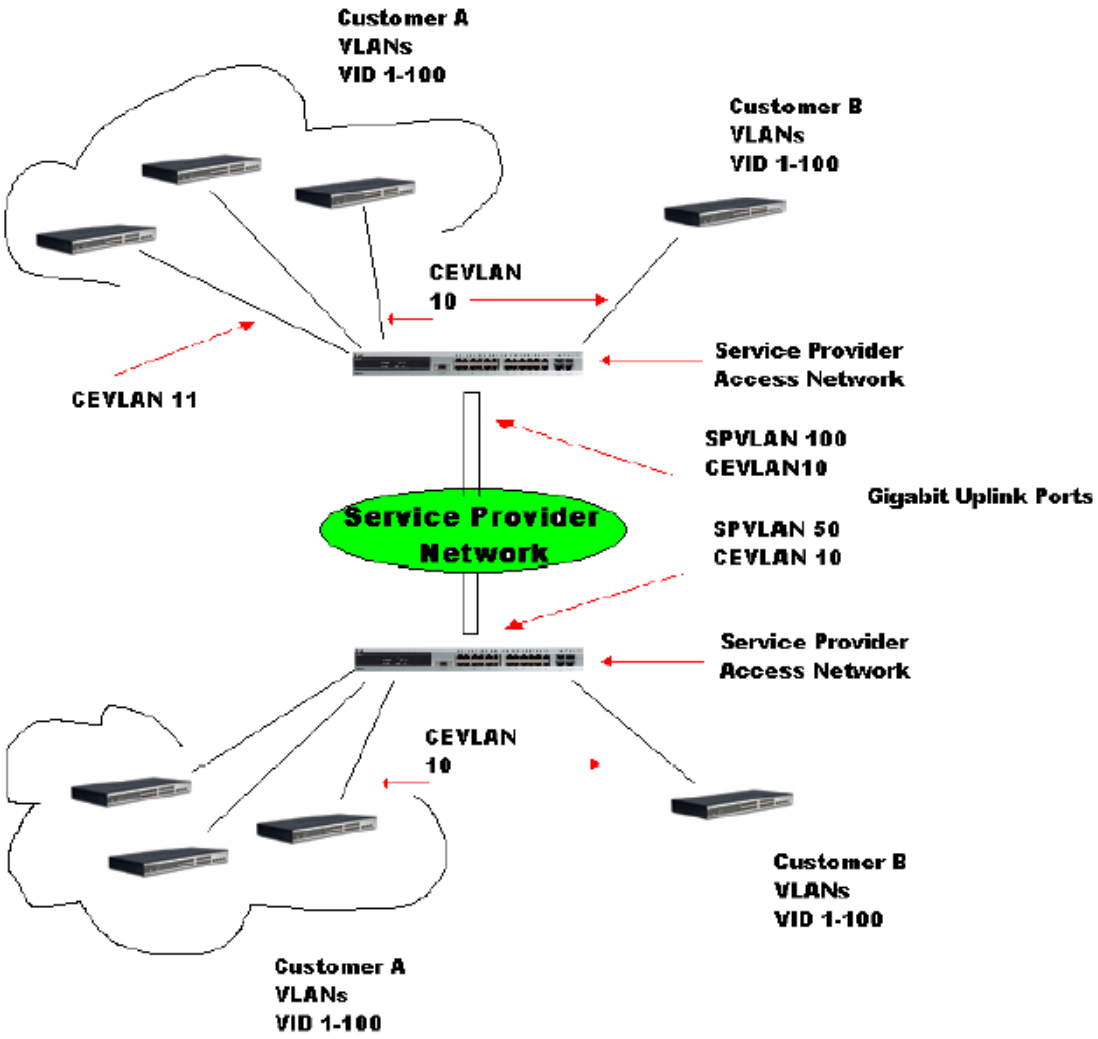


Рисунок 7.6. Пример Double VLAN

В приведенном примере коммутатор поставщика услуги доступа к сети (Provider Edge коммутатор) – устройство, создавшее и поддерживающее Double VLANs. Обе CEVLANs (VLANs заказчика), 10 и 11, тегированы с SPVID100 у провайдера услуг доступа к сети и поэтому принадлежат к одной VLAN на сети провайдера, становясь таким образом членом двух VLANs. Таким образом, заказчик может воспринимать их как обычные VLANs, а поставщик услуг может создать Double VLANs заказчика с помощью одного SPVLAN, маршрутизируя трафик на коммутаторе провайдера. Эта информация затем попадает в главную сеть провайдера и рассматривается здесь уже как одна VLAN, с одним набором протоколов и одним способом маршрутизации.

Нормы для Double VLANs

Необходимо соблюдать некоторые правила и нормы при построении Double VLAN.

1. На пограничном коммутаторе провайдера на всех портах должны быть настроены SPVID и соответствующий ему TPID.

2. Все порты должны быть настроены как порты доступа или Uplink-порты. Порты доступа могут быть только портами Ethernet, в то время как Uplink-порты могут быть только портами Gigabit.

3. Пограничные коммутаторы поставщика услуг должны поддерживаться кадры как минимум 1522 байта или больше, с учетом добавления SPVID тега.

4. Порты доступа не должны тегироваться поставщиком услуг, Uplink-порты должны тегироваться поставщиком услуг.

5. На коммутаторе не могут сосуществовать как Double, так и нормальные VLANs. Если меняется тип VLAN, все списки контроля доступа (ACL) сбрасываются и должны быть перенастроены.

6. Когда подключена Double VLAN, протокол GVRP должен быть отключен.

7. Все пакеты, присланные с CPU на порт доступа не должны содержать теги.

8. Следующие функции должны быть отключены, когда коммутатор находится в режиме Double VLAN:

- Guest VLANs
- Web-интерфейс контроля доступа
- IP Multicast routing (широковещательная маршрутизация по IP)
- GVRP
- Все повторяющиеся функции 802.1Q VLAN

Static VLAN Entry

Войдя в папку **L2 Features**, нажмите **VLAN>Static VLAN Entry**, чтобы открыть следующее окно:

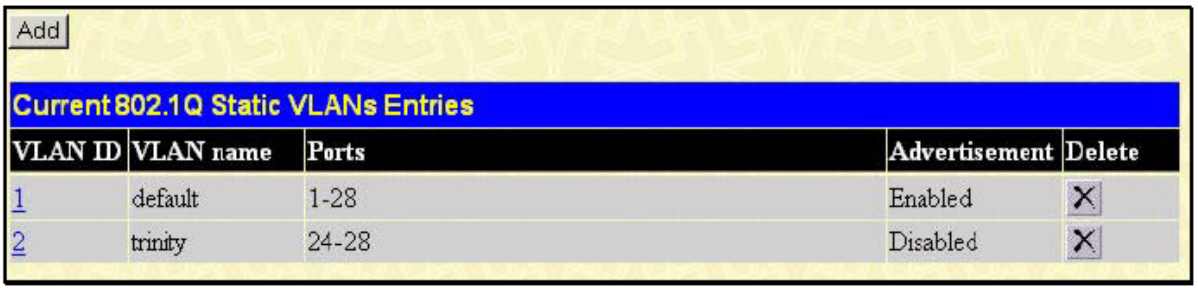


Рисунок 7.7. Окно Current 802.1Q Static VLANs Entries

Окно **802.1Q Static VLANs** показывает все сконфигурированные VLANs (имя и ID). Для удаления 802.1Q VLAN следует кликнуть по соответствующей *X* под надписью **Delete**.
Для создания нового 802.1Q VLAN, необходимо в окне **802.1Q Static VLANs** кликнуть по кнопке **Add**. Появится новое окно, как показано ниже. Окно предназначено для конфигурирования настроек порта и для связи уникального имени и номера с новым VLAN. Описание параметров представлено в таблице нового окна:

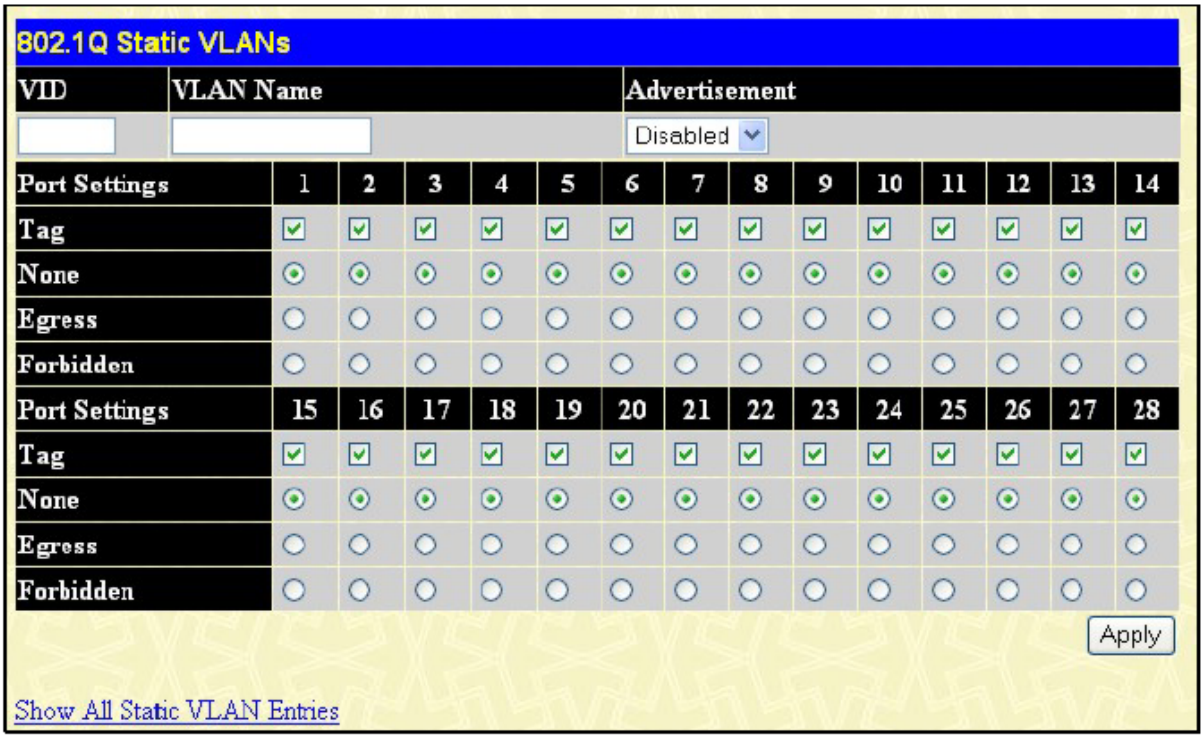


Рисунок 7-8. Окно 802.1Q Static VLANs - Add (добавить)

Для возвращения в окно **Current 802.1Q Static VLANs Entries** следует кликнуть на ссылку Show All Static VLAN Entries. Чтобы изменить уже существующий 802.1Q VLAN необходимо нажать на соответствующую кнопку **Modify**. Появится новое меню для конфигурирования настроек порта и связи уникального имени и номера с новым VLAN. Описание параметров представлено в таблице ниже.

Примечание: Коммутатор поддерживает до 4к постоянных VLAN

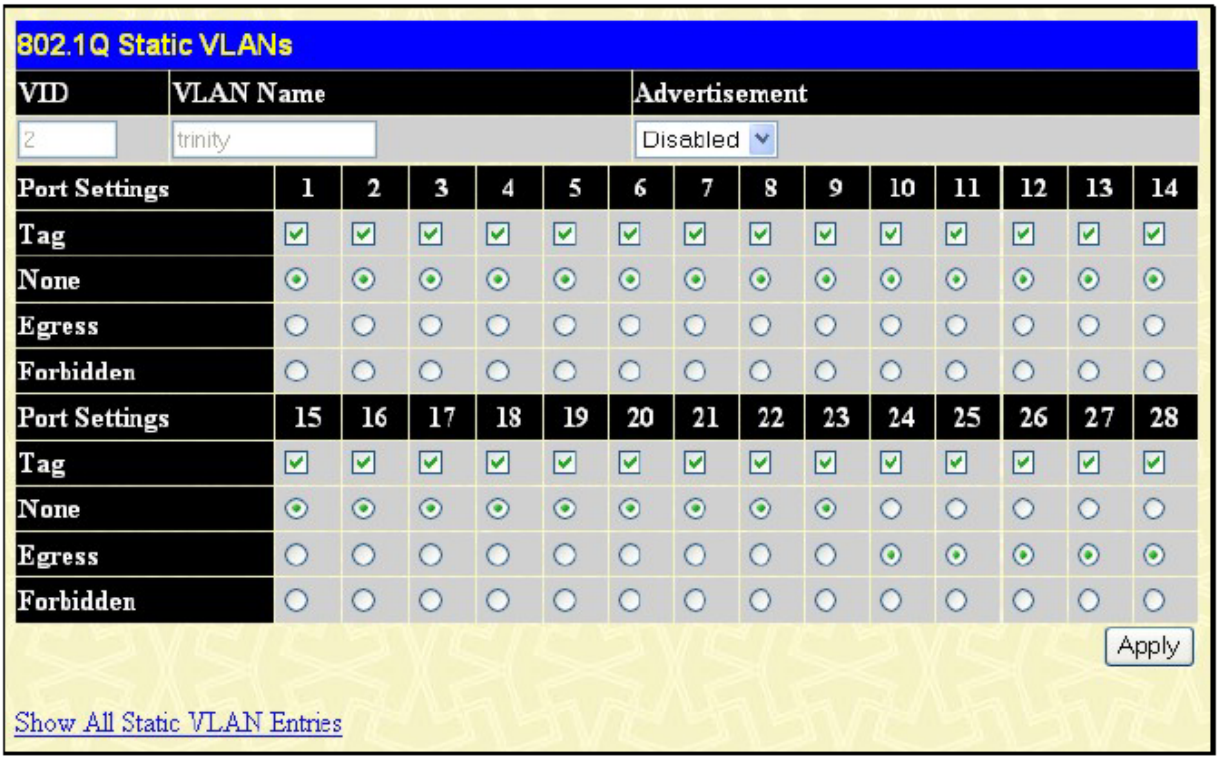


Рисунок 7-9. Окно 802.1Q Static VLANs – Modify (Изменить)

Следующие параметры могут быть установлены в окнах **Add** или **Modify 802.1Q Static VLANs**.

Параметр	Описание
VID (VLAN ID)	Позволяет ввести VLAN ID в окне **Add** или отображает в окне **Modify** VLAN ID уже существующих VLAN. Сети VLAN идентифицируются по имени или VID.
VLAN Name	Позволяет ввести имя нового VLAN в окне **Add** или редактировать имя VLAN в окне **Modify**.
Advertisement	При выборе этой функции Коммутатор сможет посылать GVRP-пакеты на внешние устройства, регистрируя, что они могут присоединяться к существующей сети VLAN.
Port Settings	Позволяет отдельному порту быть назначенным членом VLAN.
Tag	Определяет порт как 802.1Q тегирующий или 802.1Q нетегирующий. Отметка означает, что порт тегирующий.
None	Позволяет назначить отдельный порт как не член VLAN
Egress	Используется для определения порта, как постоянного члена VLAN. Egress-порты – это порты, которые передают трафик внутри VLAN. Эти порты могут быть также тегирующими или нетегирующими.
Forbidden	Используется для определения порта, как не члена VLAN. Такому порту динамически запрещено быть членом VLAN.

Для применения настроек нажмите **Apply.**

Установки GVRP

В меню **L2 Features** откройте папку **VLAN** и нажмите **GVRP Setting.**

Окно **802.1Q Port Settings** показано ниже. Данное окно позволяет определять, будет ли Коммутатор давать коммутаторам GARP VLAN Registration Protocol (GVRP) конфигурационную информацию по VLAN. Так же Ingress Checking может использоваться для ограничения трафика путём фильтрации входящих пакетов, PVID которых не соответствует PVID порта. Результат можно увидеть в таблице под конфигурационными параметрами, как показано ниже:

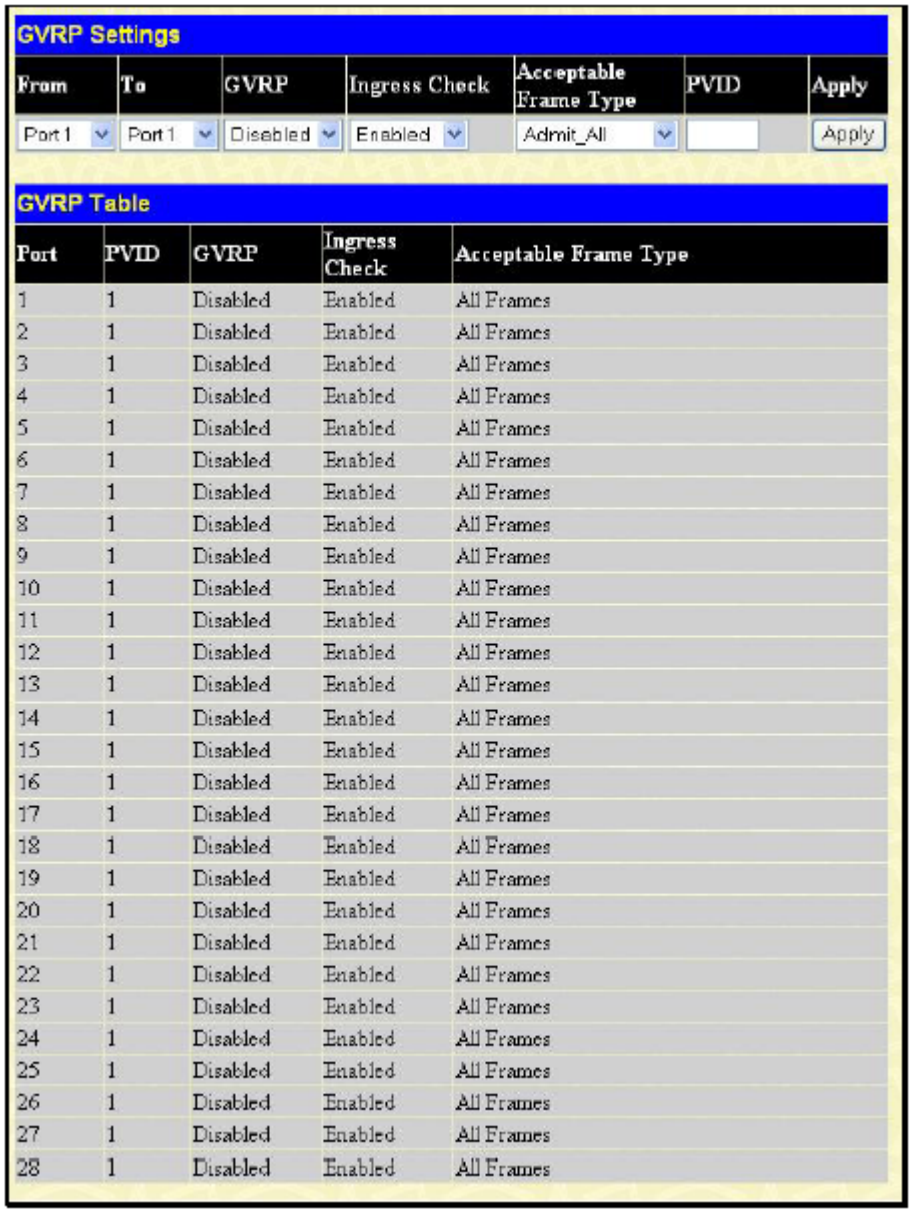


Рисунок 7-10. 802.1Q

Можно установить следующие параметры:

Параметр	Описание
Ingress Check	Данное поле может принимать значения Enabled и Disabled. Значение Enabled позволяет порту сравнивать VID пришедшего пакета с PVID порта. Если они различны, то порт отбросит пакет. Значение Disabled включает ingress-фильтр. По умолчанию ingress-проверка отключена.
From/To	Эти два поля позволяют указать диапазон портов, которые будет включены в VLAN на основе портов. VLAN конфигурируются в окне **802.1Q Port Settings**.
PVID	Редактируемое поле, которое отображает VID конкретного порта, который может быть вручную привязан к VLAN при создании в таблице 802.1Q Port Settings. По умолчанию Коммутатор соединяет все порты с VLAN по умолчанию с VID=1. PVID используется для пометки исходящих пакетов и для фильтрации входящих пакетов. Если порт определён, как
GVRP	Group VLAN Registration Protocol (GVRP) динамически делает порт членом VLAN. По умолчанию GVRP отключен.

	принимающий только тегированные фреймы, а поступают нетегированные пакеты, тогда порт добавит 802.1Q тег, используя PVID для записи VID в тег. Когда пакет достигает пункта его назначения, принимающее устройство будет использовать PVID принятия решения о пересылке пакета. Если порт принимает пакет и Ingress-фильтр включён, порт сравнит VID пришедшего пакета с его PVID. Если они неравны, то порт отбросит пакет. Если равны, то порт примет пакет.
Acceptable Frame Type	Это поле означает тип фрейма, поступившего на порт. Пользователь может выбрать либо *Tagged Only*, значит будут приниматься только VLAN тегированные фреймы, либо *Admit_All*, означает, что будут приниматься и тегированные, и нетегированные фреймы. По умолчанию выбрано значение *Admit_All.*

Нажмите **Apply** для применения сделанных изменений.

Guest VLAN

В меню **L2** откройте папку **VLAN** и нажмите **Guest VLAN Settings.** На дисплее появится следующее окно. Помните, чтобы установить Guest 802.1x VLAN, пользователь сначала должен сконфигурировать обычную VLAN и затем перевести ее в Guest VLAN состояние.

Следующие параметры могут быть изменены для подключения guest 802.1x VLAN.

Параметр	Описание
VLAN Name	Введите имя VLAN, предварительно созданной для настройки как guest 802.1x
Operation	Позволяет пользователю подключать или выключать порты, используемые для guest 802.1x VLAN, с помощью располагаемого ниже списка портов Port List.
Port List	Используя выпадающее меню, установите список подключаемых/выключаемых портов для guest 802.1x VLAN.

Нажмите **Apply** для подключения guest 802.1x VLAN. После правильной настройки **Guest VLAN Name** и относящиеся к ней порты будут указаны в нижней части окна, как показано в примере выше.

DOUBLE VLAN

В меню **L2 Features** откройте папку **VLAN** и нажмите **Double VLAN Settings.** На дисплее появится следующее окно

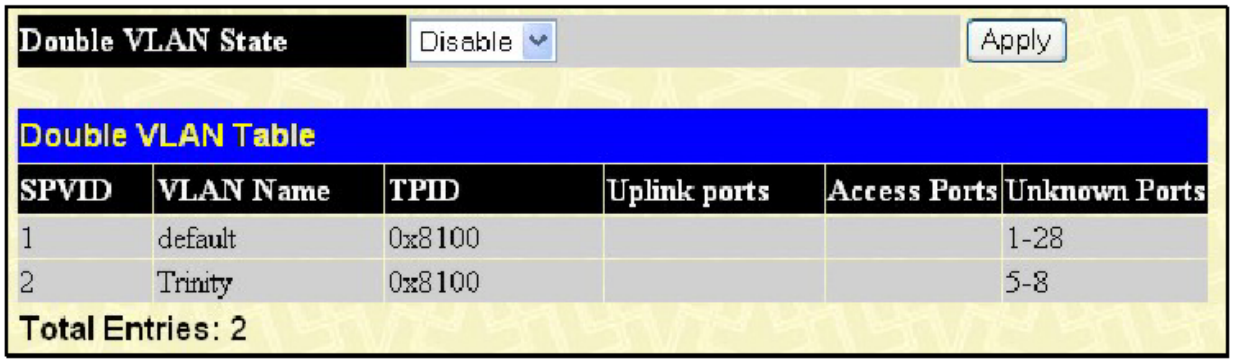


Рисунок 7.12. Double VLAN Table (отключено)

Для настройки Double VLAN измените состояние **Double VLAN** на **Enabled.** В результате окно примет вид, как указано ниже и появится возможность настроить Double VLAN**.**

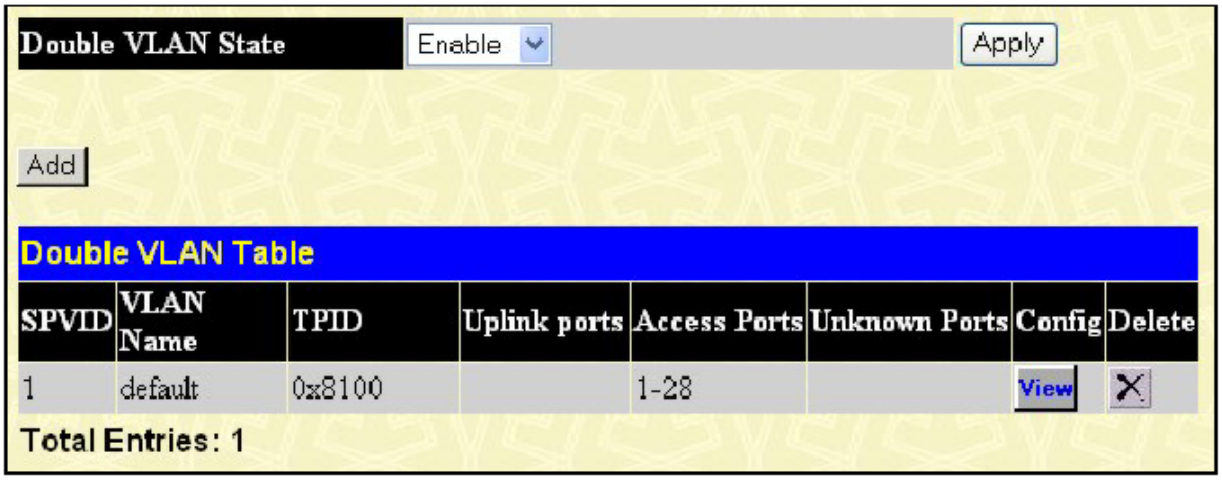


Рисунок 7.13 Double VLAN Table (включено)

Ниже объясняется значение параметров, указанных в предыдущем окне.

Параметр	Описание
Double VLAN State	Используя выпадающее меню, подключайте или отключайте функцию **Double VLAN** на коммутаторе. Подключении функции **Double VLAN** возвращает все предыдущие конфигурации VLAN к заводским настройкам по умолчанию
SPVID	Номер VLAN ID потенциального поставщика услуг VLAN.
VLAN Name	Имя VLAN на коммутаторе
TPID	Tagged Protocol ID соответствующей VLAN, который будет использован для идентификации этой потенциальной Double VLAN. Tagged Protocol ID пишется в шестнадцатиричной системе счисления.
Uplink Ports	Эти порты установлены как uplink порты на коммутаторе. Uplink-порты предназначены для связи VLANs коммутатора с VLANs поставщика услуг на удаленном источнике. Только порты Gigabit могут быть настроены как uplink-порты.
Access Ports	Эти порты установлены как порты доступа на коммутаторе. Порты доступа предназначены для связи VLANs коммутатора с VLANs заказчика. Порты Gigabit не могут быть сконфигурированы как порты доступа.
Unknown Ports	Здесь указываются порты, которые являются частью VLAN, но пока не определен их тип (доступа или uplink)
Config	Нажмите кнопку «View» для настройки этой VLAN как Double VLAN. После чего перед пользователем появится новое окно помощи по настройке Double VLAN.
Delete	Нажмите соответствующий знак для перемещения данной VLAN за пределы Double VLAN конфигурации.

Для создания Double VLAN нажмите кнопку **Add**. В результате будет воспроизведено следующее окно для настройки пользователем.

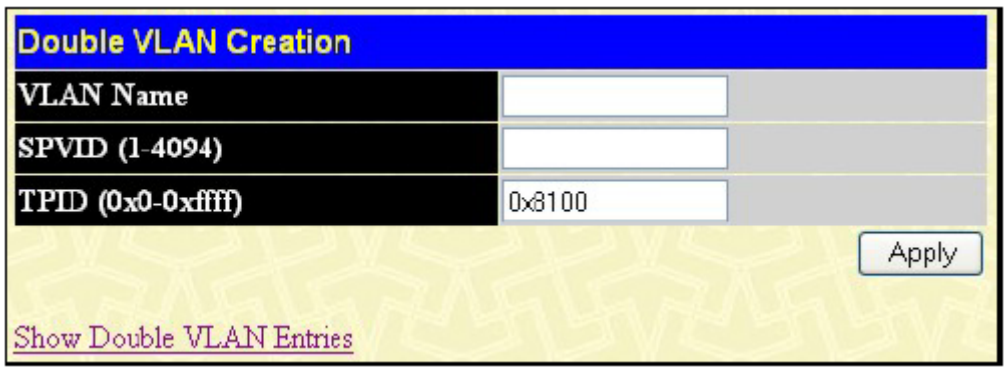


Рисунок 7.14. Double VLAN Creation

Для создания Double VLAN, введите следующие параметры и нажмите **Apply**.

Параметр	Описание
VLAN Name	Введите имя предварительно созданной VLAN для настройки
SPVID	Введите значение VID VLAN поставщика услуг, целое число от 1 до 4094.
TPID	Введите значение TPID в шестнадцатиричной форме для поддержки идентификации VLAN поставщика услуг.

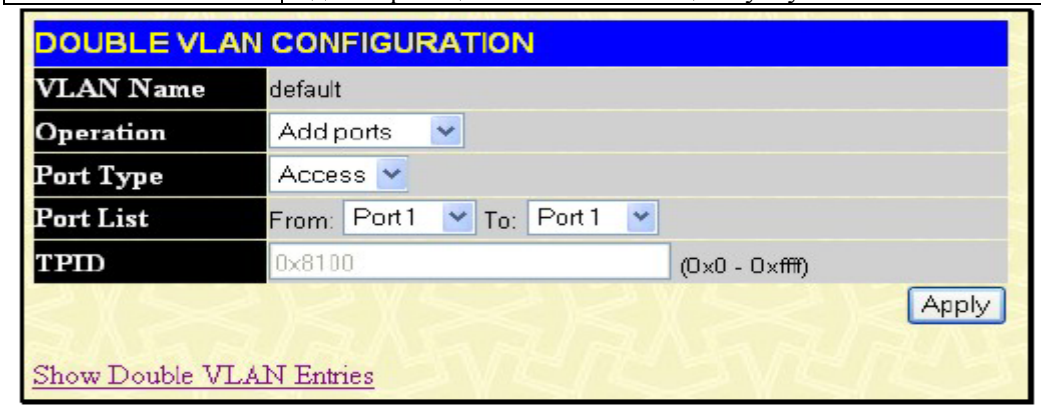


Рисунок 7.15. Double VLAN Configuration

Для настройки Double VLAN , введите следующие параметры и нажмите **Apply.**

Параметр	Описание
VLAN Name	Введите имя предварительно созданной VLAN для настройки
Operation	Позволяет совершить одно из трех действий: *Add Ports* (Добавить порты) – Позволит пользователям добавить в VLAN поставщика услуг , используя поле Port list, расположенное ниже. *Delete Ports* (Удалить порты) – позволит пользователям переместить порты из конфигурации VLAN поставщика услуг, используя поле Port list, расположенное ниже. *Config TPID* – позволит пользователям настроить Tagget Protocol ID поставщика услуг VLAN, выражается в шестнадцатиричной форме.
Port Type	Позволяет пользователю выбрать тип порта, используемого VLAN

	провайдера. Пользователь может выбрать: - *Access* - Access порты предназначены для подключения VLANs коммутатора к VLANs заказчика.
Port List	Используйте поля From и To для установки списка портов, которые подключены или выключены из провайдера.
TPID	Tagged protocol ID идентификатор. Введите новый идентификатор в шестнадцатеричной форме для помощи в идентификации пакетов VLAN провайдера.

Trunking (Образование агрегированных каналов)

Понятие магистральной группы каналов связи

Магистральная группа каналов связи (Port trunk groups) используется для объединения портов в одну высокоскоростную магистраль. DES-3800 поддерживает до тридцати двух магистральных групп каналов связи с количеством портов от 2 до 8 на группу. Может быть достигнута потенциальная скорость передачи 8000Мбит/с.

Коммутатор видит все порты в магистральной группе каналов связи как один порт. Данные, посылающиеся на специальный хост (удалённый адрес), всегда могут быть посланы на порт в магистральной группе каналов связи.

Примечание: если какой-либо порт в магистральной группе каналов связи будет отключен, данные, поступающие на отключенный порт, будут распределены по другим портам группы.

Объединение портов в группу позволяет использовать их как одну линию. Это даёт такую величину полосы пропускания, которая является кратной полосе пропускания одной связи.
Объединение портов обычно используется для связи полосы пропускания сетевых устройств, таких как сервера, с магистралью сети.
Коммутатор позволяет создавать до тридцати двух групп, каждая из которых включает в себя количество портов от 2 до 8. Объединённые линии должны быть непрерывными (они должны содержать последовательные номера портов) за исключением двух гигабитных портов, которые могут представлять только отдельную линию. Все порты группы должны быть членами одной и той же VLAN, их STP-статусы, статическая таблица многоадресной рассылки, контроль трафика; сегментация трафика и предустановки 802.1p должны быть одинаковы. Функции блокировки порта, зеркалирования порта и 802.1X не должны быть выбраны в магистральной группе каналов связи. К тому же, объединённые линии должны быть с одинаковой скоростью и сконфигурированы как полный дуплекс.

Master Port (главный порт) группы конфигурируется пользователем, и все конфигурационные опции, включая конфигурацию VLAN, которая может быть применена к Master Port, применены ко всей группе.
Распределение нагрузки в магистральной группе применяется автоматически, и в случае отказа порта в группе сетевой трафик автоматически направляется на оставшиеся в группе порты.
Spanning Tree Protocol (протокол покрывающего дерева) будет воспринимать группу, как одну связь на уровне коммутатора. На уровне портов STP будет использовать параметры главного порта при вычислении стоимости порта и определения состояния агрегированного канала связи. Если на Коммутаторе сконфигурированы две излишние группы, STP блокирует одну группу, в тоже время STP блокирует единичный порт, который является избыточной связью.

Агрегирование каналов

Для настройки добавления порта в определенную группу агрегированных каналов нажмите на **Link Aggregation** в папке **Trunking ,** находящейся в свою очередь в папке **L2 Features**, откроется следующее окно.

Для настройки магистральной группы каналов связи нажмите кнопку **Add**, чтобы добавить новую группу. Окно **Link Aggregation Group Configuration** (показано ниже) используется для установки групп. Чтобы изменить группу нажмите Hyperlinked Group ID. Чтобы удалить группу нажмите значок **X** под надписью **Delete**, в **Link Aggregation Group Entries** таблице.

Значения параметров, изменяемых пользователем:

Параметр	Описание
Group ID	Выбирается ID группы от 1 до 32
State	Магистральные группы каналов связи могут быть Enabled или Desabled. Это сделано для того, чтобы группы можно было включать или отключать. Используется при диагностике, для быстрой локализации полосы пропускания сетевых устройств, или для создания резервной копии группы, которая не находится под автоматическим контролем.
Master Port	Устанавливается главный порт группы, используя выпадающее меню.
Member Ports	Выбор членов группы. В группу могут входить до восьми портов.
Flooding Port	В магистральной группе каналов связи должен быть выделен один порт для широковещательной рассылки и нераспознанных адресаций.
Active Port	Отмечается порт, который в настоящее время пересылает данные.
Type	Здесь можно выбрать *Static* или *LACP* (Link Aggregation Control Protocol). *LACP* позволяет автоматическое определение связей в магистральной группе каналов связи.

После установки параметров, следует нажать Apply, чтобы настройки вступили в силу. Успешно созданная группа будет отображаться в таблице **Link Aggregation Group Entries**, показанной на рисунке 7-17.

Настройки LACP Port

Окно **LACP Port Settings** используется в сочетании с окном **Link Aggregation** для создания магистральной группы каналов связи на Коммутаторе. Используя следующее окно, пользователь может установить, какие порты будут активными или пассивными при обработке и посылке контрольных LACP-кадров. Чтобы получить это окно, нажмите **L2 Features>Trunking >LACP Port Settings.**
Пользователь может установить следующие параметры:

Параметр	Описание
From/To	В последовательной группе портов может быть выбран начальный порт.
Mode	*Active* – активные LACP-порты, которые способны обрабатывать и посылать контрольные LACP-кадры. Это позволяет соответствующим LACP-устройствам согласовывать объединённую связь, так что группа может быть динамически изменена, когда это необходимо. Для того, чтобы использовать возможность менять группу портов – добавлять или удалять порты из группы, по крайней мере на одном из устройств должен быть определён активный LACP–порт. Оба устройства должны поддерживать LACP.

	Passive – LACP – порты, установленные в состояние пассивные, не могут посылать контрольные кадры LACP. В случае, когда необходимо разрешить группе портов согласовывать настройки и делать необходимые изменения, хотя бы одно устройство должно иметь активный LACP-порт(смотри выше).

После установки параметров, следует нажать **Apply**, для применения изменений. В таблице LACP-портов отображаются активные или/и пассивные порты.

IGMP

IGMP (Internet Group Management Protocol) snooping (шпионение) позволяет Коммутатору распознавать IGMP – запросы и ответы, посылаемые между станциями сети или устройствами и IGMP-хостом. Когда включен IGMP snooping, коммутатор может открыть или закрыть порт на определённое устройство, базированное на IGMP-сообщениях, проходящих через Коммутатор.

Для того чтобы использовать IGMP Snooping, это сначала должно быть определено в настройках Коммутатора (смотри **DES-3800 Web Management Tool**). Затем можно сделать тонкую настройку для каждой VLAN, нажав по ссылке **IGMP Snooping** в папке **L2 Features**. Когда IGMP snopping включён, Коммутатор может открыть или закрыть порт для определённого члена группы широковещательной рассылки, базированного на IGMP-сообщениях, проходящих через Коммутатор. Коммутатор отслеживает IGMP – сообщения и прекращает посылать широковещательные пакеты, когда больше нет хостов, запрашивающих продолжения посылки.

IGMP Snooping

Окно **IGMP Snooping Group Entries** используется для просмотра настроек **IGMP Snooping**. Для изменения настроек, надо кликнуть по кнопке **Modify** соответствующего VLAN ID.
После нажатия на кнопку **Modify** откроется окно **IGMP Snooping Settings**, представленное ниже:
Следующие параметры доступны для просмотра и изменения.

Параметр	Описание
VLAN ID	Это идентификатор VLAN, который наряду с именем VLAN, определяет VLAN, для которого пользователь желает изменить настройки IGMP snooping.
VLAN Name	Имя VLAN, которое наряду с ID VLAN, определяет VLAN, для которого пользователь желает изменить настройки IGMP snooping.
Query Interval	Данное поле используется для задания временного интервала (в секундах) между IGMP-запросами. Возможны значения от 1 до 65535. Значение по умолчанию 125.
Max Response Time	Задаёт максимальное время до посылки IGMP-ответа. Возможны значения от 1 до 25 (в секундах). Значение по умолчанию 10.
Robustness Variable	Эта переменная используется при предполагаемой потере пакетов. Если потеря пакетов на VLAN, как ожидается, будет высокой, значение Robustness Variable должно быть увеличено, чтобы покрыть увеличенную потерю пакетов. Возможны значения от 1 до 255. Значение по умолчанию 2.
Last Member Query Interval	Это поле указывает максимальный промежуток времени между отправкой групповых сообщений-запросов, включая те, которые были отправлены в ответ на запрос о выходе из группы. Значение по умолчанию =1
Host Timeout	Это максимальное количество времени в секундах, в течение которого сетевому узлу разрешается оставаться членом многоадресной группы без отправки коммутатору запроса о вступлении в группу. Значение по

	умолчанию = *260*.
Route Timeout	Максимальное время хранения маршрута в таблице адресов (в секундах). Значение по умолчанию 260.
Leave Timer	Это максимальный временной интервал в секундах между получением коммутатором сообщения Leave от клиента и исключением клиента из группы. Если до истечения этого времени не получено никакой информации об обратном, клиент исключается из группы.
Querier State	Значение *Enabled* – для включения IGMP-запросов, *Disabled* – для отключения. Значение по умолчанию – *Disabled*.
Querier Router Behavior	Это поле доступно только для чтения. Оно описывает поведение маршрутизатора при посылке IGMP-пакетов. *Querier* будет означать , что маршрутизатор уже отослал IGMP-пакеты. *Non-Querier* будет означать , что маршрутизатор еще не отослал IGMP-пакеты. Это поле будет доступно для чтения только при нахождении полей **Querier State и State** в состоянии *Enabled* (Подключен).
State	Значение *Enabled* – для применения IGMP snopping. Значение по умолчанию – *Disabled (отключено).*
Fast Leave	Этот параметр позволяет пользователю подключить функцию Fast Leave. При подключении этой функции, членам широковещательной группы будет разрешено покидать группу немедленно(а не в соответствии с настройкой **Last Member Query Interval)** после получения коммутатором пакета Leave. По умолчанию эта функция отключена (Disabled).

Нажмите Apply для применения настроек. Для возврата в окно **IGMP Snooping Group Settings** нажмите Show All IGMP Group Entries.

Spanning Tree (Алгоритм покрывающего дерева)

Коммутатор поддерживает три версии Spanning Tree (протокол покрывающего дерева): 802.1d STP, 802.1w Rapid STP и 802.1s MSTP. 802.1s MSTP знаком большинству сетевых профессионалов. Однако, 802.1d STP, 802.1w Rapid STP и 802.1s MSTP были недавно введены в управляемые коммутаторы D-link, ниже представлено краткое введение в технологию и настройку 802.1d STP, 802.1w Rapid STP и 802.1s MSTP.

802.1s MSTP

Multiple Spanning Tree Protocol (MSTP) - стандарт установленный IEEE, который позволяет multicast VLAN увязать с single spanning tree instance, обеспечивает множественные связи внутри сети. Поэтому MSTP балансирует загрузку трафика, предотвращает широкомасштабные разрушения, когда один spanning tree instance не работает. Это способствует более быстрой конвергентности новой топологии при неработающих spanning tree instance. Фреймы, определённые для таких VLAN, обрабатываются быстро и полностью через мосты, использующие любой из трёх протоколов (STP, RSTP или MSTP).
Этот протокол так же метит BDPU-пакеты, чтобы принимающие устройства могли различить spanning tree instance, области spanning tree и VLAN-ы, связанные с ними. MSTI ID классифицирует эти instance (экземпляр). MSTP соединяет multiple spanning trees с Common и Internal Spanning Tree (CIST). CIST автоматически распознаёт области MSTP, их максимально возможный диапазон, и выступает, как виртуальный мост, который поставляет единичный spanning tree. Следовательно, фреймы различных VLAN, будут следовать различными маршрутами в пределах установленных областей сети, осуществляется простая и быстрая обработка фреймов независимо от административных ошибок в определении VLAN в соответствующих spanning tree.
Каждый Коммутатор, использующий MSTP, снабжён MSTP конфигурацией, в которой присутствуют следующие три атрибута:

1. Конфигурационное имя задаётся цифробуквенной строкой не более 32 символов (вводится в поле **Configuration Name**, в окне **MST Configuration Identification**).
2. Редакция конфигурации (здесь называется Revision Level, находится в окне **MST Configuration Identification**).
3. Таблица на 4096 элементов (здесь называется VID List, находится в окне **MST Configuration Identification**) которая будет ассоциировать каждую из 4096 возможных VLAN, поддерживаемых коммутаторами для данной копии.

Для использования MSTP-функции Коммутатора, надо сделать следующие три шага:

1. На Коммутаторе должны быть установки MSTP (находятся в окне **STP Bridge Global Settings**, в поле **STP Version**).
2. Скорректировать spanning tree до того как будет задан MSTP instance (здесь называется **Priority**, в окне **MSTConfiguration Table**, когда конфигурируются настройки MSTI ID).
3. VLAN, которые будут предоставлены для общего доступа должны быть добавлены в MSTP Instance ID (здесь называется VID List в окне **MST Configuration Identification**, когда конфигурируются настройки MSTI ID).

802.1w Rapid Spanning Tree

В Коммутаторе используются три версии протокола Spaning Tree, Multiple Spanning Tree Protocol (MSTP), определённый как стандарт IEEE 802.1s; Rapid Spanning Tree Protocol (RSTP), определённый как IEEE 802.1w и версия совместимая с IEEE 802.1d STP. RSTP может работать с оборудованием, поддерживающим IEEE 802.1d, однако, будут потеряны преимущества RSTP.

IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) произошёл от стандарта 802.1d STP. RSTP был разработан для преодоления некоторых ограничений STP, которые мешают некоторым функция новых коммутаторов, одни из них – функции 3-го уровня, которые всё чаще и чаще исполняются Ethernet коммутаторами. Основные функции и терминология такая же как в STP. Большинство настроек для STP также используются для RSTP. Данная глава знакомит с некоторыми новшествами в STP и показывает основные различия между двумя протоколами.

Состояние портов

Основные различия между этими тремя протоколами состоят в способе перехода портов в состояние пересылки и механизме этого перехода, относящегося к роли порта (пересылающий или не пересылающий) в топологии. MSTP и RSTP комбинируют пересылку запрещающих статусов, блокирование или прослушивание с использованием 802.1d создаёт state Discarding (отвергающий статус). В этом случае порты не посылают пакеты данных. В STP порт посылает запрещённое состояние, состояние блокирования или прослушивания; в RSTP/MSTP создаётся статус Discarding. Таким образом, нет функциональных различий. Порт остаётся неработающим. В Таблице 7-1 показано сравнение port state transition трёх протоколов.

Все три протокола вычисляют топологию сети одинаково. Каждый сегмент обладает единственным путём к корневому мосту. Все мосты прослушивают BPDU-пакеты. Однако BPDU-пакеты посылаются слишком часто с каждым Hello-пакетом. BPDU-пакеты посылаются даже если BPDU-пакет был не принят. Однако, связь между мостами чувствительна к статусам связи. В конечном счете, это различие приводит к более быстрому обнаружению неудавшихся связей, и таким образом, более быстрому регулирование топологии. Недостатком 802.1d является отсутствие непосредственной обратной связи между смежными мостами.

802.1d MSTP	802.1w RSTP	802.1d STP	Пересылка	Изучение
Отказ	Отказ	Отключен	Нет	Нет
Отказ	Отказ	Блокировка	Нет	Нет
Отказ	Отказ	Прослушивание	Нет	Нет
Изучение	Изучение	Изучение	Нет	Да
Пересылка	Пересылка	Пересылка	Да	Да

Таблица 7-1. Сравнение статусов портов

RSTP способен к более быстрому переходу к статусу пересылки – он больше не зависит от таймера смены состояний – RSTP-мосты чувствительны к обратной связи от других RSTP-связей. Порту нет необходимости получать топологию сети для стабилизации перед переходом в статус пересылки. Для того чтобы быстро позволить этот переход, протокол вводит два новых понятия: edge port (пограничный порт) и point-to-point (P2P) порт.

Пограничный порт

Edge port конфигурируемый, предназначен для использования в качестве порта, напрямую соединяемого с сегментом сети, где не может быть создана петля. Например, порт напрямую соединяется с отдельной рабочей станцией. Порты, которые определены как Edge port, посылают статус пересылки немедленно без прохождения статусов прослушивания и изучения. Edge port сбрасывает свой статус, если он принял BPDU-пакет, сразу же становясь портом spanning tree.

P2P-порт

Порт P2P также способен на быструю передачу. Порт P2P может использоваться для соединения с другими мостами. Все порты под RSTP/MSTP работают в дуплексном режиме и являются портами P2P, если это не было отключено в ручных настройках.

Совместимость 802.1d/802.1w/802.1s

MSTP или RSTP совместимы с устаревшим оборудованием и при необходимости способны автоматически корректировать BPDU-пакеты в 802.1d формате. Однако, любой сегмент, использующий 802.1d STP не может способствовать быстрой передаче и быстрому изменению топологии. Протокол также предусматривает возможность частичного обновления оборудования, использующего MSTP или RSTP.
Spanning Tree Protocol (STP) ведёт обработку на двух уровнях:

1. На уровне коммутатора глобально осуществлены настройки.
2. На уровне порта, параметры настройки осуществлены в определенной пользователем группе портов.

Глобальные установки STP-моста

Для того, чтобы открыть следующее окно, откройте папку **Spanning Tree** в меню **L2 Features**, нажмите на ссылку **STP Bridge Global Settings**.

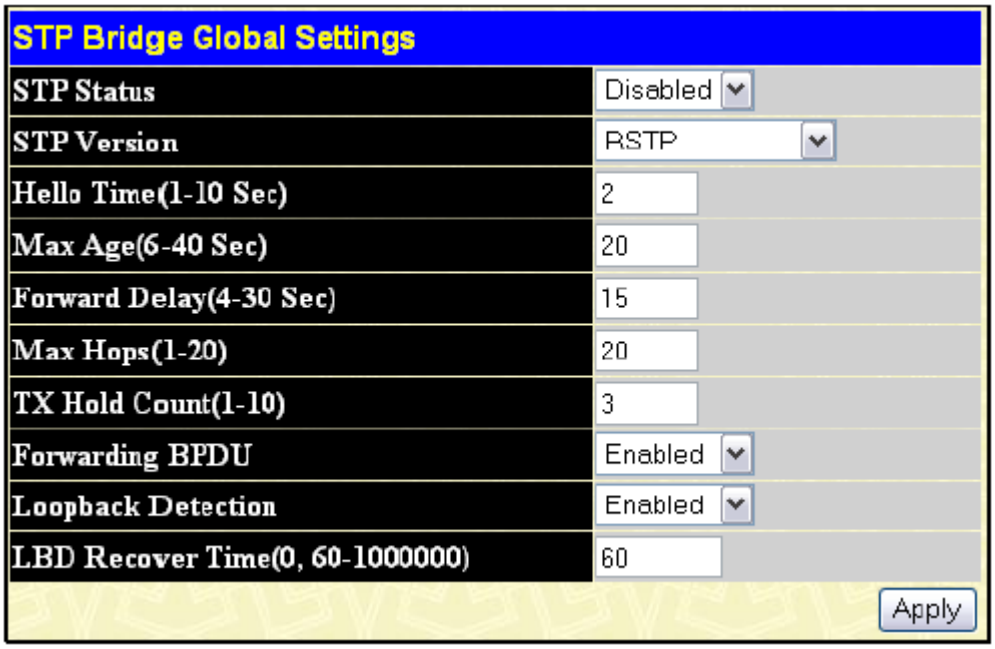


Рисунок 7.25. STP Bridge Global Settings окно – RSTP (по умолчанию)

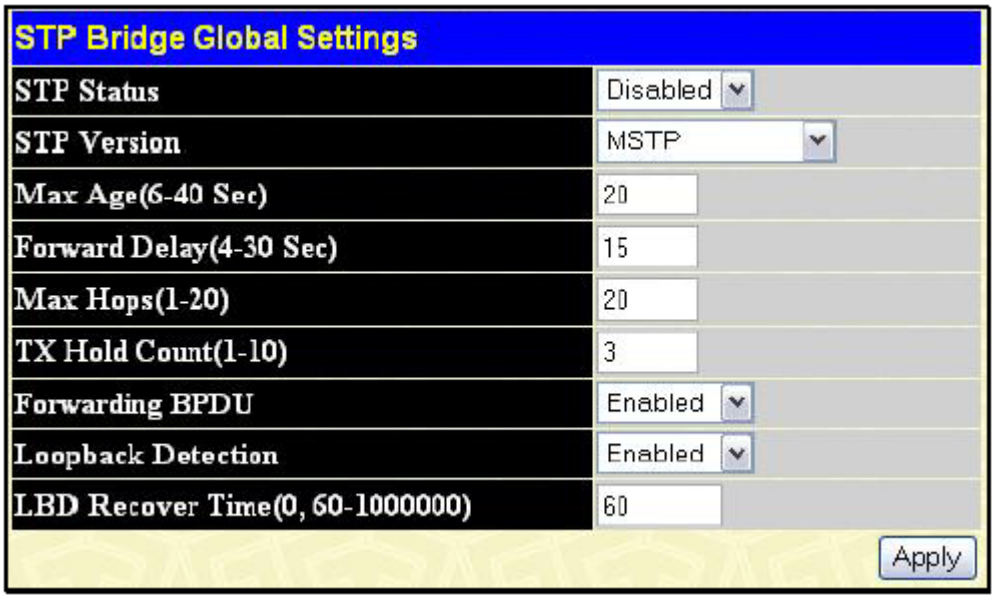


Рисунок 7.26. STP Bridge Global Settings window - MSTP

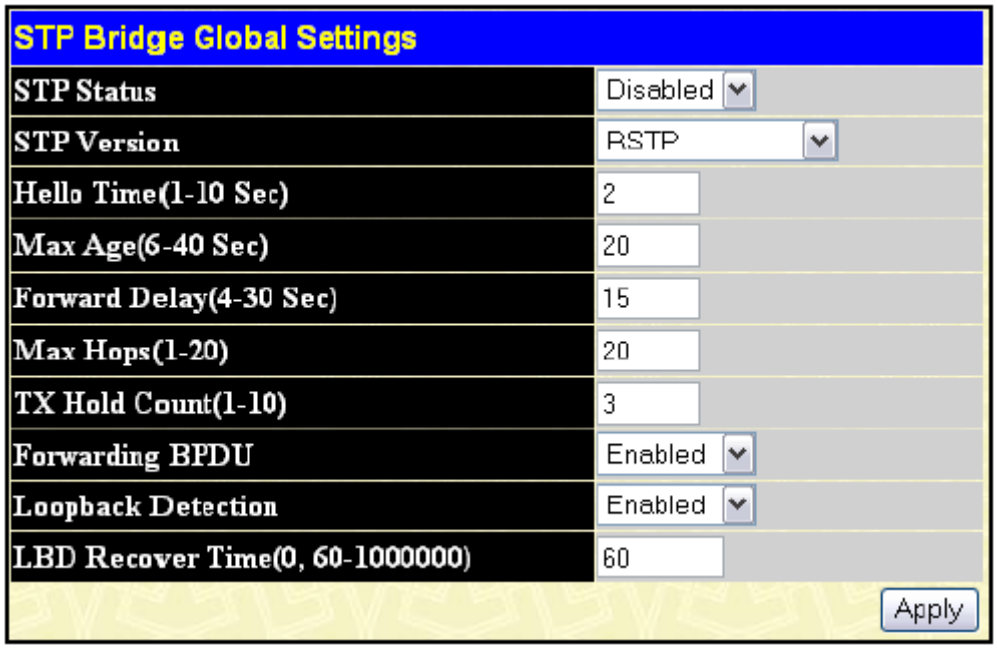


Рисунок 7.27. STP Bridge Global Settings – STP Compatible окно

Примечание: Hello Time не может быть больше, чем Max. Age. Otherwise, в этом случае возникнет ошибка конфигурации. Следует придерживаться следующего формата при установке параметров:
Max. Age = 2 x (Forward Delay - 1 second)
Max. Age = 2 x (Hello Time + 1 second)

Можно установить следующие параметры:

Параметр	Описание
Spanning Tree Protocol	В выпадающем меню можно выбрать или отменить функцию STP на

	коммутаторе. Значение по умолчанию *Disabled*.
BridgeMax Age (6-40 сек)	Max Age может быть установлен для того, чтобы устаревшая информация не блуждала бесконечно по сети, мешая продвижению новой. Когда установлен Root Bridge, данный параметр помогает определить, что у Коммутатора конфигурация spanning tree совместима с другими устройствами LAN. Если параметр не установлен, и BPDU-пакеты не были ещё получены, Коммутатор стартует свою собственную посылку BPDU-пакетов к другим коммутаторам для того, чтобы получить роль Root Bridge. Коммутатор станет Root Bredge в том случае, если у других коммутаторов Bridge Identifier ниже. Пользователь может выбрать значение от 6 до 40 секунд. Значение по умолчанию 20.
Bridge Hello Time (1-10 сек)	Значение данного параметра может быть от 1 до 10 секунд. Это интервал между двумя передачами BPDU-пакетов, посланных на Root Bridge, для оповещения других коммутаторов, что это действительно Root Bridge.
Bridge Forward Delay (4 -30 сек)	Данный параметр может принимать значения от 4 до 30 секунд. Это время, которое коммутатор находится в состоянии listening при переходе от состояния blocking к состоянию forwarding.
Bridge Priority(0-61440)	Приоритет коммутатора может быть установлен в значение от 0 до 61440. Это число используется при голосовании между коммутаторами на сети с целью определения управляющего коммутатора. Чем ниже это число, тем выше приоритет коммутатора и выше вероятность, что он станет управляющим коммутатором.
Default Path Cost	Поле, доступное только для чтения, отображает протокол, используемый для определения стоимости ошибок маршрутизации на порт. **802.1T** будет вычислять значение этого 32-битного параметра с использованием специальной формулы, основанной на пропускной способности порта
STP Version	Выпадающее меню позволяет выбрать версию STP, установленную на коммутаторе. Возможны 2 следующих значения: *STPCompatibility* – выберите этот параметр для глобальной установки на коммутаторе Spanning Tree Protocol (STP) *RST*P - выберите этот параметр для глобальной установки на коммутаторе Rapid Spanning Tree Protocol (RSTP)
TX Hold Count	Используется для установки количества Hello-пакетов за интервал. Можно установить значение от 1 до 10. Значение по умолчанию 3.
Forwarding BPDU	Это поле может принимать значения *Enabled* или *Disabled*. Когда данный параметр выбран, это позволяет пересылку STP BPDU-пакетов от других сетевых устройств. Значение по умолчанию *Enabled*.
Loopback Detection	Эта функция позволяет временно блокировать STP на Коммутаторе, когда BPDU-пакеты были возвращены на коммутатор. Если Коммутатор обнаружит, что это его собственный BPDU-пакет, это будет обозначать, что в сети образовалась петля. STP автоматически заблокируется и администратору будет послано предупреждение. Когда время **LBD Recover Time** истечёт, порт LBD STP перестартует (поменяет свой статус с discarding). Пользователь может включить или отключить данную функцию. По умолчанию функция включена.

LBD Recover Time	Это поле устанавливает время ожидания для STP порта перед сменой STP статуса. 0 означает, что LBD автоматически перестартовывать не будет и его состояние администратор будет менять вручную. Пользователь может установить значение от 60 до 1000000 секунд. Значение по умолчанию 60 секунд.

Примечание: Функция **Loopback Detection** может быть установлена на коммутаторе, только если она настроена в обоих окнах: и на **STP Global Settings window**, и на **STP Port Settings window.** При настройке этой функции только в одном из указанных окон не приведет к полному включению **Loopback Detection** функции.

Нажмите **Apply** для применения сделанных настроек.

Таблица конфигурации MST

Следующее окно **Current MST Configuration Identification** позволяет пользователю конфигурировать MSTI интерфейс на коммутаторе. Эти установки идентифицируют multiple spanning tree instance, установленные на Коммутаторе. Первоначально Коммутатор обладает CIST (Common Internal Spanning Tree), параметры которого пользователь может изменить, нельзя изменить или удалить только MSTI ID. Для того, чтобы открыть окно **Current MST Configuration Identification**, кликните **L2 Features> Spanning Tree > MST Configuration Table**.

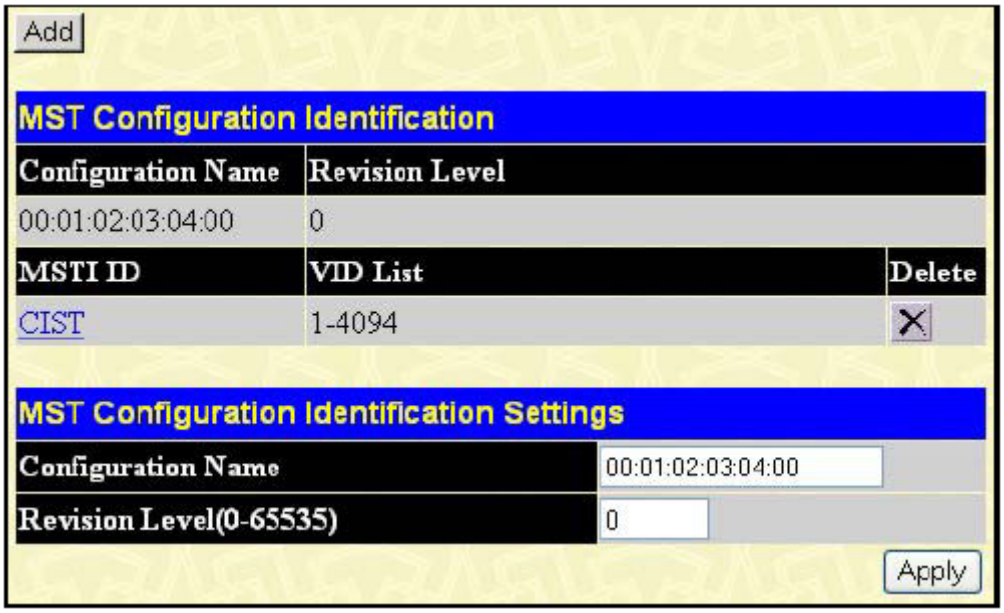


Рисунок 7.28. MST Configuration Identification and Settings окно

Окно представленное выше содержит следующую информацию:

Параметр	Описание
Configuration Name	Предварительно заданное на Коммутаторе имя идентифицирует MSTI (Multiple Spanning Tree Instance). Если это имя не было задано, в поле будет отображаться MAC-адрес устройства MSTP. Это поле также может быть задано в окне STP Bridge Global Settings.

Revision Level	Значение данного поля позволяет Configuration Name идентифицировать MSTP-регион, сконфигурированный на Коммутаторе. Данный параметр принимает значение от 0 до 65535 и по умолчанию составляет 0.
MSTI ID	Это поле показывает список MSTI ID Коммутатора. Это поле обеспечивает наличие CIST MSTI, который может быть изменён, но не удалён. Нажатие на гиперссылку имени откроет новое окно для настройки параметров, связанный с данной MSTI.
VID List	Это поле показывает список VLAN ID. Которые связаны с определенной MSTI.

Нажмите **Add** для того, чтобы открыть следующее окно:

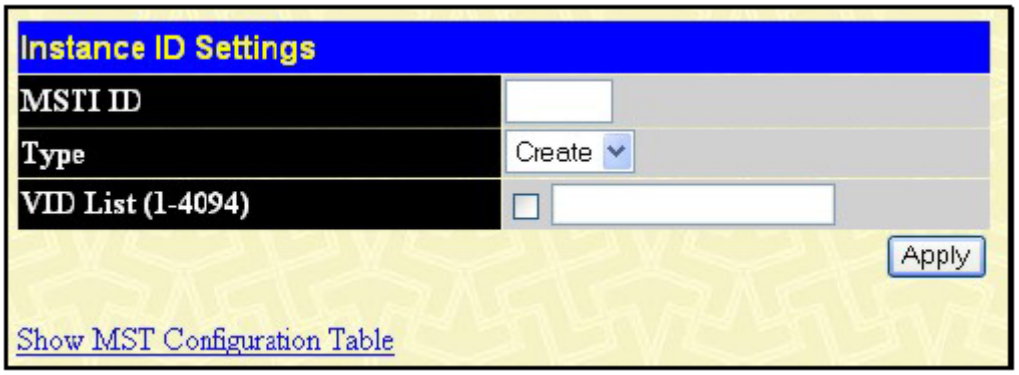


Рисунок 7- 29. Instance ID Settings window – Add

Для создания MSTI пользователь может настроить следующие параметры:

Параметр	Описание
MSTI ID	Допускается выбор значения от 1 до 15 для установки нового MSTI на Коммутаторе.
Type	Значение Create означает, что создаётся новый MSTI. Когда создаётся новый MSTI, другое значение выбрать невозможно.
VID List (1-4094)	Это поле используется для определения диапазона VID для VLAN, сконфигурированных на Коммутаторе. Диапазон значений от 1 до 4094.

Для применения настроек нажмите **Apply**.
Для конфигурирования CIST кликните по ссылке **Current MST Configuration Identification,** откроется следующее окно:

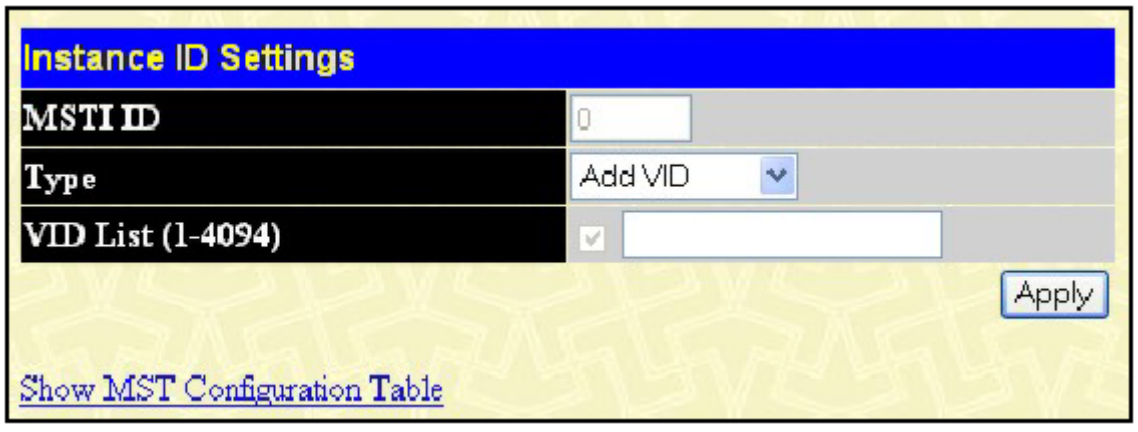


Рисунок 7.30. Instance ID Settings window - CIST modify

Пользователь может сконфигурировать следующие параметры CIST:

Параметр	Описание
MSTI ID	Значение MSTI ID равно 0 и не может быть изменено.
Type	Это поле дает возможность пользователю при желании изменить способ изменения MSTI настроек. Существует два варианта: • *Add VID*- выберите этот параметр для добавления новых VIDs в MSTI ID, в соответствии с параметром VID List. • *Remove VID*- выберите этот параметр для перемещения VIDs из MSTI ID, в соответствии с параметром VID List.
VID List (1-4094)	Это поле используется для определения диапазона VID для VLAN, сконфигурированных на Коммутаторе. Диапазон значений от 1 до 4094. Это поле доступно только, когда сконфигурирован CIST.

Для применения настроек нажмите **Apply**.

Для конфигурирования параметров установленной ранее MSTI**,** нажмите на ссылку с номером MSTI ID, после чего откроется следующее окно для настройки:

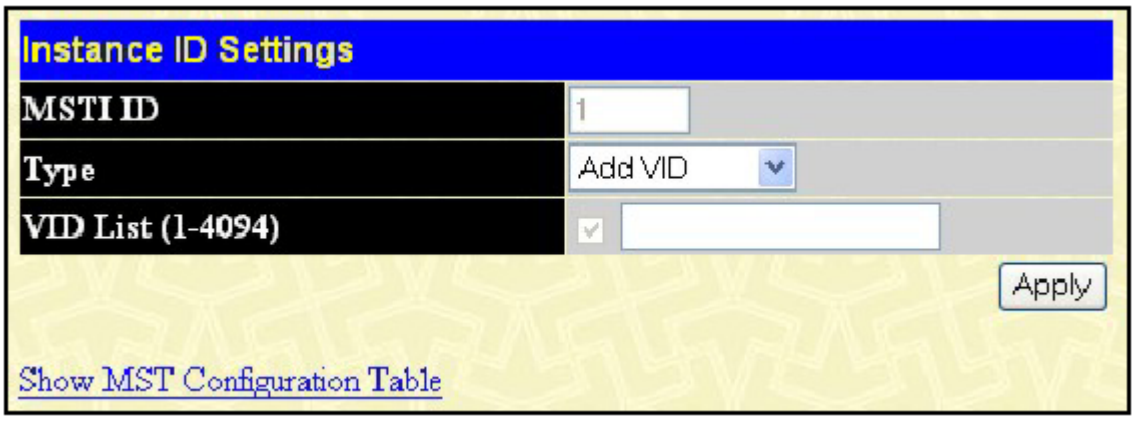


Рисунок 7.31. Instance ID Settings window – modify

Пользователь может сконфигурировать следующие параметры MSTI на Коммутаторе:

Параметр	Описание
MSTI ID	Отображает MSTI ID предварительно установленный пользователем.
Type	Этот параметр позволяет пользователю выбрать способ изменения настроек MSTI. Пользователь может сделать следующий выбор: *Add* – для добавления VID в MSDI ID. В этом случае будет доступно поле VID List. *Remove* – для удаления VID из MSDI ID. В этом случае будет доступно поле VID List. *Delete* – для удаления данного MSDI ID. *Set Priority Only* – для установки приоритета MDSI ID. Это поле используется вместе с полем Priority.
VID List (1-4094)	Это поле используется для определения диапазона VID для VLAN, сконфигурированных на Коммутаторе. Диапазон значений от 1 до 4094. Это поле доступно только, когда значение поля **Type** *Add* или *Remove*.

Для применения настроек нажмите **Apply**.

Информация о портах MSTP

Данное окно отображает текущую информацию о MSTP портах и может быть использовано дня обновления конфигурации порта. При возникновении петли функция MSTP использует свой приоритет для установки статуса forwarding. Интерфейсы, которые должны первыми осуществлять передачу, должны быть с высшим приоритетом. В том случае, когда приоритеты одинаковые, MSTP функция выбирает из таблицы MAC-адресов интерфейс с наименьшим MAC-адресом, остальные интерфейсы будут заблокированы. Стоит помнить, что чем меньше значение приоритета, тем выше приоритет.
Для просмотра следующего окна следует нажать **L2 Features > Spanning Tree > MSTP Settings**:

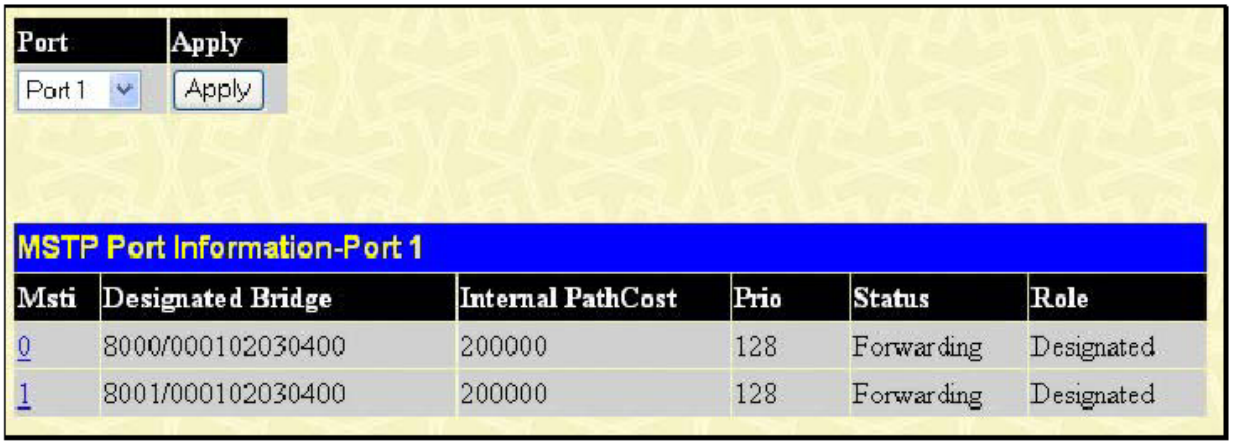


Рисунок 7.32. MSTP Port Information окно

Для того, чтобы увидеть MSTI настройки определённого порта, следует выбрать номер порта в верхнем левом углу окна и кликнуть **Apply**. Для изменения настроек определённого MSTI интерфейса, надо кликнуть по соответствующему MSTI ID, откроется следующее окно:

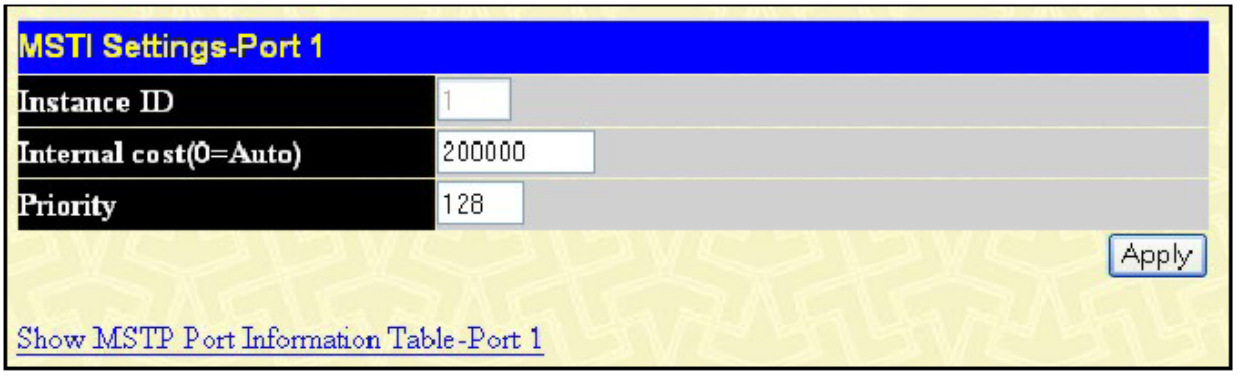


Рисунок 7.33. MSTI Settings окно

Параметр	Описание
Instance ID	Отображает MSTI ID в данной конфигурации. Нулевое значение данного поля означает, что выбрано CIST (значение по умолчанию MSTI).
Internal cost (0=Auto)	Этот параметр устанавливается для представления относительной стоимости передачи пакетов на определённые порты, когда интерфейс выбран внутри копии STP. Значение по умолчанию 0 (авто). Возможны два варианта: • 0 (авто) – устанавливает самый быстрый и оптимальный маршрут. В качестве значения по умолчанию была взята скорость media speed of the interface. • Значение от *1* до *2000000* – установить наилучший маршрут при возникновении петли. Чем ниже данное значение, тем выше скорость передачи.

Priority	Можно задать значение от *0* до *240* для установки приоритета порта. Интерфейс, который передаёт данные первым, обладает высшим приоритетом. Чем меньше значение данного параметра, тем выше приоритет.

Для применения настроек нажмите **Apply**.

Настройки копии STP

Следующее окно отображает MSTI, в настоящий момент установленные на Коммутаторе. Для просмотра следующей таблицы нажмите **L2 Features > Spanning Tree > STP Instance Settings**:

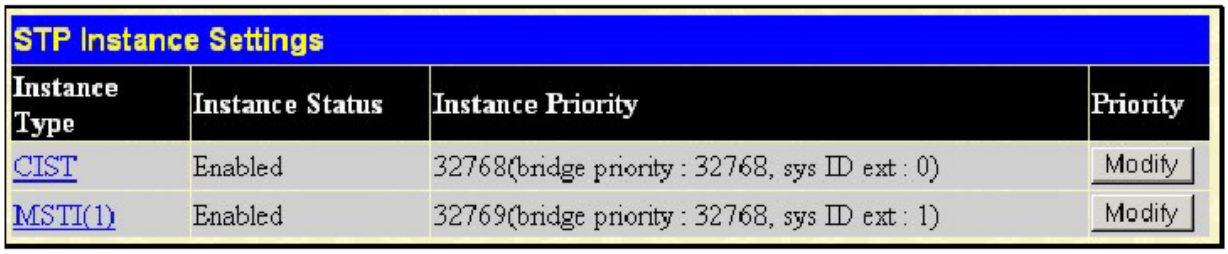


Рисунок 7.34. STP Instance Table окно

Здесь отображена следующая информация:

Параметр	Описание
Instance Type	Отображает тип(ы) реализации STP в текущей конфигурации Коммутатора. Каждый тип классифицируется по MSTI ID. CIST обращается к установкам MSTI по умолчанию, сконфигурированным на Коммутаторе.
Instance Status	Отображает текущий статус MSTI ID.
Instance Priority	Отображает приоритет MSTI ID. Наименьший приоритет будет у Root Bridge.

Для принятия настроек необходимо нажать **Apply**.
Нажмите кнопку **Modify** для изменения приоритета MSTI. В результате откроется следующее окно для настройки:

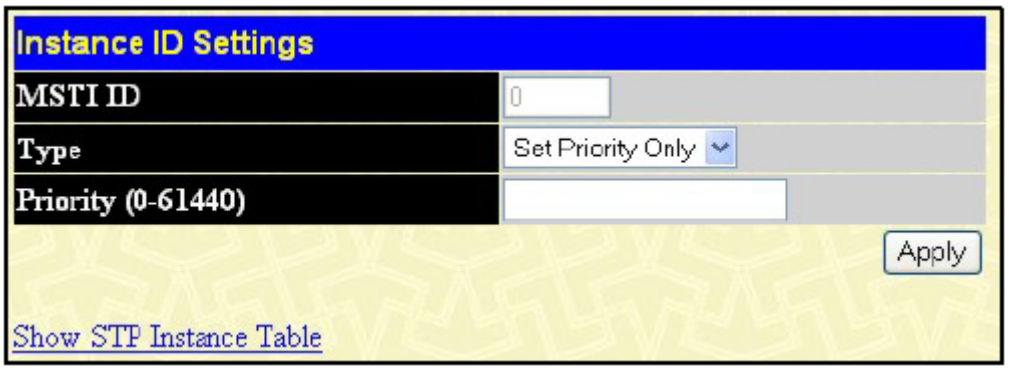


Рисунок 7.35. STP Instance Settings - modify priority окно

Параметр	Описание
MSTI ID	Отображает MSTI ID изменяемой копии.
Type	Поле Type в этом окне должно быть постоянно установлено в состояние Set

	Priority Only.
Priority (0-61440)	Введите новое значение приоритета в поле Priority.

Для принятия новых настроек приоритета нажмите **Apply**

Настройки STP-порта

STP можно настроить на портовой основе. Для просмотра следующего окна необходимо кликнуть **L2 Features > Spanning Tree > MST Port Information**

STP Port Settings

From	To	External Cost (0=Auto)	Hello Time	Migrate	Edge	P2P	Forward BPDU	LBD	State
Port 1	Port 1	0	1	Yes	False	True	Disabled	Disabled	Enabled

Apply

STP Port Settings Table

Port	External Cost	Hello Time	Edge	P2P	Forward BPDU	LBD	Port STP
1	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
2	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
3	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
4	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
5	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
6	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
7	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
8	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
9	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
10	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
11	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
12	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
13	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
14	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
15	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
16	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
17	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
18	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
19	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
20	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
21	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
22	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
23	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
24	AUTO/200000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
25	AUTO/20000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
26	AUTO/20000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
27	AUTO/20000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled
28	AUTO/20000	2/2	No/No	Auto/Yes	Disabled	Disabled	Enabled

Рисунок 7.36. STP Port Settings окно

В дополнение к установкам параметров Spanning Tree, использующимся на уровне коммутаторов, коммутатор позволяет конфигурацию групп портов. Каждая группа портов будет обладать своим Spanning Tree, со своими конфигурационными настройками. STP группа будет использовать параметры уровня коммутаторов, заданными ранее, а также приоритетом порта и стоимостью

порта. Spaning tree группы STP работает также как spanning tree на уровне коммутаторов но понятие корневого моста замещается понятием корневого порта. Корневой порт – это порт группы, который выбирается на основе приоритета и стоимости порта и служит для подключения групп к сети. Избыточные связи будут блокированы как только будут блокированы избыточнее связи на уровне коммутаторов. На уровне коммутаторов STP блокирует избыточные связи между коммутаторами (и аналогичных сетевых устройств). На уровне портов STP блокирует избыточные связи внутри STP группы. Целесообразно определять STP группу соответствующую группе VLAN портов.

Можно настроить следующие установки STP порта:

Параметр	Описание
From/To	Последовательная группа портов, может быть сконфигурирована, начиная с выделенного порта.
External Cost	Этот параметр определяет метрику, которая показывает относительную стоимость передачи пакетов к списку определённых портов. Port Cost может быть установлен автоматически или задан определённым значением. Значение по умолчанию 0 (авто). *0 (авто)* – автоматически устанавливает оптимальную скорость пересылки пакетов на порт(ы). Значения Port Cost по умолчанию: для 100Мбит/с порта=200000; для порта Gigabit =20000 *Значение от 1 до 200000000* – определяет внешнюю стоимость. Чем меньше значение, тем выше приоритета порта.
Hello Time	Интервал между передачами конфигурационных сообщений назначенным портом на другие устройства в LAN. Пользователь может выблать значение от 1 до 10 секунд. Значение по умолчанию 2 секунды. Это поле доступно только, когда на Коммутаторе выбран MSTP.
Migration	При установке значения «yes» порты будут посылать RSTP BPDU-пакеты на порты.
Edge	Выбор значения *True* определяет порт, как пограничный. Пограничный порт не может создать петлю, однако, он может потерять свой статус, если в сети произошли изменения, потенциально ведущие к образованию петли. Пограничный порт не должен принимать BPDU-пакеты. Если был принят BPDU-пакет, это приведёт к автоматической потере статуса пограничного порта. Выбор значения *False* означает, что порт не является пограничным портом.
P2P	Значение True означает, что связь общего пользования point-to-point (P2P). P2P-порты похожи на пограничные порты, однако они ограничены, тогда как P2P-порты поддерживают полный дуплекс. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. Значение False означает, что порт не является P2P-портом. Значение Auto позволяет порту быть со статусом P2P всегда, когда возможно и оперировать так, как если бы значение P2P-статуса было *True*. Если порт не может поддерживать этот статус (например, если порт был принудительно поставлен в режим полу-дуплекса), значение P2P –статуса изменится на *False*. Значение по умолчанию для данного параметра *True*.
Forward BPDU	Значение True позволит пересылку BPDU-пакетов с сетевых устройств на назначенные порты. Для этого STP должен быть глобально отключён И пересылка BPDU-пакетов глобально разрешена (глава **STP Bridge Global Settings**).

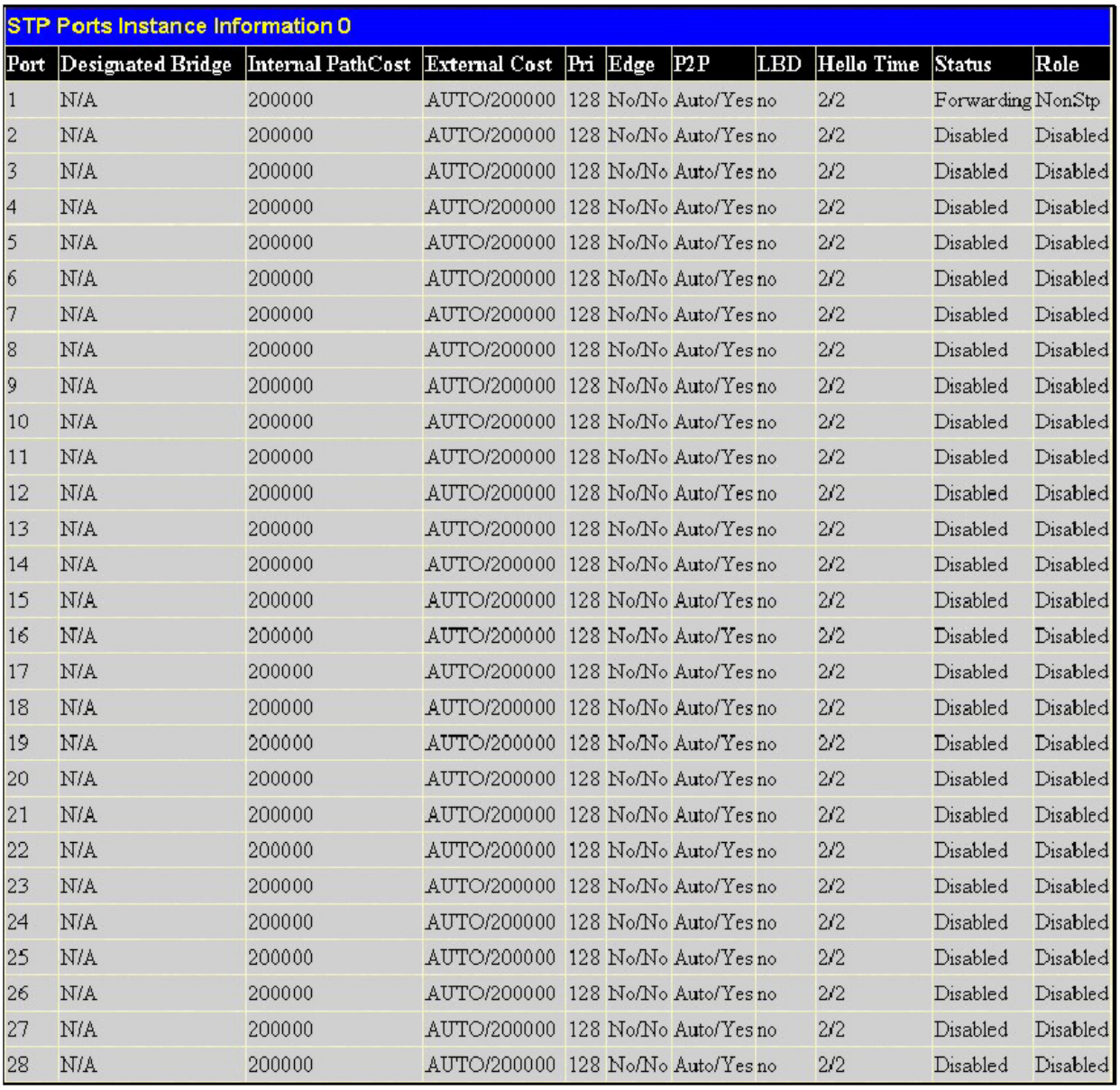
	Значение по умолчанию *False*, в этом случае BPDU-пакеты не пересылаются, даже если STP отключен.
LBD	Используется для включении/отключения функции обнаружения петли (loop-back detection) на портах коммутатора, сконфигурированных ранее. Для получения подробной информации стоит обратиться к главе **STP LoopBack Prevention.**
State	Позволяет включит/отключить STP для выбранных групп портов. Значение по умолчанию *Enabled*.

Для принятия настроек нажмите **Apply**.

Примечание: если требуется осуществить пересылку BPDU-пакетов на базе портов, следует сделать следующие установки: 1. STP должен быть глобально отключён, 2. Пересылка BPDU должна быть глобально включена. Эти параметры заданы по умолчанию, конфигурируются в меню **STP Bridge Global Settings**, рассмотренному ранее.

Копии информации STP- порта

Информация о ранее созданных копиях STP-порта доступна для просмотра в окне **STP Port Instance Information window.** Чтобы увидеть это окно, нажмите **L2 Features> Spanning Tree >STP Port Information of Instance.**Вся информация в этом окне доступна только для чтения и ранее описана в данном разделе. Каждый порт снабжен информацией, относящейся к индивидуальным настройкам spanning tree порта.



STP Ports Instance Information 0

Port	Designated Bridge	Internal PathCost	External Cost	Pri	Edge	P2P	LBD	Hello Time	Status	Role
1	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Forwarding	NonStp
2	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
3	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
4	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
5	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
6	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
7	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
8	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
9	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
10	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
11	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
12	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
13	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
14	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
15	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
16	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
17	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
18	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
19	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
20	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
21	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
22	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
23	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
24	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
25	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
26	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
27	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled
28	N/A	200000	AUTO/200000	128	No/No	Auto/Yes	no	2/2	Disabled	Disabled

Рисунок 7.37. STP Ports Instance Information окно

Forwarding

Unicast Forwarding

Следующие рисунок и таблица описывают, как установить на коммутаторе Unicast Forwarding. Откройте папку Forwarding в меню **L2 Features** и нажмите на ссылку **Unicast Forwarding**.

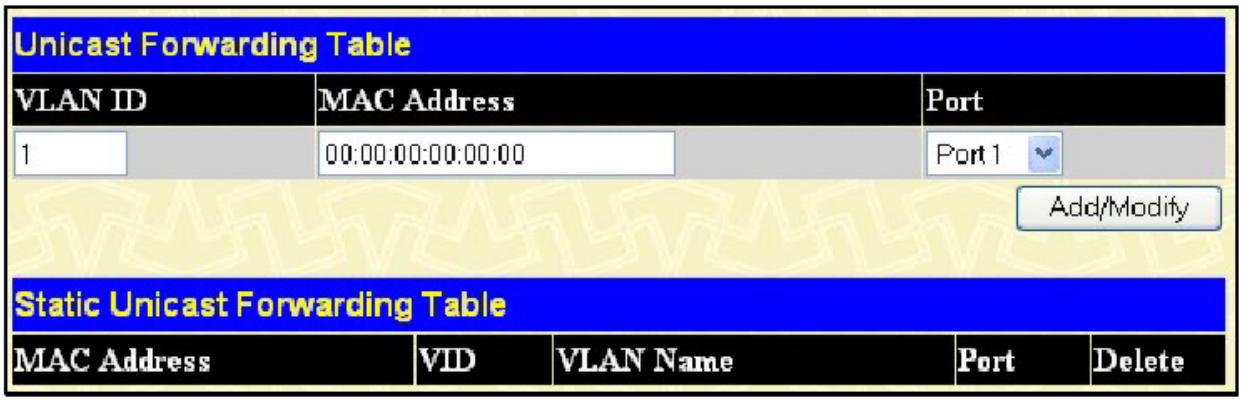


Рисунок 7- 38. Unicast Forwarding Table окно

Для добавления или редактирования записей следует добавить/изменить следующие параметры и нажать **Add/Modify**:

Параметр	Описание
VLAN ID (VID)	ID VLAN (идентификатор VLAN), на который ссылается вышеупомянутый Unicast MAC address.
MAC Address	MAC-адрес, на который будут постоянно пересылаться пакеты. Это может быть unicast MAC address.
Allowed to Go Port	Позволяет выбрать номер порта, на который будет ссылаться выше упомянутый MAC-адрес.

Для удаления записи из **Unicast Forwarding Table**, следует кликнуть по соответствующему ***X*** под заголовком **Delete**.

Multicast Forwarding

Следующий рисунок и таблица демонстрируют, как создать **Multicast Forwarding** (многоадресная рассылка) на Коммутаторе. Необходимо открыть папку **Forwarding** из **L2 Features,** нажать на ссылку **Multicast Forwarding**, после чего откроется следующее окно:

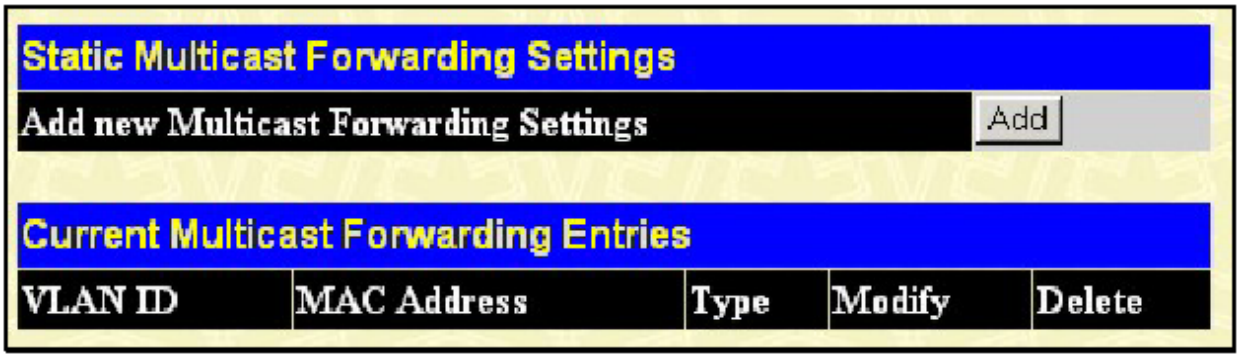


Рисунок 7.39. Static Multicast Forwarding Settings окно

Окно **Static Multicast Forwarding Settings** отображает все записи, содержащиеся в таблице многоадресной рассылки Коммутатора. Для открытия окна **Setup Static Multicast Forwarding Table** следует нажать на кнопку **Add**. Откроется окно, представленное ниже:

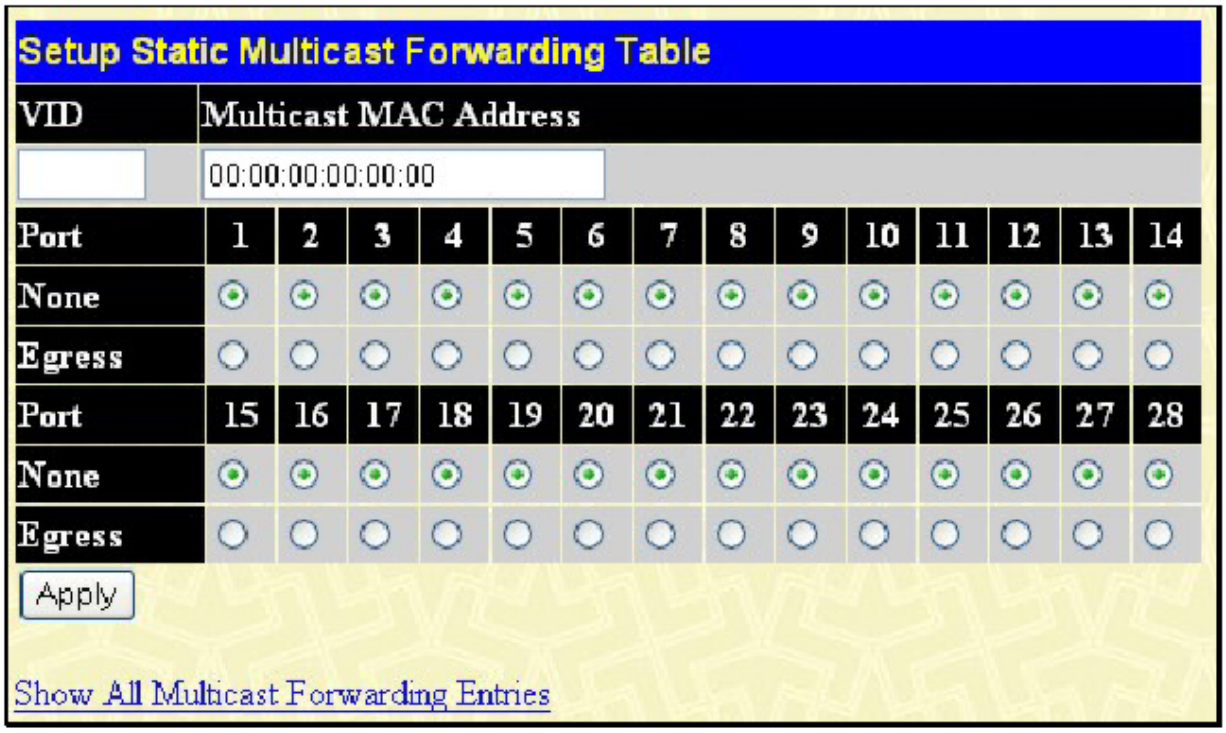


Рисунок 7.40. Setup Static Multicast Forwarding Table окно

Могут быть установлены следующие параметры:

Параметр	Описание
VID	Идентификатор VLAN, которой принадлежит соответствующий MAC-адрес.
Multicast MAC Address	MAC-адрес постоянного источника multicast-пакетов. Это должен быть multicast MAC-адрес.
Port Settings	Позволяет выбрать порты, которые будут членами multicast-группы и порты, которым запрещено присоединяться динамически или которые могут присоединиться к multicast-группе, используя GMRP. Существуют значения: *None* – нет ограничений на порт, динамически присоединяющийся к multicast-группе. Когда выбрано значение None, порт не может быть членом Static Multicast Group. *Egress* – порт постоянный член multicast-группы.

Для принятия настроек нажмите **Apply**. Для удаления записи из **Static Multicast Forwarding Table**, следует кликнуть по соответствующему ***X*** под заголовком **Delete**. Чтобы вернуться в окно **Static Multicast Forwarding Settings**, надо кликнуть по ссылке **Show All Multicast Forwarding Entries.**

Раздел 8 – Функции 3 уровня

Настройки IP-интерфейса
Настройки MD5 Key
Настройки Route Redistribution
Настройки статического/динамического маршрута
Настройка Route Preference
Настройка статического ARP
RIP
OSPF
DCHP/BOOTP Relay
DNS Relay
VRRP
Настройка маршрутизации IP Multicast

Данный раздел поможет пользователю в настройках функций безопасности на коммутаторе. Представлена подробная информация по таким опциям, как настройки IP-интерфейса, настройки MD5 Key, Route Redistribution, Static/Default Route, Route Preference, Static ARP, RIP, OSPF, DCHP/BOOTP Relay, DNS Relay, VRRP и IP Multicast Routing Protocol.

IP Multinetting

IP Multinetting –функция, которая позволяет неоднократно назначать одни и те же IP-интерфейсы в одной и той же VLAN. Это очень удобно для администратора, когда количество исходных IPs-интерфейсов недостаточно и сетевой администратор не хочет увеличивать количество IP-интерфейсов. IP Multinetting - это возможность назначить другой IP-интерфейс на той же самой VLAN, не нарушая работу исходных станций или установок исходного интерфейса .
Для IP multinetting может быть установлено два типа интерфейсов, *первичный* и *вторичный*, и каждый IP-интерфейс должен быть классифицирован как один из них. Первичный интерфейс подразумевает под собой всегда без исключений первый интерфейс, созданный в сети VLAN. Все другие созданные интерфейсы может быть рассмотрены только как вторичные. Возможно установить до пяти интерфейсов на одной VLAN (один первичный и до четырех вторичных), и в большинстве случаев они будут независимы друг от друга. Первичные интерфейсы не могут быть удалены, если VLAN содержит вторичный интерфейс. Однажды созданные пользователем множественные интерфейсы для определенной VLAN (*первичный и вторичный*) не могут быть изменены в другой VLAN.

 **Ограничения применения**: Широковещательный маршрутизатор не может быть соединен с IP-интерфейсами, использующими функции IP multinetting.

 **Примечание:** Только первичный IP-интерфейс будет поддерживать совместимый с BOOTP агент.

IP Multinetting представляет собой очень ценный инструмент для сетевых администраторов, которым необходимо большое количество IP-адресов, но в тоже время использование коммутатора в режиме IP Multinetting может стать причиной проблем с поиском неисправностей и пропускной способностью и в результате сможет стать лишь временным решением. Возможно возникновение следующих проблем:

- Коммутатор должен затрачивать дополнительные ресурсы при формировании пакетов для IP Multinetting.

- Возрастает количество широковещательных данных(например, RIP- upgrade пакеты и RIM hello пакеты)

Настройки IP-интерфейса

Установку VLAN необходимо начинать с установки соответствующего IP-интерфейса. Пример подобной установки приведен ниже:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineer	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Таблица 8.1. Пример VLAN – назначенные порты

В этом случае, необходимо шесть IP-интерфейсов. Таким образом, CIDR-нотация 10.32.0.0/11(или 11 бит) схема адресации будет работать.

Эта схема адресации будет давать маску подсети 11111111.11100000.00000000.00000000(в двоичной системе счисления) или 255.224.0.0 (в десятичной системе счисления).

Используя IP-адресов вида 10.xxx.xxx.xxx, в приведенном выше примере можно будет организовать 6 сетевых адресов и 6 подсетей. Любой IP-адрес из разрешенного диапазона IP-адресов в каждой подсети может быть выбран в качестве IP-адреса IP-интерфейса на коммутаторе. В качестве примера, мы выбрали IP-адрес, больший на 1, чем сетевой адрес IP-интерфейса.

VLAN Name	VID	Network Number	IP Address
System (default)	1	10.32.0.0	10.32.0.1
Engineer	2	10.64.0.0	10.64.0.1
Marketing	3	10.96.0.0	10.96.0.1
Finance	4	10.128.0.0	10.128.0.1
Sales	5	10.160.0.0	10.160.0.1
Backbone	6	10.192.0.0	10.192.0.1

Таблица 8.2. Пример VLAN - Назначенные IP-интерфейсы

Шесть IP-интерфейсов, IP-адреса которых приведены выше, с маской подсети 255.224.0.0 могут быть введены в окне **IP Interface Settings**.

Для установки IP-интерфейсов на коммутаторе:

Зайдите в папку **L3 Features** и нажмите на ссылку **IP Interfaces Settings,** откроется следующее диалоговое окно.

Рисунок 8.1. Окно IP Interface Table

Для установки нового IP-интерфейса нажмите на кнопку **Add**. Для редактирования существующего IP-интерфейса нажмите на записи под заголовком **Interface Name**. В результате обоих действий пользователь получит доступ к показанному ниже окну.

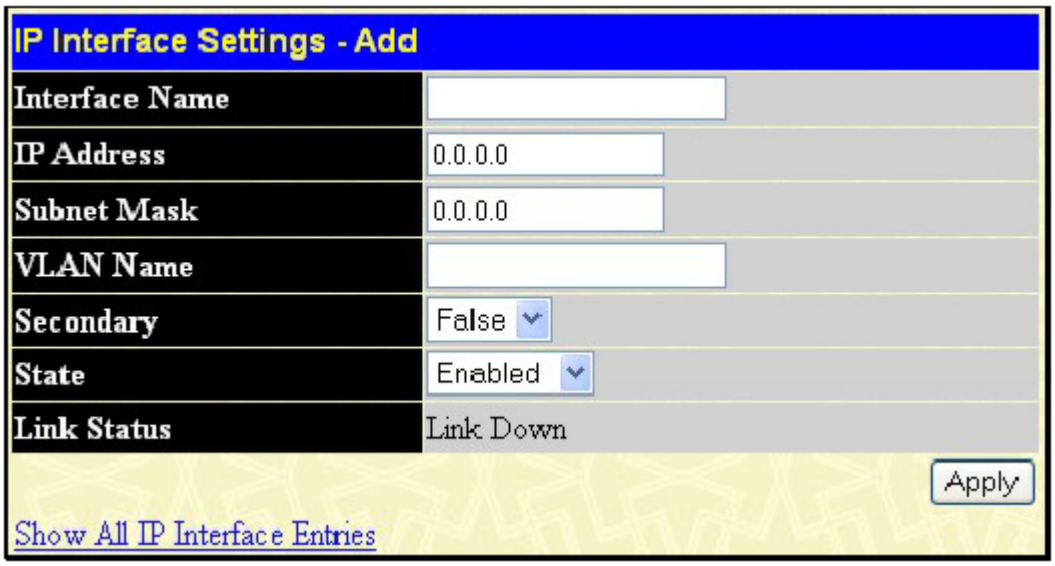


Рисунок 8.2. IP-Interface Settings – Add

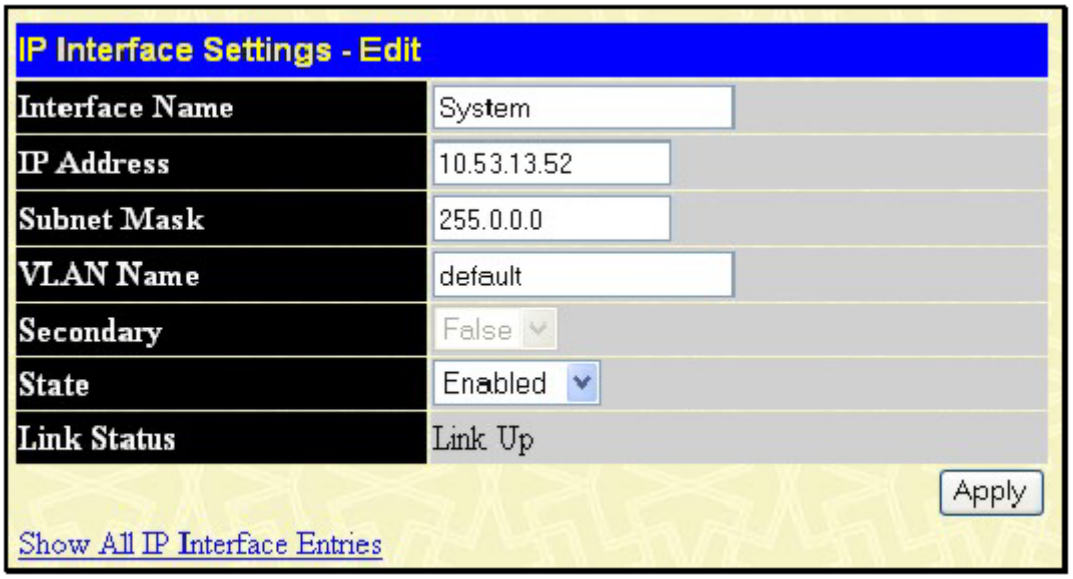


Рисунок 8.3. IP-Interface Settings – Edit

В поле **Interface Name** введите имя вновь создаваемого интерфейса (в случае если редактируется уже существующий IP-интерфейс, то его имя уже введено в верхнем поле, как показано выше). Введите в соответствующие поля IP-адрес и маску подсети. Установите в выпадающем меню поля **State** состояние *Enabled* и нажмите Apply, чтобы завершить установку IP-интерфейса. Для просмотра записей в **IP Interface Table,** нажмите ссылку Show All IP Interface Entries . Воспользуйтесь диалоговым окном Save Changes для введения изменений NV-RAM.

Следующие поля могут быть установлены.

Параметр	Описание
IP Address	Данное поле позволяет ввести IP-адрес, назначаемый данному IP-интерфейсу
Subnet Mask	Данное поле позволяет ввести маску подсети, применяемую к данному IP-интерфейсу.
Interface Name	Поле, отображающее имя IP-интерфейса. По умолчанию имя IP-интерфейса – «System».
VLAN Name	Данное поле позволяет ввести имя VLAN, к которой принадлежит IP-

	интерфейсу
Secondary	Используя выпадающее меню, установите значение данного поля в состояние *True* или *False*. Значение *True* устанавливает вторичный интерфейс, в то время как значение *False* устанавливает первичный интерфейс указанной выше VLAN. Вторичные интерфейсы могут быть установлены только после установки первичных.
State	Это поле может принимать в выпадающем меню значения *Enabled* или *Disabled*. Это поле определяет активен ли интерфейс или нет.
Link Status	Это поле, доступное только для чтения отображает текущий статус IP-интерфейса на коммутаторе. *Link Up* означает, что IP-интерфейс установлен и работает на коммутаторе. *Link Down* будет обозначать, что IP-интерфейса нет в текущих настройках и/или он выключен на коммутаторе.

Для применения настроек нажмите **Apply.**

MD5 Key Settings

В окне **«MD5 Key Settings»** можно задать 16-ти символьный ключ профиля сообщения версии 5 (Message Digest − version 5, MD5), который будет использоваться для аутентификации каждого пакета, которыми обмениваются между собой маршрутизаторы OSPF. Ключ представляет собой механизм безопасности для ограничения обмена информацией о топологии сети в рамках домена маршрутизации OSPF. Созданные ключи MD5 могут быть использованы в дальнейшем в меню **OSPF**. Для настройки ключа MD5 необходимо открыть следующее окно, для этого нажмите: **Layer 3 Features ⇨ MD5 Key Settings.**

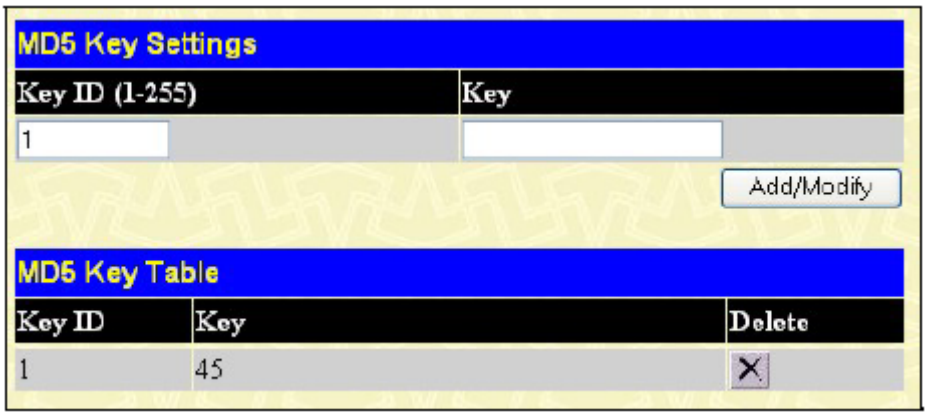


Рисунок 8.4 – Окно «MD5 Key Settings and Table»

Можно настроить следующие параметры:

Параметр	Описание
Key ID (1-255)	Для идентификации ключа MD5 введите число от 1 до 255.
Key	Введите ключ, представляющий собой буквенно-цифровую последовательность длиной от 1 до 16 символов с учетом регистра, он используется для генерации профиля сообщения, который, в свою очередь, применяется для аутентификации пакетов OSPF в пределах домена маршрутизации OSPF.

Для ввода нового идентификатора ключа нажмите **Add**, а для удаления записи Key ID, нажмите соответствующую кнопку ✕ под заголовком *Delete*.

Route Redistribution Settings (Настройки перераспределения маршрутов)

Перераспределение маршрутов позволит маршрутизаторам, работающим по различным протоколам, обмениваться информацией по маршрутам. Это достигается сравнением маршрутов, хранящихся в таблицах маршрутизации различных маршрутизаторов, и установкой соответствующих метрик. Коммутаторы обмениваются этой информацией в соответствии с индивидуальным протоколом маршрутизации. Коммутатор может перераспределять информацию по маршрутам между всеми маршрутизаторами сети, работающих по протоколам OSPF или RIP. Информация по маршрутам, занесенная в таблицу Static Routing Table на локальном xStack коммутаторе, также перераспределяется. Источником информации по маршрутам являются OSPF и таблица статической маршрутизации Static Routing Table. Информация по маршрутам будет перенаправлена RIP. Следующая таблица иллюстрирует разрешенные значения метрик маршрутизации и виды (или формы) информации маршрутизации, которая будет перенаправлена.

Рисунок 8.3 – Окно «Route Redistribution Source Table»

Route Source	Metric	Type
OSPF	0 to 16	All Internal External ExtType1 ExtType2 Inter-E1 Inter-E2
RIP	0 to 16777214	Type 1 Type 2
Static	0 to 16777214	Type 1 Type 2
Local	0 to 16777214	Type 1 Type 2

Ввод комбинации internal external type_1 type_2 в поле Type эквивалентен вводу значения all, комбинации external type_1 type_2 – вводу значения external, комбинации internal external - вводу значения all. Введение метрики 0 означает прозрачность.

В этом окне будет распределяться информация маршрутизации между OSPF и RIP. Для доступа к окну **Route Redistribution Settings,** нажмите **L3 Features> Route Redistribution Settings:**

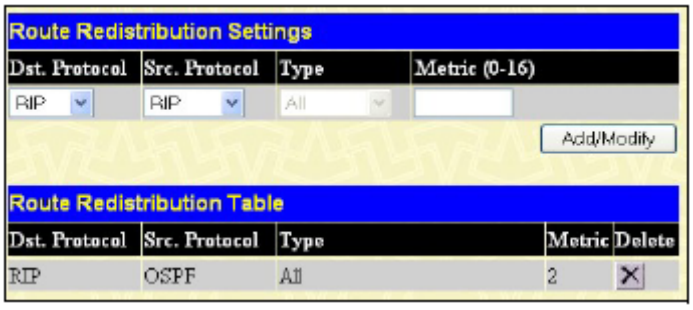


Рисунок 8.5 – Окно «Route Redistribution Settings and Table»

Следующие параметры доступны для просмотра и установки.

Параметр	Описание
Dst. Protocol	Выберите протокол *RIP* или *OSPF* для устройства, являющегося адресатом информации.
Src. Protocol	Выберите протокол *RIP, OSPF, Static* или *Local* для устройства, являющегося источником информации.
Type	Выберите один из шести методов вычисления значения метрики: *All, Internal, External, ExtType1, ExtType2, Inter-E1, Inter-E2*. Для просмотра соответствий метода и значения метрики для каждого возможного протокола устройства, являющегося источником информации, обратитесь к таблице, приведенной выше.
Metric	Определите стоимость интерфейса OSPF от 0 до 16, она является аналогом Hop Count для протокола маршрутизации RIP.

Для того чтобы изменения вступили в силу, нажмите **Add/Modify**.

Примечание: Протоколы устройств, являющихся источником (Src. Protocol) и адресатом (Dst. Protocol) информации, не могут быть одними и теми же.

Настройки маршрутизатора статического/по умолчанию

Записи в таблицу Switch's forwarding table могут быть сделаны как на основании MAC-адресов , так и IP-адресов. Static IP forwarding назначается вводом IP-адреса в таблицу коммутатора **Static IP Routing Table**. Чтобы увидеть следующее окно, нажмите **L3 Features > Static/Default Route Settings**.

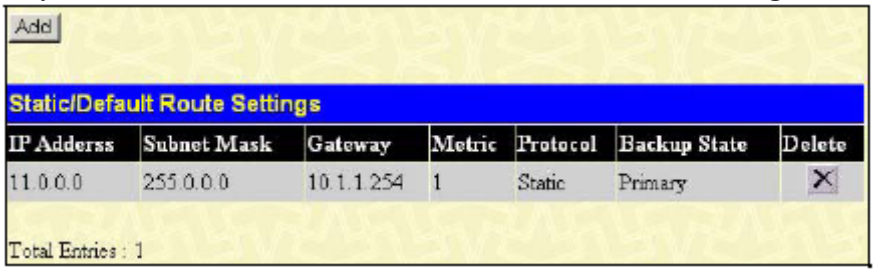


Рисунок 8.6 – Окно «Static/Default Route Settings»

В этом окне показаны следующие параметры

Параметр	Описание
IP Address	IP-адрес маршрутизатора статического/по умолчанию
Subnet Mask	Соответствующая введенному в таблицу IP-адресу маска подсети
Gateway	Соответствующий введенному в таблицу IP-адресу шлюз
Metric	Представляет значение метрик IP-интерфейса, введенных в таблицу. В этом поле можно прочитать значение между 1 и 65535 для настроек OSPF или между 1и 16 для настроек RIP.
Protocol	Представляет протокол, используемый для внесения записей IP-интерфейсов в таблицу маршрутизации. Это поле может содержать OSPF, RIP, Static или Local
Backup State	Представляет состояние резервной копии (Backup) данного IP-интерфейса. В данном поле можно прочитать *Primary* или *Backup*.
Delete	Нажмите «X» для удаления соответствующей записи из таблицы Static/ Default Route Settings.

Для ввода IP-интерфейса в окно коммутатора Static/Default Route Settings, нажмите кнопку **Add** для воспроизведения следующего окна:

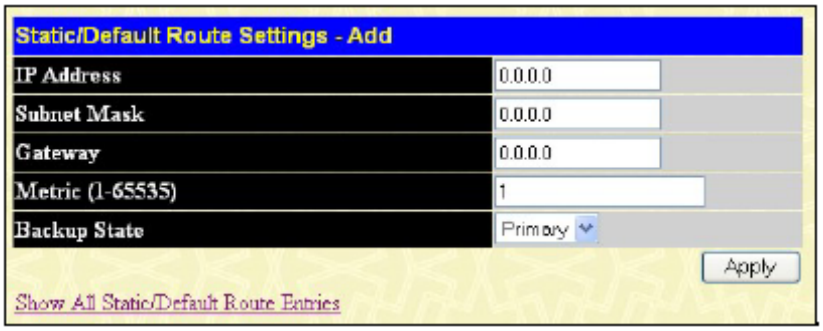


Figure 8- 7. Static/Default Route Settings – Add window
Следующие параметры могут быть установлены:

Параметр	Описание
IP Address	Позволяет ввести IP-адрес статического маршрутизатора в таблицу маршрутизации коммутатора.
Subnet Mask	Позволяет ввести маску подсети, соответствующую введенному выше IP-адресу.
Gateway	Позволяет ввести IP-адрес шлюза для IP-адреса, введенного выше.
Metric(1-65535)	Позволяет ввести метрики протокола маршрутизации, определяющие количество маршрутизаторов между коммутатором и указанным выше IP-адресом.
Backup State	Пользователь может выбрать между двумя значениями *Primary* или *Backup*. Если с маршрутизатором первичным статическим/по умолчанию произойдут неполадки, то Backup маршрутизатор возьмет на себя его функции. Примите во внимание, что первичный и Backup маршрутизаторы не могут иметь один и тот же шлюз.

Для применения настроек нажмите **Apply.**

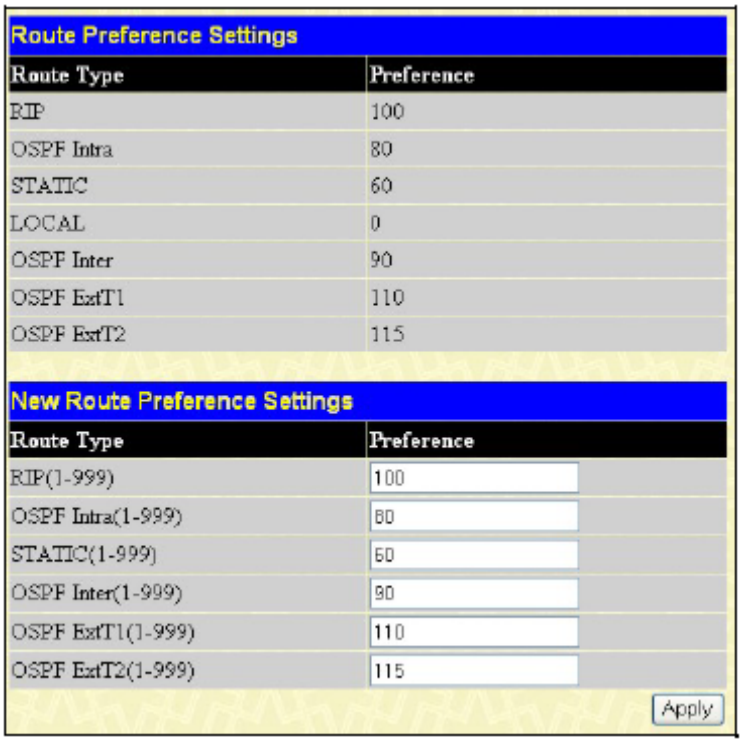
Настройки предпочтительного маршрута (Route Preference Settings)

(Route Preference)Предпочтительный маршрут – это способ для маршрутизатора выбрать наилучший маршрут, когда есть два или более маршрутизатора в одном и том же направлении, поддерживающие различные протоколы маршрутизации. Большинство протоколов маршрутизации не совместимы при их совместном использовании. Этот коммутатор поддерживает и может быть настроен под многие протоколы маршрутизации как отдельный коммутатор или, что более важно, при использовании функций стекирования и Single IP Management коммутатора. Таким образом, способность коммутатора обмениваться информацией маршрутизации и выбирать лучший маршрут играет важную роль в оптимальном использовании коммутатора и его производительности.

Изначально коммутатор принимает решение по выбору оптимального маршрута, обращаясь к таблице Route Preference Settings коммутатора. Эта таблица может быть просмотрена путем нажатия **Configuration>L3 IP Networking>Route Preference Settings**. Здесь содержится список возможных протоколов маршрутизации, возможных в текущей настройке коммутатора, а также параметр **Preference**, который определяет наиболее надежный для пакетов протокол в каждом конкретном случае. Ниже приводится список настроек по умолчанию коммутатора.

Route Type	Validity Range	Default Value
Local	0 - Permanently set on the Switch and not configurable.	0
Static	1 - 999	60
OSPF Intra	1 - 999	80
OSPF Inter	1 - 999	90
RIP	1 - 999	100
OSPF ExtT1	1 - 999	110
OSPF ExtT2	1 - 999	115

Как показано выше, при маршрутизации маршрут *Local* будет всегда выбран первым, а следующим наиболее надежным маршрутом является *Static,* поскольку у него второе по меньшинству значение Default Value. Для установки более высокой надежности маршрута используйте команду **New Route Preference Settings** window. Например, если пользователь желает сделать наиболее надежным маршрутом RIP, он может изменить его Default Value так, чтобы оно стало самым маленьким по сравнению с другими (меньше, чем у Static = 60).
Пользователь перед установкой предпочтительного маршрута должен ознакомиться со следующим:
1. Два маршрута не могут иметь одинаковые значения Preference. Ввод одинаковых значений Preference может стать причиной неполадок на коммутаторе из-за того, что коммутатор не сможет принять решение.
2. Если пользователь не осведомлен обо всех особенностях и функциях протоколов маршрутизации на коммутаторе, изменение значения Preference коммутатора по умолчанию может стать причиной петель маршрутизации или черных дыр
3. После изменения route preference значения для определенного протокола маршрутизации, этот протокол необходимо перезагрузить, потому что ранее выученные маршруты должны быть удалены с коммутатора. Коммутатор должен выучить маршруты снова.
Чтобы увидеть **Route Preference Settings** окно, нажмите **L3 Features > Route Preference Settings:**



Следующие параметры могут быть установлены и просмотрены:

Параметр	Описание
RIP (1-999)	Введите значение от 1 до 999 для установки значения route preference для RIP. Чем меньше значение, тем больше вероятность, что данный протокол будет выбран как наилучший маршрут для пакетов маршрутизации. По умолчанию значение равно 100.
OSPF Intra (1-999)	Введите значение от 1 до 999 для установки значения route preference для OSPF Intra. Чем меньше значение, тем больше вероятность, что данный протокол будет выбран как наилучший маршрут для пакетов маршрутизации. По умолчанию значение равно 80.
Static(1-999)	Введите значение от 1 до 999 для установки значения route preference для Static. Чем меньше значение, тем больше вероятность, что данный протокол будет выбран как наилучший маршрут для пакетов маршрутизации. По умолчанию значение равно 60.
OSPF Inter (1-999)	Введите значение от 1 до 999 для установки значения route preference для OSPF Inter. Чем меньше значение, тем больше вероятность, что данный протокол будет выбран как наилучший маршрут для пакетов маршрутизации. По умолчанию значение равно 90.
OSPF ExtT1(1-999)	Введите значение от 1 до 999 для установки значения route preference для OSPF ExtT1. Чем меньше значение, тем больше вероятность, что данный протокол будет выбран как наилучший маршрут для пакетов маршрутизации. По умолчанию значение равно 110.
OSPF ExtT2(1-999)	Введите значение от 1 до 999 для установки значения route preference для OSPF ExtT2. Чем меньше значение, тем больше вероятность, что данный протокол будет выбран как наилучший маршрут для пакетов маршрутизации. По умолчанию значение равно 115.

Для применения настроек нажмите **Apply**

Статическая таблица ARP

Address Resolution Protocol (ARP) – TCP/IP-протокол, который конвертирует IP-адреса в физические адреса. Данная таблица позволяет сетевым менеджерам просматривать, определять, модифицировать и удалять ARP-информацию для определённых устройств.
Статические записи могут быть определены в ARP-таблице. Когда статические данные определены, перманентные данные вводятся и используются для трансляции IP-адресов в MAC-адреса.
Чтобы открыть окно **Static ARP Table** откройте папку **Configuration**, затем откройте папку **Layer 3 IP Networking**, нажмите на ссылку **Static ARP Table**.

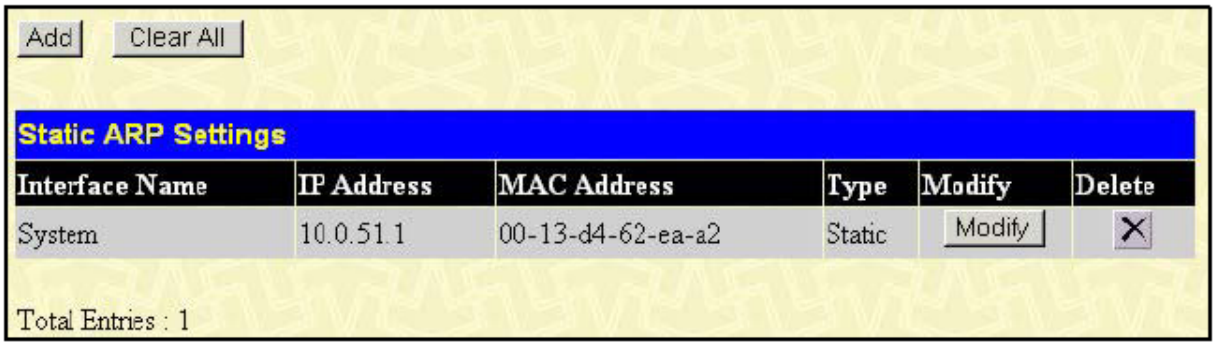


Рисунок 8.9. Static ARP Settings window

Для добавления новой записи следует нажать на кнопку **Add**, как показано в следующем окне конфигурации:

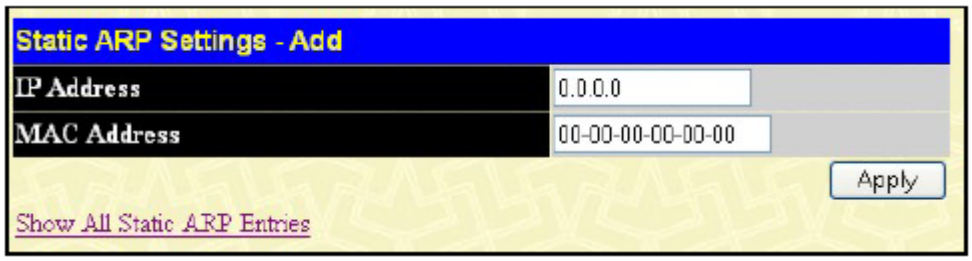


Рисунок 8.10. Static ARP Table - Add window

Могут быть установлены следующие поля:

Параметр	Описание
IP Address	IP-адрес ARP-записи.
MAC Address	MAC-адрес ARP-записи.

После ввода IP-адресов и MAC-адресов ARP-записи, следует кликнуть по кнопке **Apply** для принятия настроек. Для полной очистки статических ARP-установок необходимо кликнуть по кнопке **Clear All**.

Примечание: Коммутатор поддерживает до 255 статических ARP-записей.

RIP

Routing Information Protocol является протоколом дистанционно-векторной маршрутизации. Существует два вида сетевых устройств, работающих с RIP – активные и пассивные. Активные

устройства информируют о маршрутах другие устройства посредством RIP-сообщений, в то время как пассивные могут только слушать эти сообщения. И активные, и пассивные маршрутизаторы обновляют их таблицы маршрутизации на основе RIP-сообщений, которыми обмениваются активные маршрутизаторы. Только маршрутизаторы могут запускать RIP в активном режиме .

Каждые 30 секунд маршрутизатор, поддерживающий RIP, пересылает обновленную информацию по маршрутизации- пары сетевых адресов и расстояние (представленное в виде количества хопов (от англ. hop- прыжок, транзитный учаток) или маршрутизаторов между оповещаемым маршрутизатором и удаленной сетью). Таким образом, вектор – это сетевой адрес и расстояние, измеряемое в количестве маршрутизаторов между локальным маршрутизатором и удаленной сетью.

Протокол RIP выражает расстояние в виде целого числа хопов от одной сети до другой. Маршрутизатор – это один хоп от непосредственно присоединенной сети, два хопа от сети, которую можно достигнуть через еще один маршрутизатор. Чем больше маршрутизаторов между источником и приемником, тем больше значение RIP-расстояния (или числа хопов).

Здесь представлены несколько правил процесса обновления таблицы маршрутизации, усовершенствующие исполнение и надежность. Маршрутизатор не подставит в таблицу вновь выученный маршрут, если новый маршрут имеет то же число хопов (иногда называемое «стоимость»). Таким образом, обученные маршруты остаются до тех пор, пока не появится новый маршрут с меньшим количеством транзитных участков.

Когда обученные маршруты введены в таблицу маршрутизации, включается таймер. Этот таймер перезапускается каждый раз, когда маршрутизатор получает уведомление. Если маршрутизатор не получил уведомление, этот маршрутизатор удаляется из таблицы маршрутизации.

Протокол RIP не предусматривает явного метода для обнаружения петель маршрутизации. Многие варианты RIP включают механизм авторизации (пароль) для предотвращения изучения маршрутизатором ошибочных маршрутов от неавторизованных маршрутизаторов.

Для увеличения стабильности, число хопов RIP протокола должно не превышать максимального значения. Бесконечным количеством числа хопов (т.е. сеть недоступна) считается более 16 хопов. Другими словами, если сеть находится на расстоянии больше, чем 16 маршрутизаторов, локальный маршрутизатор будет рассматривать сеть как недоступную.

RIP также может обладать низкой сходимостью (удаляя противоречивые, недоступные маршруты и петли), потому что RIP-сообщения передаются относительно медленно по сети.

Проблема низкой сходимости может быть решена, используя split horizon update, когда маршрутизатор не передает информацию о маршруте обратно к интерфейсу, от которого была получена эта информация. Это сокращает вероятность образования переменных петель мрашрутизации.

Удержание может быть использовано, чтобы заставить маршрутизатор игнорировать обновление маршрутов в течение определенного периода времени (обычно 60 секунд). После этого новое обновление маршрута будет получено. Это позволяет всем маршрутизаторам на сети получить это сообщение.

Мрашрутизатор может «poison reverse» маршруту, добавив бесконечный (16) счетчик транзитных участков в уведомление. Это обычно используется в связи с инициированием обновления, что заставляет маршрутизатор немедленно рассылать информацию, если получены обновления от недоступной сети.

Формат сообщений RIP версии 1

Выделяют два типа RIP-сообщений: сообщения информации маршрутизации и информационные запросы. Оба типа сообщений имеют одинаковый формат. Поле Command определяет действия в соответствии со следующей таблицей:

Command (Команда)	Обозначение
1	Запрос полной или частичной информации маршрутизации
2	Ответ, содержащий пару сеть-расстояние из таблицы маршрутизации получателя
3	Включение режима трассировки (устар.)
4	Отключение режима трассировки (устар.)
5	Зарезервировано для внутреннего

	использования Sun Microsystem
9	Запрос обновления
10	Ответ обновления
11	Подтверждение приема обновления

Командные коды RIP

Поле Version содержит номер версии протокола (1 в данном случае) и используется, чтобы получатель определил, с использованием какой версии RIP был послан пакет.

Сообщения RIP 1

Применение RIP не ограничивается протоколом TCP/IP. Формат адреса протокола RIP может поддерживать до 14 октетов (при применении IP оставшиеся 10 октетов должны быть установлены в 0). Другие сетевые протоколы могут быть определены в поле Family of Source Network (протокол IP имеет значение 2). Это будет определять, как интерпретировать поле адреса.
RIP определяет, что IP-адрес 0.0.0.0 принадлежит маршрутизатору по умолчанию.
Расстояния, измеряемые в хопах, вводятся в поля Distance to Source Network и Distance to Destination Network.

Интерпретация маршрута RIP 1

RIP был разработан для использования адресными схемами классов и не включает явного определения маски подсети. Расширенная версия 1 позволяет маршрутизаторам обмениваться адресами подсетей, но только если маска подсети, применяемая на сети, точно такая же, как маска подсети, применяемая для данного адреса. Это означает, что RIP версии 1 не может быть использован для передачи бесклассовых адресов.
Маршрутизаторы, работающие на основе RIP v1, должны отсылать различные сообщения обновления для каждого IP-интерфейса, к которому они подсоединены. Интерфейсы, которую используют ту же маску подсети, что и сеть маршрутизатора, могут содержать маршруты с маской подсети, другие интерфейсы – не могут. Тогда маршрутизатор будет оповещать в сети только о простых маршрутах.

Расширения RIP версии 2

RIP версии 2 включает явный ввод маски подсети. Таким образом, RIP v.2 может быть использован для передачи адресов с масками подсети различной длины или бесклассовые адреса CIDR. В RIP v2 также добавлен явное задание следующего хопа, что увеличивает схождение и помогает предотвратить образование петель маршрутизации.

Формат сообщений RIP 2

Формат сообщений, используемый RIP 2, представляет собой расширение формата RIP 1:
RIP 2 также добавляет 16-битный таг маршрута, который запоминается и передается с информацией обновления маршрутизатора. Он может быть использован для идентификации источника маршрута.
Поскольку номер версии в RIP2 занимает тот же самый октет, что и в RIP1 обе версии протокола могут быть использованы на одном маршрутизаторе одновременно, не мешая друг другу.

Глобальные настройки RIP

Чтобы установить RIP для IP интерфейсов, настроенных на коммутаторе, пользователь должен глобально подключить RIP на коммутаторе и затем установить RIP-настройки для каждого IP-интерфейса. Для глобальной установки RIP на коммутаторе, откройте **L3 Features** и затем откройте папку **RIP** и нажмите на ссылку **RIP Global Settings**, чтобы получить доступ к следующему окну:

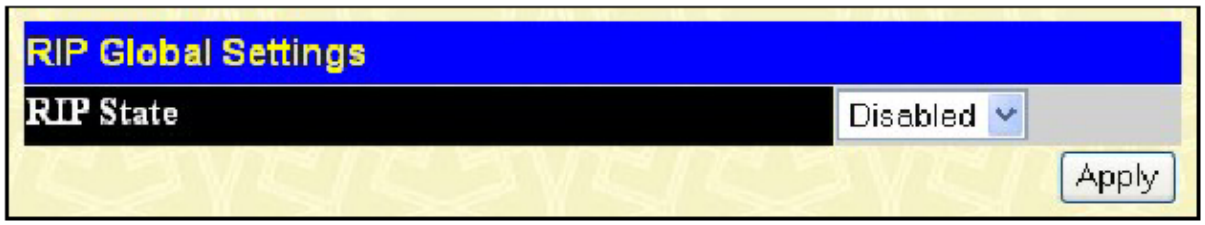


Рисунок 8.11 RIP Global Settings window

Для подключения RIP просто выберите **Enabled**, используя выпадающее меню, и нажмите **Apply**.

Настройки RIP-интерфейса

Настройки RIP устанавливаются для каждого IP-интерфейса коммутатора. Нажмите ссылку **RIP Interface Settings** в папке **RIP**. Появится меню в виде таблицы, отражающее текущие настройки IP-интерфейсов на коммутаторе. Для установки RIP-настроек для индивидуальных IP-интерфейсов, нажмите на гиперссылку **Interface Name**.

RIP Interface Settings

Interface Name	IP Address	TX Mode	RX Mode	Auth.	State
System	10.53.13.52	V2 Only	V1 and V2	Disabled	Disabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled
_	0.0.0.0	0	0	Disabled	Enabled

Рисунок 8.12. RIP Interface Settings window

Нажмите на гиперссылку имени интерфейса, для которого Вы хотите настроить RIP. Вы получите доступ к следующему меню:

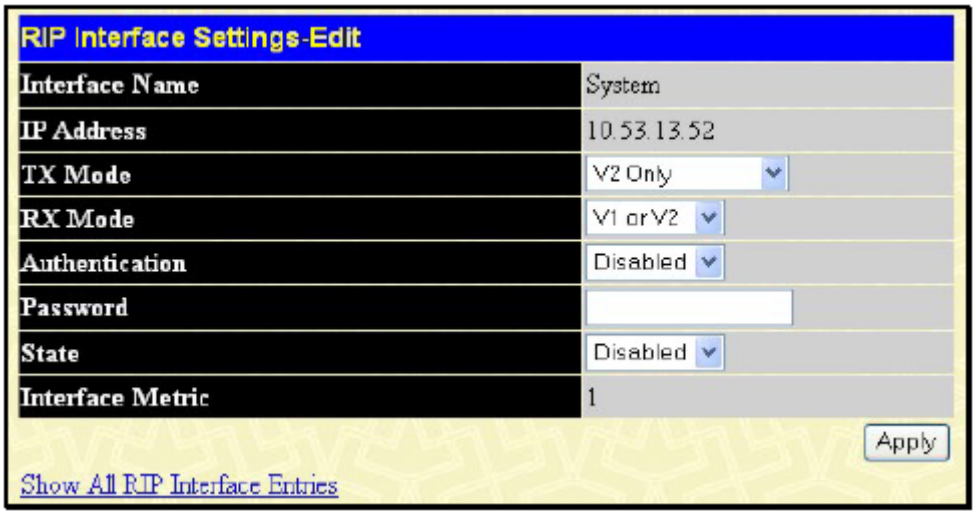


Рисунок 8.13. RIP Interface Settings - Edit window

Чтобы получить описание возможных параметров для настройки RIP-интерфейса, обратитесь к таблице, показанной ниже. Следующие RIP-настройки могут быть применены к каждому IP-интерфейсу.

Параметр	Описание
Interface Name	Имя IP-интерфейса, на котором устанавливается RIP. Этот интерфейс должен быть сначала установлен на коммутаторе.
IP Address	IP-адрес, соответствующий имени IP-интерфейса, указанному в поле выше
TX Mode	Данное поле можно переключить между *Disabled*, *V1 Only*, *V1 Compatible* и *V2 Only*. Это поле определяет, какая версия RIP протокола будет использована для передачи RIP-пакетов. Состояние *Disabled* запрещает передачу RIP-пакетов.
RX Mode	Данное поле можно переключить между *Disabled*, *V1 Only*, *V1 Compatible* и *V2 Only*. Это поле определяет, какая версия RIP протокола будет использована для интерпретации полученных RIP-пакетов. Состояние *Disabled* запрещает прием RIP-пакетов.
Authentication	Данное поле можно переключить между *Disabled* и *Enabled* для определения, будет ли маршрутизатор перед обменом таблицами маршрутизации запрашивать пароль для аутентификации.
Password	Пароль, используемый для аутентифицированного взаимодействия между маршрутизаторами на сети.
State	Данное поле можно переключить между *Disabled* и *Enabled* для отключения или подключения RIP-интерфейса на коммутаторе.
Interface Metric	Поле, доступное только для чтения. Определяет значение метрики текущих настроек IP-интерфейса.

Для применения настроек нажмите **Apply**

OSPF

Протокол маршрутизации OSPF использует алгоритм *link-state* для определения маршрутов до сети назначения. «Link»- это интерфейс маршрутизатора и «*state*» - это описание этого интерфейса и его отношения с соседними маршрутизаторами. «State» содержит такую информацию, как IP-адрес, маска подсети, тип сети, к которой присоединяется интерфейс, другие маршрутизаторы, присоединенные к сети и т.д. Link-states(состояния каналов) затем собираются в базе данных, которая поддерживается маршрутизаторами, работающими с OSPF.
OSPF устанавливает, как маршрутизаторы будут взаимодействовать с поддерживаемой ими базой данных состояний канала (LSDB), и определяет несколько принципов топологии сетей, которые используют OSPF.

Для ограничения количества трафика по обновлению состояния каналов между маршрутизаторами, в OSPF определена концепция *Area*(область). Все маршрутизаторы из одной области имеют точно такую же базу данных состояния каналов. И изменения в этой базе данных на одном маршрутизаторе запускает обновления в базе данных состояния каналов всех остальных маршрутизаторов в этой области. Маршрутизаторы, которые имеют интерфейсы, подключенные к больше, чем одной области, называются *Border Routers* (пограничные маршрутизаторы) и несут ответственность за распределение информации.
Одна из областей определяется как *Area 0* или *Backbone.* Эта область является центральной в сети, и все остальные области имеют присоединение к этой области (через маршрутизатор). Только маршрутизаторы, присоединенные к *Backbone*, и OSPF построена таким образом, что изменения информации маршрутизации в других областях будут переданы в *Backbone* и затем передаются другим маршрутизаторам области во время состояния покоя сети .
При построении сети с применением OSPF, обычно желательно начинать с *Backbone (Область 0)* для взаимодействия «со внешним миром».

Link-State алгоритм

OSPF-маршрутизаторы используют алгоритм Link-state для построения дерева кратчайшего пути во всех направлениях, известных маршрутизатору. Ниже приводится упрощенное пошаговое описание алгоритма:

- Когда запускается OSPF или когда изменяется информация маршрутизации, маршрутизатор генерирует уведомление о состоянии канала (link-state). Это уведомление представляет собой специально отформатированный пакет, который содержит информацию о состоянии всех каналов маршрутизатора.
- Это уведомление о состоянии канала рассылается всем маршрутизаторам области. Каждый маршрутизатор, который получает уведомление о состоянии канала, будет сохранять данное уведомление и затем пересылать его копию другим маршрутизаторам.
- Когда база данных по состоянию каналов каждого маршрутизатора обновлена, все маршрутизаторы будут строить дерево кратчайшего пути во всех направлениях. IP-таблица маршрутизации затем будет откорректирована с учетом адресом назначения, соответсвующей стоимости и адресом назначения.
- Базы данных состояний канала обновлены, деревья кратчайших путей вычислены и IP-таблицы маршрутизации записаны – если нет последующих изменений в сети OSPF (таких как отключение сетевого канала), то в сети совсем немного OSPF-трафика.

Алгоритм кратчайшего пути

Кратчайший путь до пункта назначения вычисляется при помощи алгоритма Дейкстера. Каждый маршрутизатор располагается в корне дерева, и затем вычисляется кратчайший путь до каждого пункта назначения на основе общей стоимости достижения каждого пункта назначения из множества возможных маршрутов. Каждый маршрутизатор будет затем иметь его собственное дерево кратчайшего пути (в зависимости от его положения в сетевой области), при этом все маршрутизаторы области будут иметь и применять одну и ту же базу данных состояний канала. Следующие разделы описывают информацию, которая используется при построении дерева кратчайшего пути.

Стоимость OSPF

Каждый OSPF-интерфейс имеет соответствующую стоимость (также называемую «Метрика»), которая представляет собой служебную информацию, необходимую для передачи пакетов через этот интерфейс. Эта стоимость обратно пропорциональна полосе пропускания интерфейса (чем выше полоса пропускания интерфейса, тем ниже его стоимость). Таким образом, более высокая стоимость пересылки (и более длительные задержки по времени) при отправке пакетов по 56кбит/с dial-up соединению, нежели чем по 10Мбит/с Ethernet соединению. Для вычисления стоимости OSPF используется следующая формула:
Стоимость = 100 000 000/ полосу пропускания в битах/с

Например, стоимость 10 Мбит/с Ethernet-линии будет равна 10, а стоимость преодоления 1,544 Мбит/с T1-линии будет равна 64.

Дерево кратчайшего пути

Для построения дерева кратчайшего пути для маршрутизатора A, показанного на диаграмме ниже, маршрутизатор A устанавливается в корне дерева и вычисляется наименьшая стоимость маршрута для каждого пункта назначения.

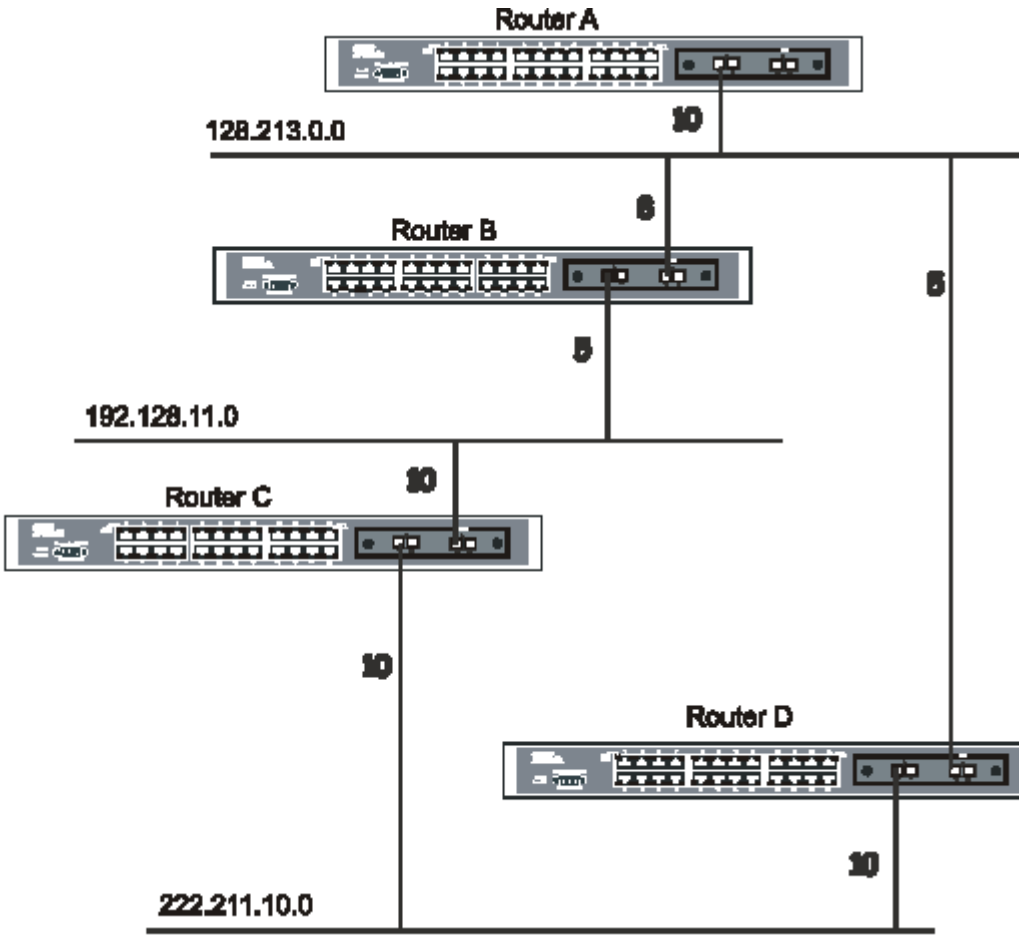


Рисунок 8- 14. Построение дерева кратчайшего пути

Приведенная выше диаграмма показывает сеть, с точки зрения маршрутизатора A. Маршрутизатор A может достигнуть 192.213.11.0 через маршрутизатор B со стоимостью 10+5=15. Маршрутизатор A может достигнуть 222.211.10.0 через маршрутизатор C со стоимостью 10+10=20. Маршрутизатор A может достигнуть 222.211.10.0 через маршрутизатор B и маршрутизатор C со стоимостью 10+5+10=25, но стоимость будет выше, чем для маршрута через маршрутизатор C. Маршруты большей стоимостью не будут включены в дерево кратчайшего пути маршрутизатора A. В результате дерево кратчайшего пути для маршрутизатора A будет выглядеть так:

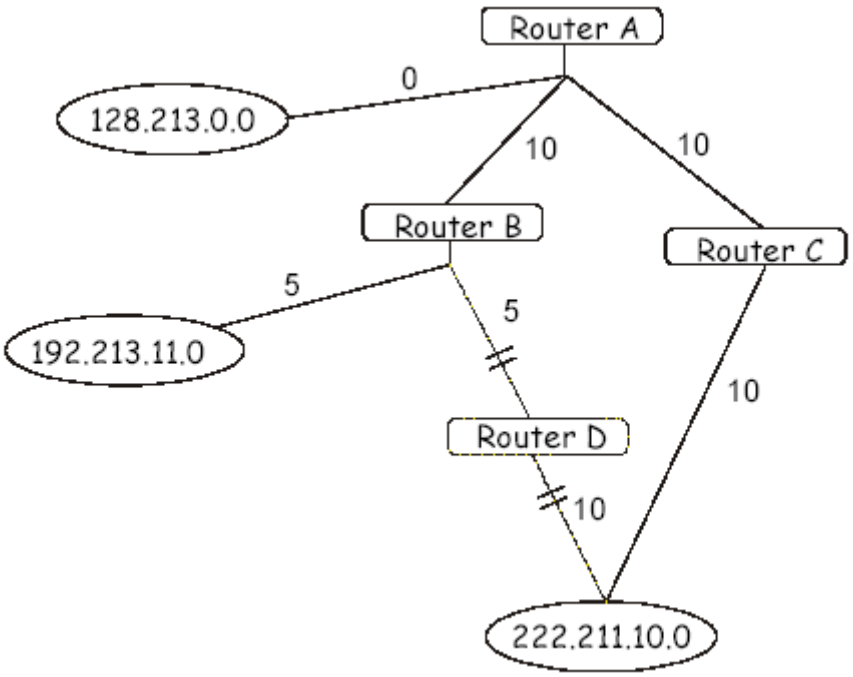


Рисунок 8.15. Построение дерева кратчайшего пути

Заметьте, что данное дерево кратчайшего пути построено только с точки зрения маршрутизатора A. Например, стоимость канала от маршрутизатора B до маршрутизатора A не имеет значения при построении дерева кратчайшего пути для маршрутизатора A, но очень важна, когда маршрутизатор B строит собственное дерево кратчайшего пути.

Отметим также, что стоимость достижения напрямую подключенных сетей составляет 0, в то время как стоимость достижения других сетей вычисляется путем построения дерева кратчайшего пути.
Маршрутизатор A может теперь построить его таблицу маршрутизации, используя сетевые адреса и стоимости, вычисленные выше при построении дерева кратчайшего пути.

Области маршрутизации и пограничные маршрутизаторы

Обновление информации о состоянии каналов пересылается на все маршрутизаторы сети. OSPF применяет концепцию «областей», чтобы определять, где расположены на сети маршрутизаторы, которым необходимо переслать отдельные обновления о состоянии каналов. Это помогает гарантировать, что обновления информации по маршрутизации не будут распространены по всей сети, а также сокращает полосу пропускания для обновления таблиц маршрутизации различных маршрутизаторов.

Маршрутизаторы, которые присоединены к более, чем одной области, называются пограничными маршрутизаторами (Border Routers, BR). Пограничный маршрутизатор должен распределять необходимую информацию маршрутизации и ее изменения между областями.
Области относятся к интерфейсам маршрутизатора. Маршрутизатор, все интерфейсы которого относятся к одной и той же области, называется внутренним маршрутизатором (Internal Router). Маршрутизатор, который имеет интерфейсы во многих областях, называется пограничным маршрутизатором. Маршрутизаторы, которые выполняют роль шлюзов для других сетей (возможно использование других протоколов маршрутизации), называются Autonomous System Border Routers (ASBRs, пограничные маршрутизаторы автономной системы)

Пакеты состояния каналов

Существует определенное количество различных пакетов состояния каналов. Четыре из них представлены ниже:

- Обновления состояния каналов маршрутизатора – здесь описываются каналы маршрутизации до пунктов назначение внутри области;
- Общая информация об обновлении «Link-state» - производится пограничным маршрутизатором и описывает каналы сети за пределами области, но в пределах автономной системы (Autonomous System, AS).
- Обновления состояния каналов сети –производятся областями множественного доступа, которые имеют более, чем один присоединенный маршрутизатор. Один из маршрутизаторов выбирается как отмеченный маршрутизатор (Designated Router), и этот маршрутизатор создает обновления состояния каналов сети, описывая каждый маршрутизатор сегмента.
- Внешние обновления состояния каналов - производятся пограничными маршрутизаторами автономной системы и описывает маршруты, выходящие за пределы автономной системы, или маршрут по умолчанию за пределами автономной системы.

Формат этих обновлений состояния каналов более детально описывается ниже.

Обновления link-state пересылаются всем маршрутизаторам текущей области. Эти обновления описывают пункты назначения, доступные со всех интерфейсов маршрутизатора.

Общая информация об обновлении «Link-state» генерируется пограничными маршрутизаторами для распределения информации маршрутизации между другими сетями автономной системы. Обычно вся общая информация об обновлении состояния канала пересылается на магистраль сети (область 0) и затем пересылается во все другие области сети. Маршрутизаторы также должны распределять информацию маршрутизации из пограничного маршрутизатора автономной системы среди маршрутизаторов сети, чтобы создать и поддерживать маршруты к другим автономным системам.

Обновления состояния каналов сети генерируются маршрутизатором, выбранным в качестве «отмеченного маршрутизатора», на сегменте множественного доступа. (с больше чем одним присоединенным маршрутизатором). Эти обновления описывают все маршрутизаторы сегмента и их сетевые подключения.

Внешние обновления состояния каналов несут информацию маршрутизации в сети, находящиеся за пределами автономной системы.

Пограничный маршрутизатор автономной системы обязан генерировать и распределять эти обновления.

OSPF-аутентификация

OSPF-пакеты могут быть аутентифицированы как пришедшие от высоконадежных маршрутизаторов с использованием предварительно назначенных паролей. По умолчанию маршрутизаторы не используют пароли. Существует также два других метода аутентификации – простая аутентификация паролем (ключем) и аутентификация профилем сообщения (MD-5).

Аутентификация профилем сообщения (MD-5)

Аутентификация MD-5 – это криптографический метод. На каждом маршрутизаторе устанавливается ключ и идентификатор ключа. Затем маршрутизатор, применяя математический алгоритм, генерирует профиль сообщения, который получается из OSPF-пакета, ключа и идентификатора ключа. Этот профиль сообщения (число) затем прикрепляется к пакету. Ключ не передается по проводам и включается число неубывающей последовательности, чтобы предотвратить взлом защиты путем воспроизведения оригинала.

Простая аутентификация паролем

Пароль (или ключ) может быть установлен на основе области. Маршрутизаторы одной области с одним доменом маршрутизации должны быть установлены с одним и тем же ключом. Этот метод может быть уязвим для пассивных атак, когда используется анализатор линий для определения пароля.

Магистральная сеть (Backbone) и Area 0

OSPF ограничивает количество требуемых обновлений состояния канала между маршрутизаторами путем определения областей, с которыми данный маршрутизатор взаимодействует. Когда установлено более одной области, одна из них назначается как область 0, также называемая магистраль сети.
Магистраль сети находится в центре всех остальных областей – все области сети имеют физическое(или виртуальное) соединение с магистралью через маршрутизатор. OSPF позволяет распределять информацию маршрутизации путем ее пересылки в область 0, откуда информация может быть переслана во все другие области (и всем другим маршрутизаторам) на сети.
В ситуациях, когда необходимо организовать области, но невозможно обеспечить физическое соединение с магистралью, может быть установлен виртуальный канал к магистрали.

Виртуальные каналы

Виртуальные каналы служат двум целям:

- Подключение областей, которые не имеют физического соединения с магистралью.
- Временное подключение к магистрали в случае разрыва связи с областью 0.

Области, не присоединенные физически к области 0

Все области OSPF-сети должны иметь физическое соединение с магистралью, но в некоторых случаях невозможно физически присоединить к магистрали удаленную область. В этом случае, устанавливается виртуальный канал для присоединения удаленной области к магистрали сети. Виртуальный маршрут - это логический маршрут между двумя пограничными маршрутизаторами, которые имеют общую область, причем один из пограничных маршрутизаторов присоединен к магистрали.

Разделение магистрали

OSPF позволяет также установить виртуальные каналы между частями магистрали в случае их разрыва. Это эквивалентно объединению двух различных областей 0 при помощи логического пути между каждой областью 0. Также виртуальные каналы могут быть добавлены для резерва, чтобы предотвратить отказы в работе маршрутизатора. Виртуальный канал – канал, организованный между двумя пограничными маршрутизаторами, которые оба имеют соединение с соответствующим областями 0.

Соседние маршрутизаторы

Маршрутизаторы, которые присоединены к одной и той же области или сегменту становятся соседями в этой области. Соседи выбираются с помощью Hello-протокола. Широковещание по IP используется для посылки Hello-пакетов другим маршрутизаторам сегмента. Маршрутизаторы становятся соседними, когда они видят себя, указанными в Hello-пакете другого маршрутизатора, отправленном другим маршрутизатором из того же сегмента.
Чтобы стать соседними, любые два маршрутизатора должны соответствовать следующим условиям:

- **Area ID**(идентификатор области) – Два маршрутизатора, имеющие общий сегмент – их интерфейсы должны принадлежать к одной и той же области в этом сегменте. Конечно, эти интерфейсы должны принадлежать к одной и той же подсети и иметь ту же самую маску подсети.
- **Authentication** (Аутентификация) – OSPF позволяет назначать пароль для отдельной области. Два маршрутизатора, одного и того же сегмента и принадлежащие к одной и той же сети, должны иметь один и тот же OSPF-пароль, прежде чем они станут соседями.
- **Hello и Dead Intervals** – Hello интервал определяет время промежуток времени в секундах между Hello-пакетами, которые посылает маршрутизатор на OSPF-интерфейс. Dead-интервал – это количество секунд, пока при отсутствии hello-пакетов от одного из маршрутизаторов соседние маршрутизаторы объявят данный маршрутизатор неработающим. OSPF-маршрутизаторы обмениваются hello-пакетами в каждом сегменте, чтобы подтвердить друг другу свое наличие в сети и выбрать Designated Router

(отмеченный маршрутизатор) на сегменте множественного доступа. Требование OSPF, чтобы эти интервалы были одинаковы для любых двух соседних маршрутизаторов. Если один из этих интервалов отличается, эти маршрутизаторы не могут стать соседними на отдельном сегменте сети.

- **Stub Area флаг** – Любые два маршрутизатора также должны иметь один и тот же флаг в их hello-пакетах, если они становятся соседними.

Смежности

Смежные маршрутизаторы не ограничиваются обычным обменом hello-пакетами и участием в процессе обменом базой данных состояния канала (LSDB). В OSPF один маршрутизатор выбирается как Designated Router (отмеченный маршрутизатор, DR), а другой маршрутизатор назначается как Backup Designated Router (резервный Designated Router,BDR). Все остальные коммутаторы сегмента будут взаимодействовать с DR для обновления базы данных состояний канала и обмена информацией. Эти ограничения полосы пропускания необходимы для обновления базы данных состояний канала.

Выбор Designated маршрутизатора

Выбор DR и BDR достигается при помощи Hello-протокола. Маршрутизатор с самым высоким OSPF-приоритетом на данном сегменте множественного доступа становится DR для этого сегмента. Если OSPF-приоритеты нескольких маршрутизаторов равны, то DR становится маршрутизатор с наименьшим идентификатором Router ID. По умолчанию значение OSPF-приоритета равно 1. Равный 0 приоритет означает, что маршрутизатор не может быть выбран в качестве DR.

Построение смежностей

Для построения смежных взаимоотношений два маршрутизатора подвергаются многошаговому процессу. Ниже приводится упрощенное описание необходимых шагов:
Down – не возможен прием информации ото всех маршрутизаторов сегмента
Attempt- на нешироковещательной сети множественного доступа (такой как Frame Relay или X.25), это состояние указывает, что давно не поступала информация от соседнего маршрутизатора. Все усилия будут направлены на взаимодействие с соседним маршрутизатором путем путем посылки hello-пакетов для сокращения Poll-интервала.
Init – Интерфейс обнаружил Hello- пакет, пришедший от соседнего маршрутизатора, но двусторонняя связь пока не установлена.
Two-way – двусторонняя связь с соседним маршрутизатором установлена. Маршрутизатор видит свой адрес в hello-пакетах, приходящих от соседнего маршрутизатора. В конце этой ступени будет сделан выбор маршрутизаторов BR и BDR, и маршрутизаторы решат, будут ли они продолжать строить смежности или нет. Решение будет принято в зависимости от того, является ли один из данных маршрутизаторов DR или BDR, а также построен ли канал «точка-точка» или виртуальный канал.
Exstart (начало обмена)- маршрутизаторы устанавливают порядковый номер, которая будет использоваться при обмене пакетами информации. Порядковый номер гарантирует, что информация не будет перепутана, если более поздний пакет придет раньше своего предшественника. При этом один из маршрутизаторов становится первичным, а второй соответственно вторичным. Для получения информации первичный маршрутизатор будет опрашивать вторичный.
Exchange – маршрутизаторы будут описывать базу данных состояния канала путем обмена пакетами описания базы данных.
Loading – маршрутизаторы завершают обмен информацией. Маршрутизаторы имеют лист запроса состояний канала и лист повторной передачи состояний канала. Любая информация, которая покажется неполной или устаревшей, будет размещена в листе запроса. Любые разосланные обновления будут размещены в листе повторной передачи состояний канала, пока не будет получено подтверждение.

Full- Теперь смежность завершена. Соседние коммутаторы полностью смежны. Смежные коммутаторы имеют одинаковую базу данных состояний каналов.

Смежности для интерфейсов «Точка-точка»

OSPF- маршрутизаторы, которые подключаются с использованием интерфесов «точка-точка» (такие как серийный линии), уже имеют смежности. В этом случае в понятиях BR и BDR нет необходимости.

Форматы OSPF-пакетов

OSPF-пакеты всех типов начинаются со стандартного 24-битного заголовка. Выделяют пять типов пакетов. Сначала опишем заголовок, а в последующих разделах все типы пакетов.

Все OSPF-пакеты (кроме hello-пакетов) пересылают уведомления о состоянии каналов. Пакеты обновления состояния каналов рассылаются через OSPF-домен маршрутизации.

- Заголовок OSPF-пакета
- Hello-пакет
- Пакет описания базы данных
- Пакет запроса состояния каналов
- Пакет обновления состояния каналов
- Пакет подтверждения состояния каналов

Заголовок OSPF-пакета

Каждый OSPF-пакет предваряется общим заголовком размером 24 байт. Этот заголовок содержит необходимую информацию, чтобы принимающий маршрутизатор определил принимать ли пакет для дальнейшей обработки.
Формат заголовка OSPF-пакета показан ниже.

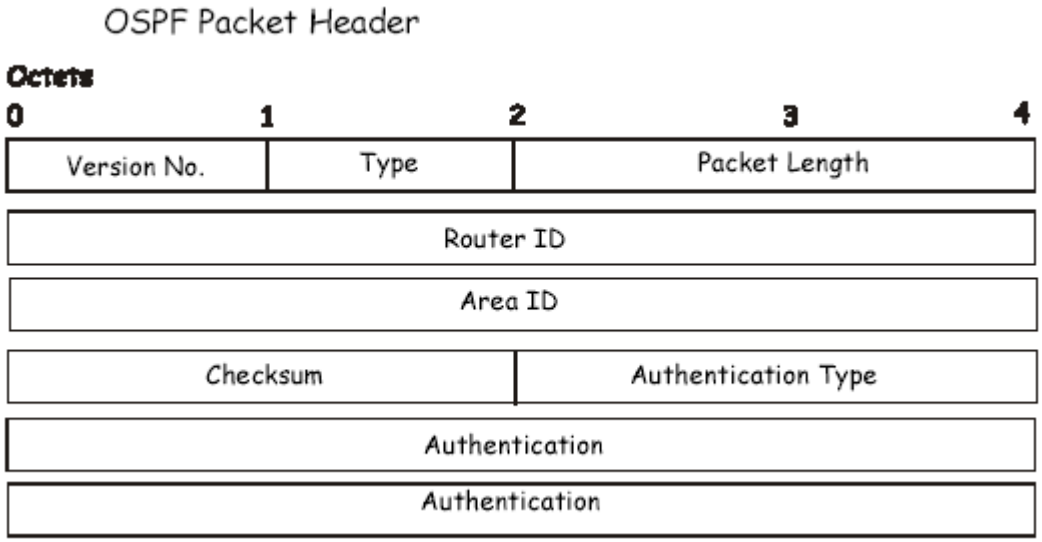


Рисунок 8.17. Формат заголовка OSPF-пакета

Поле	Описание
Version No.	Номер версии OSPF
Type	Тип OSPF-пакета. Возможны следующие варианты: Hello, Database Description (Пакет описания базы данных), Link-State Request (Пакет запроса состояния каналов), Link-State Update (Пакет обновления состояния каналов), Link-State Acknowledgment (Пакет подтверждения состояния каналов)
Packet Length	Длина пакета в байтах, включая длину заголовка(24 байт).

Router ID	Идентификатор маршрутизатора (Router ID), отправившего пакет.
Area ID	32-хбитное число, определяющее область, к которой этот пакет принадлежит. Все OSPF-пакеты сопоставлены с определенной областью. Пакеты, проходящие через виртуальный канал получают идентификатор области магистральной сети 0.0.0.0
Checksum	Стандартная проверочная сумма IP, которая включает всё содержимое пакета, кроме поля 64-битного поля аутентификации.
Authentication Type	Тип применяемой аутентификации
Authentication	64-битное поле, применяемое в схеме аутентификации

Hello-пакет

Hello-пакеты – OSPF-пакеты первого типа. Такие пакеты периодически посылаются на все интерфейсы, включая виртуальные каналы, в порядке установки и поддержки взаимодействия с соседними маршрутизаторами. Добавим, что hello-пакеты широковещательны для физических сетей, поддерживающих широковещание, давая возможность для динамического поиска соседних маршрутизаторов.
Все маршрутизаторы, подключенные к общей сети, должны установить определенные параметры, такие как сетевая маска, Hello-интервал и Dead-интервал маршрутизатора. Эти параметры включены в hello-пакеты, поэтому эти различия могут препятствовать тому, чтобы маршрутизаторы стали соседями.
Формат hello-пакета показан ниже.

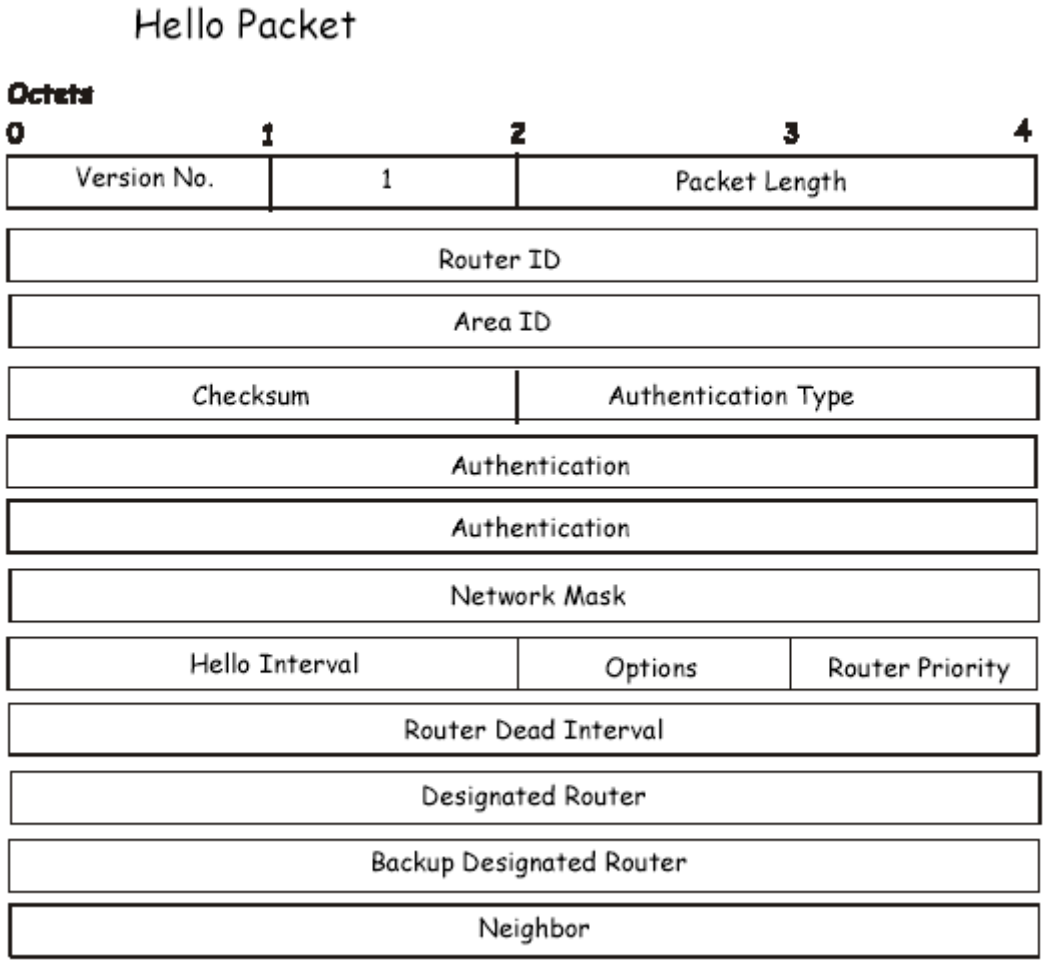


Рисунок 8.18. Hello-пакет

Поле	Описание
Network Mask	Соответствующая данному интерфейсу сетевая маска

Options	Дополнительные возможности, поддерживаемые маршрутизатором
Hello Interval	Количество секунд между hello-пакетами маршрутизатора
Router Priority	Значение Router Priority (приоритет) маршрутизатора
Router Dead Interval	Количество секунд, которое должно пройти, чтобы «замолчавший» маршрутизатор был признан неисправным.
Designated Router	Идентификатор DR для данной сети со стороны извещаемого маршрутизатора. Здесь DR определяется по IP-адресу интерфейса на сети.
Backup Designated Router	Идентификатор BDR для данной сети. Здесь BDR определяется по IP-адресу интерфейса на сети. Значение этого поля устанавливается как 0.0.0.0, если BDR отсутствует.
Field	Описание
Neighbor	Идентификаторы маршрутизаторов, от которых должны приходить действительные hello-пакеты до истечения Dead-интервала маршрутизатора.

Пакет описания базы данных

Пакеты описания базы данных - OSPF-пакеты второго типа. Маршрутизаторы обмениваются этими пакетами, когда начинается процесс установления смежности. Эти пакеты описывают содержимое топологической базы данных. Может понадобиться много пакетов, чтобы описать базу данных.
Для этих целей существует процедура запроса-ответа. Один из маршрутизатором назначается ведущим, а другой - ведомым. Ведущий маршрутизатор посылает пакеты описания базы данных (запросы), которые подтверждаются ведомым маршрутизатором при помощи пакетов описания базы данных(ответы). Ответы связаны с запросами через порядковые номера пакетов описания базы данных (DD sequence numbers).

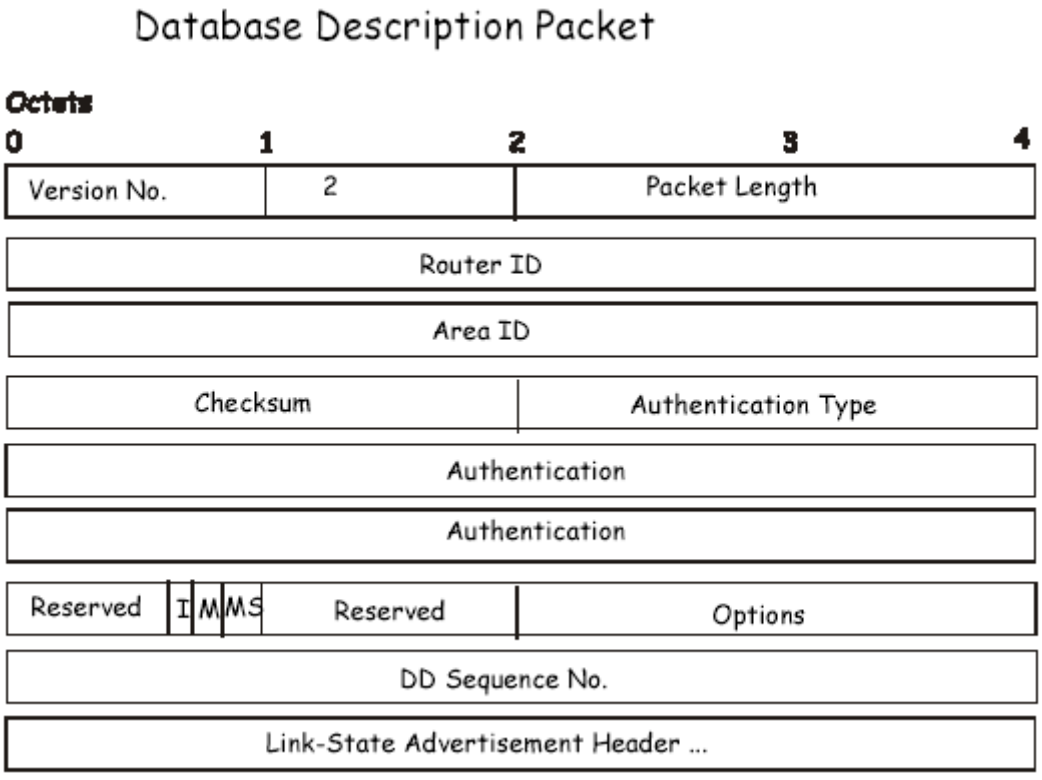


Рисунок 8.19. Пакет описания базы данных

Поле	Описание
Options	Дополнительные возможности, поддерживаемые маршрутизатором.
I-bit	Initial-бит. Когда этот параметр равен 1, то данный пакет является первым в последовательности пакетов описания базы данных.
M-bit	More-бит. Когда этот параметр установлен в 1, то это означает , что будет передано больше пакетов описания базы данных.
MS-bit	Master-Slave- бит. Когда это параметр равен 1, это означает, что маршрутизатор является ведущим в процессе обмена базами данных. 0 означает противоположное.
DD Sequence Number	Используется для того, чтобы восстановить порядок следования пакетов описания базы данных. Начало передаваемых пакетов однозначно определяется Initial-бит. Затем значение данного поле увеличивается на 1, пока не будет передана полная база данных.

Оставшаяся часть пакета состоит из записи топологической базы данных. Каждое оповещение о состоянии канала в базе данных описывается его заголовком оповещения о состоянии канала.

Пакет запроса состояния каналов

Пакеты запроса состояния каналов - OSPF-пакеты третьего типа. После обмена пакетами описания базы данных с соседним маршрутизатором, маршрутизатор может обнаружить, что некие части его топологической базы данных устарели. Пакеты запроса состояния каналов применяются для запроса более свежей информации по определенной части базы данных. Может понадобиться использование многих пакетов запроса состояния каналов. Также посылка пакетов запроса состояния каналов является последним шагом при установлении смежности.
Маршрутизатор, посылающий пакет запроса состояния канала, держит в памяти также копию запрашиваемой части базы данных, определяемую порядковым номером, контрольной суммой и длительностью, хотя эти поля не определены в пакете запроса состояния базы данных. Маршрутизатор может получить в ответ и более последние копии.

Формат пакета запроса состояния канала показан ниже.

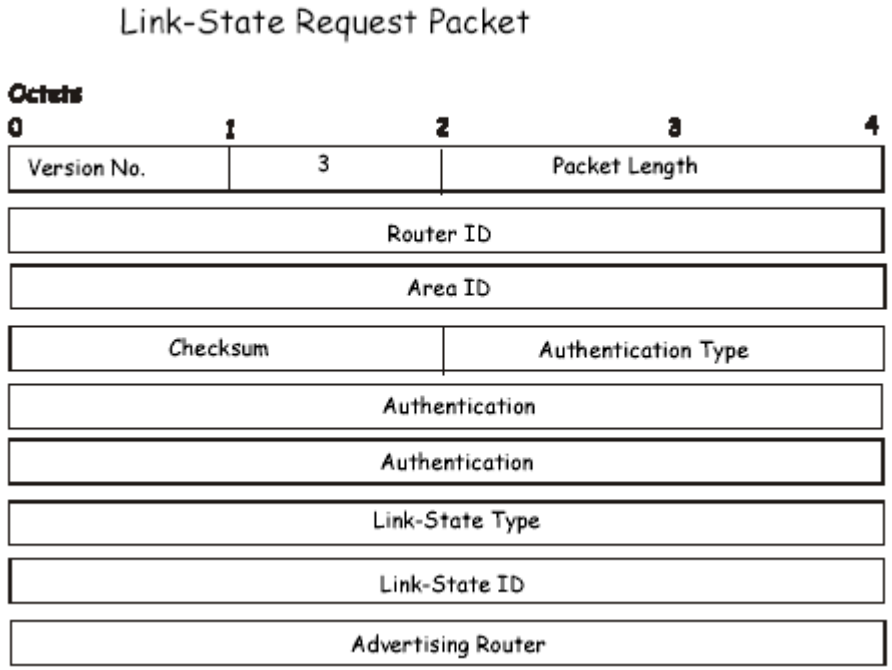


Рисунок 8.20. Пакет запроса состояния каналов

Каждое запрашиваемое оповещение определяет его тип состояния канала, идентификатор состояния канала и оповещаемый маршрутизатор, но не его копию. Пакеты запроса состояний канала пригодны для запросов большинства последних копий.

Пакет обновления состояния каналов

Пакеты запроса состояния каналов - OSPF-пакеты четвертого типа. Эти пакеты обеспечивают широковещательную рассылку объявлений о состоянии канала. Каждый пакет обновления состояний каналов содержит совокупность объявлений о состояний каналов, находящихся на расстоянии одного хопа (Hop) от его источника. Несколько объявлений о состоянии канала могут быть включены в простой пакет.
Пакеты обновления состояния канала широковещательны, поэтому они могут распространяться только на сети, поддерживающей эти функции. Чтобы сделать процедуру широковещательной рассылки надежной, получение объявления о состоянии канала подтверждаются пакетами подтверждения состояния каналов. Если необходима повторная передача определенных объявлений о состоянии каналов, повторно передаваемые объявления всегда передаются односторонними пакетами обновления состояния каналов.
Формат пакета обновления состояния канала показан ниже:

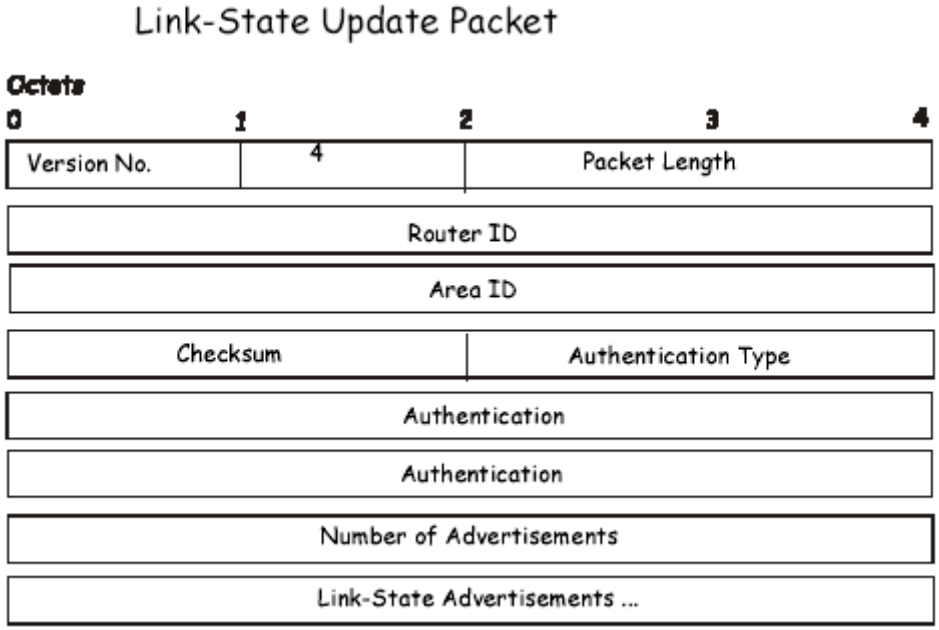


Рисунок 8.21. Пакет обновления состояния каналов

Основная часть пакета обновления состояния каналов состоит из списка объявлений о состоянии каналов. Каждое объявление о состоянии канала начинается с общего 20-битного заголовка объявления о состоянии каналов. В других случаях формат каждого из пяти типов объявлений о состоянии каналов различен.

Пакет подтверждения состояния каналов

Пакеты подтверждения состояния каналов - OSPF-пакеты пятого типа. Чтобы сделать широковещательную рассылку объявлений о состоянии каналов надежной, получение объявления явно подтверждается. Подтверждение завершается путем посылки и получения пакетов подтверждения состояния каналов. Множество полученных объявлений о состоянии каналов могут быть подтверждены при помощи одного пакета.
В зависимости от состояния отправляющего интерфейса и источника объявлений о состоянии канала, пакет подтверждения состояния канала будет послан или на широковещательный адрес AllSPFRouters (все SPF-маршрутизаторы) или на широковещательный адрес AllDRouters (все DR-маршрутизаторы), или же как односторонний (в одном направлении) пакет.
Формат пакета подтверждения состояния канала похож на формат пакета описания базы данных. Тело обоих пакетов – простой список заголовков объявлений о состоянии каналов.
Формат пакета подтверждения состояния каналов показан ниже:

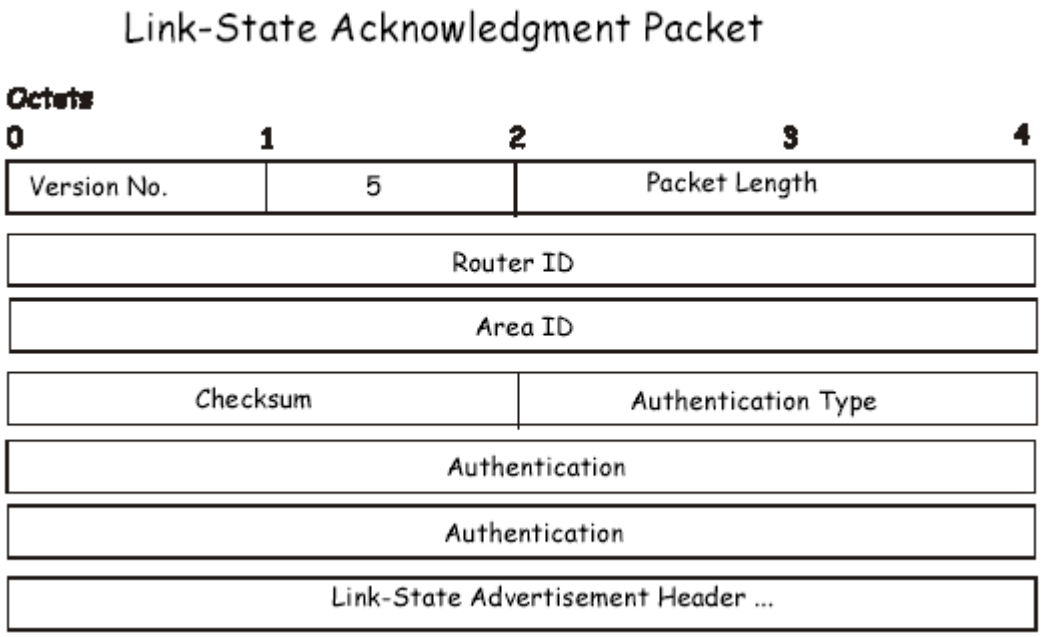


Рисунок 8.22. Пакет подтверждения состояния каналов

Каждое подтверждаемое объявление ос состоянии каналов описывается заголовком объявления о состоянии канала. Он содержит всю информацию, необходимую для идентификации как самого объявления, так и его текущей копии.

Форматы объявлений о состоянии каналов

Существует пять основных типов объявлений о состоянии каналов. Каждое объявление о состоянии канала начинается со стандартного 20-байтного заголовка. В следующих дальше разделах отображаются отдельные типы объявлений о состоянии каналов.
Каждое объявление о состоянии каналов описывает часть OSPF-домена маршрутизации. Каждый маршрутизатор является источником объявлений о состоянии каналов. Кроме того, когда маршрутизатор выбирается как Designated Router, он порождает объявления о состоянии сетевых каналов. Совокупность объявлений о состоянии каналов называется базой данных о состоянии каналов или топологической базой данных.

На основе базы данных состояний каналов каждый маршрутизатор строит дерево кратчайшего пути, корнем которого является он сам. Это приводит к формировании таблицы маршрутизации.

Ниже приведены четыре типа объявлений о состоянии канала, каждое из которых использует общий заголовок о состоянии канала. А именно:

- Объявления о состоянии каналов маршрутизатора
- Объявления о состоянии сетевых каналов
- Объявления о состоянии всех каналов
- Объявления о состоянии каналов автономных систем.

Заголовок объявления о состоянии канала

Вся объявления о состоянии канала начинаются с общего 20-байтного заголовка. Этот заголовок содержит достаточно информации для того, чтобы однозначно идентифицировать объявления (Link State Type, Link State ID, Advertising Router). В одно и то же время на домене маршрутизации могут существовать множество копий объявлений о состоянии канала. Поэтому необходимо определить, какая из копий является самой последней. Это завершается путем проверки полей Link state age, порядковый номер Link state, контрольная сумма Link state, которые также содержатся в заголовке объявления о состоянии канала.
Формат заголовка объявления о состоянии канала показан ниже:

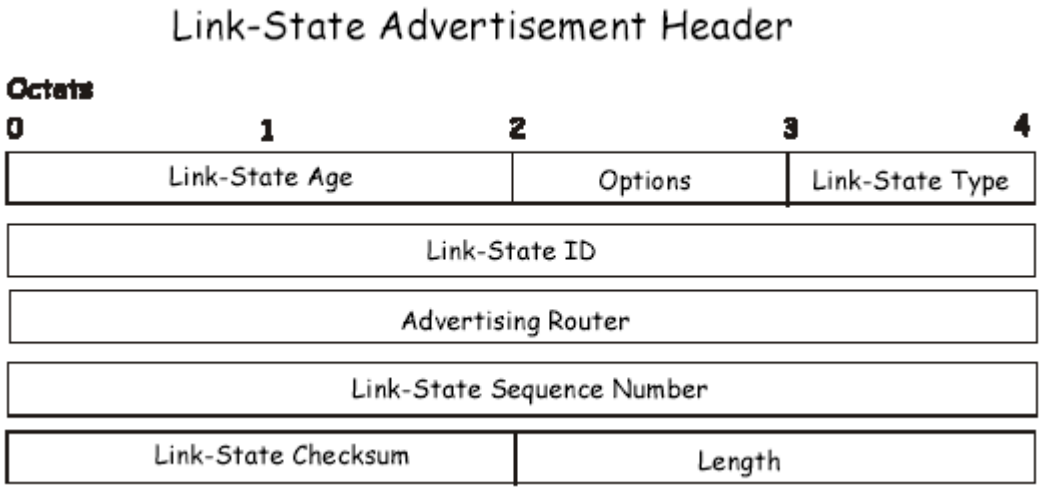


Рисунок 8.23. Заголовок объявления о состоянии каналов

Поле	Описание
Link State Age	Время в секундах с того времени, как было инициировано объявление о состоянии канала
Options	Дополнительные возможности, поддерживаемые описываемой частью домена маршрутизации
Link State Type	Тип объявления о состоянии канала, каждый из которых имеет свой формат. Выделяют следующие типы : Router Links, Network Links, Summary Links (IP Network), Summary Link (ASBR), AS External Links.
Link State ID	Это поле определяет часть Интернет-среды, которая будет описана посредством объявления. Содержимое этого поля зависит от типа объявления о состоянии каналов.
Advertising Router	Идентификатор маршрутизатора (Router ID), который породил объявление о состоянии канала. Например, в объявлениях о состоянии сетевого канала этот параметр принимает значение Router ID сетевого Designated Router.
Link State Secuence Number	Обнаруживает старые или дублирующие объявления о состоянии каналов. Последующие копии объявлений о состоянии канала дают следующий порядковый номер объявления о состоянии канала.
Link State Checksum	Контрольная сумма Флетчера располагается в конце объявления о состоянии канала и включает в себя заголовок объявления, за исключением Link State Age Field.
Length	Длина в байтах объявления о состоянии канала, включая 20-байтный заголовок объявления.

Объявления о состоянии каналов маршрутизатора

Объявления о состоянии каналов маршрутизатора являются первым типом объявлений. Каждый маршрутизатор области порождает объявления о состоянии каналов маршрутизатора. Эти объявления описывают состояние и стоимость каналов маршрутизатора в своей области. Все каналы маршрутизатора в своей области должны описываться в одном объявлении о состоянии каналов маршрутизатора.
Формат объявления о состоянии каналов маршрутизатора показан ниже.

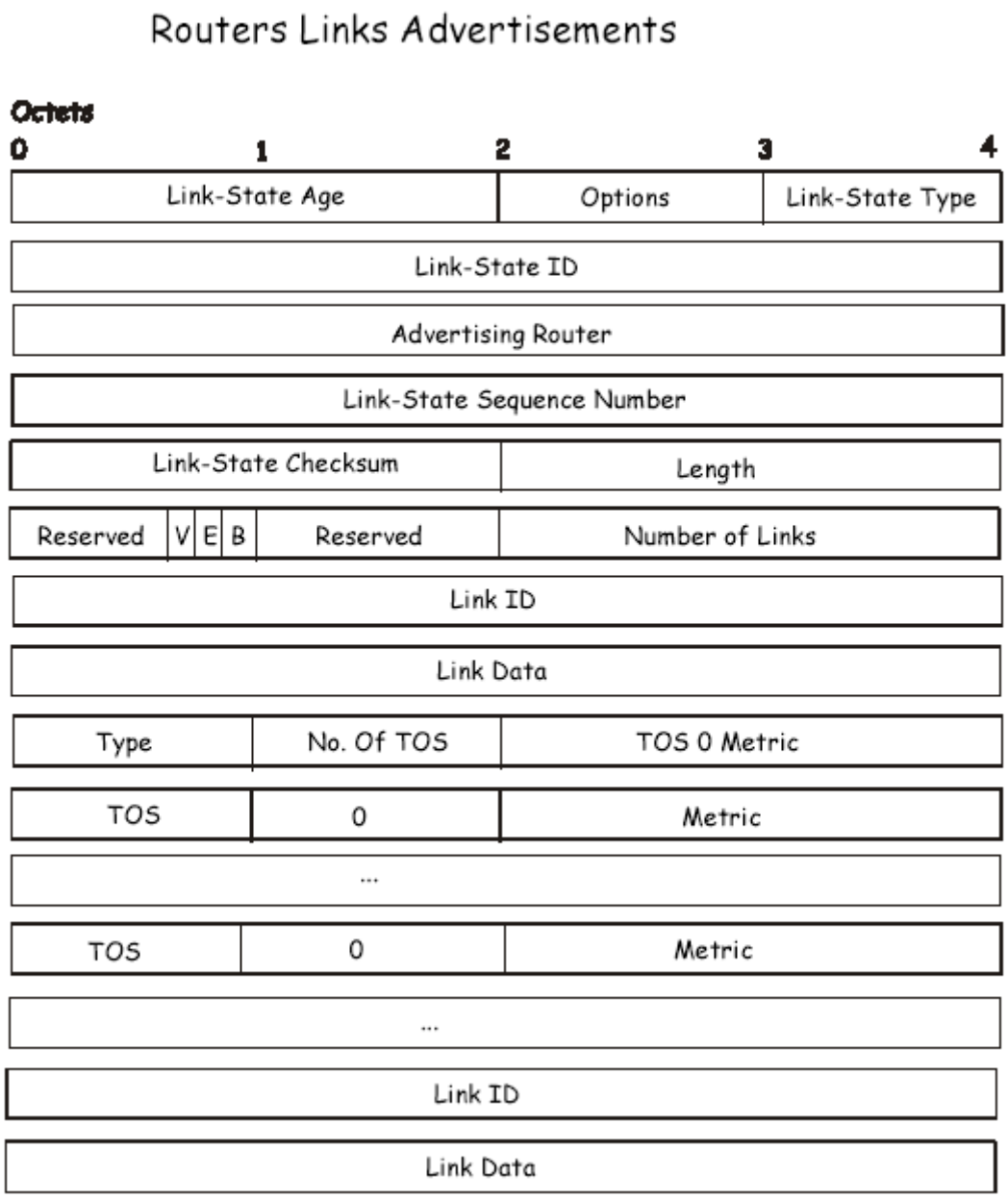


Рисунок 8.24. Объявления о состоянии каналов маршрутизатора

В объявлениях о состоянии каналов маршрутизатора поле идентификатор состояния канала (Link State ID) устанавливается в значение идентификатора OSPF-маршрутизатора. T-бит устанавливается в поле Option тогда и только тогда, когда маршрутизатор способен вычислить отдельно количество маршрутизаторов для каждого IP Type of Service (ToS). Объявления о состоянии каналов маршрутизатора распространяются только по одной области.

Поле	Описание
V-bit	Когда этот бит установлен, маршрутизатор является конечной точкой активного виртуального канала, который использует описываемую область в качестве транзитной области (V – для виртуального канала до конечной точки)
E-bit	Когда этот бит установлен, то маршрутизатор граничит с автономной системой (E – от External (внешний)).
B-bit	Когда этот бит установлен, маршрутизатор является пограничным маршрутизатором в области (B от Border (граница))
Number of Links	Количество каналов маршрутизатора, описываемых данным

	объявлением о состоянии каналов маршрутизатора.

Следующие поля используются для описания каждого канала маршрутизатора. Каждый канал маршрутизатора относится к определенному типу. Поле Type определяет тип описываемого канала. Это может быть канал к транзитной сети, к другому маршрутизатору или к тупиковой (stub) сети. Значения всех других полей, описывающих каналы маршрутизатора, зависит от типа канала. Например, каждый канал имеет соответствующее 32-битное поле данных. И для каналов к тупиковым сетям это поле определяется по маске IP-адреса сети. Для других же типов канала поле Link Data(данные канала) определяется по соответствующему IP-адресу интерфейса.

Поле	Описание
Type	Быстрая классификация каналов маршрутизатора. Возможны следующие варианты: соединение «точка-точка» с другим маршрутизатором, соединение с транзитной сетью, соединение с тупиковой сетью, виртуальный канал.
Link ID	Определяет объект, к которому подсоединяется данный канал маршрутизатора. Значение зависит от типа канала. Когда идет соединение с объектом, который также является источником объявлений о состоянии канала (например, с другим маршрутизатором или транзитной сетью), идентификатор канала Link ID равен Link State ID (идентификатору состояния канала) объявления о состоянии канала от соседнего маршрутизатора. Это служит ключом для нахождения объявления в базе данных состояния канала. Возможны следующие варианты: Router ID соседнего маршрутизатора, IP –адрес Designated Router. Номер IP-сети/подсети.
Link Data	Содержимое снова зависит от поля Type. Для соединений с тупиковой сетью, здесь указывается маска IP-адреса сети. Для неограниченных соединений «Точка-точка» здесь указывается значение индекса MIB-II. Для других типов канала это поле определяет соответствующий адрес IP-интерфейса маршрутизатора. Это необходимо в процесспостроения таблицы маршрутизации, когда вычисляется IP-адрес следующего хопа.
No. of TOS	Количество метрик различных типов сервиса (Type of Service, TOS), установленных для этого канала, не считая обязательной метрики для TOS 0. Если никакие дополнительные метрики TOS не назначены, это поле остается равным 0.
TOS 0 Metric	Стоимость использования данного канала маршрутизатора для TOS 0.

Для каждого канала, отдельные метрики могут быть определены для каждого Type of Services (TOS). Метрика для TOS 0 должна также быть включена, что обсуждалось выше. Метрики для остальных TOS описываются ниже. Заметим, что стоимости стальных TOS, значение которых не определено, по умолчанию приравниваются к значению стоимости TOS 0. Метрики должны быть отсортированы по возрастанию расшифрованных значений TOS. Например, метрика для TOS 16 должна всегда следовать за метрикой TOS 8, когда обе определены.

Поле	Описание
TOS	IP-адрес TOS, к которому эта метрика относится.
Metric	Стоимость использования исходящего канала маршрутизатора для для трафика определенного TOS.

Объявления о состоянии сетевых каналов

Объявления о состоянии сетевых каналов являются вторым типом объявлений. Объявления о состоянии сетевых каналов. Такие объявления порождаются каждой транзитной сетью в данной области. Транзитная сеть – это сеть множественного доступа, к которой присоединено более одного маршрутизатора. Designated Router сети является источником объявлений о состоянии сетевых каналов. Объявление описывает все присоединенные к сети маршрутизаторы, включая и Designated Router. Поле Link State ID объявления указывает IP-адрес интерфейса Designated Router.

Расстояние от сети до всех присоединенных к ней маршрутизаторов равно 0 для всех TOS. Поэтому нет необходимости определять поля TOS и Metric в объявлении о состоянии сетевых каналов.
Формат объявления о состоянии сетевых каналов показан ниже:

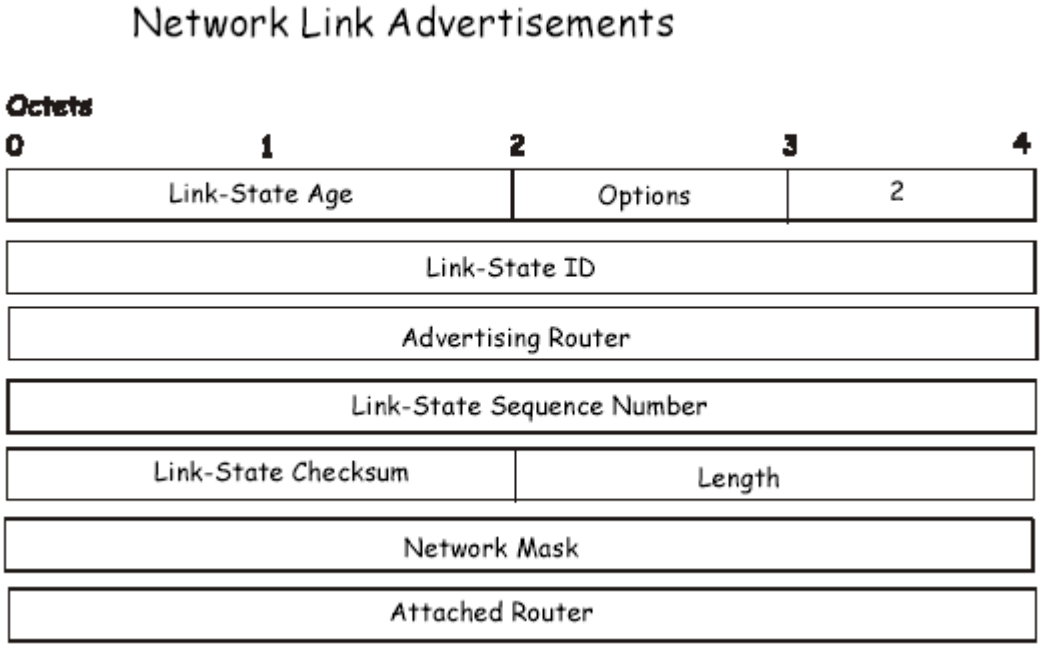


Рисунок 8.25. Объявление о состоянии сетевых каналов

Поле	Описание
Network Mask	Маска IP-адреса сети
Attached Router	Идентификаторы маршрутизаторов, присоединенных к сети. Представлены идентификаторы только тех маршрутизаторов, которые имеют полную смежность с Designated Router, а также сам DR.

Объявления о состоянии всех каналов

Объявления о состоянии всех каналов являются третьим и четвертым типами объявлений. Эти объявления порождаются граничными маршрутизаторами области. Отдельное объявление о состоянии всех каналов создается для каждого известного маршрутизатору направления, принадлежащему автономной системе, лежащей за пределами области.
Тип 3 объявления о состоянии всех каналов используется, когда точка назначения- IP-сеть. В этом случае поле Link State ID является номером IP-сети. Когда точка назначения- граничащий с автономной системой маршрутизатор, применяются объявления четвертого типа, и поле Link State ID приравнивается к идентификатору граничащего с автономной системой OSPF-маршрутизатора. Кроме этих отличий в поле Link-state ID, форматы объявлений о состоянии канала типа 3 и типа 4 идентичны:

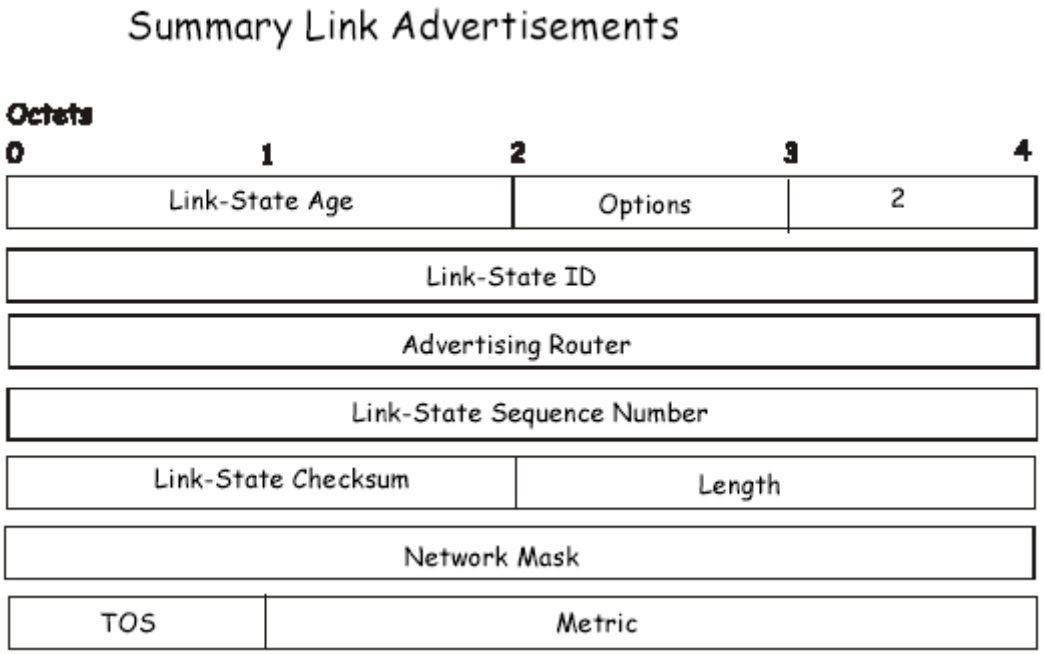


Рисунок 8.26. Объявление о состоянии всех каналов

Для тупиковой области объявление типа 3 могут быть также использованы для описания маршрута по умолчанию на базе области. Маршруты по умолчанию используются в тупиковой области вместо широковещательной рассылки полного количества внешних маршрутов. Когда описывается общий маршрут по умолчанию, Link State ID объявления всегда устанавливается как направление по умолчанию 0.0.0.0, и сетевая маска 0.0.0.0.

Отдельные стоимости могут быть объявлены для каждого IP TOS. Заметьте, что стоимость для TOS 0 должна быть включена и всегда указываться первой. Если T-бит установлен в состояние 0 в поле Option объявления, то только маршрут для TOS 0 описан. В противном случае, маршруты для других значений TOS также назначены. Если стоимость определенного TOS не назначена, его стоимость по умолчанию устанавливается такая же, как для TOS 0.

Поле	Описание
Network Mask	Для объявлений о состоянии канала типа 3 это поле показывает IP-адрес маски сети назначения. Например, если сеть назначения класса A, то значение 0xff000000.
TOS	Type of Service, к которому относится следующая стоимость.
Metric	Стоимость этого маршрута. Выражается в тех же единицах, что и стоимость интерфейса в маршрутизаторе в объявлениях о состоянии канала маршрутизатора.

Объявления о состоянии каналов автономной системы

Объявления о состоянии каналов автономной системы являются объявлениями типа 5.Источником этих объявлений являются граничащие с автономной системой маршрутизаторы. Для каждой известной маршрутизатору точки назначения, которая принадлежит автономной системе, создается отдельное объявление о состоянии канала.

Объявления о состоянии каналов автономной системы обычно описывают отдельное внешнее направление. Для этих объявлений поле Link State ID определяет номер IP-сети. Объявления о состоянии каналов автономной системы также используются для описания маршрута по умолчанию. Маршруты по умолчанию используются, когда не назначен специальный маршрут в данном направлении. При описании маршрута по умолчанию, поле Link State ID также

устанавливается в значение адреса по умолчанию – 0.0.0.0, маска сети также устанавливается в значение 0.0.0.0.

Формат объявления о состоянии каналов автономной системы имеет формат, как показано ниже:

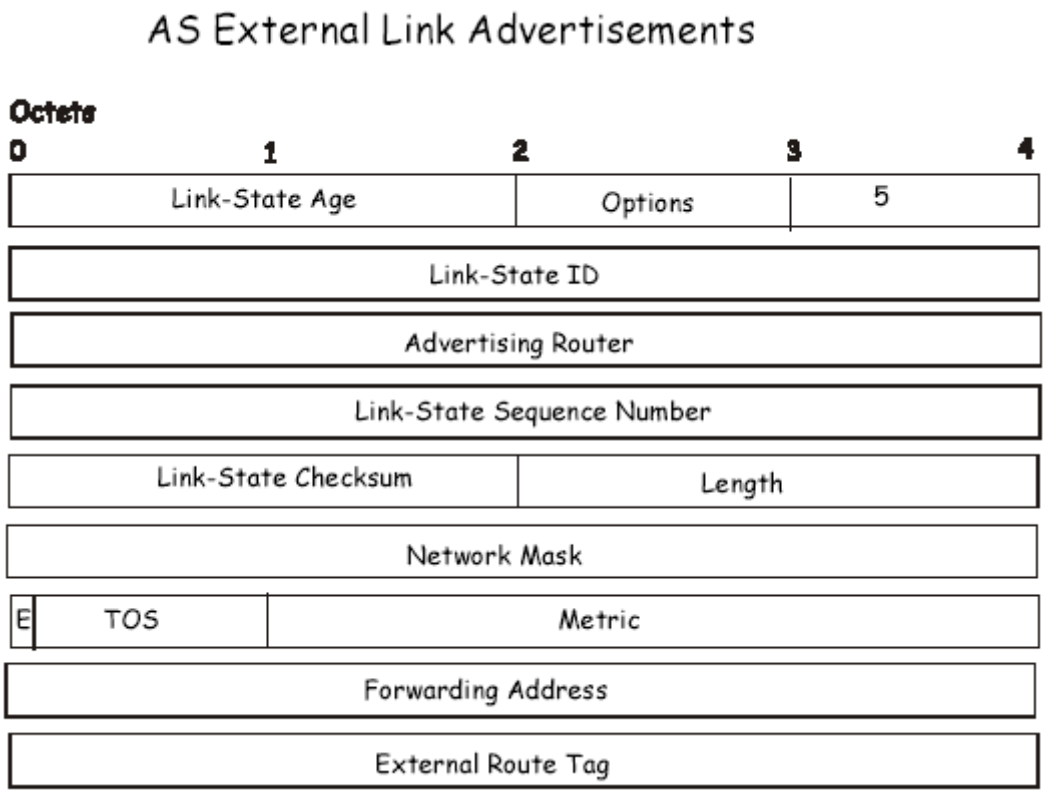


Рисунок 8.27. Объявление о состоянии каналов автономной системы

Поле	Описание
Network Mask	Маска IP-адреса для объявляемого направления
E-bit	Тип внешней метрики. Если E-бит установлен, метрика определена как внешняя метрика типа 2. Это означает, что метрика рассматривается больше, чем другой маршрут. Если E-бит равен 0, то это определяет использование внешней метрики типа 1. Это означает, что она сравнивается с метрикой Link-state.
Forwarding Address	Поток данных для объявляемого направления будет пересылаться на этот адрес. Если этот адрес установлен в значение 0.0.0.0, то поток данных будет пересылаться к источнику объявления.
TOS	TOS, к которому относится следующая стоимость.
Metric	Стоимость этого маршрута. Интерпретация этой метрики зависит от значения внешнего типа индикации (см. выше E-бит)
External Route Tag	32-битное поле, назначенное каждому внешнему маршруту. Это поле не используется непосредственно протоколом OSPF.

Глобальные настройки OSPF

Меню **OSPF Global Settings** позволяет пользователю подключать или отключать OSPF на коммутаторе- без изменения конфигурации OSPF на коммутаторе. Нажмите **L3 Features>OSPF>OSPF Global Settings,** чтобы получить следующее окно**.** Для подключения OSPF, сначала добавьте **OSPF Route ID** (смотрите ниже), выберите *Enabled* в выпадающем меню **State** и нажмите кнопку **Apply**.

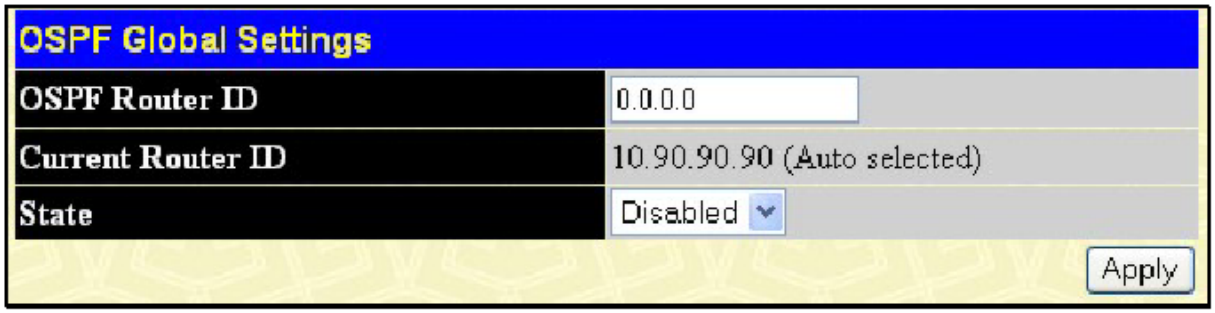


Рисунок 8.28. OSPF Global Settings окно

Для общей установки OSPF применяются следующие параметры:

Поле	Описание
OSPF Route ID	32-битное число (в том же формате, что и IP-адрес xxx.xxx.xxx.xxx), которое однозначно определяет коммутатор в OSPF-домене. Часто назначают самый высокий IP-адрес, назначенный коммутатору(маршрутизатору). В этом случае, это будет 10.53.13.189, но также должен быть уникальное 32-битное число. Если введено 0.0.0.0, самый высокий IP-адрес, назначенный коммутатору, станет OSPF Route ID.
Current Route ID	Отображает идентификатор OSPF Route ID, используемый коммутатором в настоящее время.
State	Позволяет глобально включать/выключать OSPF глобально на коммутаторе без изменения конфигурации OSPF.

Настройка OSPF области(Area)

Это меню позволяет устанавливать идентификаторы OSPF Area и обозначать эти области как **Normal** (нормальная) или **Stub** (тупиковая)**.** Нормальные OSPF области позволяют базе данных о состоянии каналов объявлять о маршрутах в сетях, которые являются внешними по отношению к данной области. Тупиковые области не позволяют базе данных о состоянии каналов объявлять о внешних маршрутах. Тупиковые зоны по умолчанию используют общий внешний маршрут (0.0.0.0 или Область 0) для соединения с внешними точками назначения.

Для установки конфигурации OSPF области нажмите ссылку **Layer 3 Features>OSPF>OSPF Area Settings** для открытия следующего диалогового окна:

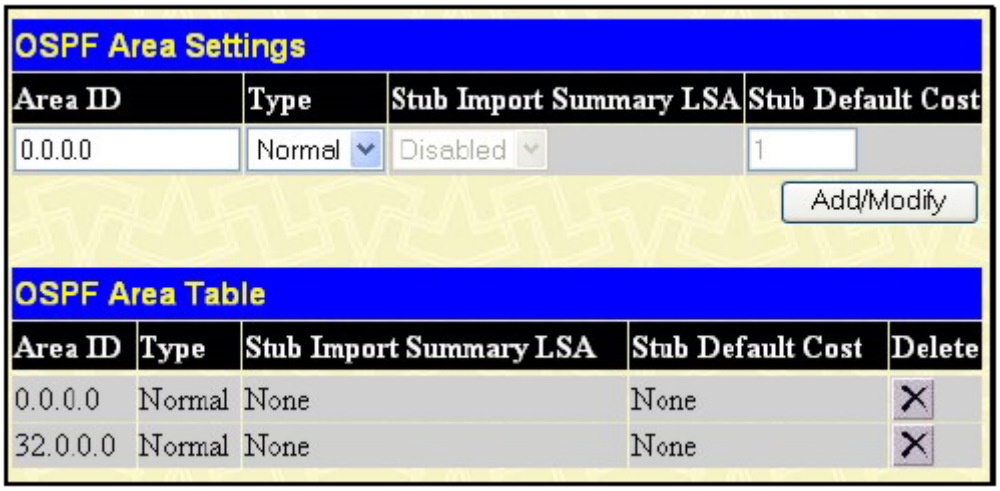


Рисунок 8.29. OSPF Area Settings and Table window

Для добавления OSPF-области в таблицу, впечатайте уникальный идентификатор области (**Area ID**, смотрите ниже) и выберите **Type** в выпадающем меню. Для настройки тупиковой (Stub) области, выберите *Enabled* или *Disabled* из **Stub Import Summary LSA** выпадающего меню и определите **Stub Default Cost**. Нажмите кнопку **Add/Modify** для добавления соответствующего идентификатора области в таблицу.
Для удаления идентификатора области Area ID, нажмите соответствующий значок в колонке **Delete**.

Для изменения существующей записи в списке, впечатайте **Area ID** записи, которую Вы собираетесь отредактировать, введите изменения и нажмите кнопку **Add/Modify.** Измененный идентификатор OSPF Area ID появится в следующей таблице.

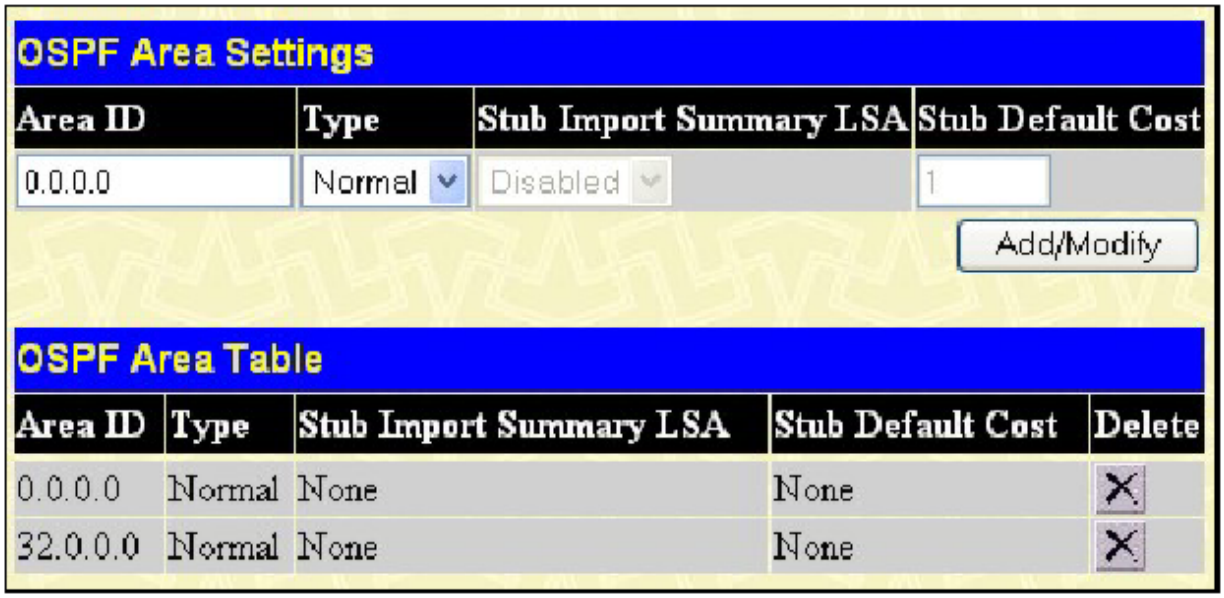


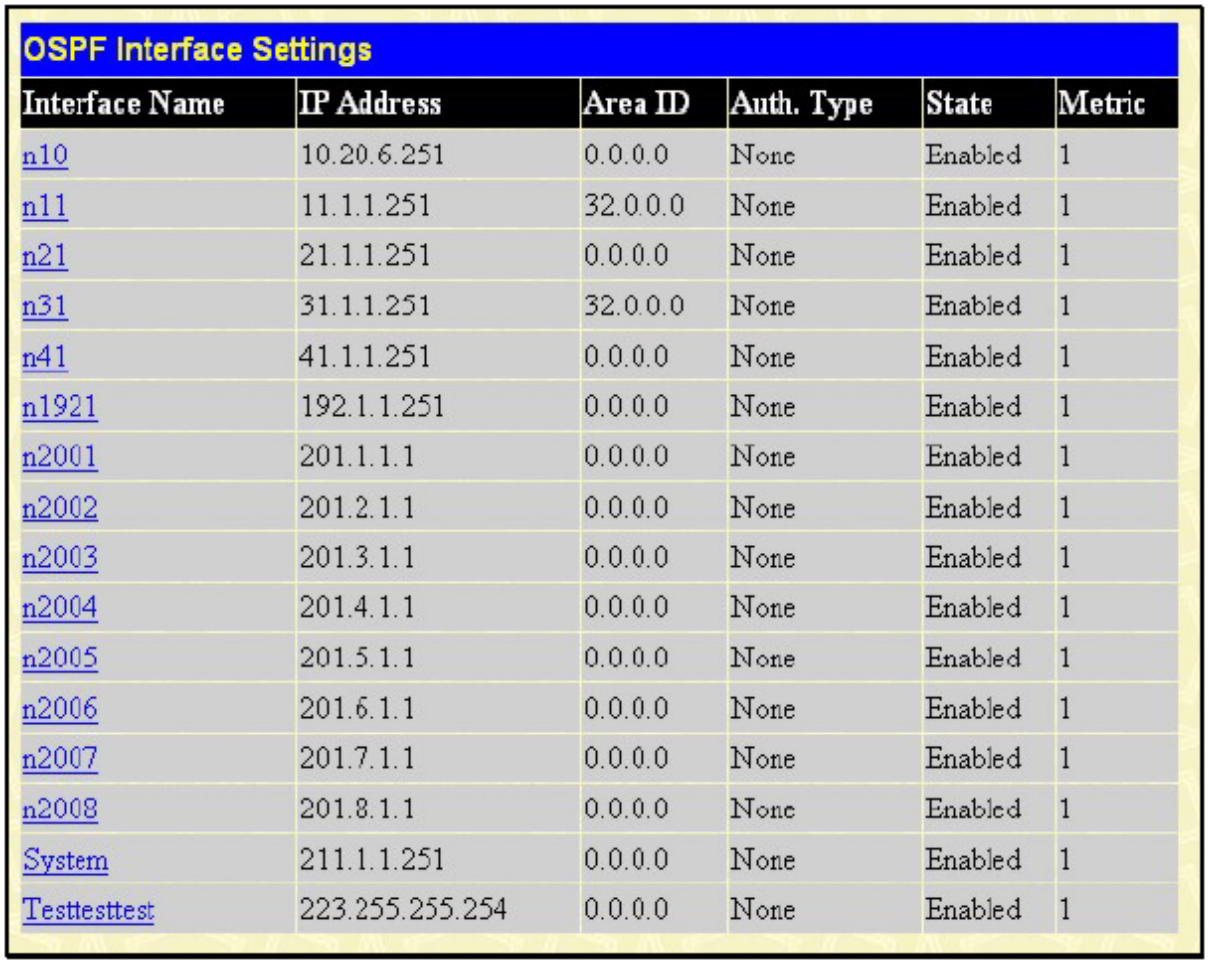
Рисунок 8.30.Пример окна OSPF Area Settings

Ознакомьтесь с описанными ниже параметрами для информации о настройках OSPF Area ID Settings.
Возможны следующие параметры настройки Area ID Settings.

Параметр	Описание
Area ID	32-битное число формата IP-адреса (xxx.xxx.xxx.xxx), которое однозначно определяет область OSPF в OSPF-домене.
Type	Поле может переключаться между Normal(нормальная) и Stub (тупиковая), используя пространственное меню. Когда оно переключено в положение *Stub*, появляются дополнительные поля **Stub Import Summary LSA** и **Stub Default Cost.**
Stub Import Summary LSA	Отображает, будет ли разрешено перемещение объявлений о состоянии всех каналов в другие области.
Stub Default Cost	Отображает стоимость по умолчанию маршрута до тупиковой зоны (0-65535). По умолчанию установлено в значение 1.

Настройки OSPF-интерфейса

Для установки OSPF-интерфейсов нажмите **L3 Features>OSPF>OSPF Interface Settings** для просмотра OSPF настроек для существующих IP-интерфейсов. Если не один IP-интерфейс не был установлен (кроме установленного по умолчанию системного интерфейса), то появится список только настроек системного интерфейса. Для изменения установок для IP-интерфейса, нажмите на гиперссылку имени интерфейса, чтобы увидеть меню настройки для этого интерфейса.



OSPF Interface Settings

Interface Name	IP Address	Area ID	Auth. Type	State	Metric
n10	10.20.6.251	0.0.0.0	None	Enabled	1
n11	11.1.1.251	32.0.0.0	None	Enabled	1
n21	21.1.1.251	0.0.0.0	None	Enabled	1
n31	31.1.1.251	32.0.0.0	None	Enabled	1
n41	41.1.1.251	0.0.0.0	None	Enabled	1
n1921	192.1.1.251	0.0.0.0	None	Enabled	1
n2001	201.1.1.1	0.0.0.0	None	Enabled	1
n2002	201.2.1.1	0.0.0.0	None	Enabled	1
n2003	201.3.1.1	0.0.0.0	None	Enabled	1
n2004	201.4.1.1	0.0.0.0	None	Enabled	1
n2005	201.5.1.1	0.0.0.0	None	Enabled	1
n2006	201.6.1.1	0.0.0.0	None	Enabled	1
n2007	201.7.1.1	0.0.0.0	None	Enabled	1
n2008	201.8.1.1	0.0.0.0	None	Enabled	1
System	211.1.1.251	0.0.0.0	None	Enabled	1
Testtesttest	223.255.255.254	0.0.0.0	None	Enabled	1

Рисунок 8.31. OSPF Interface Settings окно

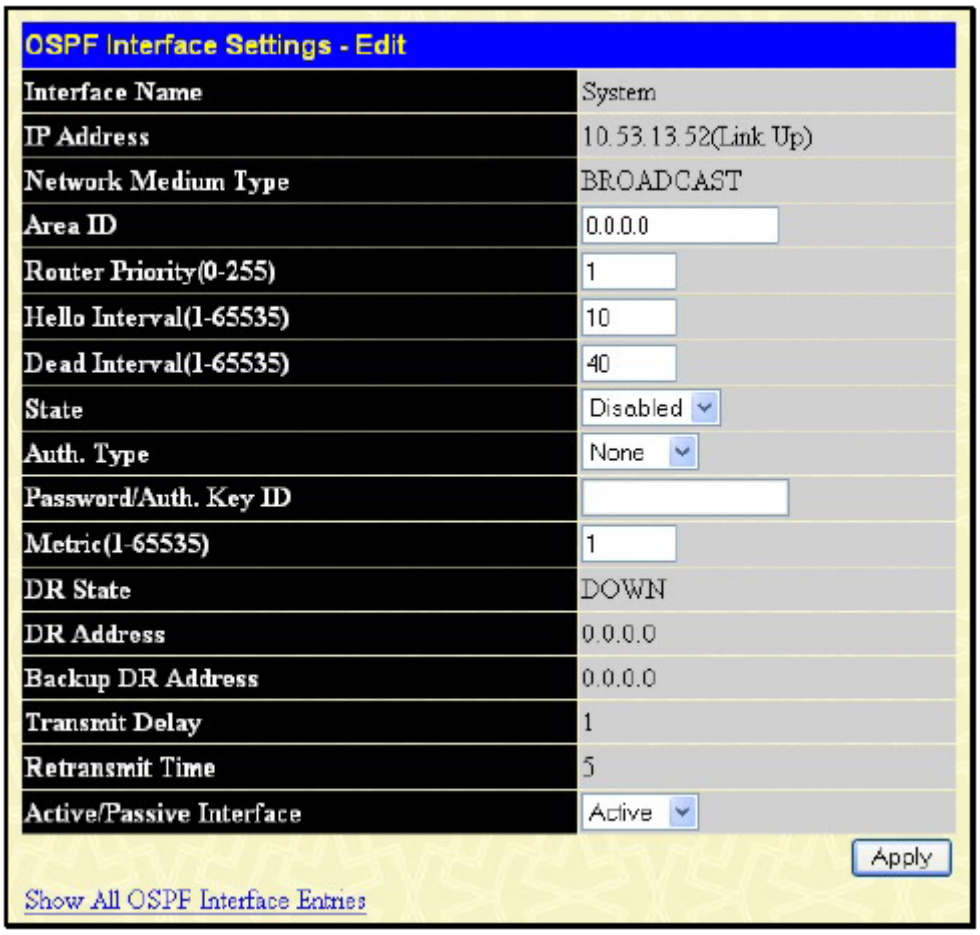


Рисунок 8.32. OSPF Interface Settings - Edit окно

Установите отдельно каждый IP- интерфейс отдельно с помощью меню **OSPF Interface Settings-Edit**. Когда установки введены, нажмите кнопку **Apply**. Новые установки появятся в виде списка в таблице **OSPF Interface Settings**. Для возврата в **OSPF Interface Settings** таблицу, нажмите на ссылку Show All OSPF Interfaces Entries.
Установки OSPF интерфейса описаны ниже. Некоторые настройки OSPF-интерфейса уже упоминались раньше. Их более детальное описание можно найти ниже.

Параметр	Описание
Interface Name	Отображает IP-интерфейс, ранее установленный на коммутаторе
Area ID	Позволяет ввести OSPF Area ID, установленный выше.
Router Priority (0-255)	Позволяет ввести число между 0 и 255, представляющее OSPF-приоритет выбранной области. Если этот параметр равен 0, то коммутатор не может быть выбран в качестве Designated Router на сети.
Hello Interval (1-65535)	Позволяет определить временной интервал между передачами OSPF hello-пакетами в секундах. Принимает значение от 1 до 65535 секунд. Значения **Hello Interval** (hello-интервал), **Dead Interval** (dead-интервал), **Authorization Type** (тип авторизации) и **Authorization Key** (ключ авторизации) должны быть одинаковы для всех маршрутизаторов одной сети.
Dead Interval (1-65535)	Позволяет определить интервал времени между получением hello-пакетов от соседнего маршрутизатора, прежде чем выбранная область признает данный маршрутизатор неработоспособным.
State	Позволяет отключить OSPF-интерфейс для выбранной области без изменения конфигурации для этой области.

Auth Type	Это поле может быть переключено между **None**, **Simple** и **MD5** при помощи пространственного меню. Это позволяет выбрать схемы авторизации для OSPF-пакетов, которыми могут быть обменены через OSPF-домен. • **None**- означает отсутствие авторизации • **Simple** – используется простой пароль, чтобы определить поступил ли пакет от авторизованного маршрутизатора. Когда выбрано Simple, поле **Auth Key** позволяет ввести пароль из 8 знаков, который должен быть точно такой же, как и установленный на соседнем OSPF маршрутизаторе. • **MD5** – использует криптографический ключ, введенный в меню MD5 Key Table Configuration. Когда выбрано значение MD5, поле Auth Key ID позволяет определить Key ID, как определено в установках MD5 выше. Это должен быть тот же самый ключ, что и на соседнем маршрутизаторе.
Password/Auth. Key ID	Введите ключ Key ID длиной до 5 знаков, чтобы установить Auth. Key ID или простую авторизацию по паролю, или авторизацию MD5, как определено в предыдущем параметре.
Metric (1-65535)	Поле позволяет ввести число между 1 и 65535, представляющее собой стоимость OSPF для достижения выбранного OSPF-интерфейса. По умолчанию метрика равна 1.
DR State	Данное поле доступно только для чтения и описывает состояние IP-интерфейса по отношению к Designated Router(DR).Это поле принимает значение **DR** (если это интерфейс Designated Router) или **Backup DR** (если это интерфейс Backup Designated Router). Наибольший IP-адрес будет принадлежать Designated Router, который определяется с помощью OSPF Hello-протокола коммутатора.
DR Address	IP-адрес вышеупомянутого Designated Router.
Backup DR Address	IP-адрес вышеупомянутого Backup Designated Router.
Transmit Delay	Поле, доступное только для чтения, которое приблизительно определяет время передачи пакета обновления состояния канала через этот интерфейс.
Retransmit Time	Поле, доступное только для чтения, которое приблизительно определяет время в секундах между повторными передачами LSA через этот интерфейс.
Active or Passive Interface	Пользователь может выбрать для OSPF-интерфейса состояние **Passive** или **Active**. Активные интерфейсы активно объявляют OSPF для маршрутизаторов на другие локальные сети Intranets, которые не являются частью этой OSPF группы. Пассивные интерфейсы этого делать не могут.

Настройки виртуальных каналов OSPF

Нажмите ссылку **OSPF Virtual Interface Settings**, чтобы посмотреть текущие настройки **OSPF Virtual Interface Settings**. Это не настройки виртуального интерфейса, установленные по умолчанию, поэтому при первом просмотре этой таблицы не будет представлен список интерфейсов. Чтобы добавить новый OSPF виртуальный интерфейс в таблицу, нажмите кнопку **Add.** Появится новое меню (смотри ниже). Для изменения существующей конфигурации нажмите на гиперссылку **Transit Area ID** для записи, которую требуется изменить. Меню для изменения существующей записи такое же, как и меню для добавления новых записи. Для исключения существующей конфигурации, нажмите «x» в колонке **Delete.**

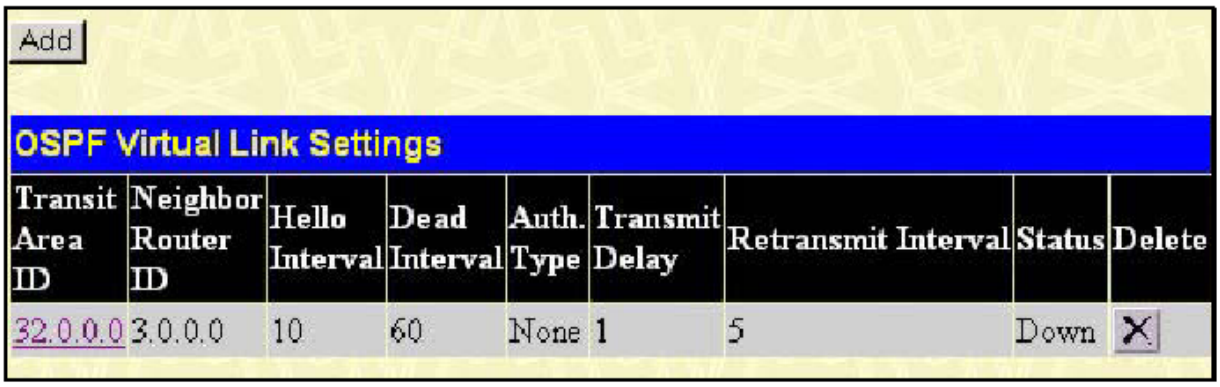


Рисунок 8.33. OSPF Virtual Interface Settings

Статус виртуального интерфейса появляется в колонке **Status**.

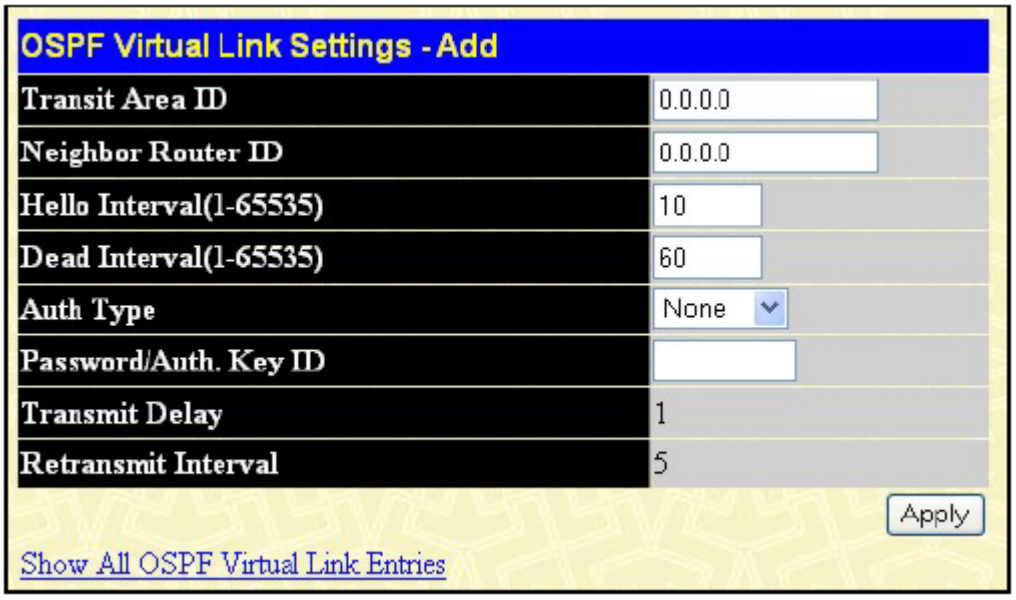


Рисунок 8.34. OSPF Virtual Link Settings – Add

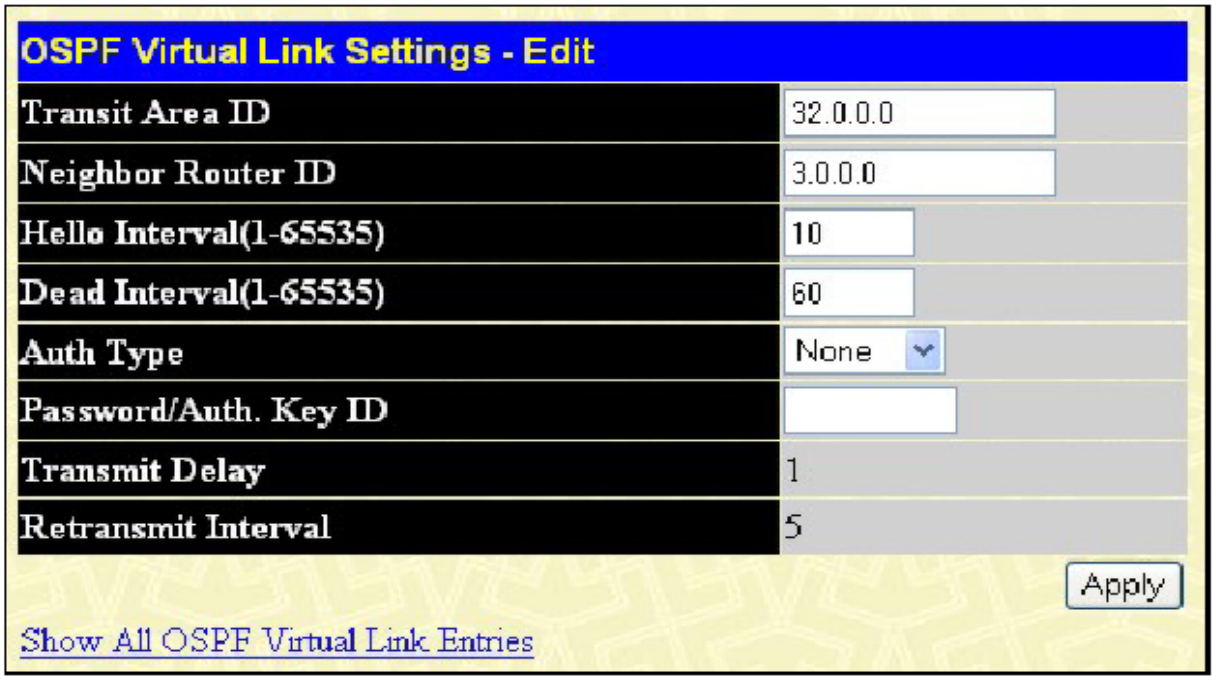


Рисунок 8.35. OSPF Virtual Link Settings - Edit

Настройте следующие параметры, если Вы добавляете или изменяете **OSPF Virtual Interface**

Параметр	Описание
Transit Area ID	Позволяет ввести предварительно установленный OSPF Area ID , который позволяет удаленной области взаимодействовать с магистралью сети (область 0). Транзитная область не может быть тупиковой областью (Stub Area) или областью магистрали сети (Backbone Area).
Neighbor Router	Идентификатор OSPF Router ID для удаленного маршрутизатора. 32-битное число в формате IP-адреса,
Hello Interval (1-65535)	Позволяет определить временной интервал между передачами OSPF hello-пакетами в секундах. Введите значение от 1 до 65535 секунд. Значения **Hello Interval** (hello-интервал), **Dead Interval** (dead-интервал), **Authorization Type** (тип авторизации) и **Authorization Key** (ключ авторизации) должны быть одинаковы для всех маршрутизаторов одной сети.
Dead Interval (1-65535)	Позволяет определить интервал времени между получением hello-пакетов от соседнего маршрутизатора, прежде чем выбранная область признает данный маршрутизатор неработоспособным. Снова оговоримся, что все маршрутизаторы на сети должны иметь одинаковые настройки.
Auth. Type	Если используется авторизация для OSPF-маршрутизаторов, то здесь необходимо выбрать ее тип. MD5 key авторизация должна быть установлена в MD5 Key Settings меню.
Password/Auth. Key ID	Введите пароль с учетом регистра клавиатуры для простой авторизации или введите MD5 Key, который был установлен в MD5 Key Settings меню.
Transmit Delay	Количество секунд, необходимое для передачи обновления состояния канала через данный виртуальный канал. Задержка транзита складывается из задержки передачи и задержки распространения. Это поле фиксированно установлено в 1.
RetransInterval	Количество секунд между повторными передачами объявлений о состоянии каналов для смежностей, принадлежащих к этому виртуальному каналу.

Для применения выполненных настроек нажмите **Apply**.

Примечание: Для корректной работы OSPF некоторые настройки должны быть одинаковы для всех составляющих OSPF устройствах. Речь идет о настройках Hello-интервала и Dead-интервала. Для сетей, использующих авторизацию для OSPF-устройств, кроме того, должны быть одинаковы тип, пароль и ключ авторизации.

Настройки объединения области OSPF (OSPF Area Aggregation Settings)

Объединение области позволяет объединить всю информацию маршрутизации, которая может содержаться в одной области, в общее объявление по сетевому адресу и маске подсети. Это позволяет сократить трафик при передаче объема объявления о состоянии канала, а также сократить объем памяти коммутатора, используемый для поддержания таблиц маршрутизации.
Нажмите **Layer 3 Features> OSPF>OSPF Area Aggregation Settings,** чтобы увидеть текущие настройки. Настройки объединения области не настроены по умолчанию, поэтому при первом обращении к меню никакие настройки Вы не увидите. Для добавления новых настроек **Area Aggregation Settings**, нажмите на кнопку **Add**. Появится новое меню, показанное ниже. Для изменения существующей конфигурации, нажмите на гиперссылку Area ID для записи, которую Вы хотите изменить. Меню для изменения существующей конфигурации точно такое же, как и меню для добавления новой записи. Для удаления существующей конфигурации, нажмите «x» в колонке **Delete** напротив конфигурации, которую Вы собираетесь удалить.

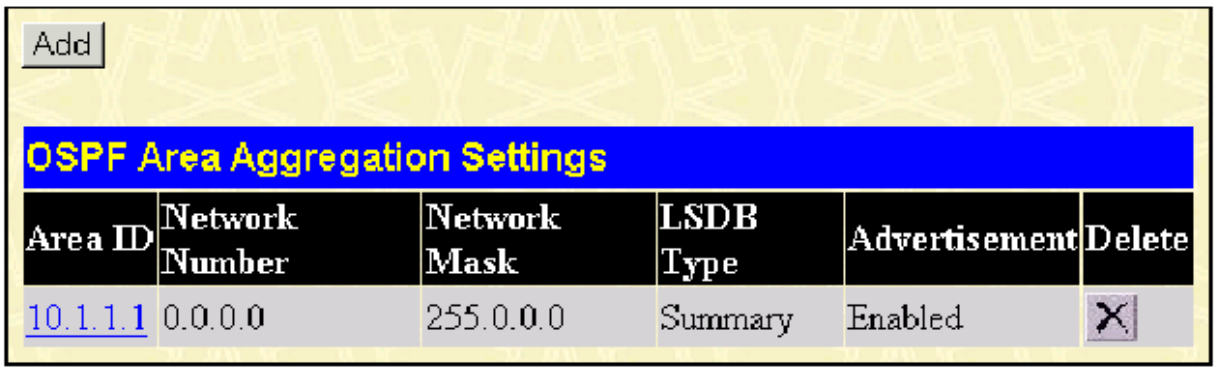


Рисунок 8.36. OSPF Area Aggregation Settings

Воспользуйтесь приводимым ниже меню для изменения настроек или добавления новых **OSPF Area Aggregation Settings.**

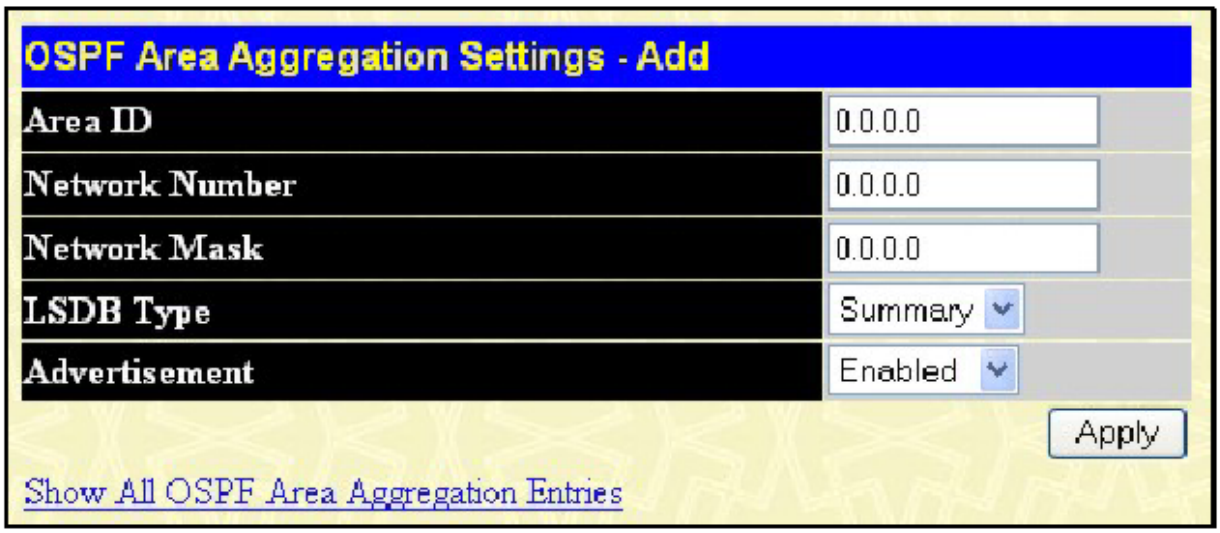


Рисунок 8.37. OSPF Area Aggregation Settings - Add

Определите настройки OSPF Aggregation Settings и нажмите кнопку **Apply** для применения сделанных настроек. Новые настройки появятся в таблице **OSPF Area Aggregation Settings**. Чтобы просмотреть таблицу, нажмите ссылку Show All Aggregation Settings для возврата в предыдущее меню.

Используйте следующие параметры для конфигурирования следующих параметров для **OSPF Area Aggregation Settings**.

Параметр	Описание
Area ID	Позволяет ввести OSPF Area ID, для которого информация маршрутизации. Этот Area ID должен быть предварительно установлен на коммутаторе.
Network Number	Иногда называется сетевой адрес. 32-битное число в форме IP-адреса, которое однозначно определяет сеть, однозначно относящуюся к OSPF Area, указанной выше.
Network Mask	Соответствующая маска подсети для сетевого номера (Network Number), определяемого выше.
LSDB Type	Определяет тип объединения адреса, который установлен как Summary.
Advertisement	Выберите *Enabled* или *Disabled*, чтобы определить будет ли выбранная OSPF область объявлять свою суммарную базу данных о состоянии каналов.

Для применения сделанных настроек нажмите **Apply**.

Настройки главного маршрута OSPF(OSPF Host Route Settings)

Главные маршруты OSPF работают по принципу, аналогичному протоколу RIP, только в данном случае для совместного использования OSPF-информации с другими OSPF-маршрутизаторами. Это используется для работы над проблемами, что должно предотвратить распределение OSPF-информации между маршрутизаторами.

Для установки главных маршрутов нажмите на ссылку **OSPF Host Route Settings.** Для добавления нового OSPF-маршрута, нажмите на кнопку **Add.** Установите соответствующие настройки в появившемся меню. Меню **Add** и **Modify** для настройки главного маршрута OSPF почти идентичны. Различие в том, что если Вы изменяете существующую конфигурацию, то Вы не сможете изменить **Host Address.** Для изменения существующей конфигурации, нажмите на гиперссылку **Host Address** в листе конфигураций, чтобы изменить и продолжить изменение метрики или идентификатора area ID**.** Для удаления существующей конфигурации, нажмите на знак «x» в колонке **Delete** напротив конфигурации, которую требуется удалить.

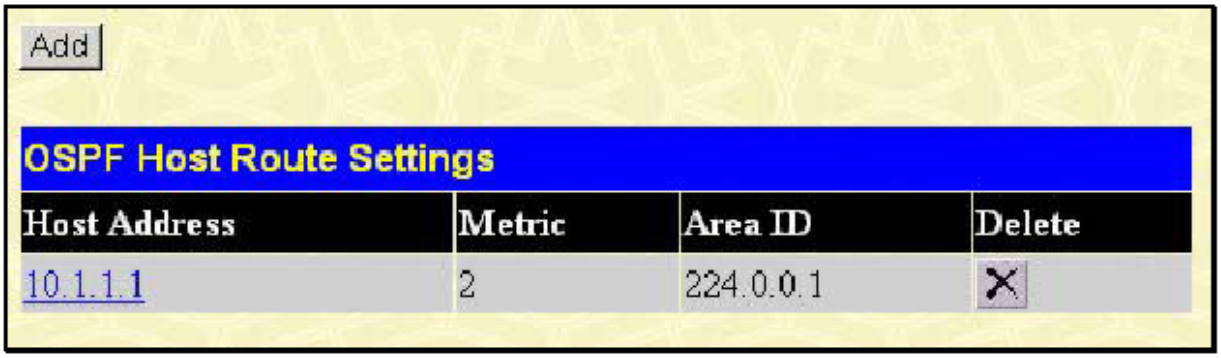


Рисунок 8.38. OSPF Host Route Settings table

Используйте меню ниже для добавления или редактирования OSPF главных маршрутов.

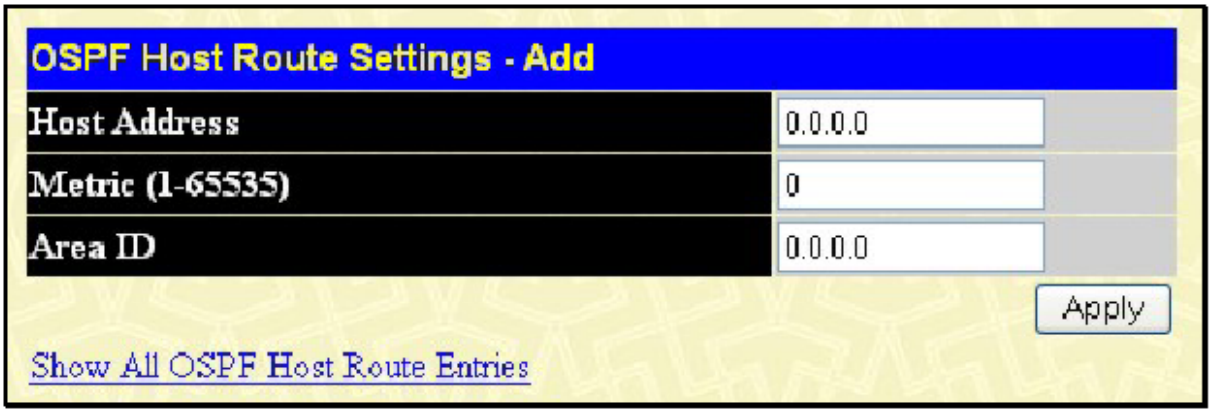


Рисунок 8.39. OSPF Host Route Settings – Add

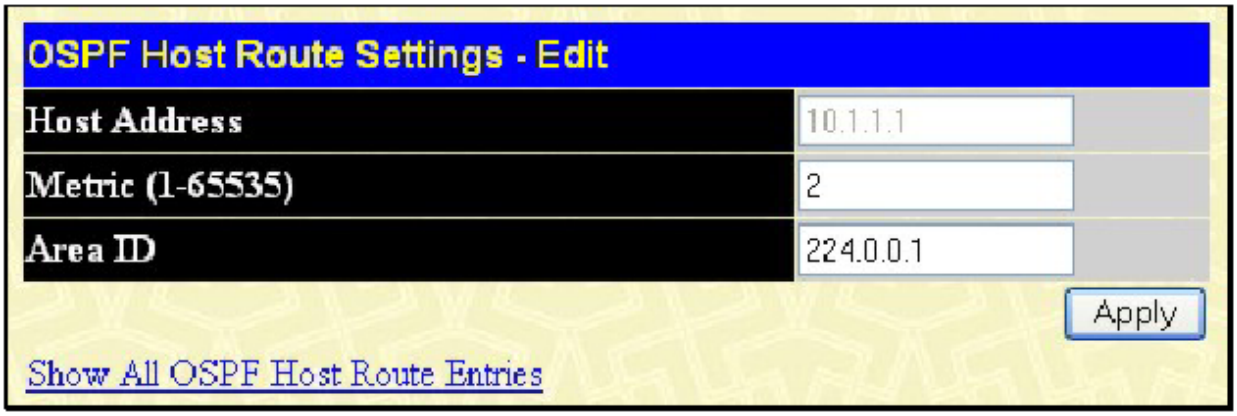


Рисунок 8.40. OSPF Host Route Settings - Edit

Определите настройки главного маршрута и нажмите кнопку **Apply** для добавления или изменения настроек. Новые настройки появятся в виде списка **OSPF Host Route Settings.** Для просмотра предыдущего окна нажмите ссылку Show All OSPF Host Route Entries.
Следующие поля устанавливаются для главного маршрута OSPF главного маршрута.

Параметр	Описание
Host Address	IP-адрес OSPF host
Metric	Значение между 1 и 65535, которое будет объявлено для этого маршрута.
Area ID	32-битное число в форме IP-адреса(xxx.xxx.xxx.xxx), которое однозначно определяет OSPF область в OSPF домене.

DHCP/BOOTP передача

Количество хопов ограничивается допустимым максимальным количеством хопов (маршрутизаторов), через которые нужно пройти для установки соединения. Если счетчик хопов в пакете больше, чем ограничение счетчика хопа, то пакет отбрасывается. Диапазон значений лежит между 1 и 16, а значение по умолчанию составляет 4. Пороговая величина времени передачи устанавливает минимальное время в секундах, которое коммутатор будет выжидать до пересылки BOOTREQUEST пакета. Если значение поля пакета в секундах пакета меньше порогового значения времени передачи, пакет будет отброшен. Значение между 0 и 65536 секундами(по умолчанию 0 секунд).

Глобальные настройки DHCP/BOOTP передачи

Для подключения и настройки **DHCP/BOOTP Relay Global Settings** (Глобальные настройки DHCP/BOOTP передачи) на коммутаторе, нажмите **L3 Features>DHCP/BOOTP Relay> DHCP/BOOTP Relay Global Settings**:

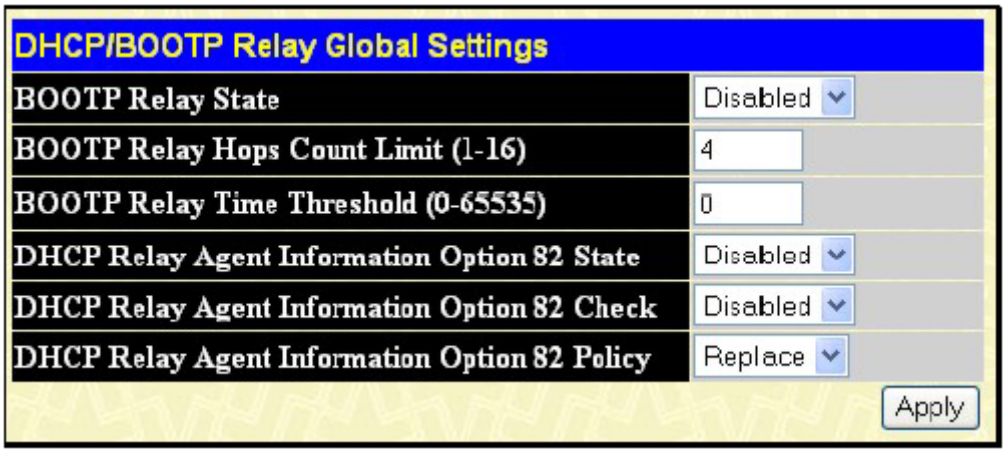


Рисунок 8.41. DHCP/ BOOTP Relay Global Settings окно

Следующие поля могут быть установлены:

Параметр	Описание
Relay State	Это поле может быть переключено между *Enabled* (Подключено) или *Disabled* (Отключено) при помощи выпадающего меню. Используется для подключения или отключения функции DHCP/BOOTP Relay (передача) на коммутаторе. По умолчанию эта функция отключена (*Disabled).*
Relay Hops Count Limit (1-16)	Это поле позволяет ввести значение между 1 и 16 для определения максимального количества хопов маршрутизаторов, через которые могут быть переданы сообщения DHCP/BOOTP. По умолчанию, значение равно 4.

Relay Time Threshold (0-65535)	Позволяет ввести значение между 0 и 65535 секундами и определяет максимальный лимит времени для передачи DHCP/BOOTP пакета. Если введено значение 0, коммутатор не будет применять это значение. В противном случае, коммутатор будет использовать это значение, наряду со счетчиком хопов для определения, стоит ли пересылать данный DHCP или BOOTP пакет.
DHCP Agent Information Option 82 State	Это поле может быть переключено между *Enabled* (Подключено) или *Disabled* (Отключено) при помощи выпадающего меню. Используется для подключения или отключения функции DHCP Agent Information Option 82 на коммутаторе. По умолчанию эта функция отключена (*Disabled).* *Enabled* – Когда поле установлено в значение *Enabled,* агент передачи будет вставлять и удалять информацию DHCP передачи (поле 82 опции) между DHCP серверами и клиентами. Когда агент передачи получает DHCP запрос, он добавляет в пакет информацию 82 опции и IP-адрес агента передачи (если агент передачи сконфигурирован). Поскольку информация 82 опции была добавлена в пакет, то он пересылается на DHCP сервер. При получении сервером DHCP-пакета, если на сервере существуют возможности 82 опции, он может ввести такие политики, как ограничение количества IP-адресов, которые могут быть назначены обычному удаленному идентификатору(remote ID) или идентификатору цепи (circuit ID). Затем DHCP-сервер отображает поле 82 опции в DHCP передачу. DHCP-сервер передает запрос поля 82 опции обратно агенту передачи, если запрос был передан на сервер через агента передачи. Коммутатор проверяет, что данные 82 опции действительно вставлены. Наконец, агент передачи удаляет поле 82 опции и пересылает пакет на порт коммутатора, который подсоединен к DHCP-клиенту, который послал DHCP-запрос. *Disabled* – Когда поле установлено в значение *Disabled,* агент передачи не будет вставлять и удалять информацию по DHCP-передаче (поле 82 опции) в сообщения между DHCP-серверами и клиентами, и настройки проверки и политики не будет эффективно.
DHCP Agent Information Option 82 Check	Это поле может быть переключено между *Enabled* (Подключено) или *Disabled* (Отключено) при помощи выпадающего меню. Это поле используется для подключения или отключения способности коммутатора для проверки достоверности поля 82 опции пакета. *Enabled*– Когда поле установлено в значение *Enabled,* агент передачи будет проверять достоверность опции 82 пакета. Если коммутатор получает пакет, содержащий поле 82 опции от DHCP-клиента, коммутатор отбрасывает этот пакет как недействительный. В пакетах, полученных от DHCP-сервера будут отбрасываться недействительные сообщения. *Disabled* – Когда поле установлено в значение *Disabled,* агент передачи не будет проверять действительность поле опции 82 пакета.
DHCP Agent Information Option 82 Policy	Это поле может быть переключено между *Replace* (Заменить), *Drop* (Отбросить) или *Keep* (Держать) при помощи выпадающего меню. *Replace*- Поле 82 опции будет заменено, если поле 82 опции уже существует в пакете, полученном от DHCP-клиента. *Drop*- Пакет будет отброшен, если поле 82 опции уже существует в пакете, полученном от DHCP-клиента. *Keep*- Поле 82 опции будет удержано, если поле 82 опции уже существует в пакете, полученном от DHCP-клиента.

Нажмите **Apply** для применения сделанных настроек.

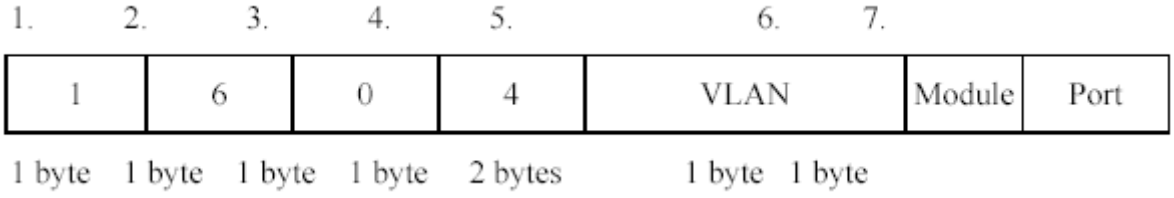
ЗАМЕЧАНИЕ: Если коммутатор получает пакет, который содержит поле 82 опции от DHCP-клиента и на коммутаторе подключена функция проверки информации, то коммутатор отбросит пакет как недостоверный. Однако в некоторых случаях, Вы должны установить клиента с полем 82 опции. В этой ситуации необходимо отключить функцию проверки информации, и тогда коммутатор не будет удалять поле 82 опции из пакета. Вы можете установить действия, которые будет совершать коммутатор при получении пакета с полем 82 опции, путем установки **DHCP Agent Information Option 82 Policy.**

Применение DHCP информации 82 опции в DES-3828P/DES-3828DC

Команда **config dhcp_relay option_82** устанавливает информацию 82 опции DHCP-агента передачи. Форматы для подопций идентификаторов цепи и удаленных идентификаторов следующие:

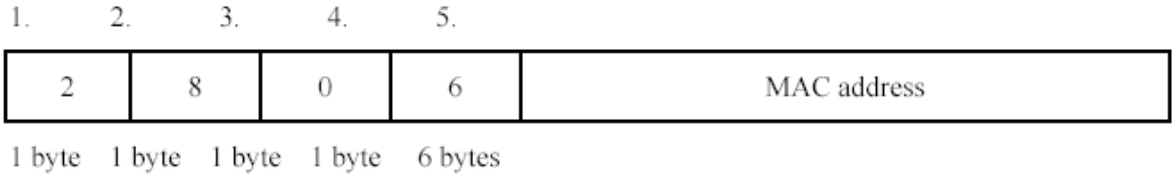
ЗАМЕЧАНИЕ: Для идентификатора цепи подопция автономного коммутатора, поле модуля всегда 0.

Формат подопции идентификатора цепи



a. тип подопции
b. длина
c. тип идентификатора цепи
d. длина
e. VLAN: входящий идентификатор VLAN ID или DHCP пакет клиента
f. Module: для автономного коммутатора всегда значение Module равно 0
g. Port: номер входящего порта для пакетов DHCP-клиента.

Формат подопции удаленного идентификатора:



1. тип подопции
2. Длина
3. Тип удаленного идентификатора
4. Длина
5. MAC address: системный MAC-адрес коммутатора.

Рисунок 8.42. Circuit ID and Remote ID Sub-option Format

Настройки интерфейса передачи DHCP/BOOTP

Настройки **DHCP/BOOTP Relay Interface Settings** позволяют пользователю задать IP-адрес сервера для соответствующей DHCP/BOOTP информации на коммутаторе. Пользователь может ввести ранее установленный IP-интерфейс на коммутаторе, который будет напрямую соединяться с DHCP/BOOTP сервером при помощи следующего окна. Установленные должным образом настройки будут отображаться в таблице **BOOTP Relay Table,** располагаемой в нижней части следующего окна, после того как пользователь нажмет на кнопку **Add** под заголовком **Apply**. Пользователь может добавить до 4-х IP-адресов серверов на каждый IP-интерфейс коммутатора. Записи могут быть удалены путем нажатия соответствующего значка «x». Для подключения и настройки на коммутаторе **DHCP/BOOTP Relay Global Settings** на коммутаторе, нажмите **L3 Features>DHCP/BOOTP Relay> DHCP/BOOTP Relay Global Settings**.

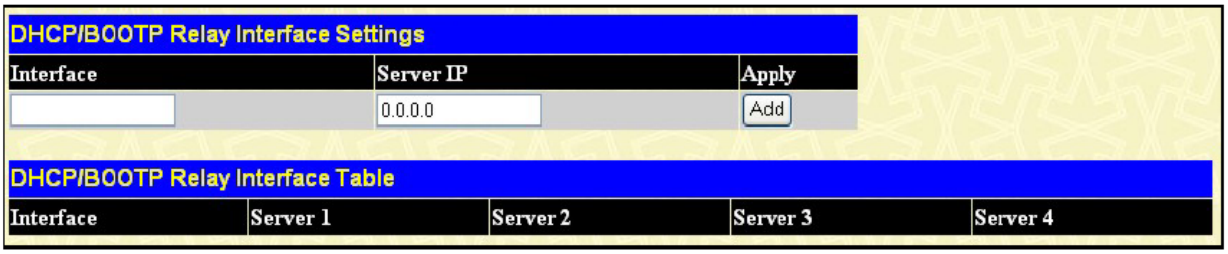


Рисунок 8.43. DHCP/BOOTP Relay Interface Settings and DHCP/BOOTP Relay Interface Table окно

Следующие параметры могут быть установлены и просмотрены:

Параметр	Описание
Interface	IP-интерфейс на коммутаторе, который может быть напрямую подключен к серверу.
Server IP	Введите IP-адрес DHCP/BOOTP сервер. До 4 IP-адресов может быть установлено для IP-интерфейса.

DNS-передача

Компьютерные пользователи предпочитают использовать тестовые имена компьютеров, с которыми они могут захотеть соединиться. Компьютерам же, в свою очередь, необходимы 32-битные IP-адреса. Поэтому необходимо поддерживать базу данных текстовых имен сетевых устройств и соответствующих им IP-адресов.
Domain Name System (DNS) используется для установления соответствия имен и IP-интерфейсов в Интернете, а также была адаптирована для использования в интранет-сетях.
Для связи через различные подсети двух DNS-серверов должна быть использована DNS Relay (DNS передача). DNS-серверы определяются по их IP-адресам.

Соответствие доменных имен адресам

Перевод имени в адрес выполняется программой, называемой Name server. Клиентская программа называется Name resolver. Name resolver может быть необходимо взаимодействовать с несколькими программами Name server для перевода имени в адрес.
DNS-серверы организованы в отчасти иерархическую форму. Обычный сервер часто хранит имена простой сети, которая подключена к маршруту DNS-сервера, обычно определяемого протоколом ISP.

Разрешение доменного имени

DNS может быть использована путем контакта с именами серверов (по одному за раз) или с помощью запроса DNS сделать полную трансляцию адреса. Клиент делает запрос, содержащий имя, тип требуемого ответа и код, указывающий должна ли DNS делать полную трансляцию имени или просто возвратит адрес следующему DNS-серверу, если получивший запрос сервер не может разрешить имя.

Когда DNS-сервер получает запрос, он проверяет, в его ли субдомене находится данное имя. Если да, то сервер переводит имя, добавляет ответ на запрос и отсылает обратно клиенту. Если DNS-сервер не может перевести имя, он определяет, какой тип ответа на имя необходим. Полный перевод называется рекурсивный ответ и требует взаимодействия сервера с другими DNS-серверами до разрешения имени. Итеративный ответ определяет, что если DNS-сервер не может дать ответа, он возвращает адрес следующего DNS-сервера, с которым будет взаимодействовать клиент.
Каждый клиент должен иметь возможность взаимодействовать как минимум с одним DNS-сервером, и каждый DNS-сервер должен иметь возможность взаимодействовать как минимум с одним сервером маршрутизации.
Адрес машины, поддерживающей DNS, обычно принадлежит DHCP или BOOTP серверу, или может быть введен вручную и установлен в автозагрузке операционной системы.

DNS Relay Global Settings (Глобальные настройки DNS-передачи)

Для установки функции DNS на коммутаторе нажмите **L3 Features>DNS Relay>DNS Relay Global Settings,** что откроет окно **DNS Relay Global Settings,** как показано ниже.

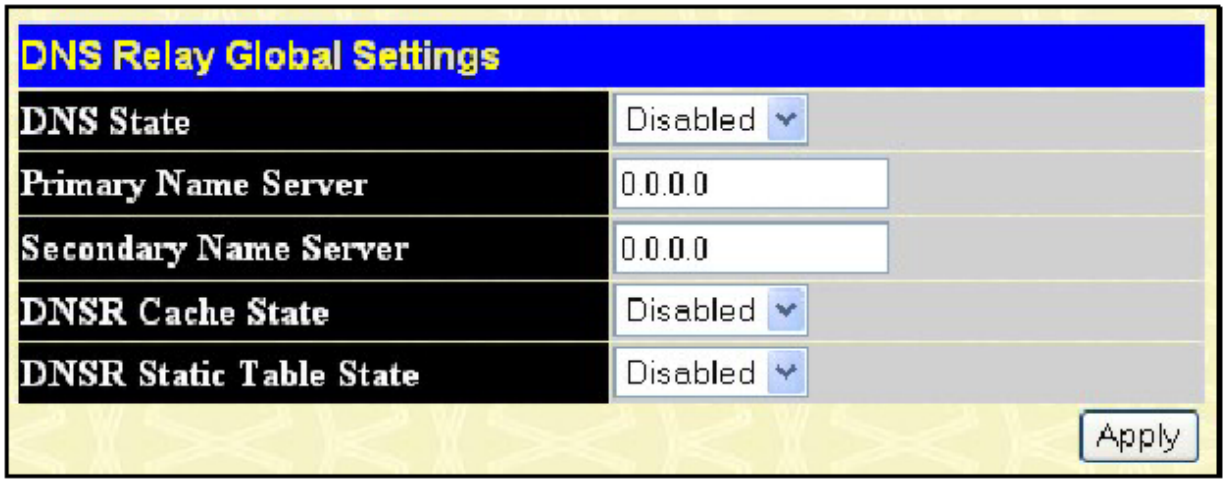


Рисунок 8.44. DNS Relay Global Settings окно

Следующие параметры могут быть установлены:

Параметр	Описание
DNS State	Это поле может быть переключено между *Enabled* (Подключено) или *Disabled* (Отключено) при помощи выпадающего меню и используется для подключения или отключения DNS передачи на коммутаторе.
Primary Name Server	Позволяет ввести IP-адрес первичного сервера доменных имен
Secondary Name Server	Позволяет ввести IP-адрес вторичного сервера доменных имен
DNSR Cache Status	Это поле может быть переключено между *Enabled* (Подключено) или *Disabled* (Отключено). Определяет, будет ли подключен DNS-кэш на коммутаторе.
DNSR Static Table State	Это поле может быть переключено между *Enabled* (Подключено) или *Disabled* (Отключено) при помощи выпадающего меню. Это поле определяет, будет ли использоваться статическая DNS-таблица или нет.

Нажмите **Apply** для применения выполненных настроек.

Настройки статической DNS передачи

Для просмотра **DNS Relay Static Settings**, нажмите **L3 Features>DNS Relay> DNS Relay Static Settings,** в результате откроется окно **DNS Relay Static Settings,** как показано ниже:

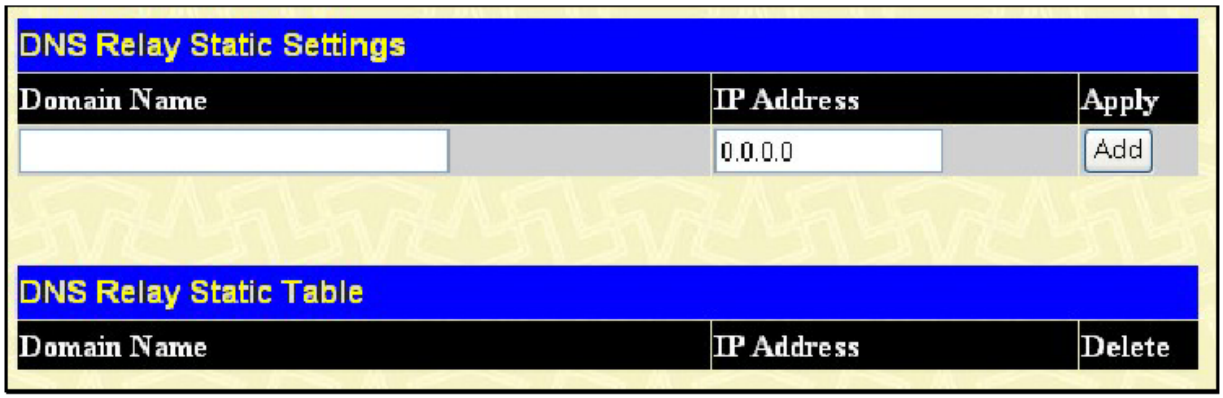


Рисунок 8.45. DNS Relay Static Settings

Для добавления записи в таблицу **DNS Relay Static Table,** просто введите **Domain Name** (Имя домена) с соответствующим IP-адресом и нажмите на **Add** под заголовком **Apply**. Успешный ввод будет отражен в таблице ниже, как показано в примере выше. Для удаления записи из таблицы, нажмите соответствующий знак «x» под заголовком **Delete.**

VRRP

Virtual Routing Redundancy Protocol (VRRP) – функция коммутатора, которая динамически назначает ответственность за виртуальный маршрутизатор на один из VRRP-маршрутизаторов на сети. VRRP-маршрутизатор, который управляет IP-адресом, соответствующему виртуальному маршрутизатору, называется Master и будет пересылать пакеты, посланные на этот адрес. Это будет позволять любому IP-адресу виртуального маршрутизатора на сети LAN быть использованным как первый хоп (маршрутизатор) к конечному узлу. Используя VRRP, администратор может достичь более доступной стоимости пути по умолчанию, без необходимости настройки каждого конечного узла для динамической маршрутизации или протоколов открытой маршрутизации.
Статически установленные маршруты по умолчанию подвержены большому количеству отказов в работе. Протокол VRRP разработан с целью исключить эти сбои путем установки выбора протокола, который назначит ответственного за виртуальный маршрутизатор на один из маршрутизаторов VRRP на сети. Когда произойдет сбой в работе виртуального маршрутизатора, выбранный протокол найдет виртуальный маршрутизатор с самым высоким приоритетом, чтобы назначить его Master-маршрутизатором на LAN. Это позволяет организовать бесперебойный канал, не зависящий от сбоев.
Для установки VRRP для виртуальных маршрутизаторов на коммутаторе, IP-интерфейс должен существовать в системе и быть частью VLAN. IP-интерфейсы VRRP могут быть назначены в каждой VLAN, а следовательно, маршрутизатору. VRRP-маршрутизаторы из одной VRRP-группы должны иметь не противоречащие друг другу настройки конфигурации для этих протоколов для оптимального функционирования.

Глобальные установки VRRP

Для глобального подключения VRRP на коммутаторе, нажмите **L3 Features>VRRP> VRRP Global Settings:**

Рисунок 8.46. VRRP Global Settings окно

В окне выше отображаются следующие поля:

Параметр	Описание
VRRP State	Используя выпадающее меню, подключите или отключите VRRP глобально на коммутаторе. По умолчанию *Disabled* (отключено).
Non-Owner Response PING	Подключение этого параметра позволит виртуальному IP-адресу пинговаться с другого хоста конечных узлов, чтобы определить есть ли соединение. По умолчанию *Disabled* (отключено).

Установки VRRP виртуального маршрутизатора

Для просмотра параметров VRRP –функции на коммутаторе, нажмите **L3 Features>VRRP> VRRP Virtual Router Settings**

Рисунок 8.46. VRRP Global Settings окно

Следующие параметры отображены в окне выше:

Параметр	Описание
VRID/Interface Name	*VRID*- отображает идентификатор виртуального маршрутизатора, установленного пользователем. Это будет однозначно определять VRRP-интерфейс на сети. *Interface Name* – имя IP-интерфейса, которые подключен к VRRP. Эта запись должна быть предварительно установлена в таблице IP-интерфейсов.
Virtual IP Address	IP-адрес виртуального маршрутизатора, установленного на коммутаторе.
Master IP Address	Отображает IP-адрес Master маршрутизатора для функций VRRP.
Virtual Routeк State	Отображает текущее состояние виртуального маршрутизатора на коммутаторе. Возможные состояния включают Initialize, Master, Backup.
State	Отображает VRRP состояние в виде соответствующей VRRP-записи.
Display	Нажмите кнопку «View» для отображения настроек для отдельных VRRP записей.
Delete	Нажмите «x» для удаления этой VRRP-записи.

Нажмите кнопку **Add** для отображения следующего окна и настройки VRRP-интерфейса.

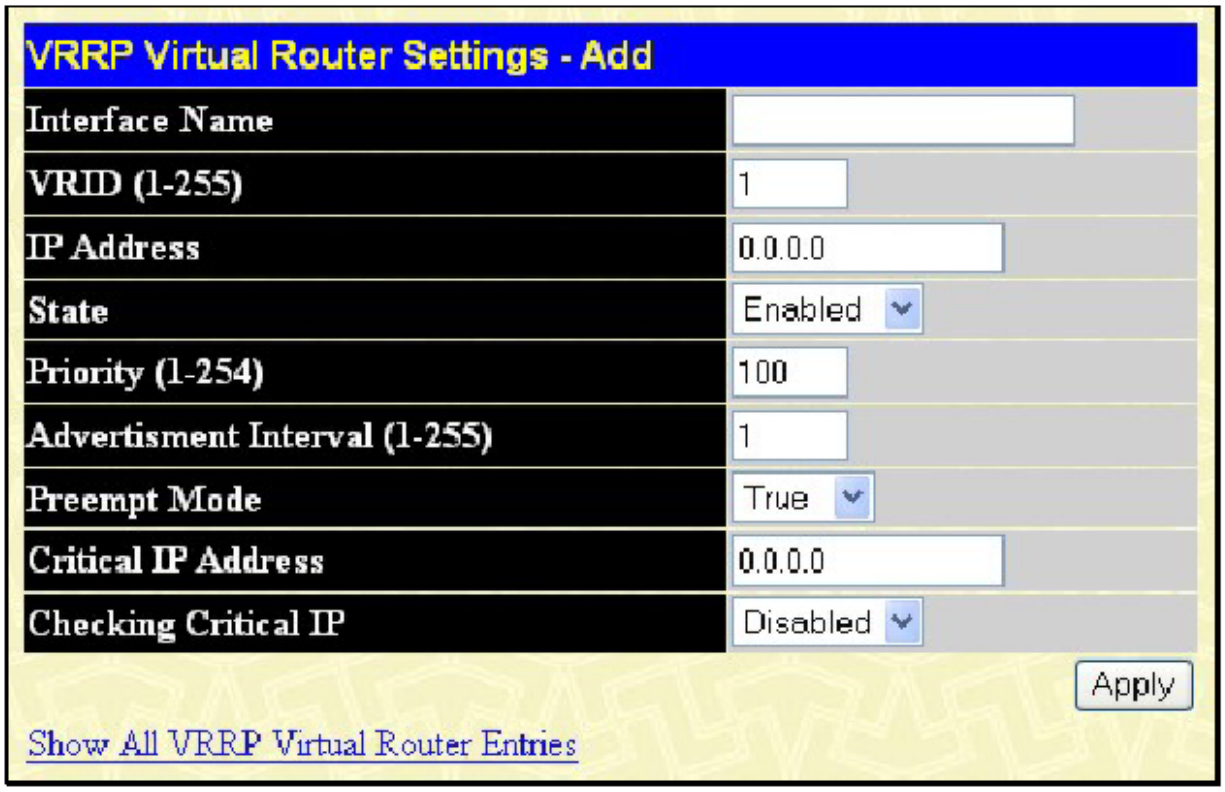


Рисунок 8.48. VRRP Virtual Router Settings - Add

Или пользователь может нажать на гиперссылку Interface Name, чтобы увидеть то же окно.

Следующие параметры могут быть установлены для корректировки существующего или создания нового VRRP-интерфейса:

Параметр	Описание
Interface Name	Введите имя ранее установленного IP-интерфейса, для которого создается VRRP-запись. IP-интерфейс должен быть назначен в VLAN на коммутаторе.
VRID (1-255)	Введите значение между 1 и 255, чтобы однозначно идентифицировать VRRP группу на коммутаторе. Все маршрутизаторы, относящиеся к этой группе, должны иметь одинаковое значение **VRID**. Это значение ДОЛЖНО отличаться по сравнению с другими VRRP-группами, установленными на коммутаторе.
IP Address	Введите IP-адрес, который будет назначен VRRP-маршрутизатору. Этот IP-адрес также является шлюзом по умолчанию, который должен быть статически назначен конечным узлам и должен быть установлен для всех маршрутизаторов, относящихся к этой группе.
State	Используется для подключения и отключения IP-интерфейса VRRP на коммутаторе.
Priority(1-254)	Введите в это поле значение от 1 до 254, чтобы определить приоритет маршрутизатора. Значение VRRP-приоритета можно определить, изменяя более высокие приоритеты VRRP-маршрутизатора на более низкие. Чем выше приоритет, тем больше вероятность, что этот маршрутизатор будет выбран выедущим маршрутизатором группы. Чем ниже приоритет, тем больше вероятность, что данный маршрутизатор станет резервным маршрутизатором. Если VRRP-маршрутизаторы имеют одно и то же значение приоритета, то маршрутизатор, имеющий наивысшее значение IP-адреса, будет назначен ведущим. По умолчанию значение равно 100.(Значение 255 зарезервировано для маршрутизатора, имеющего IP-адрес, соответствующий виртуальному маршрутизатору и поэтому устанавливается автоматически.

Advertisement Interval (1-255)	Введите значение временного интервала в секундах для передачи пакетов VRRP-сообщений. Это значение должно быть согласовано со всеми входящими в группу маршрутизаторами. По умолчанию, значение равно 1.
Preempt Mode	Эта запись будет определять поведение резервных маршрутизаторов из VRRP-группы через контроль, предпочтительней ли более высокий приоритет резервного маршрутизатора более низкому приоритету ведущего маршрутизатора. При установке значения *True* если значение приоритета резервного маршрутизатора больше, чем значение приоритета ведущего маршрутизатора, то резервный маршрутизатор становится ведущим маршрутизатором. Значение *Disable* будет отключать возможность резервного маршрутизатора стать ведущим маршрутизатором. Эта настройка должна быть согласована со всеми маршрутизаторами, входящими в VRRP-группу. По умолчанию, значение *True*.
Critical IP Address	Введите IP-адрес физического устройства, которое будет обеспечивать наиболее прямой маршрут в Internet или другую значимую сеть, соединенную с данным виртуальным маршрутизатором. Это должен быть реальный IP-адрес реального устройства на сети. Если соединение от виртуального маршрутизатора с этим IP-адресом не срабатывает, виртуальный маршрутизатор будет автоматически отключен. Новый ведущий маршрутизатор будет выбран среди резервных маршрутизаторов, относящихся к VRRP-группе. Различные важные IP-адреса могут быть назначены различным маршрутизаторам, относящимся к VRRP-группе, и поэтому могут устанавливать множество маршрутов в Internet или другие важные сетевые соединения.
Checking Critical IP	Используя выпадающее меню, подключите или отключите **Critical IP Address,** введенный выше.

Нажмите **Apply** для вступления в силу сделанных изменений.

Для просмотра настроек для отдельной VRRP, нажмите соответствующую кнопку «View» в **VRRP Interface Table,** после чего будет отображено следующее:

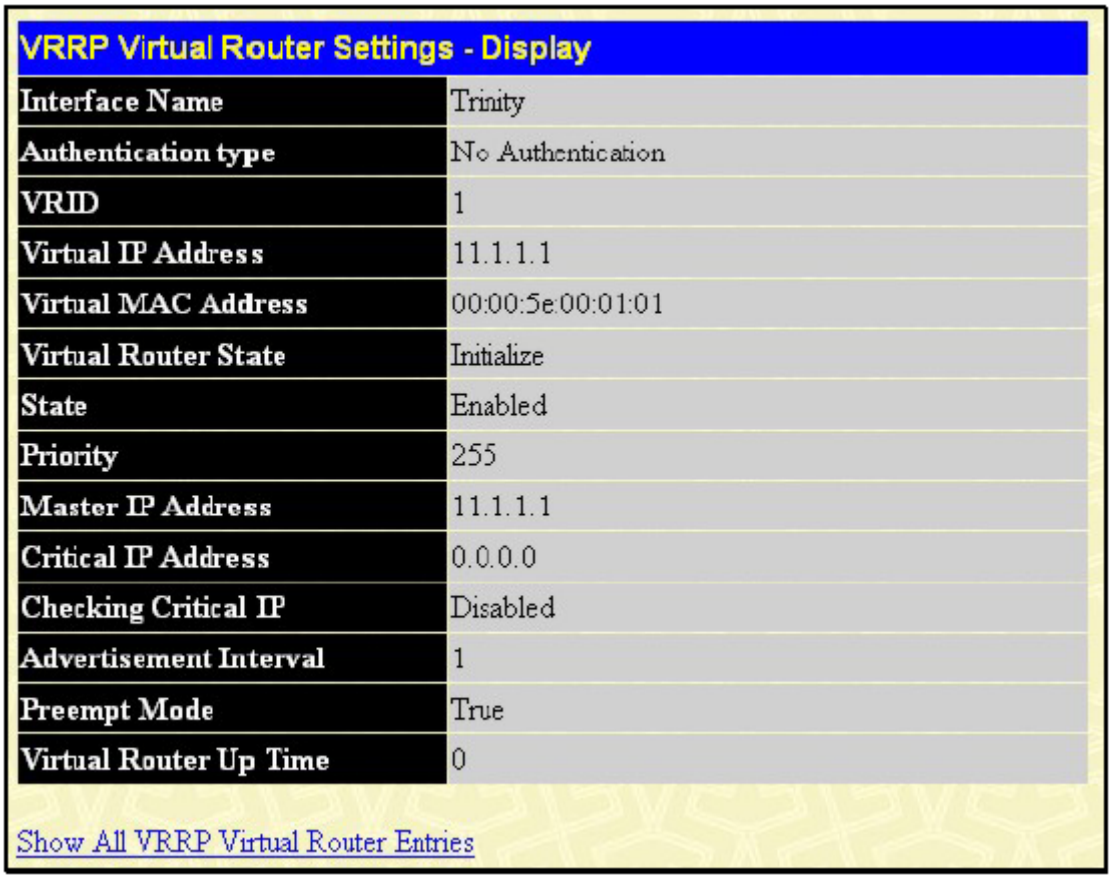


Рисунок 8.49. VRRP Virtual Router Settings - Display окно

Это окно отображает следующую информацию:

Параметр	Описание
Interface Name	Имя IP-интерфейса, который подключен для VRRP. Эта запись должна быть предварительно установлена в таблице IP Interface Settings Table.
Authentication type	Отображает тип аутентификации, используемый для сверки VRRP-пакетов, полученных от виртуального маршрутизатора. Возможные типы аутентификации включают: *No Authentication*- Аутентификация для сверки пакетов, полученных от виртуального маршрутизатора, не используется. *Simple Text Password*- Используется аутентификация с помощью простого пароля для сверки пакетов, полученных от виртуального маршрутизатора. *IP Authentication Header* - Используется аутентификация с помощью цифрового алгоритма MD5 для сверки пакетов, полученных от виртуального маршрутизатора.
VRID	Отображает идентификатор виртуального маршрутизатора, установленный пользователем.
Virtual IP Address	IP-адрес виртуального маршрутизатора, установленный на коммутаторе.
Virtual MAC Address	MAC-адрес устройства, поддерживающего виртуальный маршрутизатор.
Virtual Router State	Отображает текущий статус виртуального маршрутизатора. Возможны следующие состояния: *Initialize, Master* и *Backup*.
Admin. State	Отображает текущее состояние маршрутизатора. *Up* отображается, если виртуальный маршрутизатор подключен, а Down – если виртуальный маршрутизатор отключен.
Priority	Отображает приоритет виртуального маршрутизатора. Чем выше приоритет, тем больше вероятность, что данный маршрутизатор будет

	выбран ведущим маршрутизатором группы. Чем ниже приоритет, тем больше вероятность, что маршрутизатор станет резервным. Чем меньше это число, тем выше приоритет.
Master IP Address	Отображает IP-адрес ведущего маршрутизатора для функции VRRP.
Critical IP Address	Отображает критический IP-адрес для функции VRRP. Этот адрес будет необходим, если виртуальный маршрутизатор будет назначен ведущим.
Checking Critical IP	Отображает статус критического IP-адреса. Может быть подключен или отключен.
Advertisement Interval	Отображает временной интервал в секундах, в течение которого VRRP-сообщения пересылаются в сеть.
Preempt Mode	Отображает режим для определения поведения резервного маршрутизатора, установленного на этом VRRP-интерфейсе. True будет означать, что это будет резервный маршрутизатор, если приоритет маршрутизатора установлен выше, чем приоритет ведущего маршрутизатора. False будет отключать возможность резервного маршрутизатора стать ведущим.
Virtual Router Up Time	Отображает время в минутах, с момента которого виртуальный маршрутизатор был запущен.

Настройки VRRP аутентификации

Окно **VRRP Authentication Settings** используется для установки аутентификации для каждого интерфейса, установленного для VRRP. Эта аутентификация используется для идентификации пакетов входящих сообщений, полученных от маршрутизатора. Если аутентификация не согласована с входящими пакетами, они будут отброшены. Тип аутентификации **Authentication Type** должен согласовываться со всеми маршрутизаторами, относящимися к одной VRRP-группе. Чтобы увидеть следующее окно, нажмите **L3 Features>VRRP> VRRP Authentication Settings.**

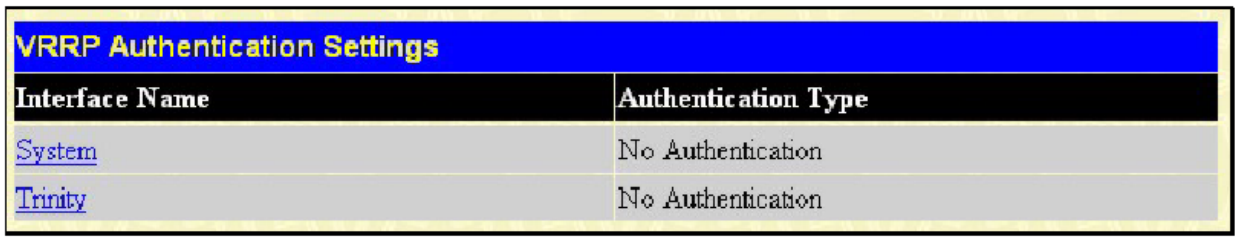


Рисунок 8.50. VRRP Authentication Settings окно

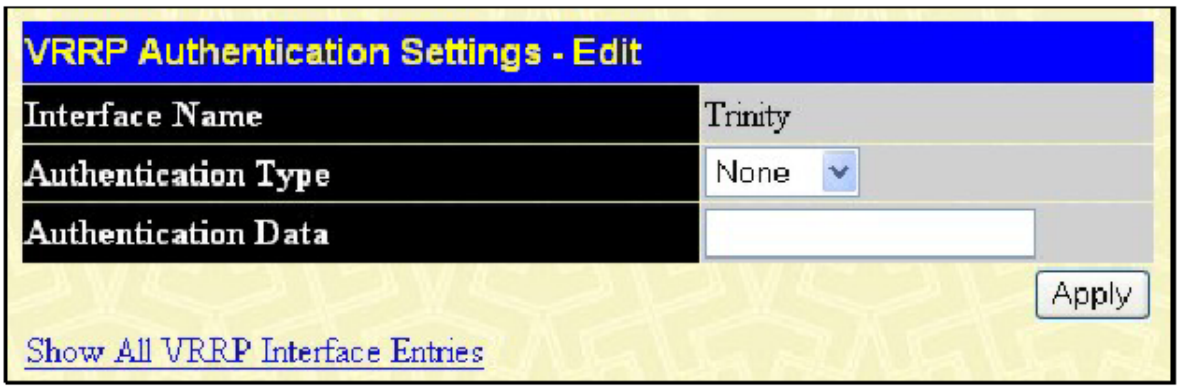


Рисунок 8.51. VRRP Authentication Settings – Edit окно

Следующие параметры могут быть просмотрены или установлены:

Параметр	Описание
Interface Name	Имя предварительно созданного IP-интерфейса для установки аутентификации VRRP.

Authentication Type	Отображает используемый тип аутентификации. **Authentication Type** должен быть согласован со всеми маршрутизаторами, принадлежащими VRRP-группе. Возможные типы аутентификации включают: *Non*- Выбор этого параметра указывает, что при обмене сообщениями VRRP аутентификация отсутствует. *Simple*- Выбор этого параметра указывает, что пользователю необходимо будет ввести пароль при аутентификации. Поле данных для сверки пакетов VRRP –сообщения, полученных маршрутизатором. Если пароль не совпадает, сообщение будет удалено. *IP* - Выбор этого параметра указывает, что пользователю необходимо будет ввести MD5 сообщение для аутентификации и второе сообщение, полученное от маршрутизатора. Если два значения не совпадают, то пакет отбрасывается.
Authentication Data	Это поле необходимо, если пользователь установил **Authentication Type** как *Simple* или *IP* - *Simple* – от пользователя потребуется ввести буквенно-цифровую последовательность не более 8 знаков длиной для идентификации VRRP-пакетов, полученных от маршрутизатора. - *IP* – от пользователя потребуется ввести сообщение MD5 для аутентификации и сравнения VRRP-сообщений, полученных от маршрутизатора.

Нажмите **Apply**, чтобы выполненные настройки вступили в силу.

IP Multicast Routing Protocol (Широковещательный IP-протокол маршрутизации)

Функции, поддерживающие широковещание по IP, добавляются в папке **IP Multicast Routing Protocol,** находящейся в папке **L3 Features. IGMP, DVMRP** и **PIM-DM** могут быть подключены или отключены на коммутаторе без изменения индивидуальных настроек протокола с помощью **DES-3800 Web Management Tool**.

IGMP

Компьютеры и сетевые устройства, которые хотят получать широковещательные пакеты, должны проинформировать близлежащие маршрутизаторы, что они станут членами широковещательной группы. При этом используется **Internet Group Management Protocol (IGMP)**. IGMP также применяется для периодической проверки неактивных членов широковещательной группы. В случаях, когда существует больше одного широковещательного маршрутизатора на подсети, один маршрутизатор выбирается как («Querier»). Затем отслеживает членство в широковещательных группах, имеющих активных членов. Информация, полученная от IGMP, затем используется для определения, будут ли широковещательные пакеты пересылаться в данную подсеть или нет. Маршрутизатор может определить, используя IGMP, что существует, по крайней мере, один член широковещательной группы на данной подсети. Если на данной подсети нет ни одного члена, то пакеты не будут пересылаться в эту подсеть.

IGMP версии 1 и 2

Члены широковещательной группы могут в любое время присоединиться или покинуть группу. Протоколом IGMP обеспечивается метод для взаимодействия маршрутизаторов при подключении к широковещательной группе или отключении от нее.
IGMP версии 1 описывается RFC1112. Он имеет фиксированную длину пакета и не содержит дополнительных данных.
Формат IGMP пакета показан ниже:

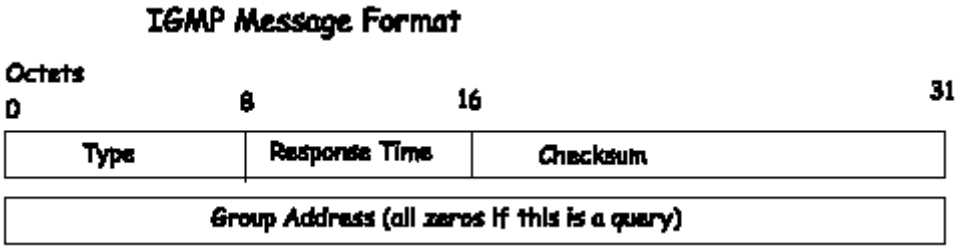


Рисунок 8- 52. Формат IGMP-сообщения

Коды типов IGMP показаны ниже:

Тип	**Значение**
0x11	Запрос на членство в группе (если адрес группы 0.0.0.0)
0x11	Специальный запрос на членство в группе (если представлен адрес группы)
0x16	Отчет о членстве (версия 2)
0x17	Оставить группу (версия 2)
0x12	Отчет о членстве (версия 1)

IGMP-пакеты дают возможность широковещательным маршрутизаторам отслеживать членство в широковещательных группах, на соответствующих им подсетях. При взаимодействии между широковещательным маршрутизатором и членом широковещательной группы по протоколу IGMP применяются следующие основные положения.
Для присоединения к группе хост посылает IGMP «report»(отчет).
Хост никогда не присылает отчет, когда он желает покинуть группу (для версии 1).
Хост посылает «leave» отчет, когда хочет покинуть группу (для версии 2).
Широковещательные маршрутизаторы периодически посылают IGMP-запросы (на групповой адрес всех хостов 224.0.0.1), чтобы определить есть ли хотя бы один член группы на подсети. Если от какой-то группы нет ответа, то маршрутизатор принимает, что на этой сети нет членов группы.
Поле Time-to-Live (TTL) сообщений запроса установлено в значение 1, при этом запросы не будут пересланы в другие подсети.
IGMP версии 2 дает некоторые усовершенствования такие, как метод выбора широковещательного маршрутизатора, посылающего запросы («querier») для каждой LAN, явные leave – сообщения и сообщения запроса, специфичные для данной группы.
Состояния, через которые проходит компьютер, чтобы войти или выйти из широковещательной группы показаны ниже:

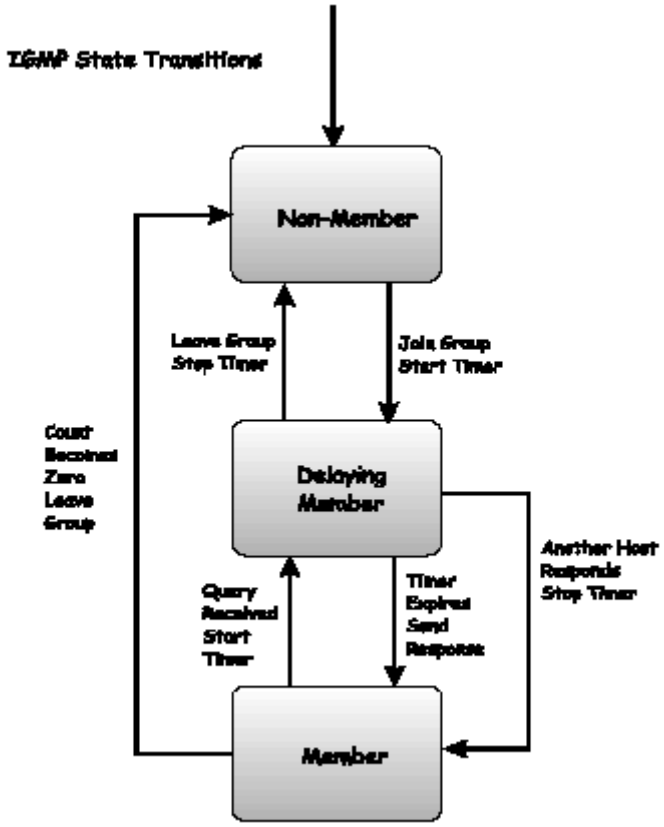


Рисунок 8- 53. IGMP State Transitions Meaning

IGMP версии 3

Текущая реализация коммутаторов xStack включает IGMP версии 3. Усовершенствование IGMP версии 3 по сравнению со второй версией включают:

- Введение SSM (Source Specific Multicast). В предыдущей версии IGMP хост получает все пакеты, которые посылаются в широковещательную группу. Теперь хост будет получать пакеты только от определенного источника(-ов). Это реализовано с помощью фильтров include(включить) и exclude(исключить), используемых для разрешения или запрещения трафика от определенных источников.
- В IGMP версии 2, отчеты могут содержать только одну широковещательную группу, в то время, как в версии 3 отчеты могут содержать множество широковещательных групп и множество источников в широковещательной группе.
- При использовании IGMP версии 2 покинуть широковещательную группу можно с помощью leave - сообщения. В IGMP версии 3 оставить широковещательную группу можно с помощью отчета, который включает блок-сообщение в групповом пакете отчета.
- Для версии 2 хост может отвечать на групповой запрос, но в версии 3 хост имеет возможность отвечать на запросы, относящиеся к определенной группе и источнику.

IGMP версии 3 обратно совместим с другими версиями IGMP.

Коды типов поддерживаемых IGMP версии 3 показаны ниже:

Тип	Значение
0x11	Запрос на членство в группе
0x12	Отчет о членстве (версия 1)
0x16	Отчет о членстве (версия 2)
0x17	Оставить группу (версия 2)
0x22	Отчет о членстве (версия 3)

Таймеры

Как говорилось ранее, в IGMP версии 3 включены фильтры для включения и выключения источников. Эти фильтры обновляются через определенное время с помощью таймеров. В IGMP версии 3 используются два вида таймеров: один для группы, другой для источника. Цель режима фильтрации – сократить время приема таким образом, что все члены широковещательной группы остаются довольны. Режим фильтрации зависит от отчетов и таймеров широковещательных групп. Эти фильтры используются для поддержания списка широковещательных источников и групп широковещательных приемников, которые более точно отражают источники и группы приемников в каждый заданный момент времени на сети.
Таймеры источника используются для поддержания источников в актуальном и активном состоянии в соответствии с широковещательной группой коммутатора. Таймеры источника обновляются, если пакет отчета группы получен коммутатором, который содержит информацию, относящуюся к группе активного источника, записывающей части пакета. Если установлен режим фильтрации exclude (Исключить), то трафик будет удален как минимум для одного определенного источника, остальные хосты могут принимать трафик от широковещательной группы. Если таймер группы закончился для широковещательной группы, режим фильтрации принимает значение «include» и другие хосты получают трафик от источника. Если пакет группового отчета не получен и режим фильтрации include, коммутатор предполагает, что трафик от источника больше не разыскивается на прикрепленной сети и список с записями источников удаляется по истечении всех таймеров.
Если список источников не записан в широковещательную группу, широковещательная группа будет удалена с коммутатора.
Таймеры также используются для членов группы IGMP версии 1 и версии 2 , которые являются частью широковещательной группы, когда коммутатор работает на IGMP версии 3. Этот таймер поддерживается хостом широковещательной группы, которая работает на IGMP версии 1 или версии 2. Получение группового отчета от хоста IGMP версии 1 или версии 2 широковещательной группы приведет к обновлению таймера.

ЗАМЕЧАНИЕ: Величина времени для всех таймеров, используемых для IGMP версии 3 может быть определена путем выполнения следующих вычислений: (Время запроса x коэффициент запаса) + один временной интервал для ответа на запрос

Установки IGMP-интерфейса

IGMP может быть установлен на коммутаторе на базе IP-интерфейса. Для просмотра таблицы **IGMP Interface Settings Table,** откройте папку **IP Multicast Routing Protocol** в **L3 Features** и нажмите **IGMP Interface Settings.** Каждый IP-интерфейс, установленный на коммутаторе, отображается в показанном ниже **IGMP Interface Settings** диалоговом окне. Для установки IGMP для отдельного интерфейса, нажмите соответствующую гиперссылку для этого IP-интерфейса. В результате откроется другое окно **IGMP Interface Settings- Edit.**

IGMP Interface Settings

Interface Name	IP Address	Version	Query Interval	Max Response Time	Robustness Variable	Last Member Query Interval	State
System	10.53.13.52	3	125	10	2	1	Disabled
Trinity	11.1.1.1	3	125	10	2	1	Disabled

Рисунок 8.54. IGMP Interface Settings окно

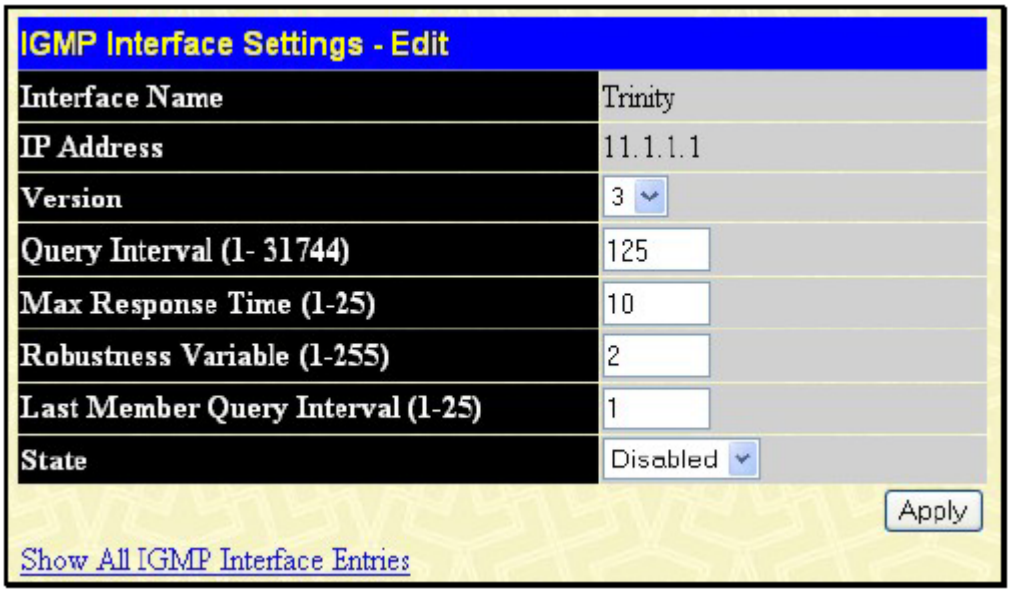


Рисунок 8.55. IGMP Interface Settings – Edit окно

Это окно позволяет настроить IGMP для каждого IP-интерфейса, установленного на коммутаторе. Возможно установить IGMP любой версии при помощи переключения поля **Version,** используя выпадающее меню. Длина временного интервала между запросами может изменяться в зависимости от введенного значения в поле **Query Interval** (от 1до 31744 секунд). Максимальная длина временного интервала между получением запроса и отправкой ответного отчета IGMP может изменяться в зависимости от введенного значения в поле **Max Response Time.**

Поле **Robustness Variable (поправочный коэффициент)** позволяет IGMP подстроиться для подсетей, которые предполагают потерю многих пакетов. Более высокое значение (максимально 255) поможет потери на подсети. Более низкое значение (минимум 2) будет использовано для меньших потерь на подсетях.

Следующие поля могут быть установлены:

Параметр	Описание
Interface Name	Отображает имя IP-интерфейса, который будет установлен для IGMP. Это должен быть предварительно установленный IP-интерфейс
IP Address	Отображает IP-адрес, соответствующий указанному выше имени IP-интерфейса.
Version	Введите версию IGMP (1,2 или 3), которая будет использоваться для интерпретации IGMP-запросов, на этом интерфейсе.
Query Interval	Позволяет ввести значение от 1 до 31744 секунд. Значение по умолчанию 125 секунд. Определяет временной интервал между посылкой IGMP-запросов.
Max Response Time	Устанавливает максимально допустимо время до посылки ответного отчета IGMP. Может быть введено значение от 1 до 25 секунд, по умолчанию – 10 секунд.
Robustness Variable	Настраиваемая переменная. Предназначена для строительства подсетей с ожидаемыми большими потерями. Может быть введено значение от 1 до 255. При этом чем больше значение данной переменной, тем большее количество пакетов может быть потеряно.
Last Member Query Interval	Определяет максимальное количество времени между сообщениями специальных запросов группы.
State	Это поле может быть переключено между *Enabled* или *Disabled* для подключения или отключения IGMP для этого IP-интерфейса. По умолчанию *Disabled.*

Нажмите **Apply** для применения выполненных настроек.

Установка DVMRP-интерфейса

Distance Vector Multicast Routing Protocol (Дистанционно-векторный широковещательный протокол маршрутизации, **DVMRP**) хоп-метод построения широковещательных деревьев доставки (delivery tree) от источников широковещательной рассылки до всех узлов сети. Поскольку дерево доставки содержит самые короткие маршруты, то DVMRP, действительно, эффективно. Поскольку информация о членстве в широковещательной группе пересылается при помощи дистанционно-векторного алгоритма, то данные передаются медленно. Поэтому применение DVMRP оптимально для сетей с большой задержкой (большим временем ожидания) и небольшой полосой пропускания, и может быть рассмотрен как широковещательный протокол «best-effort» (с негарантированной скоростью).
DVMRP схож с протоколом RIP, но он более расширен для широковещательной доставки. DVMRP строит таблицу маршрутизации, чтобы вычислить «кратчайший путь» к источнику широковещательных сообщений, но определяет стоимость маршрута (простой счетчик хопов в RIP) как относительное число, представляющее собой реальную стоимость использования этого маршрута в построении однажды установленного широковещательного дерева доставки.
Когда отправитель инициирует широковещательную рассылку, DVMRP немедленно принимает, что все пользователи на сети захотят получить широковещательное сообщение. Когда смежный маршрутизатор получает сообщение, он проверяет его по односторонней таблице маршрутизации (unicast routing table),чтобы определить интерфейс, который дает кратчайший путь по направлению к источнику. Если широковещательная рассылка была получена через кратчайший путь, тогда смежный маршрутизатор вносит информацию в свои таблицы и пересылает сообщение. Если сообщение получено не по кратчайшему пути до источника, то оно отбрасывается. Стоимость маршрута – относительное число, используемое DVMRP для вычисления, какие ветви широковещательного дерева доставки необходимо отсечь. Эта стоимость относительна по отношению к стоимостям других маршрутов, назначенных в сети.
Чем выше стоимость маршрута, тем ниже вероятность, что данный маршрут будет выбран активной ветвью широковещательного дерева доставки, при условии, что это один из альтернативных путей.

Глобальные настройки DVMRP

Для подключения DVMRP глобально на коммутаторе нажмите **L3 Features> IP Multicast Routing Protocol>DVMRP Global Settings**. Это даст возможность пользователю доступ к следующему экрану:

Рисунок 8.56. DVMRP Global Settings окно

Используя выпадающее меню, выберите *Enabled* и нажмите **Apply** для установки DVMRP-функции на коммутаторе.

Настройки DVMRP-интерфейса

Для просмотра таблицы **DVMRP Interface Table** нажмите **L3 Features> IP Multicast Routing Protocol>DVMRP Interface Settings.** Это меню позволяет настроить DVMRP для каждого интерфейса, установленного на коммутаторе. Каждый IP-интерфейс, установленный на коммутаторе, отображается в показанном ниже диалоговом окне **DVMRP Interface Configuration**. Для установки DVRMP для отдельного интерфейса, нажмите соответствующую гиперссылку для этого IP-интерфейса. В результате откроется окно **DVMRP Interface Settings.**

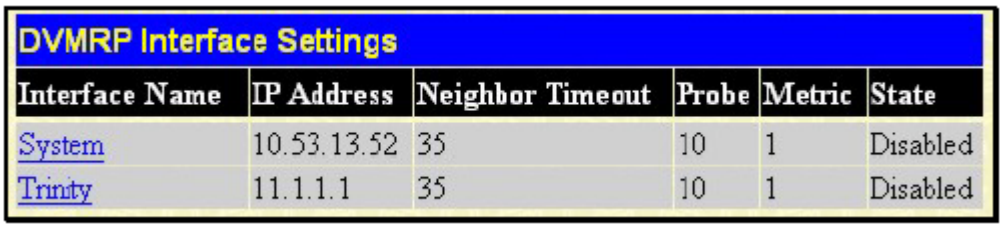


Рисунок 8.57. DVMRP Interface Settings окно

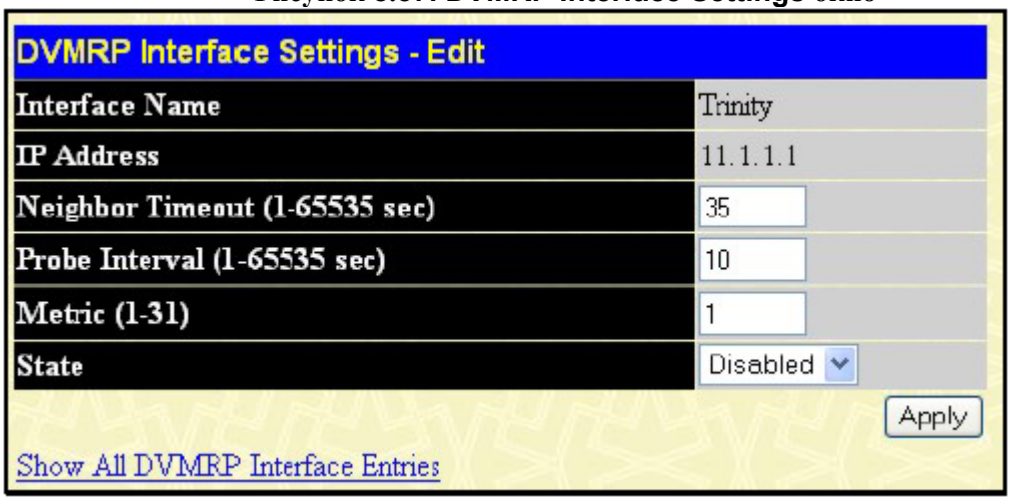


Рисунок 8- 58. DVMRP Interface Settings - Edit окно

Следующие поля могут быть установлены:

Параметр	Описание
Interface Name	Отображает имя IP-интерфейса, для которого будет установлен DVMRP. Это должен быть предварительно установленный IP-интерфейс
IP Address	Отображает IP-адрес, соответствующий указанному выше имени IP-интерфейса.
Neighbor Timeout Interval (1- 65535)	Это поле позволяет ввести значение между 1 и 65535 секундами и определяет период времени, в течение которого DVMRP будет удерживать отчеты соседнего маршрутизатора до отправки сообщения об отравленном маршруте. По умолчанию, равно 35 секунд.
Probe Interval (1-65535)	Это поле позволяет ввести значение между 1 и 65535 секундами и определяет интервал между попытками. По умолчанию, равно 10.
Metric (1-31)	Это поле позволяет ввести значение между 1 и 31 и определяет стоимость маршрута для данного IP-интерфейса. Стоимость DVMRP-маршрута – относительное число, представляющее собой реальную стоимость использования данного маршрута при построении широковещательного дерева доставки. Это число, как и в протоколе RIP, простое, но не определяется как количество хопов. По умолчанию, равно 1.
State	Это поле может быть переключено между *Enabled* или *Disabled*, и подключает или отключает DVMRP для данного IP-интерфейса. По умолчанию, *Disabled*.

Нажмите Apply для того, чтобы изменения вступили в силу. Нажмите Show All DVMRP Interface Entries для возврата в окно **DVMRP Interface Settings**.

Установка PIM-DM интерфейса

Protocol Independent Multicast- Dense Mode (PIM-DM, Протокол независимой широковещательной рассылки- плотный режим) применяется в сетях с низкой задержкой (временем ожидания) и широкой полосой пропускания, так как DIM-PM оптимизирован для гарантированной доставки широковещательных пакетов, не сокращая количество протокольных сигналов.

Протокол PIM-DM принимает, что все маршрутизаторы нижележащего уровня хотят получить широковещательные сообщения и зависят от явных сообщений об отсечении ветвей дерева доставки от нижележащих маршрутизаторов, чтобы удалить из широковещательного дерева доставки ветви, которые не содержат членов широковещательной группы.
У PIM-DM нет явных сообщений «join». Вместо этого применяется периодическая рассылка широковещательных сообщений на все интерфейсы и затем ожидание или истечения таймера (**Join/Prune Interval**), или пока нижележащие маршрутизаторы пришлют «prune» сообщение, показывающее, что на соответствующей ветви больше нет членов широковещательной группы. Затем PIM-DM удаляет данную ветвь из широковещательного дерева доставки.
Так как член удаленной ветви широковещательного дерева доставки может захотеть вступить в широковещательную группу доставки (в некоторое время в будущем), протокол периодически удаляет «prune»-информацию из базы данных и рассылает широковещательные сообщения всем интерфейсам на этой ветви. Временной интервал для удаления «prune» информации определен в **Join/Prune Interval**.

Настройка PIM-DM

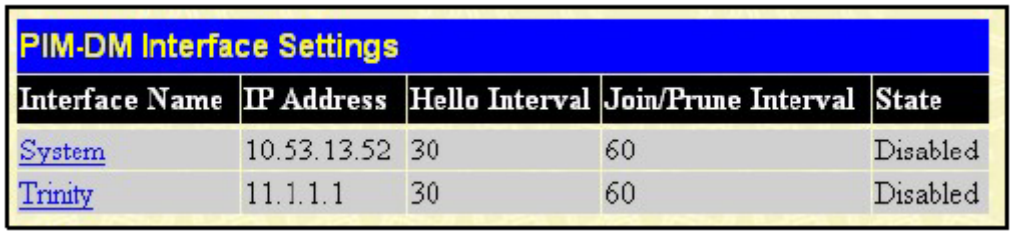
Для глобального подключения PIM-DM на коммутаторе **L3 Features> IP Multicast Routing Protocol>PIM-DM> PIM-DM Global Settings.** Это даст пользователю доступ к следующему экрану:

Рисунок 8.59. PIM DM Global Setting окно

Используя выпадающее меню, выберите *Enabled* и нажмите **Apply** для установки функций PIM-DM на коммутаторе.

Установка PIM-DM интерфейса

Для просмотра **PIM-DM Table** нажмите **L3 Features> IP Multicast Routing Protocol>PIM-DM> PIM-DM Interface Settings.** Это окно позволяет настроить PIM-DM для каждого IP-интерфейса, установленного на коммутаторе. Каждый IP-интерфейс, установленный на коммутаторе, отображается в представленном ниже **PIM-DM Interface Settings** диалоговом окне. Для настройки PIM-DM для отдельного IP-интерфейса нажмите на соответствующую гиперссылку для этого IP-интерфейса. В результате откроется окно **PIM-DM Interface Settings:**


PIM-DM Interface Settings

Interface Name	IP Address	Hello Interval	Join/Prune Interval	State
System	10.53.13.52	30	60	Disabled
Trinity	11.1.1.1	30	60	Disabled

Рисунок 8.60. PIM-DM Interface Settings окно

Для просмотра окна конфигурации для отдельной записи, нажмите на гиперссылку ее имени, и появится следующее окно:

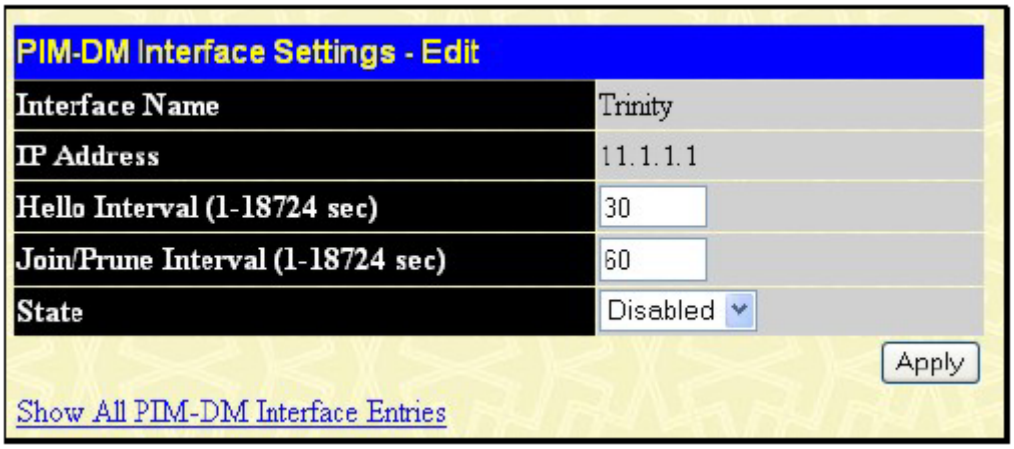


Рисунок 8.61. PIM-DM Interface Settings - Edit окно

Следующие поля могут быть установлены или просмотрены:

Параметр	Описание
Interface Name	Отображает имя IP-интерфейса, для которого будет установлен PIM-DM. Это должен быть предварительно установленный IP-интерфейс
IP Address	Отображает IP-адрес, соответствующий указанному выше имени IP-интерфейса.
Hello Interval (1-18724)	Это поле позволяет ввести значение от 1 до 18724 секунд и определяет интервал между посылками hello-пакетов другим маршрутизаторам сети. По умолчанию принимается равным 30 секундам.
Join/Prune Interval (1-18724)	Это поле позволяет ввести значение от 1 до 18724 секунд. Этот интервал также определяет временной интервал, по истечении которого маршрутизатор автоматически удаляет «prune» информацию из ветви широковещательного дерева доставки и начинает рассылать широковещательные сообщения во все ветви дерева доставки.
State	Это поле может быть переключено между *Enabled* и *Disabled* и используется для подключения или отключения PIM-DM для IP-интерфейса.

Нажмите **Apply** для применения выполненных настроек. Нажмите Show All PIM-DM Interface Entries для возврата в таблицу **PIM-DM Interface Table**.

Раздел 9 – Качество обслуживания

Контроль полосы пропускания
QoS Scheduling Mechanism
QoS Output Scheduling
802.1P Default Priority
802.1P приоритет пользователя
Настройки WRED

Коммутаторы серии DES-3800 поддерживают приоритезацию трафика. В данном разделе обсуждается реализация качества обслуживания QoS и преимущества использования приоритезации трафика согласно 802.1p.

Преимущества QoS

QoS представляет собой реализацию стандарта IEEE 802.1p, предоставляющий сетевым администраторам способ резервирования полосы пропускания для приложений, требующих большую полосу пропускания и высокий приоритет обработки данных, таких как VoIP (протокол передачи голоса по сети Интернет), Web-браузеров, файл-серверных приложений и видео конференций. Для передачи подобного трафика может потребоваться большая полоса пропускания, выделение которой может привести к ограничению полосы пропускания трафика, менее критичного к задержкам времени. На каждом порту коммутатора на аппаратном уровне осуществлена поддержка приоритезации трафика, таким образом, пакетам различных приложений будут назначаться соответствующие приоритеты. На представленной ниже схеме вы можете увидеть каким образом реализована функция приоритезации трафика 802.1p в коммутаторах серии DES-3800.

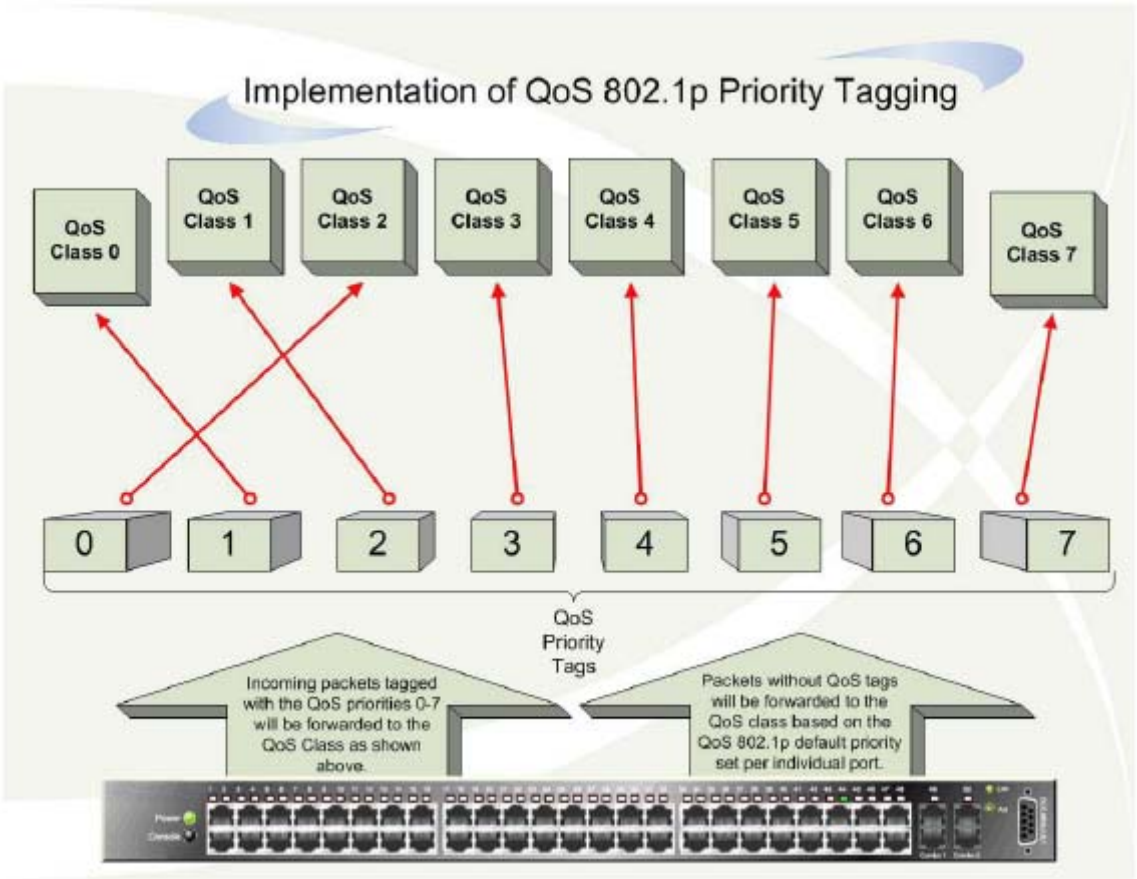


Рисунок 9.1 – Распределение пакетов по очередям приоритетов

На приведенном выше рисунке показаны настройки коммутатора по приоритетам, которые установлены по умолчанию. Седьмой класс Class-7 имеет самый высокий приоритет обслуживания из восьми возможных. Для реализации QoS пользователю необходимо настроить коммутатор, чтобы он проверял заголовки пакетов на предмет наличия тега с указанием приоритета. Затем пользователь может перенаправлять тегированные пакеты по указанным очередям коммутатора на основании приоритетов. Рассмотрим пример, пользователю необходимо организовать видеоконференцию между двумя удаленными компьютерами. Администратор может добавить тег с указанием приоритета при помощи команд Access Profile. На приемной стороне администратор настраивает коммутатор для проверки пакетов на предмет наличия тега с указанием приоритета и направляет их в очереди по соответствующим классам. Затем администратору необходимо установить приоритет для данной очереди, пакеты из которой будут обслуживаться раньше других. В результате пользователь получает пакеты настолько быстро, насколько это возможно благодаря приоритетной обработки пакетов, оптимизизирующей полосу передачи для организации видеоконференции.

Понятие QoS

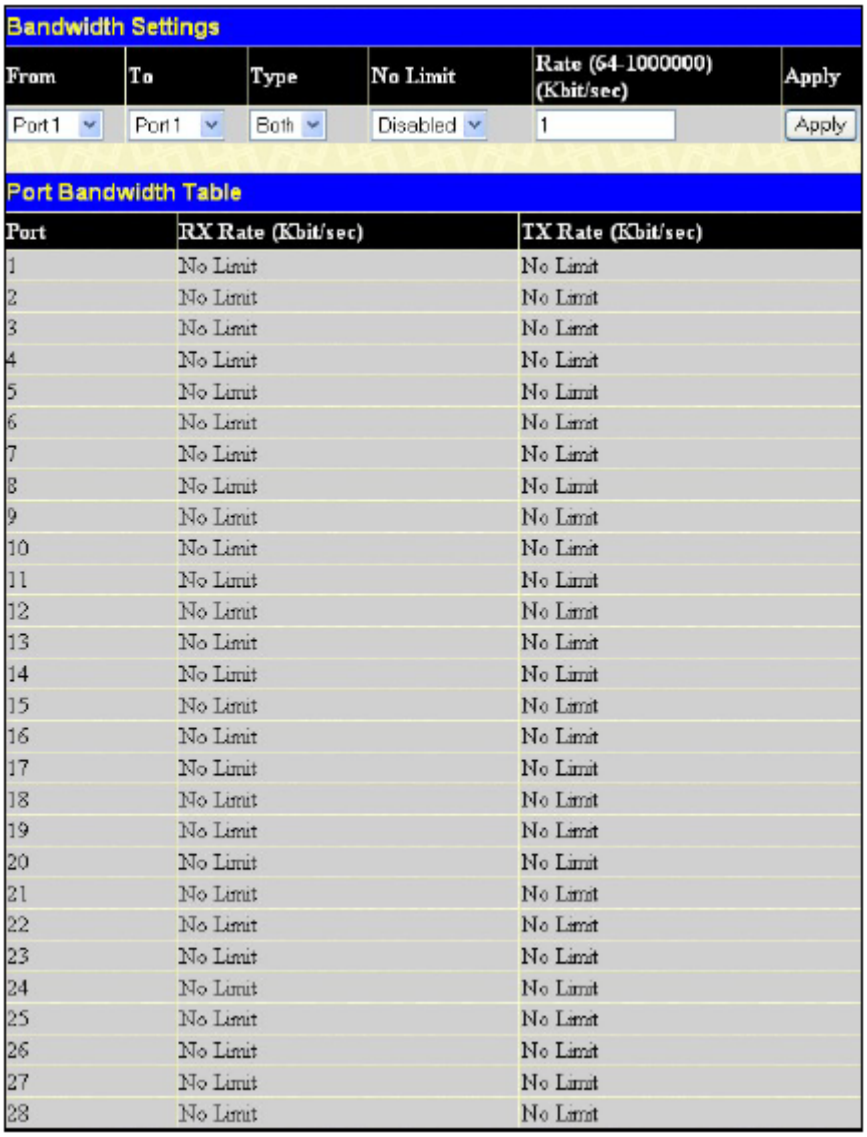
В коммутаторе существует восемь очередей приоритетов, наивысший приоритет закреплен за 7, а самый низкий за 0. Восьми приоритетам, описанным в IEEE 802.1p, ставятся в соответствие следующие приоритетные очереди:

- Приоритет 0 назначается очереди Q2
- Приоритет 1 назначается очереди Q0
- Приоритет 2 назначается очереди Q1
- Приоритет 3 назначается очереди Q3
- Приоритет 4 назначается очереди Q4
- Приоритет 5 назначается очереди Q5
- Приоритет 6 назначается очереди Q6
- Приоритет 7 назначается очереди Q7

Для соблюдения строгого порядка обработки очередей, пакеты, находящиеся в очереди с более высоким приоритетом передаются первыми. После опустошения данных очередей будут передаваться пакеты с более низкими приоритетами. В случае взвешенного циклического алгоритма количество пакетов, которое может быть отправлено каждой приоритетной очередью зависит от назначенного веса. Для настройки восьми очередей по классу трафика A-H назначается соответствующее значение веса 8~1, пакеты отправляются в следующем порядке A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1. В том случае, если очередям по классу трафика CoS назначен один и тот же вес, то каждая очередь имеет равную возможность отправки пакетов. В случае наличия очереди со значением веса 0, пакеты из нее будут передаваться до опустошения очереди. Другие очереди CoS, имеющие ненулевое значение веса, будут обслуживаться по обычной схеме взвешенного циклического алгоритма. Помните, что у коммутаторов серии DES-3800 существует 8 приоритетных очередей (и 8 очередей CoS) на каждом порту.

Полоса пропускания порта

Настройки по управлению полосой пропускания используются для установки верхнего значения для передаваемых и получаемых данных для каждого порта. Для просмотра таблицы **«Port Bandwidth Control»**, нажмите **QoS ⇨ Bandwidth Control.**



Bandwidth Settings

From	To	Type	No Limit	Rate (64-1000000) (Kbit/sec)	Apply
Port 1	Port 1	Both	Disabled	1	Apply

Port Bandwidth Table

Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit
17	No Limit	No Limit
18	No Limit	No Limit
19	No Limit	No Limit
20	No Limit	No Limit
21	No Limit	No Limit
22	No Limit	No Limit
23	No Limit	No Limit
24	No Limit	No Limit
25	No Limit	No Limit
26	No Limit	No Limit
27	No Limit	No Limit
28	No Limit	No Limit

Рисунок 9.2 – Окно «Bandwidth Settings»

Можно настроить следующие параметры:

Параметр	Описание
From/To	Последовательная группа портов, которую можно настроить, начиная с выбранного порта.
Type	Данное выпадающее меню позволяет выбрать значения между *RX* (receive), *TX* (transmit) и *Both*. Этот параметр определяет предел полосы пропускания при приёме, передаче или одновременно приёме и передаче пакетов.
No Limit	При помощи выпадающего меню вы можете установить отсутствие ограничений по пропускной способности *Enabled.*
Rate	Введите значение скорости передачи данных (кбит/с), которое будет являться ограничением для выбранного порта. Значение скорости должно быть кратным 64 и находиться в диапазоне между 64 и 1000000.

Для сохранения внесенных изменений нажмите **Apply**. Результаты настроек будут отображаться в таблице **«Port Bandwidth Table»**.

Работа по расписанию

Изменение аппаратных очередей на Коммутаторе настраивается через QoS.
При любых изменениях реализации QoS необходимо обратить внимание на то, как эти изменения повлияли на сетевой трафик в очередях с наименьшим приоритетом. Изменения в планировщике могут привести к недопустимым уровням потерь пакетов или существенно задержке передачи. Если производятся эти настройки, то важно контролировать производительность сети особенно в моменты пиков, т.к. количество узких мест может быстро возрасти из-за неподходящих параметров QoS. Для просмотра окна, представленного ниже, нажмите **QoS ⇨ QoS Scheduling Mechanism**.

Рисунок 9.3 – Окно «QoS Output Scheduling»

Параметр	Описание
Strict	Самый высокий класс трафика обслуживается в первую очередь. Передача трафика наивысшего класса будет закончена до того, как будут обработаны другие очереди.
Weight Robin	Для распределения пакетов по приоритетам классов трафика используйте взвешенный циклический алгоритм (*WRR*).

Для того чтобы настройки вступили в силу, нажмите **Apply**.

Примечание: Настройки по назначению очередей с 0 по 7 определены в IEEE 802.1p в качестве меток по приоритетам, не путайте с номерами портов.

QoS Output Scheduling

Изменение аппаратных очередей на Коммутаторе настраивается через QoS.
При любых изменениях реализации QoS необходимо обратить внимание на то, как эти изменения повлияли на сетевой трафик в очередях с наименьшим приоритетом. Изменения в планировщике могут привести к недопустимым уровням потерь пакетов или существенно задержке передачи. Если производятся эти настройки, то важно контролировать производительность сети особенно в моменты пиков, т.к. количество узких мест может быстро возрасти из-за неподходящих параметров QoS. Для просмотра окна, представленного ниже, нажмите **QoS ⇨ QoS Output Scheduling**.

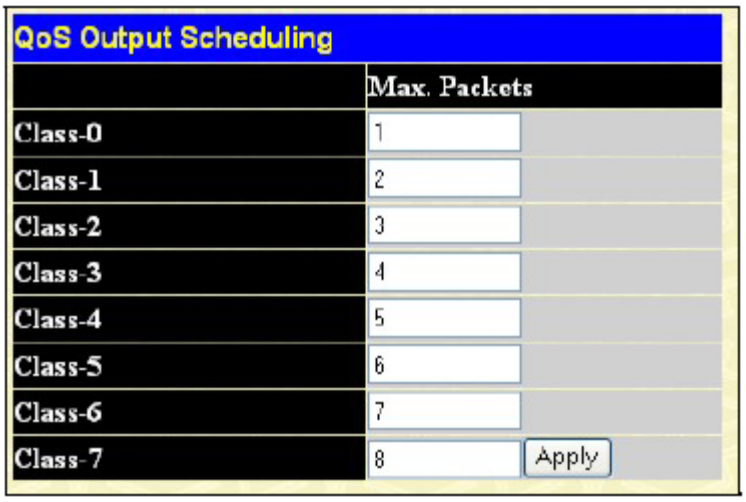


Рисунок 9.4 – Окно «QoS Output Schedule»

Параметр	Описание
Max.Packets	Максимальное количество пакетов, которое можно передать за один раз аппаратной очередью с заданным приоритетом обслуживания данного класса трафика, данное значение можно установить

Для того чтобы настройки вступили в силу, нажмите **Apply**.

Приоритет 802.1p по умолчанию

Коммутатор позволяет назначить по умолчанию на каждый порт признак приоритета 802.1p. Для просмотра окна, представленного ниже, нажмите **QoS ⇨ 802.1p Default Priority.**

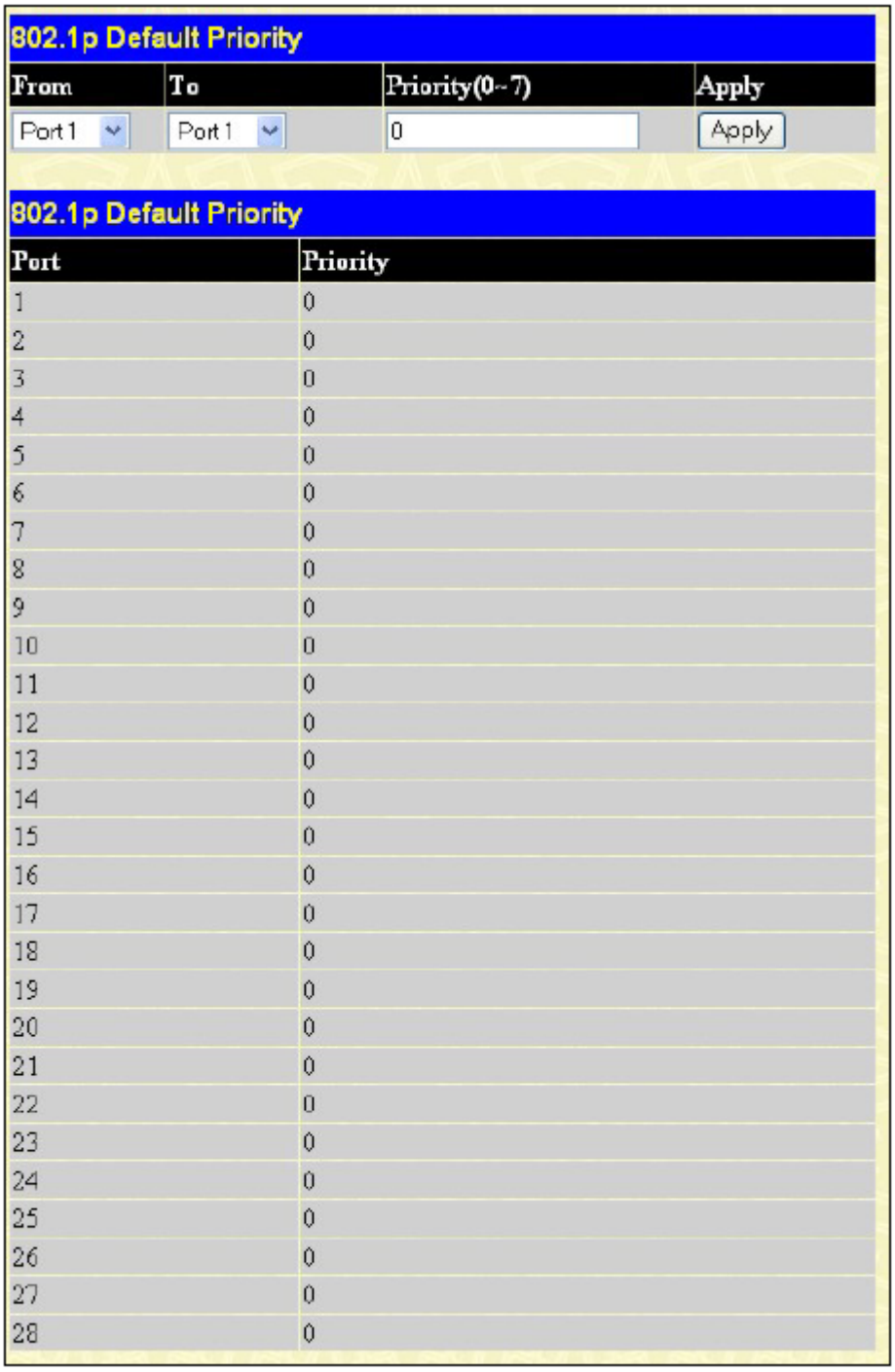


Рисунок 9.5 – Окно «802.1p Default Priority Settings»

Данное окно позволяет произвести настройку приоритетов по умолчанию согласно 802.1p на любом порту коммутатора. Приоритетные очереди нумеруются от 0, самого низкого приоритета, до 7, наивысшего. Для сохранения настроек нажмите **Apply**.

Приоритет пользователя 802.1p

Коммутатор серии DES-3800 позволяет пользователю назначать трафику любой из приоритетов 802.1p. Для просмотра окна, представленного ниже, нажмите **QoS ⇨ 802.1p User Priority.**

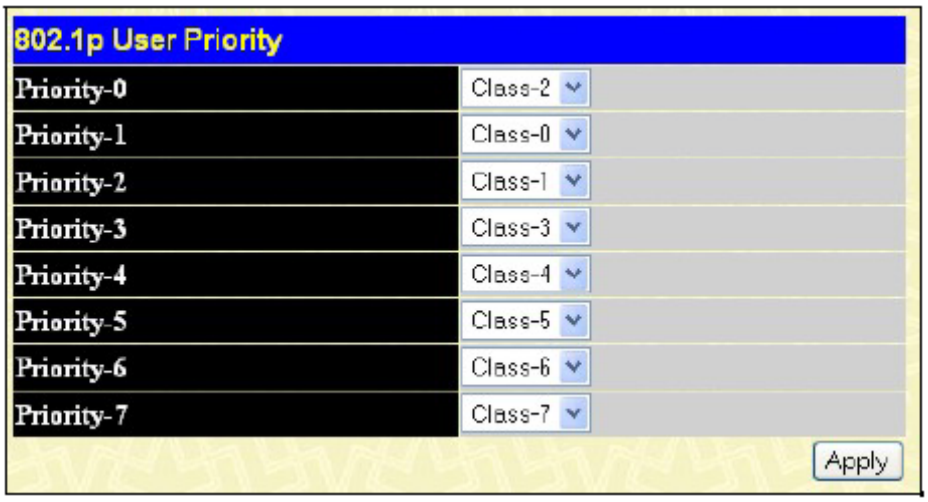


Рисунок 9.6 – Окно «QoS Class of Traffic»

Если вы назначили приоритет группе портов коммутатора, то вы можете поставить в соответствие ему один из восьми приоритетов класса обслуживания 802.1p. Для сохранения настроек нажмите **Apply**.

WRED Settings

WRED или Weighted Random Early Discard – это другая реализация QoS, которая улучшит общую пропускную способность очередей QoS. Основываясь на установленной на коммутаторе QoS функции входной очереди, данный метод будет анализировать пакеты и соответствующие очереди, и в случае переполнения пакетами входящих QoS очередей, для уменьшения потока пакетов в эти очереди будет происходить отбрасывание пакетов случайным образом.

WRED использует два способа во избежание перегрузки очередей QoS.

1. У каждой QoS очереди есть минимальный и максимальный уровень приема пакетов. Когда будет достигнут максимальный порог очереди, коммутатор начнет отбрасывать все входящие пакеты, минимизируя тем самым предоставляемую полосу пропускания. Как только уровень будет ниже минимального порога, коммутатор начнет обрабатывать входящие пакеты.
2. Когда уровень передачи входящих пакетов находится между максимальной и минимальной очередью, коммутатор использует slope (коэффициент ухудшения) вероятностную функцию для определения случайного метода удаления пакетов на основе процентного соотношения QoS очереди. Если очередь близка к наполнению, коммутатор будет увеличивать количество пакетов, отбрасываемых случайным образом для выравнивания потока пакетов в очереди и избегания переполнения высоко приоритетных очередей.

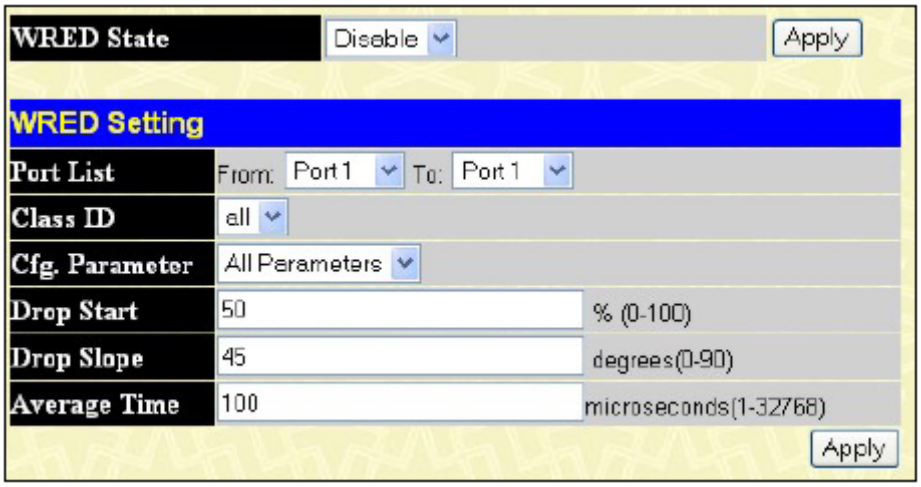


Рисунок 9.7 – Окно «WRED Settings»

Для настройки WRED заполните соответствующие поля и нажмите **Apply**. Отметим, что состояние WRED может быть включено или выключено и для этой цели есть отдельная кнопка **Apply**.

Параметр	Описание
WRED State	Позволяет пользователю включать и отключать функцию WRED без изменения ранее выполненных настроек.
Port List	Используйте выпадающее меню для выбора порта или диапазона портов для настройки WRED.
Class ID	Выберите идентификатор CoS ID от 0 до 7 для настройки параметров WRED. При выборе *all* настроенные параметры будут применены для всех очередей CoS.
Cfg. Parameter	Используйте выпадающее меню для настройки определенных параметров функции WRED для конкретной очереди или порта. Пользователь может выбрать опцию All Parameters, что позволит производить одновременную настройку Drop Start, Drop Slope и Average Time для необходимой CoS очереди, либо можно выбрать единственный параметр для настройки.
Drop Start	Выберите процентное соотношение от 0 до 100 для инициализации процесса случайного отбрасывания пакетов. Это соотношение отсчитывается от выходной QoS очереди, указанной в поле Class ID. (Как только указанная очередь достигнет установленного соотношения, коммутатор начнет отбрасывать пакеты случайным образом).
Drop Slope	Вычисляется отношение среднего размера пакетов к максимуму и минимуму Drop Start функции, определенной в предыдущем поле. Чем ближе данное значение к 90º, тем больше время ожидания отбрасывания пакетов по сравнению со значением, близким к 0º.
Average Time	Введите время (в микросекундах) проверки коммутатором CoS очереди на предмет неправильных настроек и границ, в которых функция WRED будет работать.

Раздел 10 – Списки управления доступом ACL

Таблица профилей доступа
CPU Interface Filtering

Профили доступа позволяют устанавливать условия, по которым будет осуществляться прием или отказ в приеме пакетов на основании информации, содержащейся в каждом заголовке пакета. Этими условиями может служить содержание пакетов, MAC-адрес или IP-адрес.

Таблица профилей доступа

Создание профиля доступа делится на две основные части. В первой указывается какую часть или части кадра будет проверять коммутатор, например, MAC-адрес источника или IP-адрес назначения. Во второй части вводится условие, по которому коммутатор будет определять действие над кадром. Для отображения текущих профилей доступа, откройте: **ACL ⇨ Access Profile Table.**

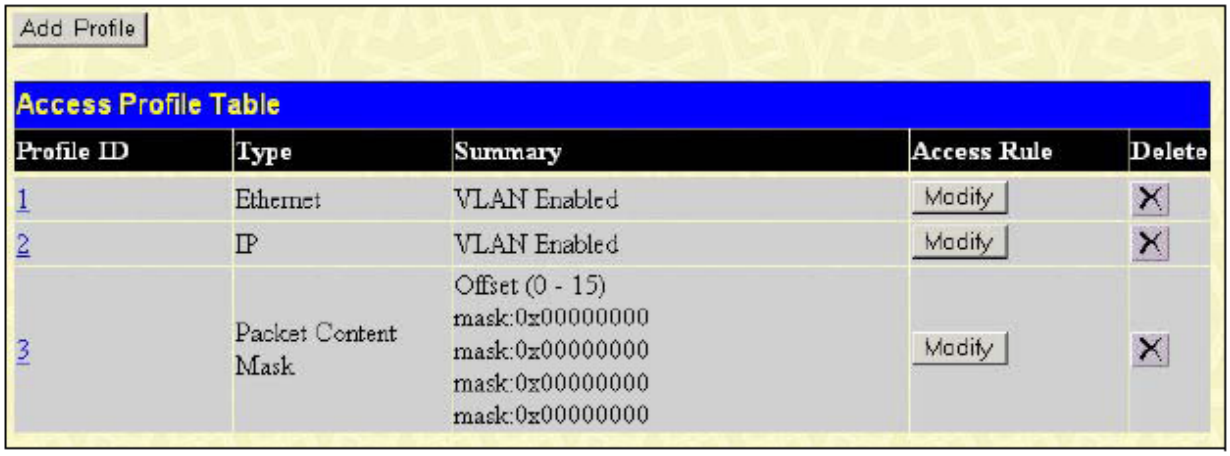


Рисунок 10.1 – Окно «Access Profile Table»

Для добавления профиля доступа в таблицу **Access Profile Table**, нажмите кнопку **Add Profile**, после чего откроется окно **Access Profile Configuration**, представленное ниже. Всего существует три окна Access Profile Configuration, одно для настройки **Ethernet**-профиля (основанного на MAC-адресе), еще одно – для настройки **IP-**профиля, т.е. основанного на IP-адресе, и одно – для **Packet Content Mask**. Вы можете переключаться между этими тремя окнами **Access Profile Configuration** с помощью выпадающего меню поля **Type**. Следующее окно, приведенное ниже, касается настройки профиля Ethernet.

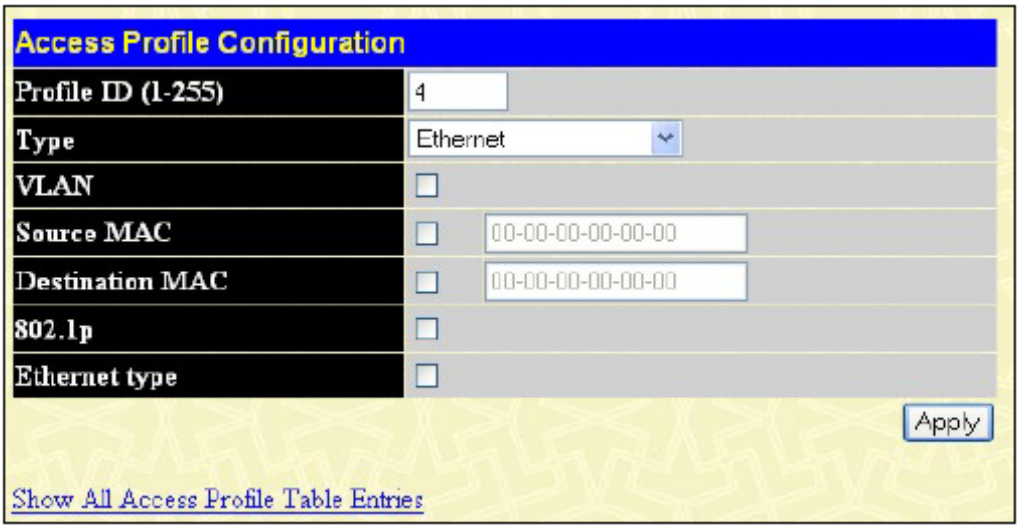


Рисунок 10.2 – Access Profile Table (Ethernet)

Можно настроить следующие параметры для профиля Ethernet .

Параметр	Описание
Profile ID (1-255)	Введите идентификатор профиля из диапазона 1 – 255.
Type	Выберите, какой профиль доступа будет использоваться: на основе Ethernet (MAC-адрес), IP-адреса или маски содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
VLAN	Выбрав данную опцию, коммутатор будет проверять идентификатор VLAN в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Source MAC	Введите маску MAC-адреса источника.
Destination MAC	Введите маску MAC-адреса назначения.
802.1p	Выбрав данную опцию, коммутатор будет проверять значение приоритета по 802.1p в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Ethernet type	Выбрав данную опцию, коммутатор будет проверять значение поля Ethernet Type в заголовке каждого пакета.

Представленное ниже окно **IP Access Profile Configuration** касается настройки IP-профиля.

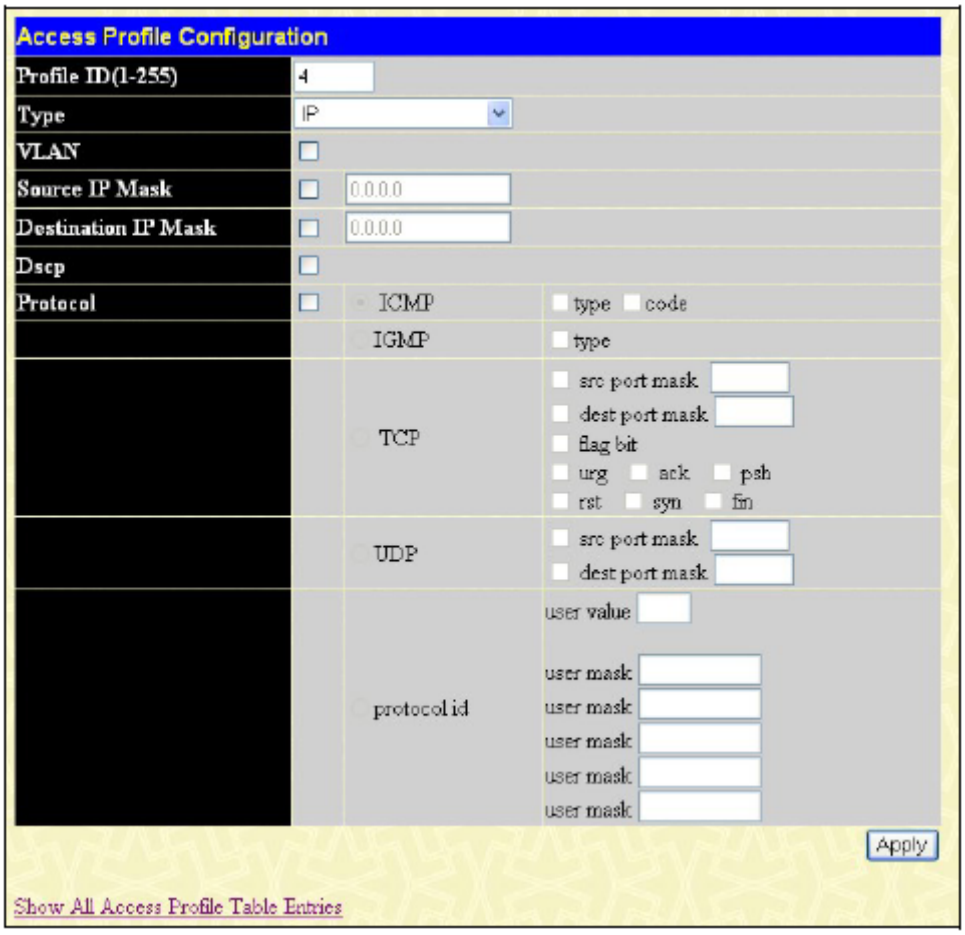


Рисунок 10.3 – Окно «Access Profile Configuration (IP)»

Параметр	Описание
Profile ID (1-255)	Введите идентификатор профиля из диапазона 1 – 255.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
VLAN	Выбрав данную опцию, коммутатор будет проверять идентификатор VLAN в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Source IP Mask	Введите маску IP-адреса источника.
Destination IP Mask	Введите маску IP-адреса назначения.
DSCP	Выбрав данную опцию, коммутатор будет проверять поле DiffServ Code в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Protocol	Выбрав данную опцию, коммутатор будет проверять значение типа протокола в заголовке каждого пакета. Вам необходимо выбрать протокол(ы) в соответствии со следующими рекомендациями: Выберите **ICMP** для того, чтобы коммутатор проверял поле протокола управляющих сообщений в Интернете (Internet Control Message Protocol) в заголовке каждого пакета.

	▪ Выберите по значению типа **Type** или кода **Code** протокола ICMP будет применяться профиль доступа. Выберите **IGMP** для того, чтобы коммутатор проверял поле межсетевого протокола управления группами (Internet Group Management Protocol) в заголовке каждого пакета. ▪ Выберите тип **Type** IGMP, по которому будет формироваться профиль доступа При выборе протокола **TCP** в качестве условия указывается номер порта. Можно использовать или маску порта источника, или/и маску порта назначения. Для фильтрации пакетов по битам флага пользователю нужно сделать отметку в соответствующем поле flag bits. По битам флага пакета определяется действие, которое нужно выполнить с этим пакетом: **urg** (urgent) , **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) , **fin** (finish). ▪ **src port mask** – задайте маску TCP порта источника в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. ▪ **dest port mask** – задайте маску TCP порта назначения в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. При выборе протокола **UDP** в качестве условия указывается номер UDP порта. Можно использовать или маску порта источника, или/и маску порта назначения. ▪ **src port mask** – задайте маску TCP порта источника в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. ▪ **dest port mask** – задайте маску TCP порта назначения в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. **protocol id** – введите значение, определяющее идентификатор протокола в заголовке пакета. Задайте маску идентификатора протокола в шестнадцатеричной системе счисления (hex 0x0-0xffff) или значение пользователя.

Для того чтобы настройки вступили в силу, нажмите **Apply**.

Ниже представлено окно конфигурации **ACL Packet Content Mask.**

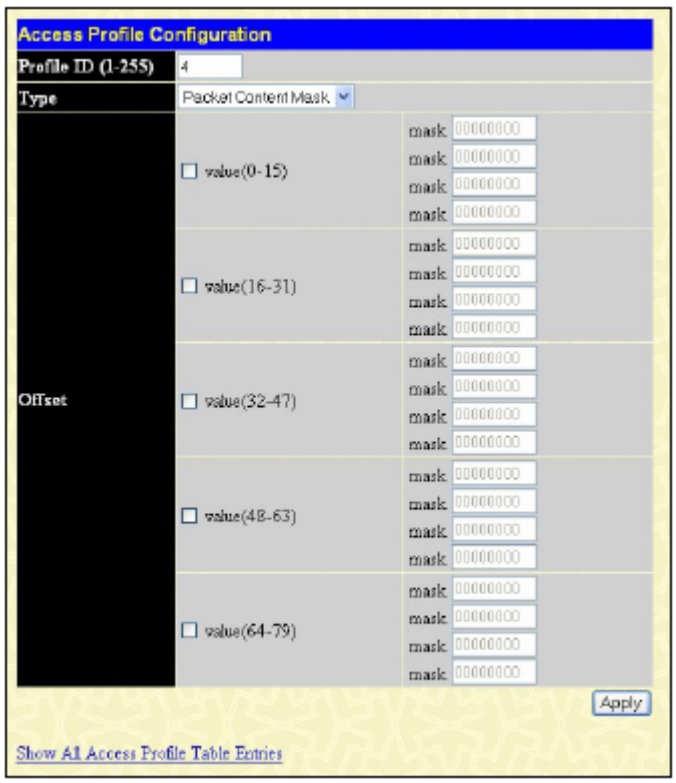


Рисунок 10.4 – Окно «Access Profile Configuration (Packet Content Mask)»

Это окно поможет пользователю в настройке коммутатора, чтобы скрыть начало заголовка пакета с заданным значением смещения. Следующие поля используются для настройки маски содержимого пакета.

Параметр	Описание
Profile ID (1-255)	Введите идентификатор профиля из диапазона 1 – 255.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
Offset	Это поле указывает, что необходимо сравнить начало заголовка пакета с указанным значением: ▪ value (0-15) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить первые 15 байт пакета. ▪ value (16-31) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 16 по 31 байт пакета. ▪ value (32-47) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 32 по 47 байт пакета. ▪ value (48-63) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 48 по 63 байт пакета. ▪ value (64-79) - Введите значение в шестнадцатеричной

	системе счисления, с которым нужно сравнить с 64 по 79 байт пакета.

Для сохранения настроек нажмите **Apply**.

Для установки правила ранее созданного профиля доступа:

Для открытия ниже приведенного окна, нажмите **ACL ⇨ Access Profile Table.**

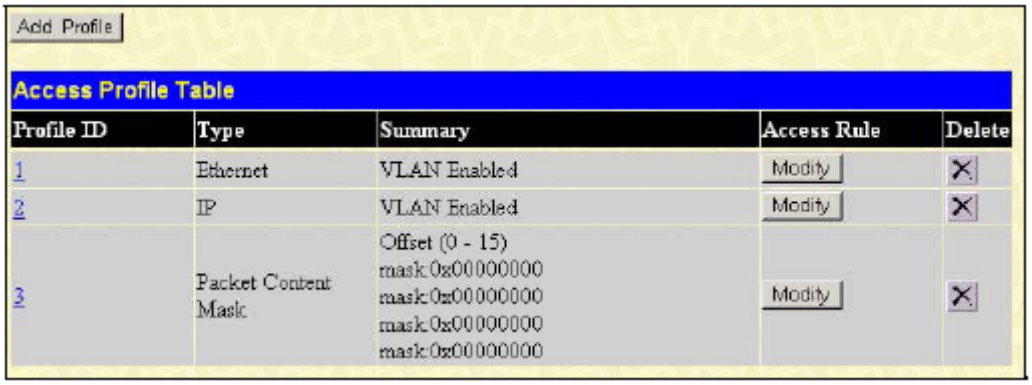


Рисунок 10.5 – Окно «Access Profile Table»

Для создания нового правила для профиля доступа нажмите **Add**, после чего отобразится окно **Access Profile Rule**. Для удаления ранее созданного правила, нажмите кнопку .

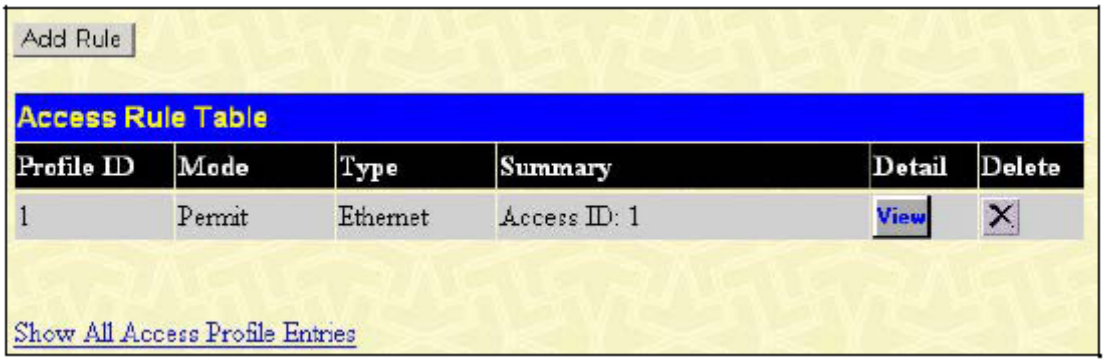


Рисунок 10.6 - Окно «Access Rule Table»

Для добавления нового правила для существующего профиля доступа нажмите **Add Rule**, после чего появится окно **«Access Rule Configuration».** Для удаления ранее созданного правила, нажмите кнопку .

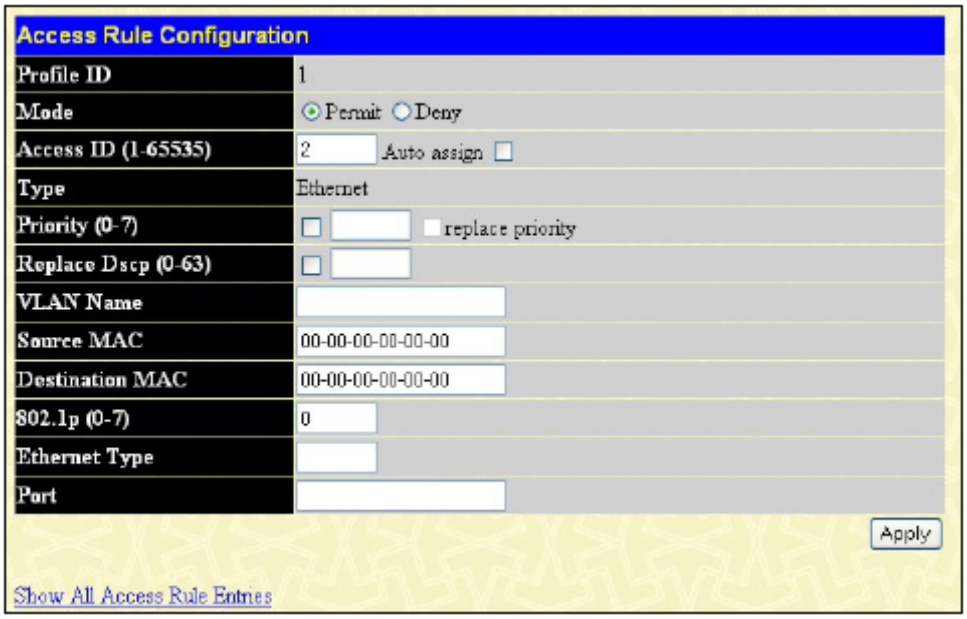


Рисунок 10.7 – Окно «Access Rule Configuration - Ethernet»

Для установки правила доступа для Ethernet, настройте следующие параметры и кликните по **Apply**.

Параметры	Описание
Profile ID	Идентификатор установленного профиля.
Mode	**Permit** - указывает на то, что пакет, который соответствует профилю будет принят и передан коммутатором в соответствии с дополнительным правилом (см. ниже). **Deny** – указывает на то, что пакет, который соответствует профилю будет отброшен коммутатором.
Access ID	Введите значение идентификатора доступа в диапазоне от 1 до 65535. ▪ **Auto Assign** – подключите данную опцию для автоматического назначения коммутатором идентификатора доступа для создаваемого правила.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
Priority (0-7)	Этот параметр задаётся, если пользователь хочет изменить приоритет по умолчанию 802.1p, предварительно установленный на коммутаторе, для определения CoS очереди, в которую будут отправляться пакеты. При заполнении заданного поля, принятые коммутатором пакеты, в соответствии с их приоритетом направляются в очередь CoS, предварительно определённую пользователем. *Replace priority with* - следует поставить отметку в данном поле, если необходимо изменить приоритет 802.1p, установленный по умолчанию, на значение поля Priority (0-7), который будет задействован при отправке пакетов в очередь CoS. В противном случае пакеты будут со своим

	первоначальным 802.1p приоритетом. Для получения большей информации об очередях приоритетов, очередях CoS и настроек 802.1p, следует обратиться к разделу QoS данного руководства.
VLAN Name	Имя ранее настроенной VLAN.
Source MAC	Введите MAC-адрес источника.
Destination MAC	Введите маску MAC-адреса назначения.
802.1p (0-7)	Введите значение приоритета 802.1p от 0 до 7, в результате чего профиль доступа будет применяться только к пакетам с установленным приоритетом.
Ethernet Type	Профиль доступа будет определяться только к пакетам с шестнадцатиричным значением поля Ethernet type (hex 0x0-0xffff) в заголовке пакета. Значение Ethernet type должно быть приведено в виде hex 0x0-0xffff, т.е. пользователь может выбрать любую комбинацию из букв (a - f) и цифр (0 - 9999).
Port	В данном поле введите номер порта для настройки правила доступа на основе портов. В случае настройки диапазона портов необходимо подключить функцию **Auto Assign** в поле Access ID, если данная опция не будет подключена, появится сообщение об ошибке и будет невозможно установить правило доступа. Начало и конец диапазона портов отделяются тире. Например, 3 означает третий порт, 2-4 означает диапазон портов со 2 по 4.

Для просмотра ранее настроенных правил, нажмите View в **Access Rule Table,** после чего появится приведенное ниже окно. При нажатии на гиперссылку Profile ID в таблице **Access Profile Table** также откроется окно **Access Rule Display.**

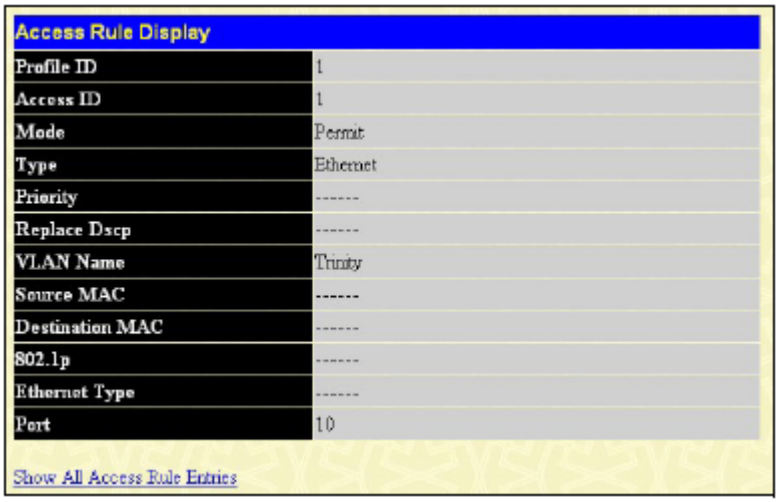


Рисунок 10.8 – Окно «Access Rule Display (Ethernet)»

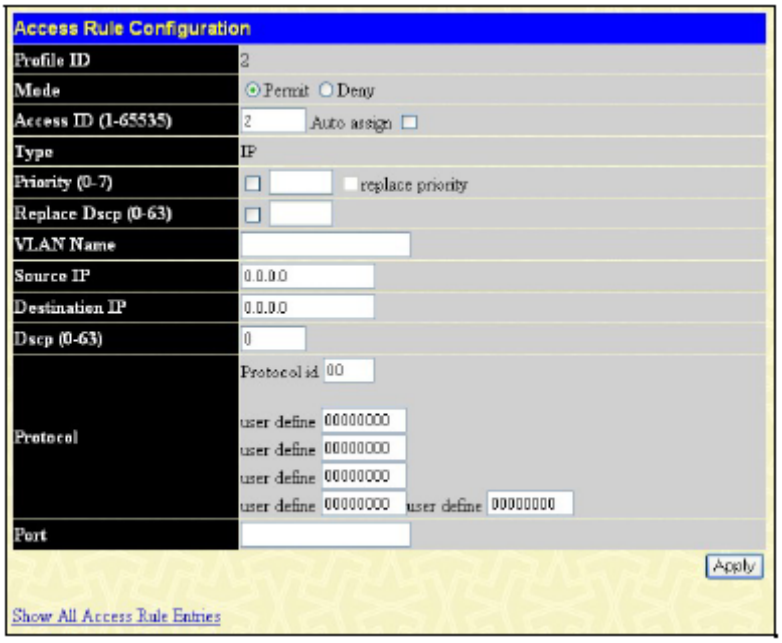


Рисунок 10.9 – Окно «Access Rule Configuration (IP)»

Настройте следующие параметры правила доступа для IP-профиля.

Параметр	Описание
Profile ID	Идентификатор установленного профиля.
Mode	**Permit** - указывает на то, что пакет, который соответствует профилю будет принят и передан коммутатором в соответствии с дополнительным правилом (см. ниже). **Deny** – указывает на то, что пакет, который соответствует профилю будет отброшен коммутатором.
Access ID	Введите значение идентификатора доступа в диапазоне от 1 до 65535. ▪ **Auto Assign** – подключите данную опцию для автоматического назначения коммутатором идентификатора доступа для создаваемого правила.
Type	Выберите, какой профиль доступа будет использоваться: на основе Ethernet (MAC-адрес), IP-адреса или маски содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
Priority (0-7)	Этот параметр задаётся, если пользователь хочет изменить приоритет по умолчанию 802.1p, предварительно установленный на коммутаторе, для определения CoS очереди, в которую будут отправляться пакеты. При заполнении заданного поля, принятые коммутатором пакеты, в соответствии с их приоритетом направляются в очередь CoS, предварительно определённую пользователем. *Replace priority with* - следует поставить отметку в данном поле, если необходимо изменить приоритет 802.1p, установленный по умолчанию, на значение поля Priority (0-7), который будет задействован при отправке пакетов в очередь CoS. В противном случае пакеты будут со своим

	первоначальным 802.1p приоритетом. Для получения большей информации об очередях приоритетов, очередях CoS и настроек 802.1p, следует обратиться к разделу QoS данного руководства.
Replace Dscp (0-63)	Данная опция выбирается для того, что бы коммутатор изменил значение DSCP (в пакетах соответствующих выбранным критериям) на значение введённое в смежном поле.
VLAN Name	Имя ранее настроенной VLAN.
Source IP	Введите маску IP-адреса источника.
Destination IP	Введите маску IP-адреса назначения.
Dscp (0-63)	Введите значение DSCP от 0 до 63, после чего коммутатор будет проверять поле DiffServ Code в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Protocol	Данное поле позволяет пользователю изменять протокол, используемый для настройки Таблицы правил доступа (**Access Rule Table)** в зависимости от выбранного протокола в **Access Profile Table**.
Port	В данном поле введите номер порта для настройки правила доступа на основе портов. В случае настройки диапазона портов необходимо подключить функцию **Auto Assign** в поле Access ID, если данная опция не будет подключена, появится сообщение об ошибке и будет невозможно установить правило доступа. Начало и конец диапазона портов отделяются тире. Например, 3 означает третий порт, 2-4 означает диапазон портов со 2 по 4.

Для просмотра ранее настроенных правил, нажмите **Access Rule Table**.

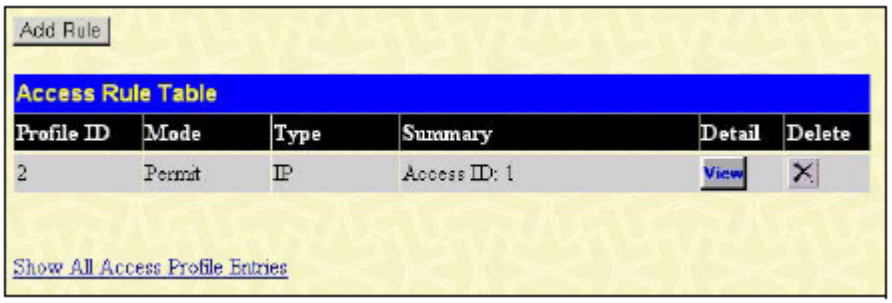


Рисунок 10.10 – Окно «Access Rule Table»

Появится окно, приведенное ниже. При нажатии на ссылку необходимого профиля Profile ID в таблице **Access Profile Table** откроется окно **Access Rule Display**.

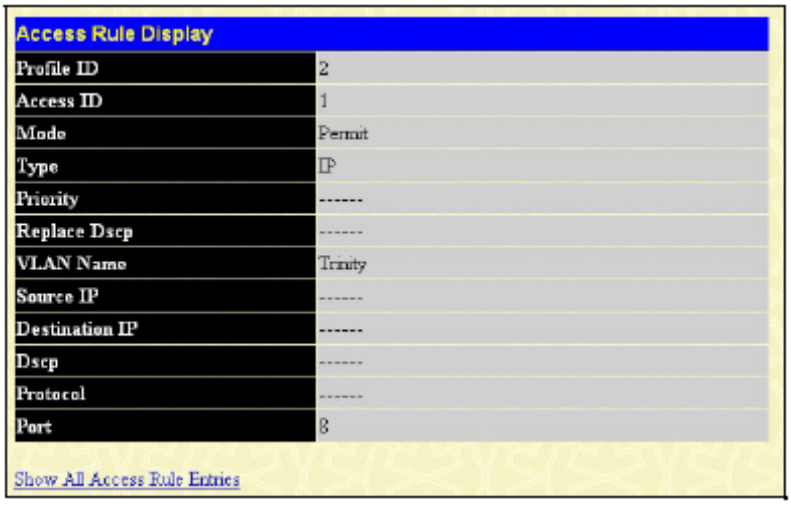


Рисунок 10.11 – Окно «Access Rule Display (IP)»

Для настройки правила доступа для Ethernet-профиля, откройте окно **Access Profile Table** (рисунок 10.5) и нажмите **Add** для добавления Ethernet-профиля доступа, после чего откроется приведенное ниже окно.
Для настройки правила доступа для **Packet Content Mask**, откройте таблицу **Access Profile Table** и для изменения **Packet Content Mask** нажмите **Modify**, что приведет к открытию данного окна:

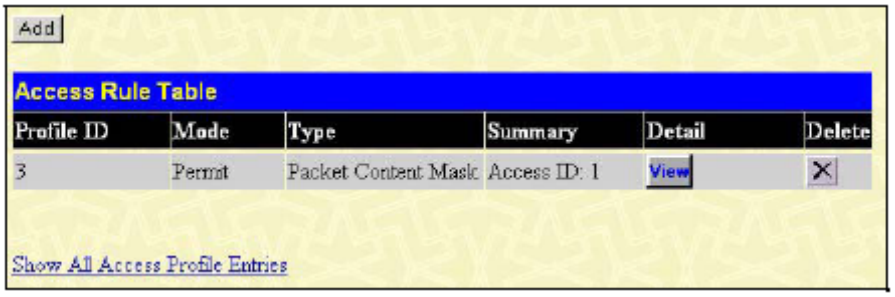


Рисунок 10.12 – Окно «Access Rule Table (Packet Content Mask)»

Для удаления ранее созданного правила, нажмите на соответствующую кнопку. Для добавления правила доступа, нажмите кнопку **Add**.

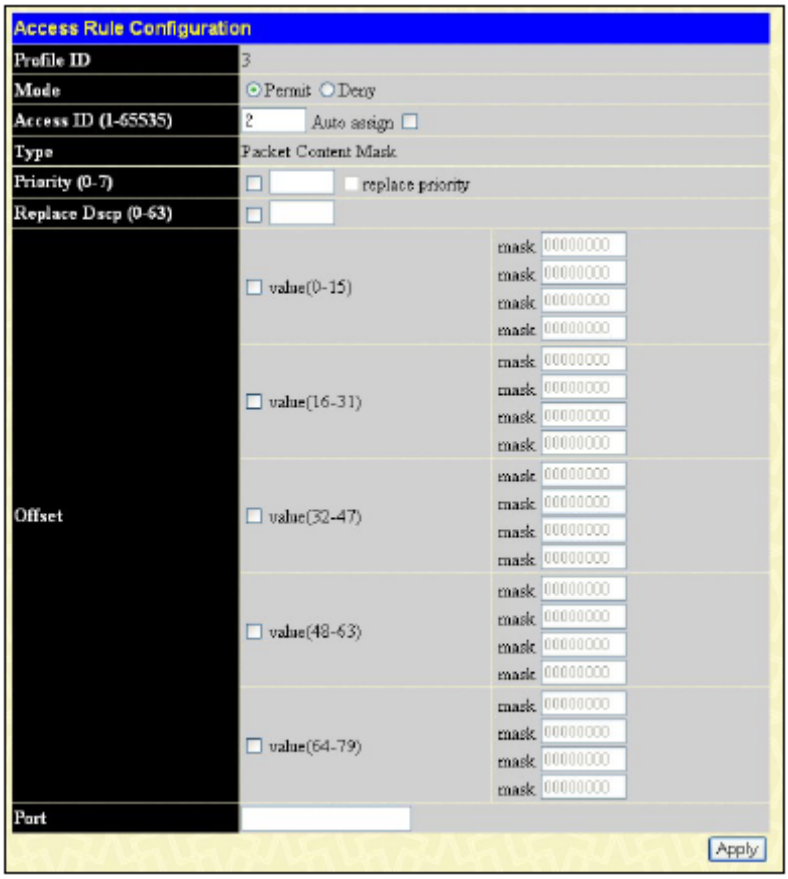


Рисунок 10.13 – Окно «Access Rule Configuration – Packet Content Mask»

Для установки правила доступа для **Packet Content Mask** настройте следующие параметры и нажмите **Apply**.

Параметр	Описание
Profile ID	Идентификатор установленного профиля.
Mode	**Permit** - указывает на то, что пакет, который соответствует профилю будет принят и передан коммутатором в соответствии с дополнительным правилом (см. ниже). **Deny** – указывает на то, что пакет, который соответствует профилю, будет отброшен коммутатором.
Access ID	Введите значение идентификатора доступа в диапазоне от 1 до 65535. ▪ **Auto Assign** – подключите данную опцию для автоматического назначения коммутатором идентификатора доступа для создаваемого правила.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
Priority (0-7)	Этот параметр задаётся, если пользователь хочет изменить приоритет по умолчанию 802.1p, предварительно установленный на коммутаторе,

	для определения CoS очереди, в которую будут отправляться пакеты. При заполнении заданного поля, принятые коммутатором пакеты, в соответствии с их приоритетом направляются в очередь CoS, предварительно определённую пользователем. *Replace priority with* - следует поставить отметку в данном поле, если необходимо изменить приоритет 802.1p, установленный по умолчанию, на значение поля Priority (0-7), который будет задействован при отправке пакетов в очередь CoS. В противном случае пакеты будут со своим первоначальным 802.1p приоритетом. Для получения большей информации об очередях приоритетов, очередях CoS и настроек 802.1p, следует обратиться к разделу QoS данного руководства.
Offset	Это поле указывает, что необходимо сравнить начало заголовка пакета с указанным значением: ▪ value (0-15) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить первые 15 байт пакета. ▪ value (16-31) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 16 по 31 байт пакета. ▪ value (32-47) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 32 по 47 байт пакета. ▪ value (48-63) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 48 по 63 байт пакета. ▪ value (64-79) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 64 по 79 байт пакета.
Port	В данном поле введите номер порта для настройки правила доступа на основе портов. В случае настройки диапазона портов необходимо подключить функцию **Auto Assign** в поле Access ID, если данная опция не будет подключена, появится сообщение об ошибке и будет невозможно установить правило доступа. Начало и конец диапазона портов отделяются тире. Например, 3 означает третий порт, 2-4 означает диапазон портов со 2 по 4.

Для просмотра настроек ранее настроенного правила, нажмите  в таблице **Access Rule Table**:

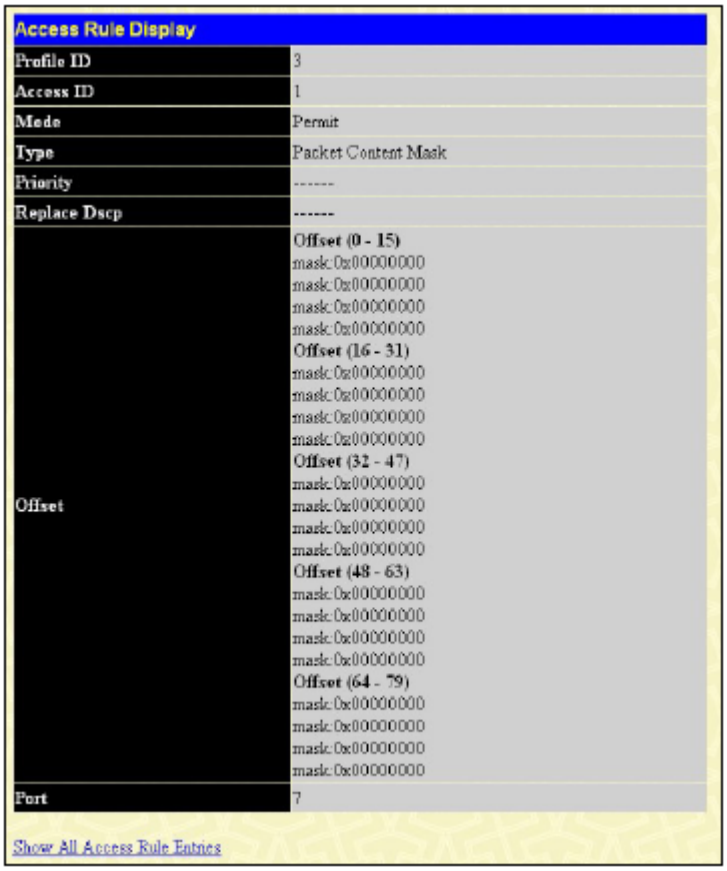


Рисунок 10.14 – Окно «Access Rule Display (Packet Content Mask)»

Фильтрация CPU-интерфейса

Вследствие ограниченных возможностей микросхем и потребностей в дополнительной безопасности коммутатора, в коммутаторы серии xStack DES-3800 включена функция CPU Interface filtering. Эта добавленная функция улучшает существующую безопасность коммутатора благодаря возможности создавать пользователем список правил доступа для пакетов, предназначенных для CPU interface коммутаторов. Похожей опцией является функция профиля доступа, упоминаемая ранее, функция CPU Interface filtering проверяет соответствующие Ethernet, IP и Packet Content Mask заголовки пакетов, предназначенных для CPU, после чего решается вопрос их доставки или же отбрасывания пакетов на основе решения пользователя. Механизм фильтрации CPU можно включать и отключать, пользователь может создавать различные списки правил не включая их немедленно в работу. Создание профиля доступа для CPU делится на две основные части:

1. указать, какую часть или части кадра будет проверять коммутатор, например, MAC-адрес источника или IP-адрес назначения.
2. ввод условия, которое коммутатор будет использовать для определения действий над кадром (принять или отбросить).

Весь процесс описывается ниже.

Таблица профилей CPU Interface Filtering

Для отображения созданных записей в таблице **CPU Access Profile Table** нажмите **ACL ⇨ CPU Interface Filtering ⇨ CPU Interface Filtering Table.** Для просмотра настроек нажмите на гиперссылку номера **Profile ID**.

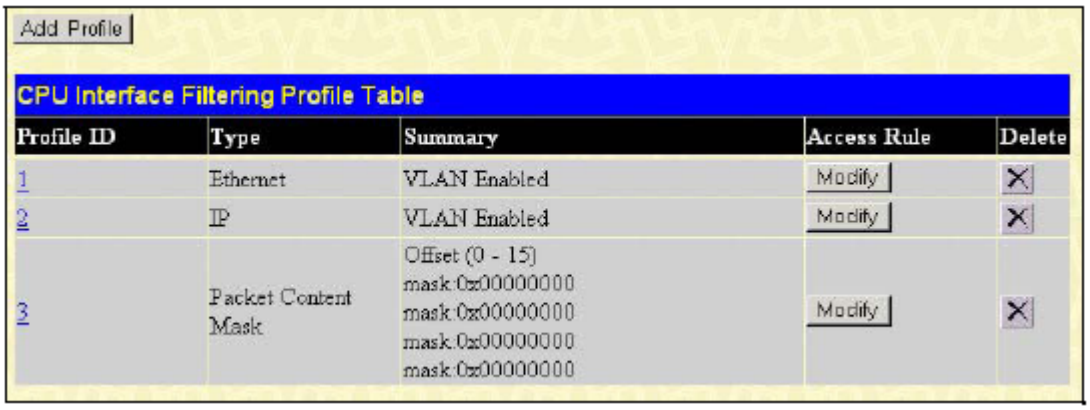


Рисунок 10.15 – Окно «CPU Interface»

Для добавления записи в таблицу **CPU Interface Filtering Profile Table** нажмите кнопку **Add**, после чего откроется представленное ниже окно **CPU Interface Filtering Profile Configuration**. Существует три окна **CPU Access Profile Configuration**: одно для настройки **Ethernet** профиля (на основе MAC-адреса), одно для настройки **IP** профиля и одно для настройки **Packet Content Mask**, между этими окнами можно переключаться с помощью поля **Type**. Ниже приведено окно **Ethernet CPU Interface Filtering Configuration**.

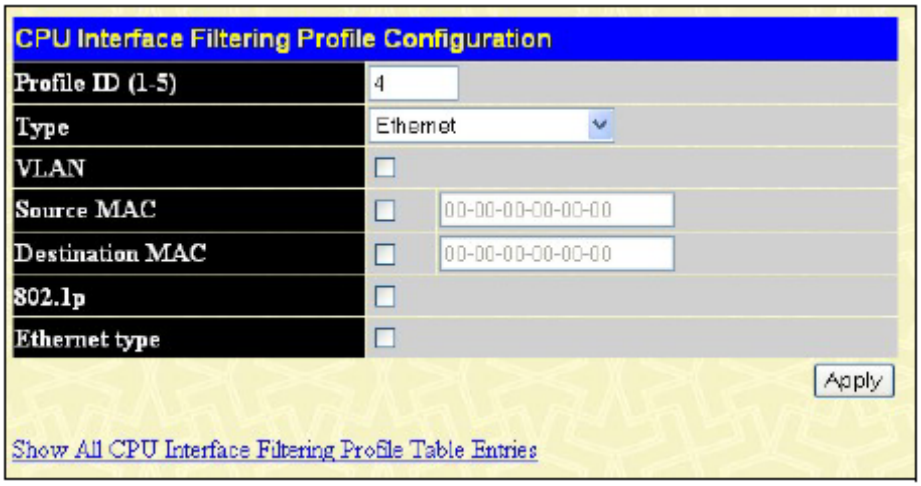


Рисунок 10.16 – Окно «CPU Interface Filtering Profile Configuration - Ethernet»

Параметры	Описание
Profile ID (1 - 5)	Идентификатор установленного профиля. Можно ввести значение от 1 до 5.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
VLAN	При выборе данной опции, коммутатор будет проверять идентификатор ID в заголовке каждого пакета, используя его в качестве полного или частичного условия для принятия решения о передаче пакета.
Source MAC	Введите MAC-адрес источника.
Destination MAC	Введите маску MAC-адреса назначения.
802.1p	Введите значение приоритета 802.1p от 0 до 7, в результате чего профиль доступа будет применяться только к пакетам с установленным приоритетом.
Ethernet Type	При выборе данной опции коммутатор будет проверять в заголовках каждого кадра поле Ethernet type.

Для сохранения выполненных настроек нажмите **Apply**.

Ниже приведено окно **CPU Interface Filtering Configuration** для **IP** профиля.

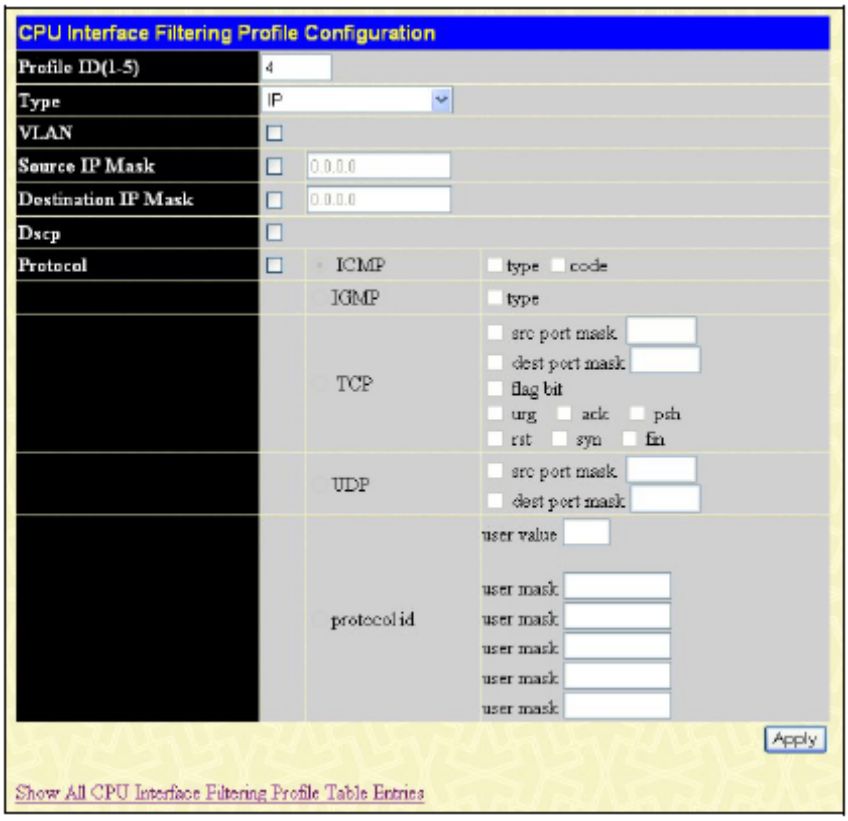


Рисунок 10.17 – Окно «CPU Interface Filtering Configuration - IP»

Параметр	Описание
Profile ID	Введите идентификатор профиля из диапазона 1 – 5.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
VLAN	Выбрав данную опцию, коммутатор будет проверять идентификатор VLAN в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Source IP Mask	Введите маску IP-адреса источника.
Destination IP Mask	Введите маску IP-адреса назначения.
DSCP	Выбрав данную опцию, коммутатор будет проверять поле DiffServ Code в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Protocol	Выбрав данную опцию, коммутатор будет проверять значение типа протокола в заголовке каждого пакета. Вам необходимо выбрать протокол(ы) в соответствии со следующими рекомендациями: Выберите **ICMP** для того, чтобы коммутатор проверял поле протокола управляющих сообщений в Интернете (Internet Control Message Protocol) в заголовке каждого пакета. ▪ Выберите по значению типа **Type** или кода **Code** протокола ICMP будет применяться профиль доступа. Выберите **IGMP** для того, чтобы коммутатор проверял поле межсетевого

	протокола управления группами (Internet Group Management Protocol) в заголовке каждого пакета. ▪ Выберите тип **Type** IGMP, по которому будет формироваться профиль доступа При выборе протокола **TCP** в качестве условия указывается номер порта. Можно использовать или маску порта источника, или/и маску порта назначения. Для фильтрации пакетов по битам флага пользователю нужно сделать отметку в соответствующем поле flag bits. По битам флага пакета определяется действие, которое нужно выполнить с этим пакетом: **urg** (urgent) , **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) , **fin** (finish). ▪ **src port mask** – задайте маску TCP порта источника в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. ▪ **dest port mask** – задайте маску TCP порта назначения в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. При выборе протокола UDP в качестве условия указывается номер UDP порта. Можно использовать или маску порта источника, или/и маску порта назначения. ▪ **src port mask** – задайте маску TCP порта источника в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. ▪ **dest port mask** – задайте маску TCP порта назначения в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. **protocol id** – введите значение, определяющее идентификатор протокола в заголовке пакета. Задайте маску идентификатора протокола в шестнадцатеричной системе счисления (hex 0x0-0xffff) или значение пользователя.

Для сохранения настроек нажмите **Apply**.

Окно **CPU Interface Filtering Profile Configuration ,** приведенное ниже – окно для **Packet Content Mask** .

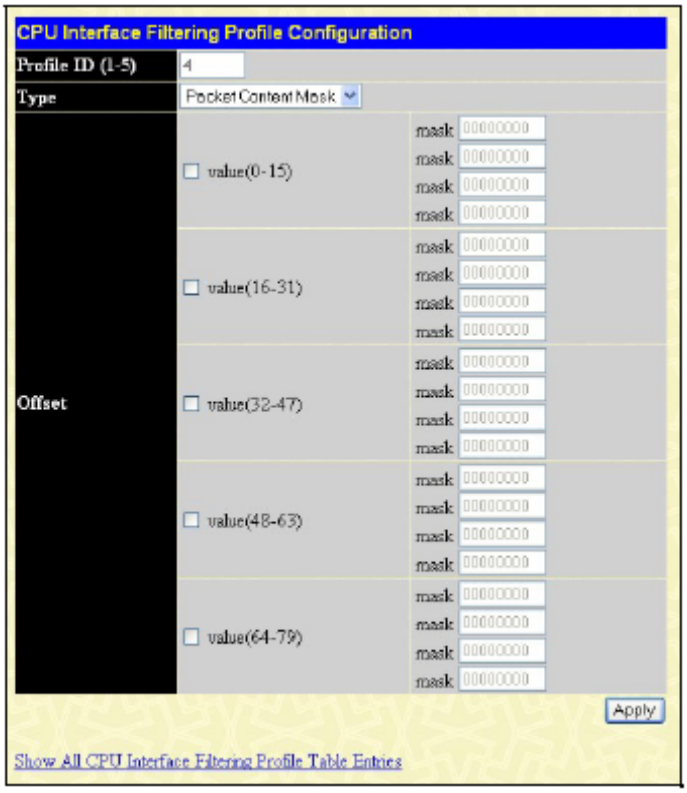


Рисунок 10.18 – Окно «CPU Interface Filtering Configuration – Packet Content»

Это окно поможет пользователю в настройке коммутатора, чтобы скрыть начало заголовка пакета с заданным значением смещения. Следующие поля используются для настройки маски содержимого пакета.

Параметр	Описание
Profile ID	Введите идентификатор профиля из диапазона 1 – 5.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
Offset	Это поле указывает, что необходимо сравнить начало заголовка пакета с указанным значением: ▪ value (0-15) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить первые 15 байт пакета. ▪ value (16-31) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 16 по 31 байт пакета. ▪ value (32-47) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 32 по 47 байт пакета. ▪ value (48-63) - Введите значение в шестнадцатеричной

	системе счисления, с которым нужно сравнить с 48 по 63 байт пакета. ▪ value (64-79) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 64 по 79 байт пакета.

Для того чтобы настройки вступили в силу, кликните по кнопке **Apply**.

Для формирования правила ранее созданного CPU Access Profile:

Для открытия **CPU Interface Filtering Profile Table** нажмите **ACL ⇨ CPU Interface Filtering.**

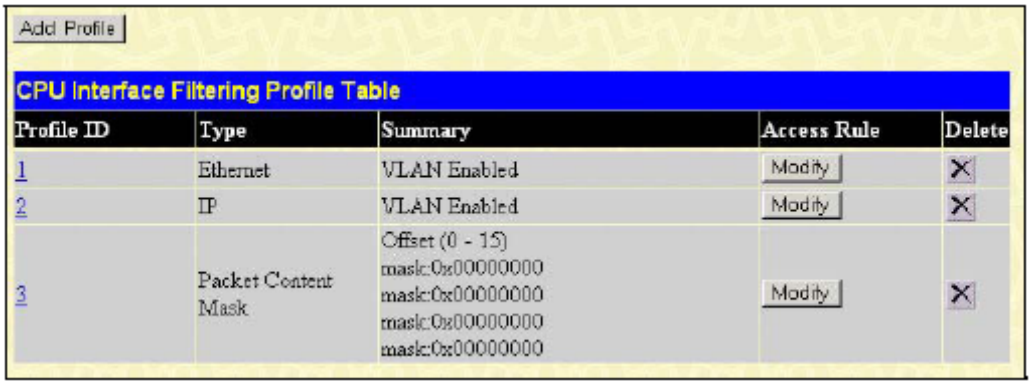


Рисунок 10.19 – Окно «CPU Interface Filtering Profile Table - Add»

В данном окне пользователь может добавить правило к ранее созданному CPU профилю доступа путем нажатия на кнопку **Add Rule** для настройки **Ethernet, IP** или **Packet Content Mask**.

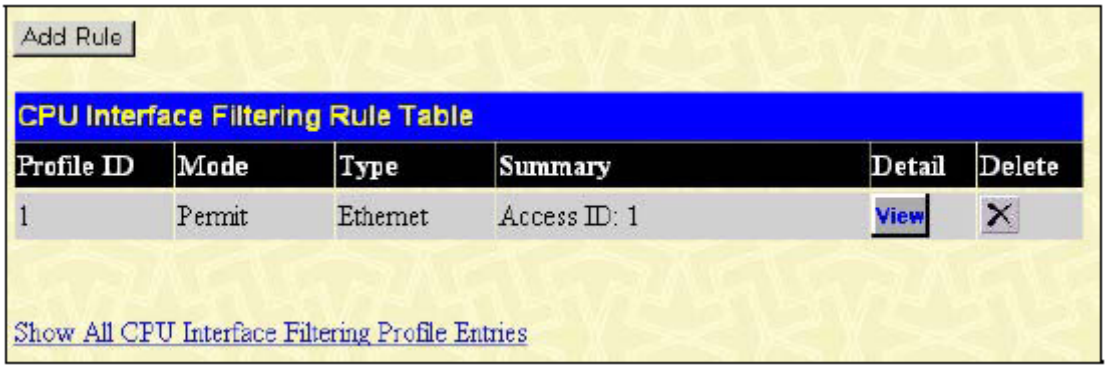


Рисунок 10.20 – Окно «CPU Interface Filtering Rule Table»

Для возвращения к окну **CPU Interface Filtering Rule Table** нажмите **Add Rule**, после чего появится обновленное окно для **Ethernet, IP** и **Packet Content** профилей.

Дли изменения правила ранее созданного CPU Access Profile Rule.

В данном окне пользователь может изменить правило, установленное ранее, путем нажатия на соответствующую кнопку **Modify**.

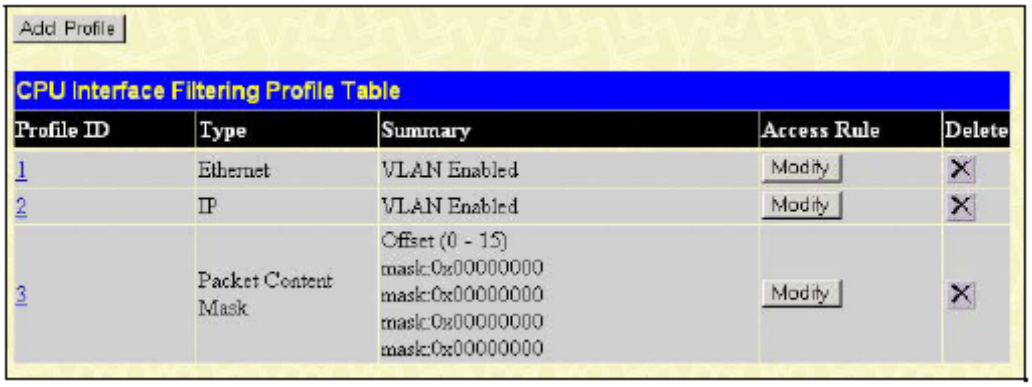


Рисунок 10.21 – Окно «CPU Interface Filtering Profile Table - Modify»

Откроется окно CPU Interface Rule Table, для просмотра ранее созданного правила нажмите View или ✕ для удаления.

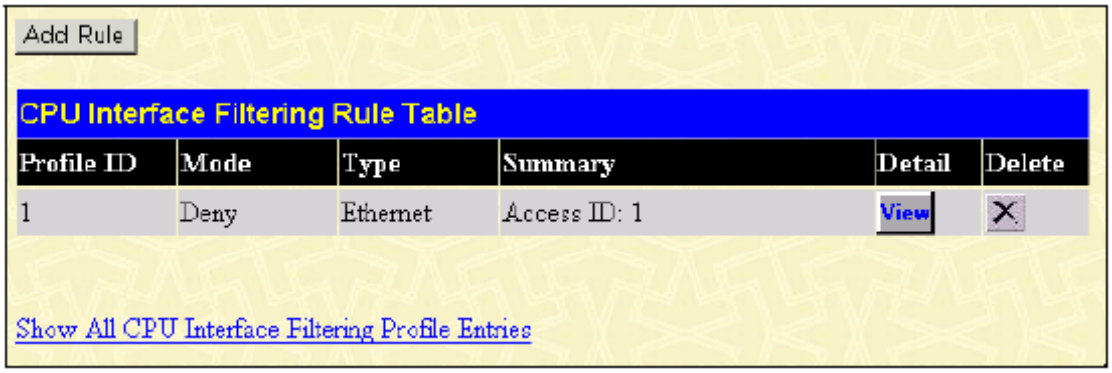


Рисунок 10.22 – Окно «CPU Interface Filtering Rule Table - Ethernet»

В окне **CPU Interface Filtering Rule Configuration** пользователь может настроить правило для ранее созданного CPU профиля доступа.

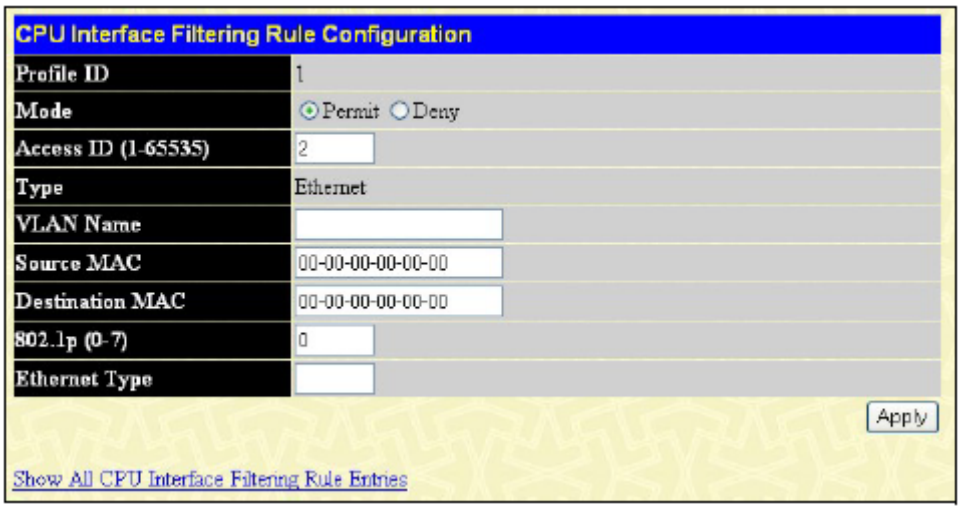


Рисунок 10.23 - Окно «CPU Interface Filtering Rule Configuration - Ethernet»

Для установки CPU правила доступа для Ethernet-профиля настройте следующие параметры и кликните **Apply**.

Параметры	Описание
Profile ID	Идентификатор установленного профиля.
Mode	**Permit** - указывает на то, что пакет, который соответствует профилю будет принят и передан коммутатором в соответствии с дополнительным правилом (см. ниже). **Deny** – указывает на то, что пакет, который соответствует профилю будет отброшен коммутатором.
Access ID	Введите значение идентификатора доступа в диапазоне от 1 до 65535.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
VLAN Name	Имя ранее настроенной VLAN.
Source MAC	Введите MAC-адрес источника.
Destination MAC	Введите маску MAC-адреса назначения.
802.1p	Введите значение приоритета 802.1p от 0 до 7, в результате чего профиль доступа будет применяться только к пакетам с установленным приоритетом.
Ethernet Type	Профиль доступа будет определяться только к пакетам с шестнадцатиричным значением поля Ethernet type (hex 0x0-0xffff) в заголовке пакета. Значение Ethernet type должно быть приведено в виде hex 0x0-0xffff, т.е. пользователь может выбрать любую комбинацию из букв (a - f) и цифр (0 - 9999).

Для просмотра ранее настроенного правила нажмите View в **Access Rule Table:**

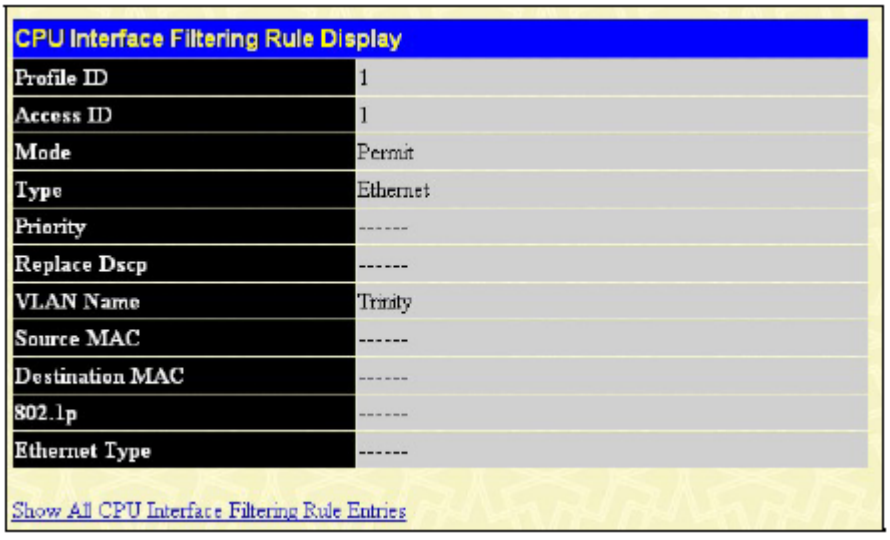


Рисунок 10.24 – Окно «CPU Interface Filtering Rule Display - Ethernet»

Следующее окно **CPU Interface Filtering Rule Table** касается IP-профиля.

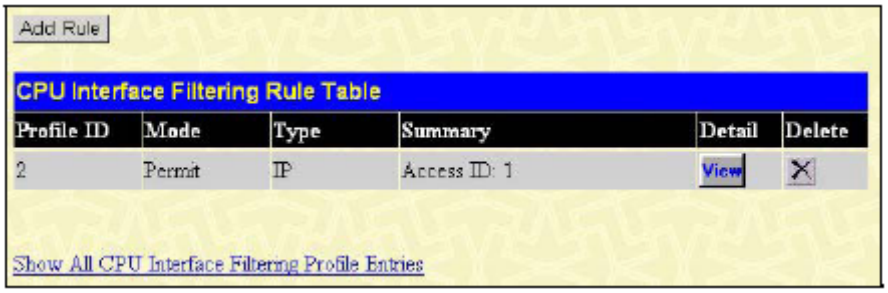


Рисунок 10.25 – Окно «CPU Interface Filtering Table - IP»

Для создания нового правила для профиля доступа нажмите кнопку **Add**. Для удаления ранее созданного правила нажмите кнопку . Следующее окно используется для настройки IP правила CPU.

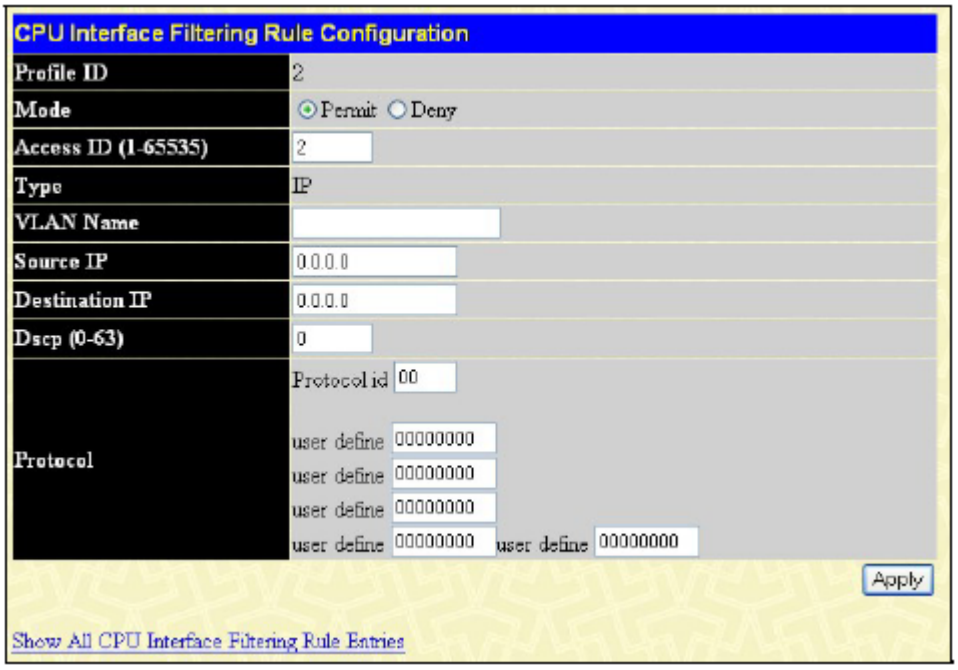


Рисунок 10.26 – Окно «CPU Interface Filtering Rule Configuration - IP»

Параметр	Описание
Profile ID	Идентификатор установленного профиля.
Mode	**Permit** - указывает на то, что пакет, который соответствует профилю, будет принят и передан коммутатором в соответствии с дополнительным правилом (см. ниже). **Deny** – указывает на то, что пакет, который соответствует профилю будет отброшен коммутатором.
Access ID	Введите значение идентификатора доступа в диапазоне от 1 до 65535.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску

	содержимого пакета *Packet Content Mask.*
VLAN Name	Имя ранее настроенной VLAN.
Source IP	Введите маску IP-адреса источника.
Destination IP	Введите маску IP-адреса назначения.
Dscp (0-63)	Введите значение DSCP от 0 до 63, после чего коммутатор будет проверять поле DiffServ Code в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.
Protocol	Данное поле позволяет пользователю изменять протокол, используемый для настройки **Access Rule Table** в зависимости от выбранного протокола в **Access Profile Table**.

Для просмотра ранее настроенного правила нажмите View в таблице **Access Rule Table**.

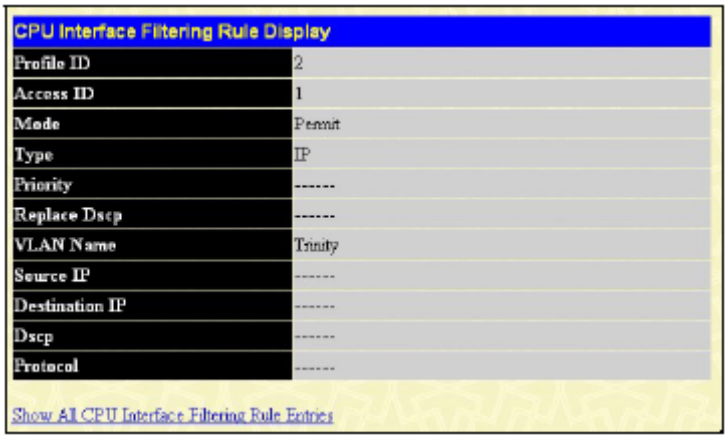


Рисунок 10.27 – Окно «CPU Interface Filtering Rule Display - IP»

Следующее окно **CPU Interface Rule Table** представляет собой таблицу правил CPU Interface для содержимого пакетов.

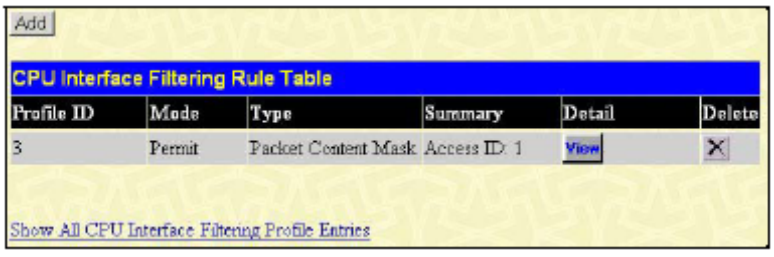


Рисунок 10.28 – Окно «CPU Interface Filtering Rule Table – Packet Content»

Для удаления ранее созданного правила выберите его и нажмите клавишу ✕. Для добавления нового правила доступа CPU нажмите кнопку **Add**.

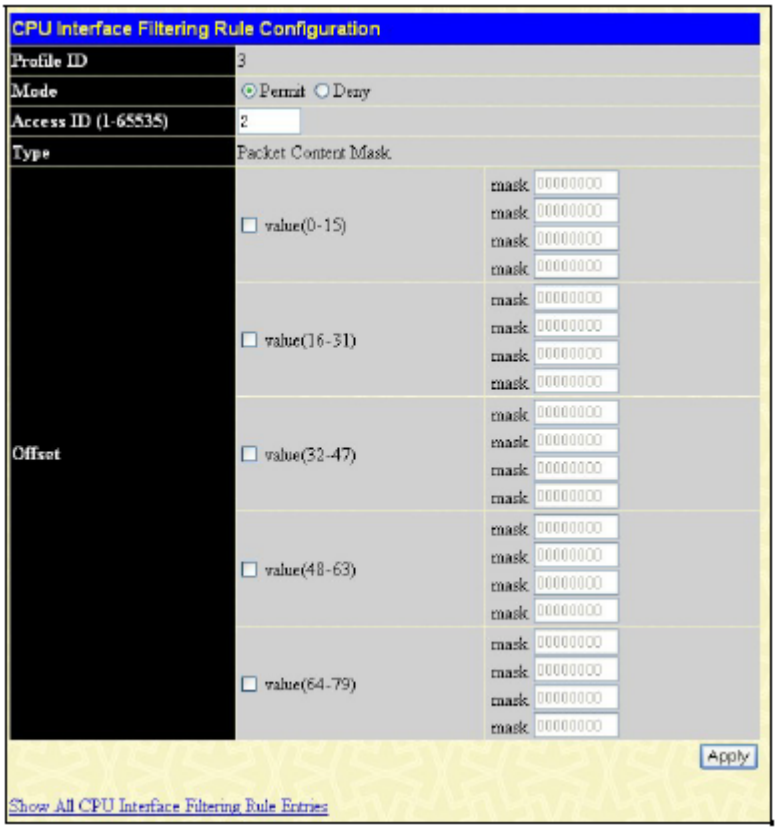


Рисунок 10.29 – Окно «CPU Interface Filtering Rule Configuration - Packet Content Mask»

Параметр	Описание
Profile ID	Идентификатор установленного профиля.
Mode	**Permit** - указывает на то, что пакет, который соответствует профилю будет принят и передан коммутатором в соответствии с дополнительным правилом (см. ниже). **Deny** – указывает на то, что пакет, который соответствует профилю, будет отброшен коммутатором.
Access ID	Введите значение идентификатора доступа в диапазоне от 1 до 65535.
Type	Выберите какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. ▪ При выборе *Ethernet* коммутатор будет проверять заголовок каждого пакета на 2 уровне. ▪ При выборе *IP* коммутатор будет проверять IP-адрес в заголовке каждого пакета. ▪ Для скрытия данных заголовка пакета установите маску содержимого пакета *Packet Content Mask.*
Offset	Это поле указывает, что необходимо сравнить начало заголовка пакета с указанным значением: ▪ value (0-15) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить первые 15 байт пакета. ▪ value (16-31) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 16 по 31 байт пакета. ▪ value (32-47) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 32 по 47

	байт пакета. ▪ value (48-63) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 48 по 63 байт пакета. ▪ value (64-79) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 64 по 79 байт пакета.

Для просмотра ранее настроенного правила нажмите View в таблице **Access Rule Table**.

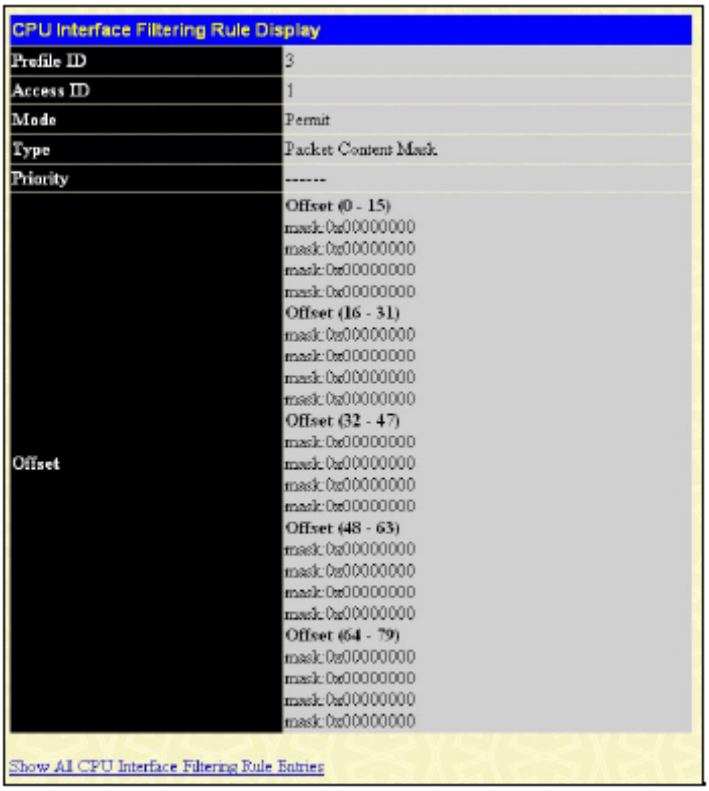


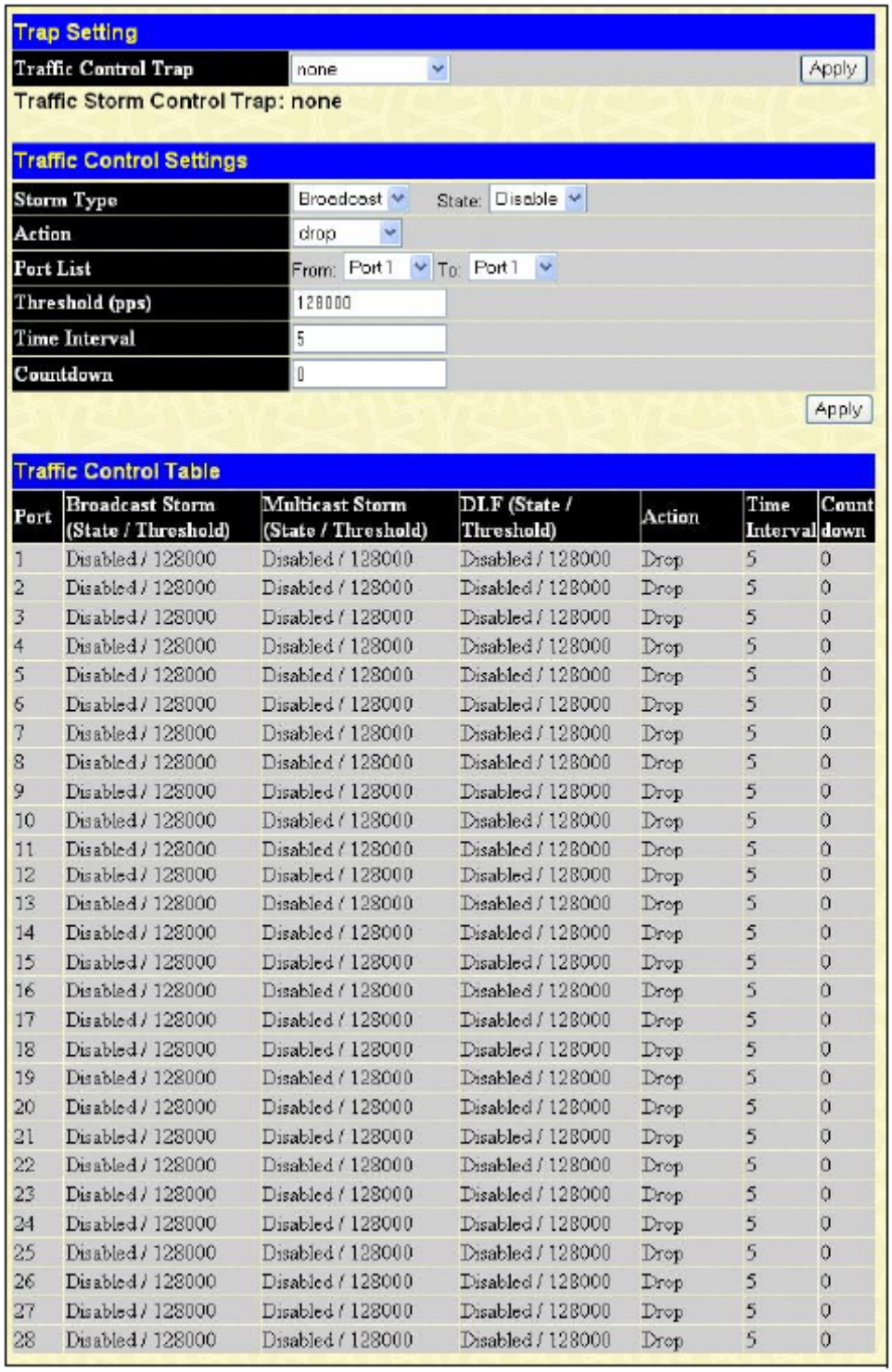
Рисунок 10.30 – Окно «CPU Interface Filtering Rule Display – Packet Content»

Раздел 11 - Безопасность

Управление трафиком
Port Security
Port Lock Entries
802.1X
Trusted Host
Access Authentication Control
Сегментация трафика
SSL
SSH
Связка IP MAC
Limited IP Multicast Range Settings
Конфигурация WAC
Safeguard Engine

Управление трафиком

Общеизвестно, что многоадресные и широковещательные пакеты создают существенную нагрузку на сеть. Порой объемы такого трафика могут возрастать вследствие злонамеренных действий или неисправного устройства (например, сетевого адаптера). Таким образом, возникают проблемы пропускной способности коммутатора, которые в свою очередь влияют на общие характеристики коммутируемой сети. Поэтому очень важно, чтобы коммутатор был оснащен функциями, позволяющими успешно бороться с пакетным штормом. Коммутатор определяет пакетный шторм, если превышен установленный пользователем порог количества многоадресных и широковещательных пакетов. При обнаружении пакетного шторма коммутатор начинает отбрасывать поступающие на него пакеты, периодически проверяя, не снизилось ли количество многоадресных и широковещательных пакетов ниже порогового значения. Данный метод может быть использован при выборе опции **Drop** в поле **Action** в представленном ниже окне. Коммутатор также сканирует и контролирует поступающие на него пакеты благодаря счетчику микросхемы. Данный метод актуален только для широковещательных или многоадресных штормов, поскольку в микросхеме есть счетчики только этих пакетов. При обнаружении шторма (при превышении порогового уровня пакетов) коммутатор отключит порт для всего входящего трафика за исключением пакетов STP BPDU в течение указанного периода времени в поле **CountDown**. Если по истечении отведенного времени пакетный шторм продолжается, порт будет переведен в режим постоянного отключения ShutDown Forever, при этом получателю Trap будет отправлено предупреждающее сообщение. Подключение отключенного ShutDown Forever порта можно осуществить только при помощи ручной настройки в окне **Port Configuration ⇨ Administration,** установив состояние Enable. Для использования данного метода контроля за штормом выберите опцию **Shutdown** в поле **Action** окна **Traffic Control Settings,** представленного ниже. Для его открытия нажмите **Security ⇨ Traffic Control**.



Port	Broadcast Storm (State / Threshold)	Multicast Storm (State / Threshold)	DLF (State / Threshold)	Action	Time Interval	Countdown
1	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
2	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
3	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
4	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
5	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
6	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
7	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
8	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
9	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
10	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
11	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
12	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
13	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
14	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
15	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
16	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
17	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
18	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
19	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
20	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
21	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
22	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
23	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
24	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
25	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
26	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
27	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0
28	Disabled / 128000	Disabled / 128000	Disabled / 128000	Drop	5	0

Рисунок 6.56 – Окно « Traffic Control Settings and Traffic Control Table»

Пользователь может установить следующие параметры:

Параметр	Описание
	Trap setting (Настройки отправки сообщений trap)
Storm Trap	Отправка сообщений о широковещательном шторме будет осуществляться при выборе одной из следующих функций управления трафиком. *None* – Независимо от выполненного действия, предпринятого механизмом управления трафиком, сообщения с предупреждением о шторме отправляться не будут. *Storm Occurred* - сообщения с предупреждением о шторме будут

	отправлены только во время наступления шторма. *Storm Cleared* - сообщения о шторме будут отправлены только тогда, когда коммутатор справится со штормом. *Both* - сообщения о шторме будут отправлены тогда, когда коммутатор обнаружит и когда ликвидирует шторм. Данная опция не может быть реализована в аппаратном виде (когда в поле Action выбрана функция Drop).
Traffic Control Settings (Настройки управления трафиком)	
Storm Type	Выберите тип шторма для обнаружения Broadcast (широковещательный), Multicast (многоадресный) или DLF, после чего в соседнем поле с помощью выпадающего меню задайте состояние данной опции: подключено или выключено.
Action	С помощью выпадающего меню выберите метод управления трафиком: *Drop* – используется аппаратный механизм управления трафиком, при котором по пороговому значению определяется пакетный шторм, после чего поступающие пакеты будут отбрасываться, пока проблема не будет разрешена. *Shutdown* – используется программный механизм управления трафиком для определения пакетного шторма. Как только шторм будет обнаружен, порт не будет принимать входящие пакеты, за исключением STP BPDU пакетов, которые необходимы для работоспособности протокола Spanning Tree на коммутаторе. Если время, установленное в поле CountDown, истечет, а пакетный шторм будет продолжаться, порт перейдет в режим Shutdown Forever, т.е. будет отключен до тех пор, пока пользователь вручную не включит его в окне **Port Configuration** (папка **Administration**). Выбор этой опции обязывает пользователя выполнить настройки временного интервала таким образом, чтобы вовремя обнаружить пакетный шторм.
Port List	Выберите порты, которые можно вернуть в рабочее состояние после отключения ShutDown при помощи ручной настройки.
Threshold	Максимальное количество пакетов в секунду, при котором будет активизироваться функция управления трафиком. Возможные значения от 0 до 255000, значение по умолчанию -128000.
Time Interval	В данном поле устанавливается временной интервал между широковещательными (многоадресными) пакетами, при котором микросхема коммутатора запустит функцию управления трафиком. Эти пакетные счетчики являются определяющим фактором при решении, когда входящие пакеты превысили пороговое значение (Threshold**)**. Это поле может быть установлено в значение от 5 до 30 секунд, по умолчанию – значение равно 5 секунд.
Count Down	Количество времени, в минутах, которое коммутатор ожидает прежде, чем отключить порт, который находится под действием пакетного шторма. Данный параметр используется только для портов, у которых в настройках в поле **Action** установлено **Shutdown**, он не работает при аппаратной реализации управлением трафика. Возможные временные настройки для данного поля 0, 5-30 минут. Время, установленное по умолчанию, равно 0, т.е. порт будет немедленно отключен.

Для того чтобы настройки вступили в силу, кликните по **Apply**.

Примечание: Управление трафиком не может быть реализовано на портах, которые используются для объединения портов (образования агрегированных каналов)

Примечание: Порты, находящиеся в режиме постоянного отключения (Shutdown forever), будут показаны как Discarding (отвергающие) в окне Spanning Tree и через эти порты все еще будут пересылаться BPDU пакеты на CPU коммутатора.

Примечание: Порты, находящиеся в режиме постоянного отключения (Shutdown forever), будут показаны как отключенные (link down) во всех окнах и экранах, пока пользователь повторно не подключит эти порты.

Port Security

Динамическое изучение MAC-адресов для заданных портов (или диапазона портов) может быть заблокировано т.о., что текущие MAC-адреса, введённые в таблицу MAC-адресов, не смогут быть изменены до тех пор, пока блокировка порта активна. Используя поле Admin State, можно выбрать значение Enabled, кликнуть по Apply, тем самым закрыв порт.
Port Security – функция безопасности. которая предотвращает подключение к заблокированным портам коммутатора неавторизованных компьютеров (с MAC-адресами источников, неизвестными компьютеру до блокировки порта или портов) и получении ими доступа к сети.
Для просмотра следующего окна, откройте папку **Security** и нажмите **Port Security**.

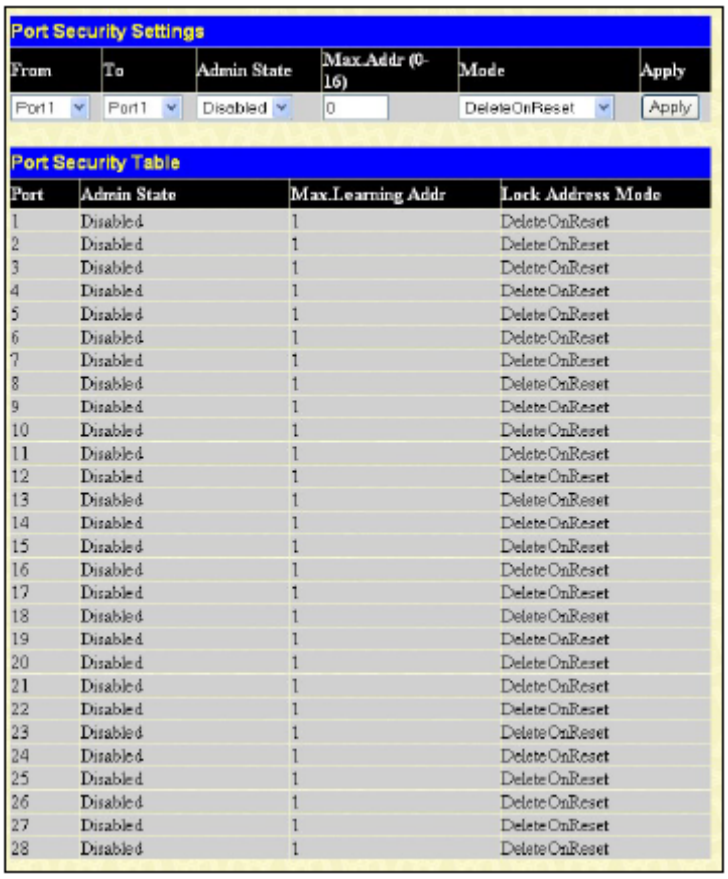


Рисунок 11- 1. Окно Port Security Settings

From/To	Последовательная группа портов, которая начинается с отмеченного порта.
Admin State	Данное выпадающее меню позволяет включить/выключить функцию Port Security (открывает/закрывает таблицу MAC-адресов для помеченного порта).
Max. Learning Addr. (0-64)	Количество MAC-адресов, которые будут в таблице MAC-адресов для выбранного коммутатора и группы портов.
Lock Address Mode	Это выпадающее меню позволяет выбрать, каким образом таблица блокировки MAC-адресов будет работать на Коммутаторе для выбранной

	группы портов: *Permanent* – закрытые адреса не будут устаревать по истечении таймера. *DeleteOnTimeout* – закрытые адреса будут устаревать по истечении таймера. *DeleteOnReset* – закрытые адреса не будут устаревать до тех пор, пока Коммутатор не будет перегружен.

Для принятия настроек нажмите **Apply**.

Port Lock Entries

Окно Port Lock Entries используется для удаления записей port security, изученных коммутатором и введенных в пересылаемую базу данных. Для просмотра следующего окна, нажмите **Security > Port Lock Entries:**

Рисунок 11.2. Port Lock Entries Table

Эта функция применима только в том случае, если поле **Mode** в окне **Port Securit**y установлено в значение **Permanent** или **DeleteOnReset,** или, другими словами, могут быть удалены только те адреса, которые постоянно изучены коммутатором. Введенные ранее в окно, показанное выше, записи могут быть удалены, нажмите значок «x» под заголовком Delete, чтобы удалить соответствующий MAC-адрес. Нажмите кнопку «Next» для просмотра следующей страницы таблицы. В этом окне отображается следующая информация:

Параметр	Описание
VID	Идентификатор записи VLAN в таблице пересылаемой базы данных, который был постоянно изучен коммутатором.
VLAN NAME	Имя VLAN записи в таблице пересылаемой базы данных, которое было постоянно изучено коммутатором.
MAC Address	MAC-адрес записи в таблице пересылаемой базы данных, который был постоянно изучен коммутатором.
Port	Идентификатор порта, который был постоянно изучен коммутатором.
Type	Тип MAC-адреса в таблице пересылаемой базы данных. Только записи, отмеченные как *Secured_Permanent* могут быть удалены.
Delete	Нажмите значок «x» в этом поле, чтобы удалить соответствующий MAC-адрес, который был постоянно изучен коммутатором

PAE Access Entity (802.1X)

Аутентификация 802.1x на основе портов и MAC-адресов

Стандарт IEEE 802.1x обеспечивает безопасность при авторизации и аутентификации пользователей для получения доступа к различным проводным и беспроводным устройствам локальной сети, используя модель доступа, основанную на клиенте и сервере. Такая модель работает на основе RADIUS сервера, который производит аутентификацию пользователей, пытающихся получить доступ к сети, путем передачи пакетов протокола Extensible Authentication Protocol over LAN (EAPOL) между клиентом и сервером. Приведенный ниже рисунок демонстрирует структуру пакета EAPOL.

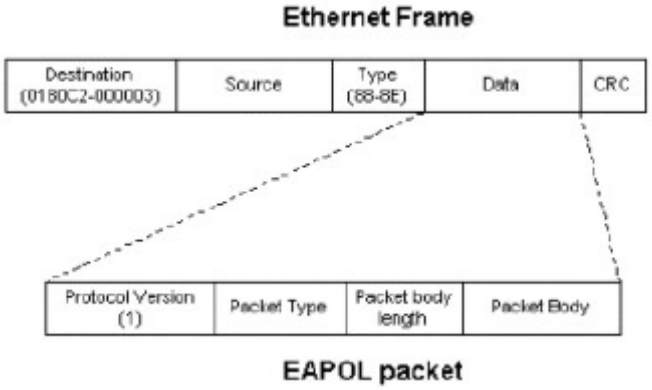


Рисунок 11.3 – Структура пакета EAPOL

Согласно данному методу неавторизованным устройствам будет запрещено подключение к локальной сети через порт, к которому присоединен пользователь. До момента авторизации через порт, к которому подключен пользователь, может проходить только трафик протокола EAPOL. Управление доступом по протоколу 802.1x включает в себя три компоненты, каждая из которых крайне важна для создания и использования устойчивого безопасного метода доступа к локальной сети.

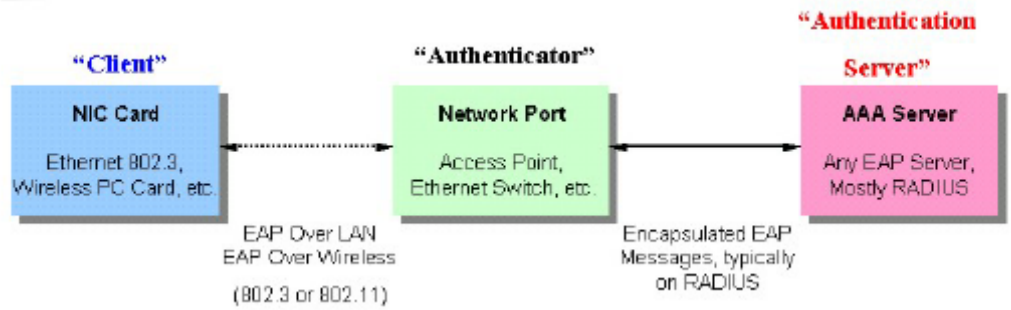


Рисунок 11.4 – Три функции протокола 802.1x

В следующем разделе дается подробное описание клиента, аутентификатора и сервера аутентификации.

Сервер аутентификации

Сервер аутентификации – это удаленное устройство, подключенное к той же сети, что и клиент, и коммутатор (аутентификатор - Authenticator), обслуживающееся RADIUS сервером и правильно настроенное на коммутаторе (Authenticator). Сервер аутентификации (RADIUS) должен производить аутентификацию клиентов, подключенных к портам коммутатора, до получения каких-либо сервисов, предоставляемых коммутатором в локальной сети. Серверу аутентификации необходимо проверять подлинность клиента, пытающегося получить доступ к сети, путем обмена секретной информацией между RADIUS сервером и клиентом с помощью пакетов EAPOL, и информировать коммутатор предоставлять или нет доступ к локальной сети и/или сервисам коммутатора.

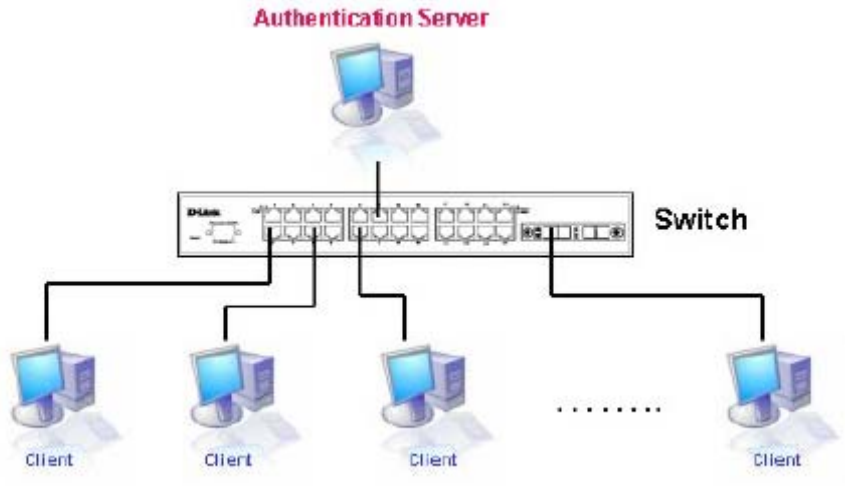


Рисунок 11.5 – Сервер аутентификации

Аутентификатор (Authenticator)

Коммутатор, который является аутентификатором, выполняет роль посредника между сервером аутентификации и клиентом. Аутентификатор выполняет две задачи при использовании протокола 802.1x: получает запрос на проверку подлинности от клиента посредством пакетов EAPOL и проверяет данную информацию при помощи сервера аутентификации, после чего пересылает ответ клиенту.

Для правильной настройки аутентификатора необходимо выполнить три шага.

1. Активировать 802.1x на устройстве **(DES-3800 Web Management Tool).**
2. Настроить 802.1x на портах **(Security ⇨ 802.1x ⇨ Configure 802.1x Authenticator Parameter).**
3. Настроить параметры сервера RADIUS **(Security ⇨ 802.1x ⇨ Authentic RADIUS Server).**

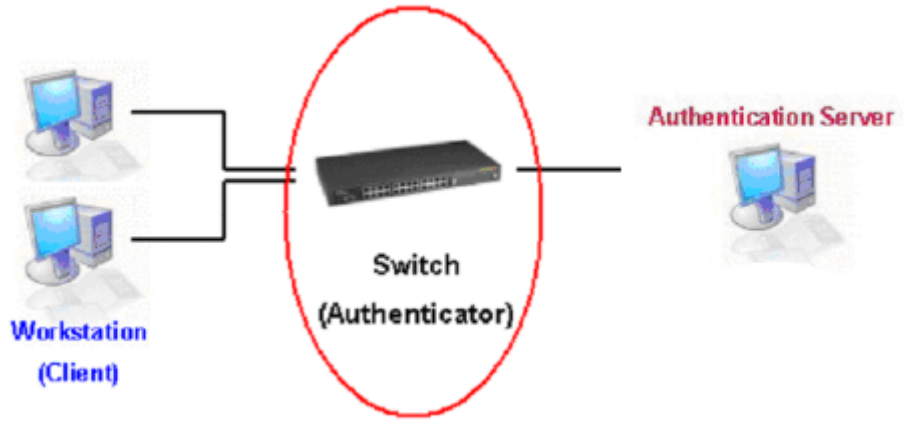


Рисунок 11.6 – Аутентификатор

Клиент

Клиент – это рабочая станция, которая запрашивает доступ к локальной сети или сервисам коммутатора. На всех рабочих станциях должно быть установлено программное обеспечение 802.1x. Для пользователей Windows XP, программное обеспечение уже встроено в операционную систему, пользователям других ОС придется установить ПО отдельно. Клиент запрашивает доступ к локальной сети или коммутатору при помощи пакетов EAPOL и отвечает на запросы коммутатора.

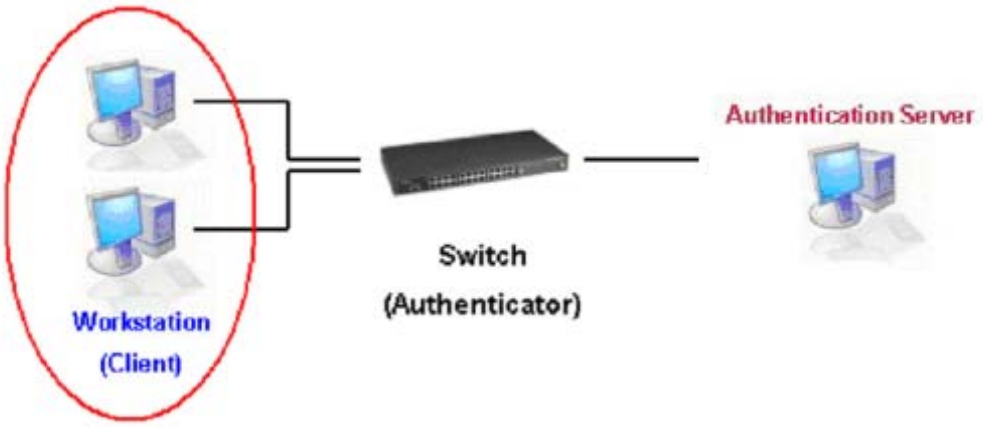


Рисунок 11.7 - Клиент

Процесс аутентификации

Используя три вида устройств, описанные выше, протокол 802.1x обеспечивает надежный и безопасный способ авторизации и аутентификации пользователей, пытающихся получить доступ к сети. До завершения аутентификации через назначенный порт коммутатора может проходить только EAPOL трафик. Порт находится в неавторизованном состоянии до тех пор, пока клиенту не будет разрешен доступ после введения правильного имени пользователя и пароля (MAC-адреса при аутентификации 802.1x на основе MAC-адресов), после чего он переходит в авторизованное состояние, позволяя передачу любого трафика через него. Приведенный ниже рисунок дает подробное описание процесса аутентификации, происходящего между тремя типами устройств.

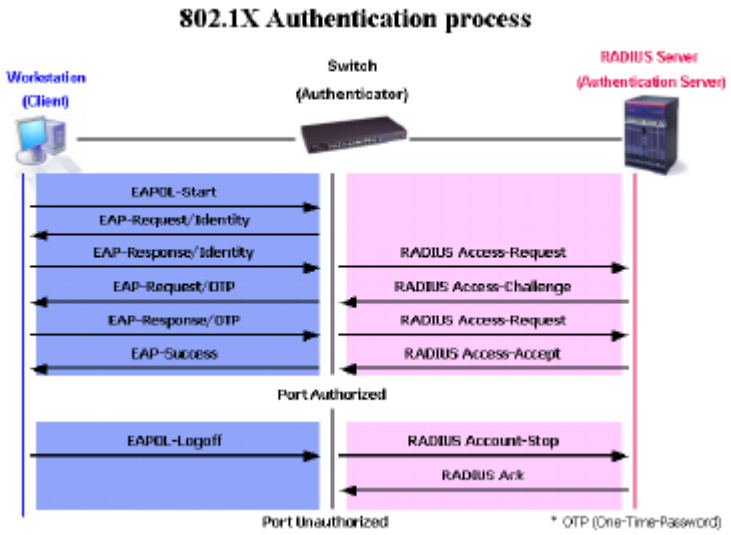


Рисунок 11.8 – Процесс аутентификации 802.1x

Реализация 802.1x на оборудовании D-Link дает возможность сетевым администраторам выбирать между двумя типами аутентификации:

1. Аутентификация на основе портов – данный метод требует аутентификации одного пользователя по порту на удаленном RADIUS сервере, после чего любой пользователь, подключенный к этому порту, может получить доступ к локальной сети.
2. Аутентификация на основе MAC-адресов – при данном методе коммутатор будет автоматически запоминать до трех MAC-адресов на порту и заносить их в список. Коммутатор, использующий удаленный RADIUS-сервер, должен аутентифицировать каждый MAC-адрес, прежде чем будет разрешен доступ к сети.

Понятие аутентификации 802.1x на основе портов и MAC-адресов

Основной целью создания стандарта 802.1x было усиление безопасности при соединении точка-точка в локальных сетях. Любой одиночный сегмент локальной сети содержит не более двух устройств, одним из которых является коммутатор, к портам которого и осуществляется подключение оборудования. Коммутатор отслеживает подключение активных устройств к каждому порту, а также переход устройства из активного состояния в неактивное. Данную деятельность можно использовать для управления за процессом авторизации порта и инициализации процедуры аутентификации подключенных устройств, в том случае, если порт находится в неавторизованном состоянии.

Аутентификация на основе портов

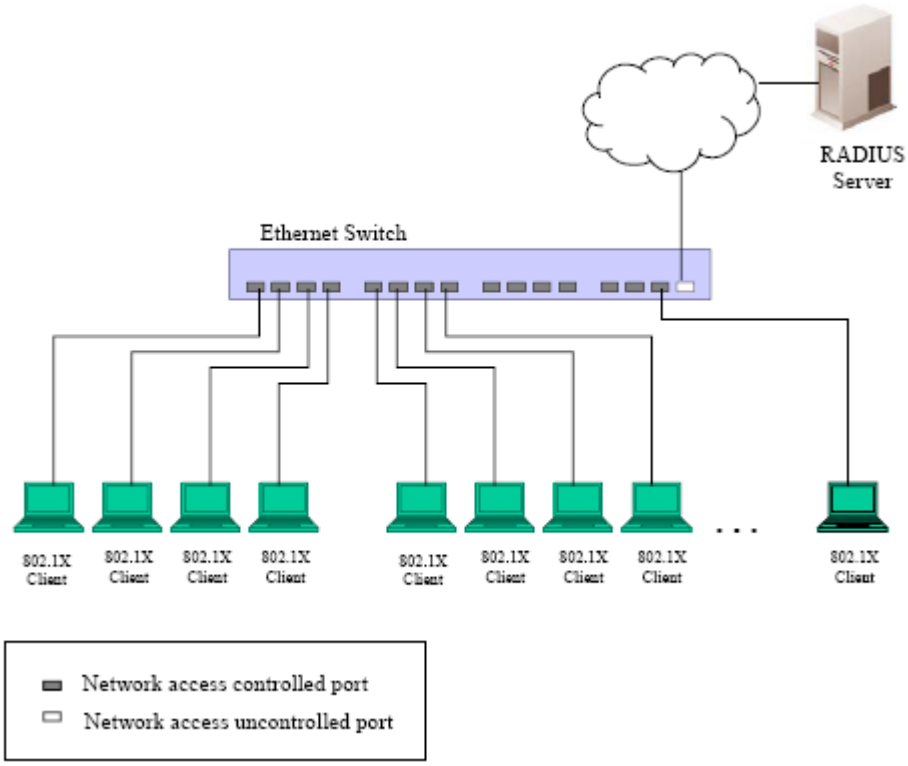


Рисунок 11.9 – Пример конфигурации сети на основе портов

В том случае, когда подключенный клиент благополучно авторизуется, порт перейдет в авторизованное состояние и весь дальнейший трафик будет беспрепятственно проходить через него, пока не произойдет событие, приводящее к смене состояния порта (из авторизованного в неавторизованное). Следовательно, если за портом находится сегмент сети с числом подключенных устройств более одного, то успешно произведенная аутентификация одного из них позволит всему оборудованию из данного сегмента получать доступ к локальной сети. Очевидно, что обеспечиваемая в данном случае безопасность подключения далека от совершенства.

Аутентификация на основе MAC-адресов

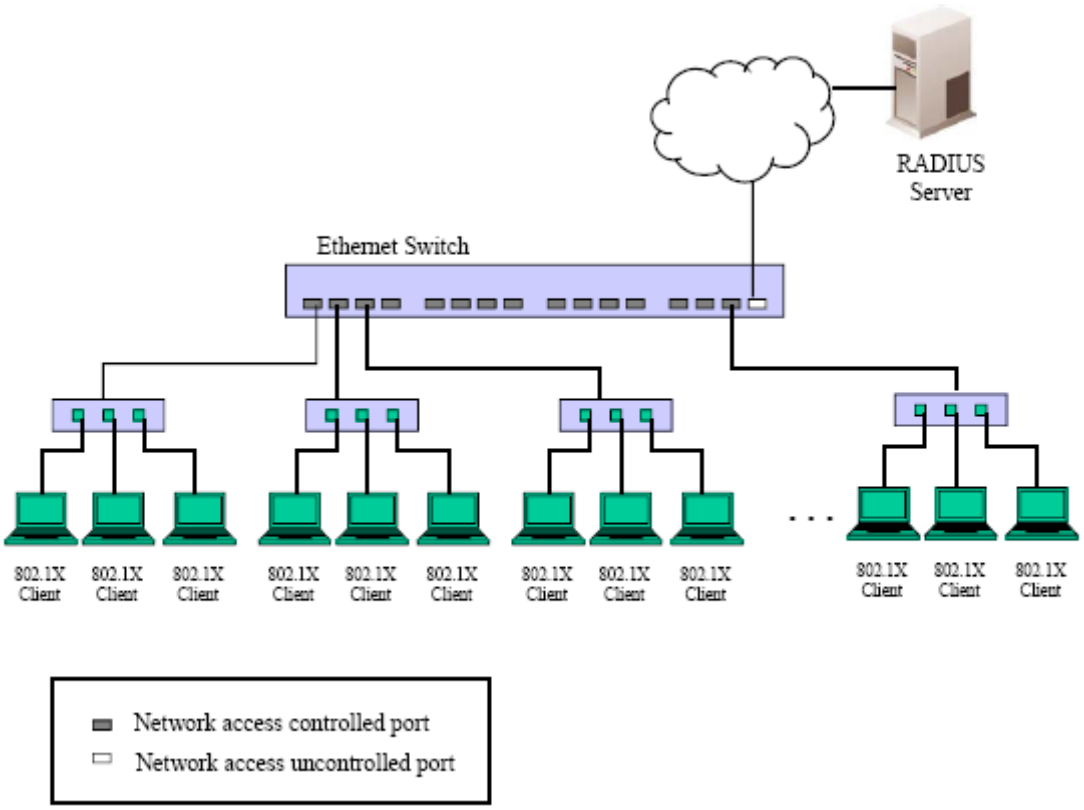
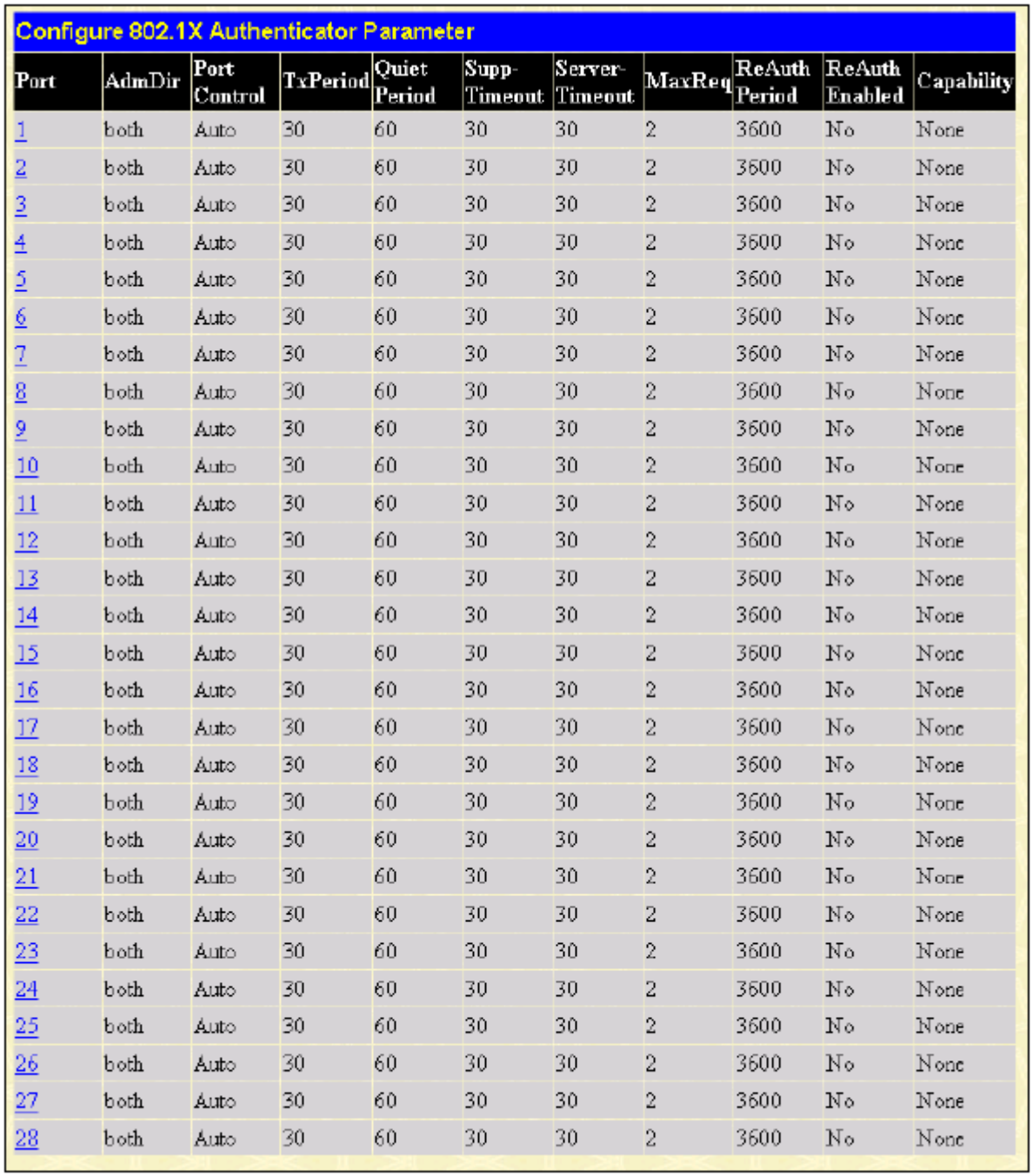


Рисунок 11.10 - Пример конфигурации сети на основе MAC-адресов

Для того чтобы успешно использовать протокол 802.1x в сегменте локальной сети, необходимо создать логические порты, по одному для каждого подключенного устройства, которому требуется доступ к локальной сети. Коммутатор, у которого за одним физическим портом находится сегмент сети, состоящий из определенного числа отдельных логических портов, будет производить контроль за каждым логическим портом с точки зрения изменений EAPOL и состояния авторизации. Коммутатор запоминает индивидуальный MAC-адрес каждого подключенного устройства и создает логический порт, через который будет производиться связь с локальной сетью.

Настройка аутентификатора

Для настройки аутентификатора по протоколу 802.1x, нажмите: **Security ⇨ Configure 802.1x Authenticator Parameter.**



Configure 802.1X Authenticator Parameter

Port	AdmDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled	Capability
1	both	Auto	30	60	30	30	2	3600	No	None
2	both	Auto	30	60	30	30	2	3600	No	None
3	both	Auto	30	60	30	30	2	3600	No	None
4	both	Auto	30	60	30	30	2	3600	No	None
5	both	Auto	30	60	30	30	2	3600	No	None
6	both	Auto	30	60	30	30	2	3600	No	None
7	both	Auto	30	60	30	30	2	3600	No	None
8	both	Auto	30	60	30	30	2	3600	No	None
9	both	Auto	30	60	30	30	2	3600	No	None
10	both	Auto	30	60	30	30	2	3600	No	None
11	both	Auto	30	60	30	30	2	3600	No	None
12	both	Auto	30	60	30	30	2	3600	No	None
13	both	Auto	30	60	30	30	2	3600	No	None
14	both	Auto	30	60	30	30	2	3600	No	None
15	both	Auto	30	60	30	30	2	3600	No	None
16	both	Auto	30	60	30	30	2	3600	No	None
17	both	Auto	30	60	30	30	2	3600	No	None
18	both	Auto	30	60	30	30	2	3600	No	None
19	both	Auto	30	60	30	30	2	3600	No	None
20	both	Auto	30	60	30	30	2	3600	No	None
21	both	Auto	30	60	30	30	2	3600	No	None
22	both	Auto	30	60	30	30	2	3600	No	None
23	both	Auto	30	60	30	30	2	3600	No	None
24	both	Auto	30	60	30	30	2	3600	No	None
25	both	Auto	30	60	30	30	2	3600	No	None
26	both	Auto	30	60	30	30	2	3600	No	None
27	both	Auto	30	60	30	30	2	3600	No	None
28	both	Auto	30	60	30	30	2	3600	No	None

Рисунок 11.11 – Окно «802.1X Authenticator Settings»

Для проведения настроек на порту, нажмите гиперссылку номера необходимого порта под заголовком «Port», после чего отобразится следующая таблица:

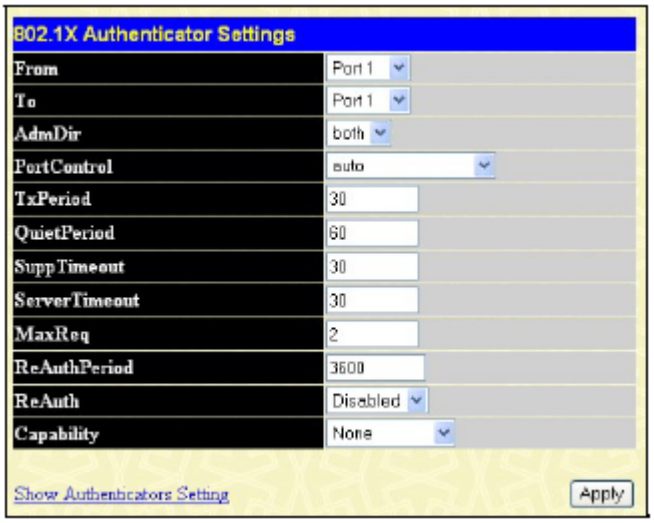


Рисунок 11.12 – Окно «802.1X Authenticator Settings - Modify»

Данное окно позволит вам произвести следующие настройки:

Параметр	Описание
From [ ] To [ ]	**Введите один порт или диапазон портов.**
AdmCtrlDir ***<both>***	**В данном поле вы можете выбрать вид трафика, подлежащего контролю.** **Если выбрано *in*, то будет производиться контроль входящего трафика, через выбранный в первом поле порт.** **Если выбрано *both,* то будет производиться контроль как входящего, так и исходящего трафика, через выбранный в первом поле порт.**
Port Control ***<Auto>***	**Данная настройка позволит контролировать состояние авторизации порта.** ***forceAuthorized* – протокол 802.1x будет отключен, что приведет к переходу порта в авторизованное состояние без обмена какими-либо аутентификационными сообщениями, т.е. через порт будет происходить передача двустороннего трафика без аутентификации клиента по протоколу 802.1x.** ***forceUnauthorized* – порт будет находиться в неавторизованном состоянии, игнорируя все попытки клиента аутентифицироваться. Коммутатор не сможет произвести аутентификацию клиента через данный интерфейс.** ***Auto* – протокол 802.1x будет подключен, в начале работы порт будет находиться в неавторизованном состоянии, через него возможно прохождение только EAPOL кадров. Процесс аутентификации начнется, когда будет наблюдаться активность канала на порту или после получения кадра EAPOL-start. Далее коммутатор идентифицирует клиента и начинает передачу аутентификационных сообщений между клиентом и сервером аутентификации.** **Настройка по умолчанию *Auto.***
TxPeriod ***<30>***	**Данное значение определяет период времени, который отводится для передачи пакетов запроса/идентификации (EAP Request/Identity) клиенту. По умолчанию данный параметр равен *30 секундам.***
QuietPeriod ***<60>***	**Время (в секундах), в течение которого коммутатор остается в режиме ожидания в том случае, если аутентификация не была пройдена. По умолчанию данный параметр равен *60 секндам.***
SuppTimeout ***<30>***	**Время обмена информацией между аутентификатором и клиентом. По умолчанию данный параметр равен *30 секундам.***
ServerTimeout ***<30>***	**Время обмена информацией между аутентификатором и сервером аутентификации. По умолчанию данный параметр равен *30 секундам.***
MaxReq ***<2>***	**В данном поле устанавливается максимальное число раз, которое**

	коммутатор может осуществлять повторную передачу EAP запроса клиенту до окончания сессии аутентификации. По умолчанию данное значение равно 2.
ReAuthPeriod <***3600***>	**Время ожидания (в секундах) перед повторной аутентификацией клиента. По умолчанию данный параметр равен *3600 секундам.***
ReAuth <***Disabled***>	**В данном поле определяется возможность повторной аутентификации с заданным периодом времени на данном порту. По умолчанию данная настройка отключена *Disabled.***
Capability	**Можно выбрать одну из двух функций для порта:** ***Authenticator* – пользователь должен пройти процесс аутентификации для получения доступа к сети.** ***None* – порт не будет контролироваться функциями протокола 802.1x.**

Для того чтобы настройки вступили в силу, нажмите **Apply**.

Сервер RADIUS

Функция RADIUS на коммутаторе позволит облегчить централизованное пользовательское администрирование, предоставляя при этом защиту от несанкционированного прослушивания сети. Для произведения настроек будет предложено три окна. Для открытия окна **«Authentic RADIUS Server»** нажмите **Security ⇨ 802.1x ⇨Authentic Radius Server.**

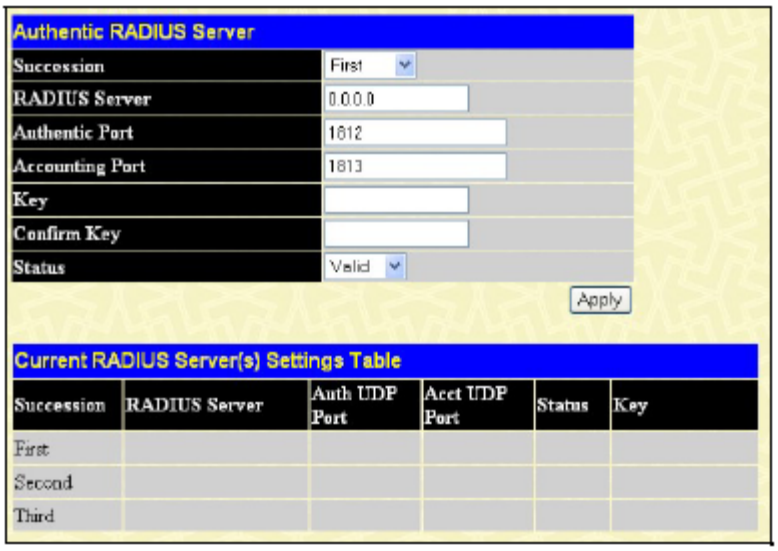


Рисунок 11.13 – Окно «Authentic RADIUS Server»

В окне отображается следующая информация:

Параметр	Описание
Succession	**Выберите сервер RADIUS для настройки: *First, Second* или *Third* (первый, второй или третий).**
RADIUS Server	**Введите IP-адрес сервера RADIUS.**
Authentic Port	**Введите UDP-порт сервера (ов) аутентификации RADIUS. По умолчанию – это порт 1812.**
Accounting Port	**Введите UDP-порт RADIUS-сервера (-ов), содержащего (-их) информацию об учетных записях пользователей. По умолчанию – это порт 1813.**
Key	**Введите ключ, идентичный тому, который вы вводили на RADIUS-сервере.**
Confirm Key	**Подтвердите ввод ключа, идентичный тому, который вы вводили на RADIUS-сервере.**
Status	**Данное поле позволяет включать *Valid* и отключать *Invalid* RADIUS сервер.**
Accounting	**Данная опция позволяет добавлять/изменять *Add/Modify* или удалять *Delete***

Method	**сервер RADIUS.**

Trusted Host

Для открытия ниже приведенного окна нажмите **Security ⇨ Trusted Host.**

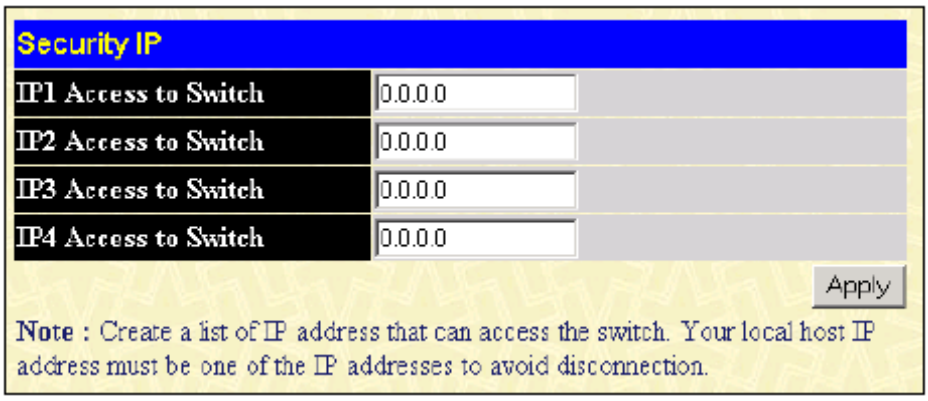


Рисунок 11.14 – Окно «Security IP Management»

Используйте функцию Security IP Management для удаленного управления коммутатором. Для разрешения удаленного управления коммутатором с одной или нескольких станций через Web-интерфейс или Telnet необходимо задать IP-адреса соответствующих станций и нажать кнопку **Apply**.

Управление аутентификацией доступа

Команды TACACS/XTACACS/TACACS+/RADIUS обеспечивают безопасный доступ к коммутатору через протоколы TACACS/XTACACS/TACACS+/RADIUS. Когда пользователь будет регистрироваться на коммутаторе или пытаться получить доступ с уровнем привилегий администратора, ему будет предложено ввести пароль. Если аутентификация TACACS/XTACACS/TACACS+/RADIUS будет разрешена на коммутаторе, то коммутатор обратится к TACACS/XTACACS/TACACS+/RADIUS-серверу для проверки пользователя. Если проверка пройдет успешно, то пользователю будет предоставлен доступ к коммутатору.

В настоящее время существует три версии протокола безопасности TACACS. Программное обеспечение коммутатора поддерживает следующие версии TACACS:

- **TACACS** (Terminal Access Controller Access Control System) – обеспечивает проверку пароля и аутентификацию пользователя, также отправляет уведомления о пользовательских действиях в целях безопасности через один или несколько централизованных TACACS-серверов, работающих по протоколу UDP для передачи пакетов.
- **Extended TACACS (XTACACS) –** Расширение протокола TACACS с возможностью обеспечения большего числа типов запросов и ответов аутентификации, чем TACACS. Данный протокол для передачи информации также использует UDP.
- **TACACS+ (Terminal Access Controller Access Control System plus**) – Обеспечивает детальный контроль доступа при аутентификации сетевых устройств. TACACS+ способствует продвижению аутентификационных команд через один и более централизованных серверов. Протокол TACACS+ шифрует весь трафик между коммутатором и TACACS+-сервером, используя протокол TCP для обеспечения надежной доставки данных.

Для того чтобы правильно работала функция безопасности TACACS/XTACACS/TACACS+/RADIUS, сервер TACACS/XTACACS/TACACS+/RADIUS должен быть настроен на устройстве, отличном от коммутатора, называемом сервером аутентификации и содержать имена пользователей и пароли для аутентификации. Когда пользователю предложат ввести имя пользователя и пароль, коммутатор обратится за подтверждением к TACACS/XTACACS/TACACS+/RADIUS-серверу, который отправит одно из трех сообщений:

- Сервер подтверждает имя пользователя и пароль, и пользователю предоставляется доступ к коммутатору с привилегиями пользователя.
- Сервер не принимает имя пользователя и пароль, пользователю отказано в доступе к коммутатору.
- Сервер не отвечает на запрос подтверждения. В данном случае коммутатор выдерживает временную паузу, определенную сервером, и переходит к следующему способу подтверждения, настроенному в списке способов.

У коммутатора есть четыре встроенные группы серверов аутентификации ***Authentication Server Groups,*** по одной на каждый из протоколов TACACS, XTACACS, TACACS+, RADIUS. Данные встроенные группы серверов аутентификации используются для аутентификации пользователей, пытающихся получить доступ к коммутатору. Пользователи устанавливают серверы аутентификации во встроенной группе серверов аутентификации в предпочтительном порядке, и, когда пользователи пытаются получить доступ к коммутатору, он сначала запрашивает первый сервер аутентификации. Если аутентификации не произойдет, будет запрашиваться второй сервер в списке и т.д. Встроенные группы серверов аутентификации могут содержать серверы, которые работают по определенному протоколу. Например, в группе серверов аутентификации TACACS могут быть только серверы TACACS. Администратор может установить до шести различных методов аутентификации в списке методов для аутентификации (TACACS/XTACACS/TACACS+/RADIUS/local/none). Эти методы должны быть занесены в список в приоритетном порядке и определены пользователем для обычной аутентификации на коммутаторе, может быть до 8 методов аутентификации. Когда пользователь будет пытаться получить доступ к коммутатору, коммутатор выберет первый метод из указанных в списке. Если первый метод аутентификации на сервере не реализуется, коммутатор будет обращаться к каждому следующему методу, занесенному в серверной группе аутентификации до тех пор, пока аутентификация не будет подтверждена или отклонена, или не закончится список.

Пожалуйста, обратите внимание, что пользователям будет предоставляться доступ к коммутатору с уровнем привилегий User. Для получения доступа с уровнем привилегий Admin, пользователю нужно открыть окно **Enable Admin** и ввести пароль, который был ранее настроен на коммутаторе администратором.

Примечание: TACACS, XTACACS и TACACS+ являются различными протоколами, не совместимыми друг с другом. Коммутатор и сервер должны иметь одни и те же настройки, использовать один и тот же протокол. (Например, если на коммутаторе установлена аутентификация TACACS, то и сервер должен работать по протоколу TACACS).

Настройка политики и параметров аутентификации

Данная команда запускает политику аутентификации, определенную администратором, для пользователей, пытающихся получить доступ к коммутатору. Когда данная политика включена, устройство проверяет список методов регистрации Login Method List и выбирает метод для аутентификации пользователя при регистрации. Для доступа к следующему окну нажмите **Security ⇨ Access Authentication Control ⇨ Authentication Policy and Parameter Settings**:

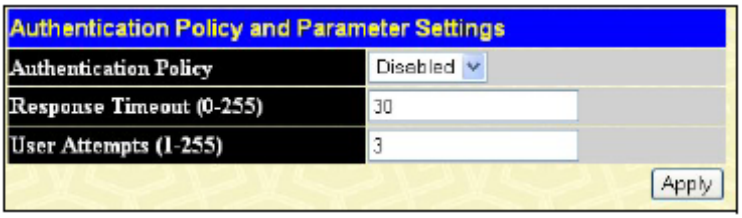


Рисунок 11.15 – Окно «Policy&Parameters Settings»

Могут быть установлены следующие параметры:

Параметры	Описание
Authentification Policy	Для включения (Enable) или выключения (Disable) политики аутентификации (Authentification Policy) на коммутаторе используйте выпадающее меню.
Response Timeout (0 – 255)	В данном поле можно установить время ожидания ответа на аутентификацию пользователя от 0 до 255 секунд. По умолчанию в настройках установлено 30 секунд.
User Attempts (1 – 255)	Данная команда настраивает максимальное количество попыток аутентификации на коммутаторе. Пользователям, исчерпавшим установленное количество попыток, будет отказано в доступе к коммутатору и дальнейшие попытки аутентификации будут заблокированы. Пользователям Интерфейса командной строки необходимо будет подождать 60 секунд перед следующей попыткой аутентификации. Пользователи Telnet и Web-интерфейса будут отключены от коммутатора. Пользователь может установить количество попыток от 1 до 255, по умолчанию их 3.

Нажмите **Apply**, чтобы введенные настройки вступили в силу.

Настройки Application Authentication

Данное окно используется для настройки приложений коммутатора (console, Telnet, SSH, web) и для регистрации на уровне пользователя и уровне администратора (Enable Admin), работающих по ранее настроенному списку методов. Для просмотра данного окна нажмите:
Security ⇨ Access Authentication Control ⇨ Application Authentication Settings

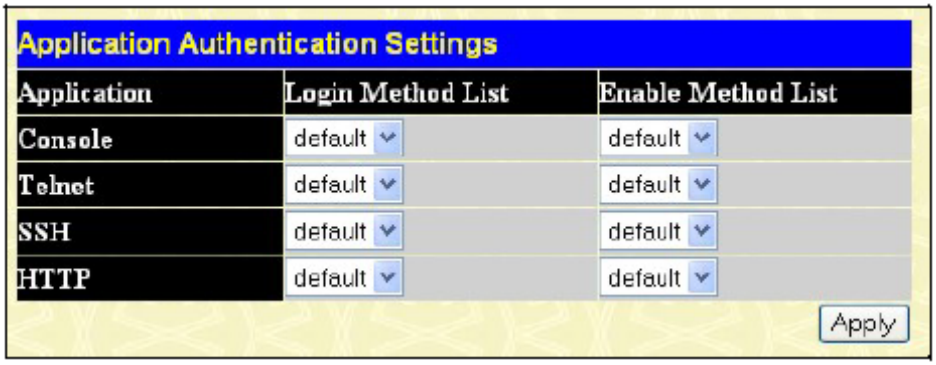


Рисунок 11.16 – Окно Application's Authentication Settings

Могут быть установлены следующие параметры:

Параметры	Описание
Application	Списки приложений настроек на коммутаторе. Пользователь может настроить Login Method List и Enable Method List для аутентификации пользователей, использующих интерфейс командной строки (Command Line Interface), Telnet, SSH и WEB (HTTP)-приложения.
Login Method List	С помощью выпадающего меню настройте приложение для обычной регистрации на уровне пользователя, используя ранее настроенный список методов. Пользователь может использовать Method List по умолчанию или другой, настроенный пользователем, Method List. Для более подробной информации посмотрите окно **Login Method Lists** в этом разделе.
Enable Method List	С помощью выпадающего меню настройте приложение для обычной регистрации на уровне пользователя, используя ранее настроенный список методов. Пользователь может использовать Method List по умолчанию или другой, настроенный пользователем, Method List. Для более подробной информации посмотрите окно **Enable Method Lists** в этом разделе.

Нажмите **Apply**, чтобы измененные настройки вступили в силу.

Настройка группы серверов аутентификации

Данное окно позволит пользователям установить на коммутаторе группу серверов аутентификации ***Authentication Server Groups***. Группа серверов – это способ, используемый для группировки TACACS/XTACACS/TACACS+/RADIUS серверов в определенную пользователем категорию для аутентификации с помощью списка методов. Пользователь может определить тип группы серверов по протоколу или по ранее настроенной группе серверов. У коммутатора есть три встроенные группы серверов аутентификации, которые нельзя удалить, но можно изменить. До восьми серверов аутентификации могут быть внесены в любую отдельную группу. Для просмотра следующего окна, нажмите **Security ⇨ Access Authentication Control ⇨ Authentication Server Group**:

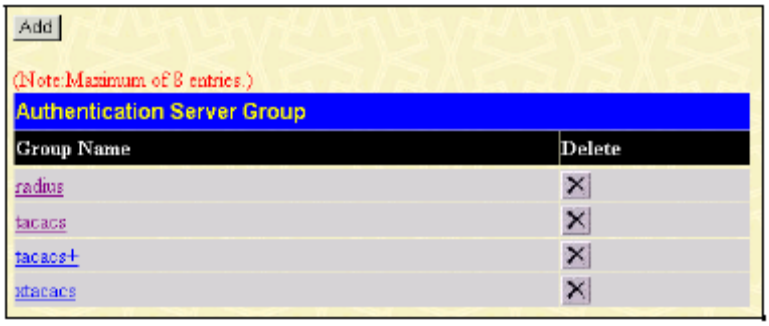


Рисунок 11.17 – Окно «Authentication Server Group Settings»

Данное окно отобразит группы серверов аутентификации на коммутаторе. У коммутатора есть четыре группы серверов аутентификации, которые нельзя удалить, но можно изменить. Для изменения группы, нажмите гиперссылку имени группы, после чего отобразится следующее окно.

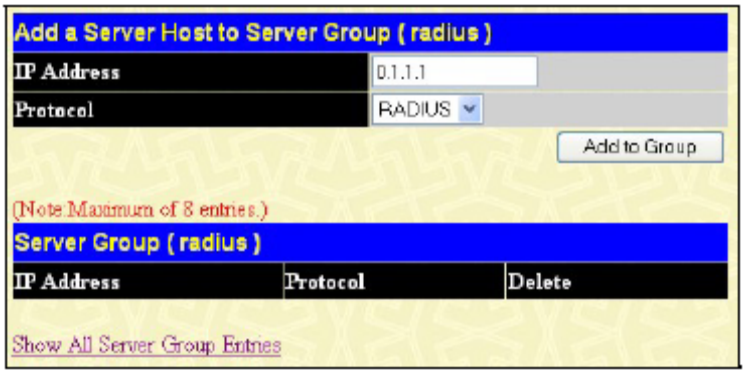


Рисунок 11.18 – Окно « Add a Server Host to Server Group (radius)»

Для добавления в список сервера аутентификации введите **IP-адрес** в поле IP Address, выберите протокол, связанный с IP-адресом группы серверов аутентификации, и нажмите **Add to Group** для добавления данного сервера аутентификации к группе. Для того чтобы добавить группу серверов, определенную пользователем, которая не отображается на экране, кликните по кнопке **Add**, после чего появится следующее окно для настроек.

Рисунок 11.19 – Окно «Authentication Server Group Table Add Settings»

Для идентификации пользователей введите название группы длиной не более 15 буквенно-цифровых символов и нажмите **Apply**. Новое имя, назначенное пользователем, появится в окне **Authentication Server Group**.

Примечание: Пользователь должен настроить сервер аутентификации, используя окно **Authentication Server Hosts**, прежде чем добавит серверы в список. Серверы аутентификации должны быть настроены согласно их определенным протоколам на центральном сервере до того, как может начать свою работу данная функция.

Примечание: 4 группы серверов могут работать только с хостами, поддерживающими точно такой же демон TACACS. Протоколы TACACS/XTACACS/TACACS+ являются отдельными логическим категориями и не совместимы друг с другом.

Серверы аутентификации

Данное окно отображает определенные пользователем серверы аутентификации ***Authentication Server Hosts*** для TACACS/XTACACS/TACACS+/RADIUS протоколов безопасности. Когда пользователь пытается получить доступ к коммутатору по возможной политике аутентификации, коммутатор отправляет аутентификационные пакеты на удаленный TACACS/XTACACS/TACACS+/RADIUS сервер. TACACS/XTACACS/TACACS+/RADIUS сервер подтвердит или отклонит запрос и отправит коммутатору соответствующее сообщение. На одном и том же сервере одновременно могут работать более одного протокола аутентификации, однако, у протоколов TACACS/XTACACS/TACACS+/RADIUS отдельные параметры, несовместимые друг с другом. Максимальное число поддерживаемых серверов 16. Для просмотра следующего окна, нажмите **Security ⇨ Access Authentication Control ⇨ Authentication Server Host**:

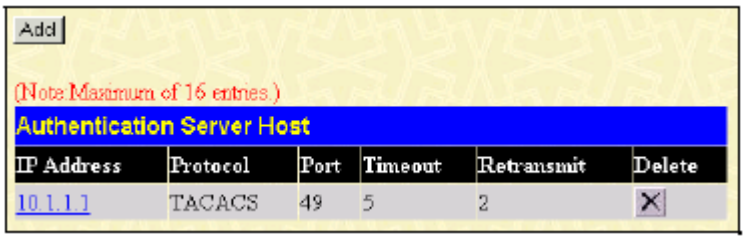


Рисунок 11.20 – Окно «Authentication Server Host Settings»

Для добавления сервера Authentication Server, нажмите кнопку **Add**, откройте следующее окно:

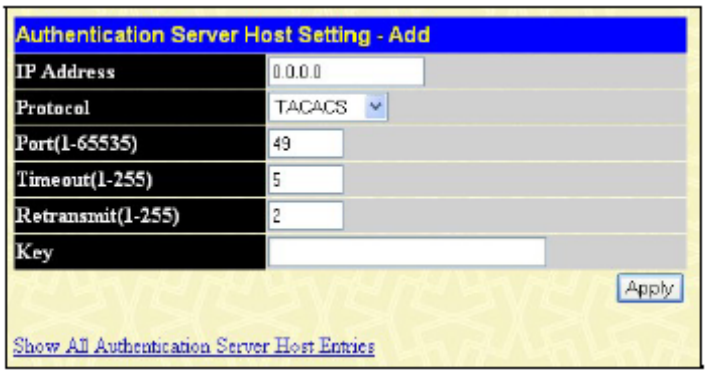


Рисунок 11.21 – Окно «Authentication Server Host Settings – Add»

Для редактирования параметров сервера аутентификации нажмите гиперссылку IP-адреса, после чего откроется следующее окно:

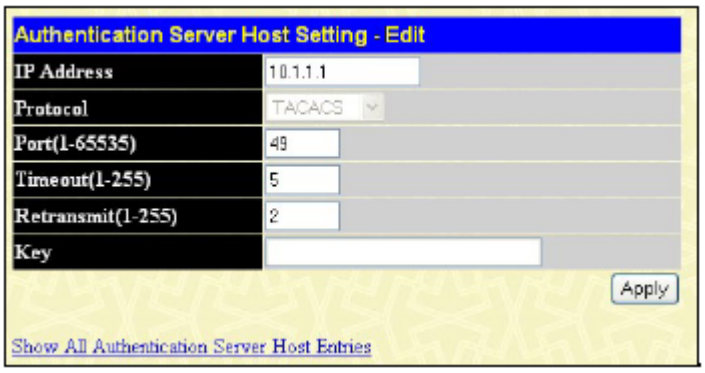


Рисунок 11.22 – Окно «Authentication Server Host - Edit»

Для добавления сервера аутентификации настройте следующие параметры:

Параметр	Описание
IP Address	IP-адрес удаленного добавленного сервера.
Protocol	Протокол, используемый сервером. Пользователь может выбрать один из следующих протоколов: ▪ TACACS – Введите данный параметр, если сервер использует TACACS протокол. ▪ XTACACS - Введите данный параметр, если сервер использует XTACACS протокол. ▪ TACACS+ - Введите данный параметр, если сервер использует TACACS+ протокол. ▪ RADIUS - Введите данный параметр, если сервер использует RADIUS протокол.
Port (1-65535)	Введите номер виртуального порта протокола аутентификации для сервера из диапазона 1 - 65535. По умолчанию для TACACS/XTACACS/TACACS+/RADIUS серверов номер порта 49 и 1813 для RADIUS сервера, но пользователь для большей безопасности может установить уникальный номер порта.
Timeout	Введите время ожидания коммутатором ответа на запрос аутентификации в секундах. По умолчанию данное значение равно 5 секундам.
Retransmit (1-255)	В данном поле введите число раз, которое устройство будет отправлять запросы аутентификации, когда TACACS сервер не отвечает.
Key	Ключ аутентификации должен использоваться только с настроенными серверами TACACS или RADIUS. Задайте буквенно-цифровую строку не более 254 символов.

Нажмите **Apply** для добавления сервера.

Примечание: На одном сервере одновременно могут работать более одного протокола аутентификации, однако у протоколов TACACS/XTACACS/TACACS+/RADIUS отдельные параметры, несовместимые друг с другом.

Списки методов аутентификации

Данная команда настроит определенный пользователем или созданный по умолчанию список методов аутентификации (Login Method List) при регистрации пользователей на коммутаторе. Последовательность методов, включенных в данную команду, повлияет на результат аутентификации. Например, если пользователь введет последовательность методов, например,

TACACS-XTACACS – local, коммутатор отправит запрос аутентификации к первому серверу TACACS в группе серверов. Если ответ от сервера не приходит, коммутатор отправляет запрос на аутентификацию второму TACACS серверу в группе серверов и т.д., пока не дойдет до конца списка. В этот момент коммутатор отправит запрос по следующему протоколу, указанному в списке, XTACACS. Если аутентификации по XTACACS не произошло, то для аутентификации пользователя используется локальная база, установленная на коммутаторе. Когда используется локальный метод, уровень привилегий будет зависеть от настроенной на коммутаторе привилегии локальной учетной записи.

Успешная регистрация, использующая эти методы, присвоит пользователю только привилегию уровня «User». Если пользователь пожелает увеличить статус до уровня администратора, то он может воспользоваться окном **Enable Admin,** в котором пользователь должен ввести предыдущий пароль, установленный администратором. (Для получения более подробной информации, касающейся команды Enable Admin, смотрите в этом разделе часть Enable Admin).

Для просмотра следующего окна, нажмите **Security ⇨ Access Authentication Control ⇨ Login Method Lists**:

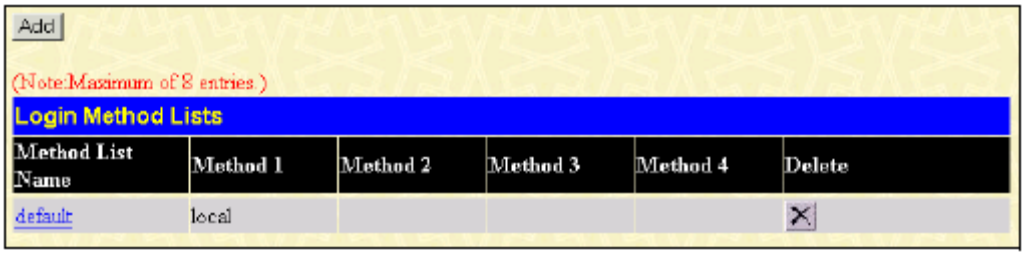


Рисунок 11.23 – Окно «Login Method Lists Settings»

Коммутатор содержит установленный список методов, который нельзя удалить, однако можно изменить. Для удаления из списка методов регистрации Login Method List, определенного пользователем, нажмите ✕ под заголовком Delete напротив соответствующей записи. Для изменения списка методов регистрации Login Method List, нажмите на гиперссылку Method List Name. Для настройки нового списка методов, нажмите кнопку **Add**. Эти действия будут приведены в том же окне для настройки:

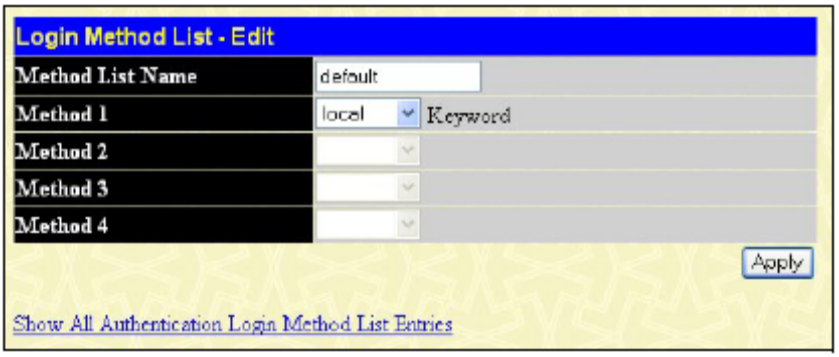


Рисунок 11.24 – Окно «Login Method List – Edit» (по умолчанию)

Рисунок 11.25 – Окно «Login Method List – Add»

Для определения Login Method List, установите следующие параметры и нажмите **Apply**:

Параметр	Описание
Method List Name	Введите название списка методов, определенного пользователем, длиной не более 15 символов.
Method 1, 2, 3,4	Пользователь может добавить один метод или комбинацию (до 4) из следующих методов аутентификации к данному списку методов: ▪ *tacacs* – добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью протокола TACACS с удаленного TACACS-сервера. ▪ *xtacacs* - добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью протокола XTACACS с удаленного XTACACS-сервера. ▪ *tacacs+* - добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью протокола TACACS+ с удаленного TACACS+-сервера. ▪ *radius* - добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью протокола RADIUS с удаленного RADIUS-сервера. ▪ *server_group* – добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью определенной пользователем группы серверов, настроенной ранее на коммутаторе. ▪ *local* - добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью локальной учетной записи пользователя в базе данных на коммутаторе. ▪ *none* – добавление данного параметра потребует аутентификации для доступа к коммутатору.

Enable Method Lists

Окно **Enable Method List Settings** применяется для установки списка методов пользователями, желающими повысить привилегии от уровня пользователя до уровня администратора (Admin), используя методы аутентификации на коммутаторе. Пользователю предоставляются привилегии уровня User на коммутаторе, для получения привилегий уровня Admin необходимо аутентифицироваться на коммутаторе методом, определенным администратором. На коммутаторе может работать максимально восемь Enable Method List, один из которых установлен по умолчанию. Этот Enable Method List, установленный по умолчанию, нельзя удалить, но можно изменить.

В зависимости от выбранной последовательности методов в этой команде будет получена соответствующая аутентификация. Например, если пользователь введет последовательность методов, подобно TACACS – XTACACS – Local Enable, коммутатор отправит запрос аутентификации сначала на первый TACACS сервер в группе серверов. Если подтверждения не

будет, коммутатор отправит запрос авторизации на второй TACACS сервер в группе серверов и т.д., пока не дойдет до конца списка.

В этот момент коммутатор отправит запрос авторизации для следующего протокола, указанного в списке, XTACACS. Если аутентификации по XTACACS не произошло, то для аутентификации пользователя используется Local Enable пароль, установленный на коммутаторе. Успешно прошедшая аутентификация, использующая любой из этих методов, даст пользователю привилегию уровня «Admin».

Примечание: Для установки Local Enable пароля, посмотрите следующий раздел под названием Local Enable Password.

Для просмотра следующей таблицы, нажмите **Security ⇨ Access Authentication Control ⇨ Enable Method Lists**:

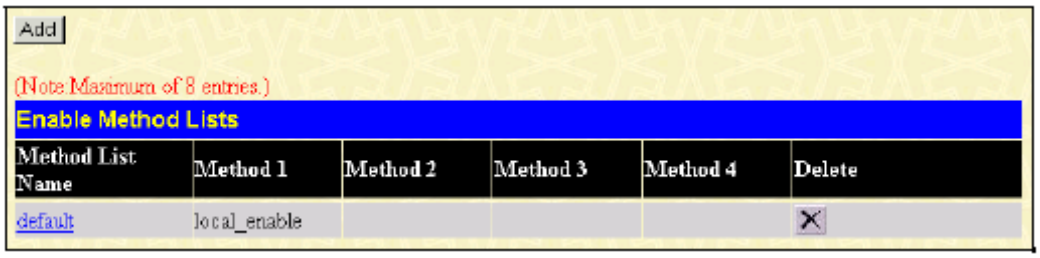


Рисунок 11.26 – Окно «Enable Method List Settings»

Для удаления Enable Method List, созданного пользователем, нажмите ✕ под заголовком Delete напротив соответствующей записи, которую хотите удалить. Для изменения Enable Method List, нажмите на гиперссылку Method List Name. Для настройки Method List, нажмите кнопку **Add**. Данные действия приведут к открытию следующего окна:

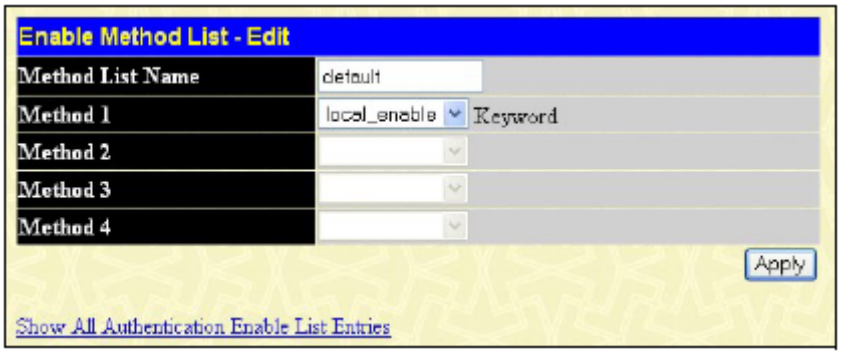


Рисунок 11.27 – Окно «Enable Method List - Edit»

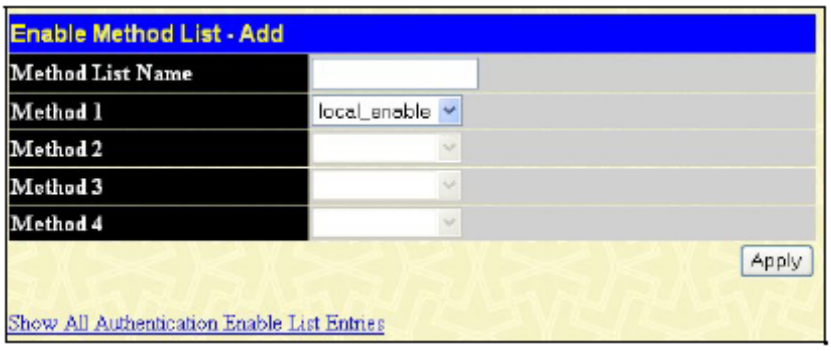


Рисунок 11.28 – Окно «Enable Method List - Add»

Для определения Enable Login Method List, установите следующие параметры и нажмите **Apply**:

Параметр	Описание
Method List Name	Введите название списка методов, определенного пользователем, длиной не более 15 символов.
Method 1, 2, 3, 4	Пользователь может добавить один метод или комбинацию (до 4) из следующих методов аутентификации к данному списку методов: ▪ *local_enable* - добавление данного параметра потребует, чтобы аутентификация пользователя происходила по local enable паролю локальной базы данных, установленной на коммутаторе. В следующем разделе под названием Local Enable Password пользователь должен установить local enable пароль. ▪ *none* – добавление данного параметра потребует аутентификации для доступа к коммутатору. ▪ *radius* - добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью протокола RADIUS с удаленного RADIUS-сервера. ▪ *tacacs* – добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью протокола TACACS с удаленного TACACS-сервера. ▪ *tacacs+* - добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью протокола TACACS+ с удаленного TACACS+-сервера. ▪ *server_group* – добавление данного параметра потребует, чтобы аутентификация пользователя происходила с помощью определенной пользователем группой серверов, настроенной ранее на коммутаторе.

Настройка Local Enable Password

Данное окно позволит настроить locally enabled пароль для команды Enable Admin. Когда пользователь выбирает метод «local_enable» для повышения привилегии от уровня пользователя до уровня администратора (Admin), ему будет предложено ввести пароль, который локально установлен на коммутаторе. Для просмотра следующего окна, нажмите **Security ⇨ Access Authentication Control ⇨ Local Enable Password**:

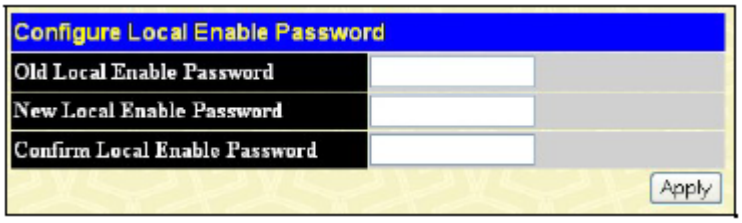


Рисунок 11.29 – Окно «Configure Local Enable Password»

Для установки Local Enable Password, установите следующие параметры и нажмите **Apply**.

Параметр	Описание
Old Local Enabled	Для того чтобы сменить пароль на новый, вам необходимо ввести в данном поле прежний пароль.
New Local Enabled	Введите новый пароль, который вы хотите установить на коммутаторе для аутентификации пользователей, пытающихся получить доступ к коммутатору с привилегиями уровня администратора. Пользователь может установить пароль длиной не более 15 символов.

Confirm Local Enabled	Подтвердите ввод нового пароля. Введение пароля в данном поле, отличного от пароля в поле New Local Enabled, приведет к появлению сообщения об ошибке.

Enable Admin

Окно **Enable Admin** необходимо для пользователей, которые регистрируются на коммутаторе с привилегиями уровня User и желают повысить привилегии до уровня Admin. После регистрации на коммутаторе, пользователи обладают только привилегиями уровня «User». Для получения привилегий уровня администратора, пользователю необходимо открыть данное окно и ввести пароль для аутентификации. Для данной функции возможные методы аутентификации TACACS/XTACACS/TACACS+/RADIUS, пользователь определяет группы серверов, local enable (локальная учетная запись на коммутаторе) или отсутствие аутентификации. В силу того, что XTACACS и TACACS не поддерживают enable функцию, пользователь должен создать специальную учетную запись на сервере, у которого имя пользователя «enable» и пароль, настроенный администратором, поддерживающий функцию «enable». Данная функция становится недоступна, когда отсутствует политика аутентификации.

Для просмотра следующего окна, нажмите **Security ⇨ Access Authentication Control ⇨ Enable Admin**:

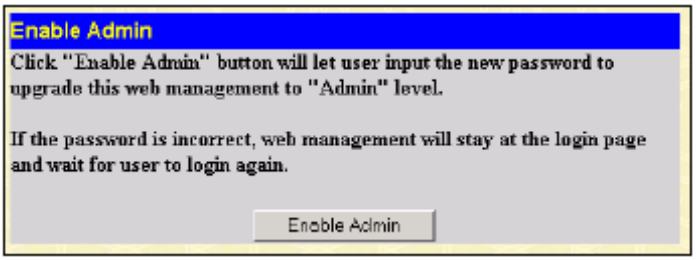


Рисунок 11.30 – Окно «Enable Admin»

Когда откроется окно, нажмите кнопку **Enable Admin**, после чего появится диалоговое окно, в котором необходимо ввести пароль и имя пользователя для аутентификации. О получении привилегий уровня администратора пользователь будет проинформирован в виде отдельного сообщения.

Рисунок 11.31 – Диалоговое окно «Enter Network Password»

Сегментация трафика

Сегментация трафика служит для разграничения доменов на уровне 2.
Она позволяет настраивать порты таким образом, чтобы они были изолированы друг от друга, но в то же время имели доступ к разделяемым портам, используемым для подключения сервером и магистрали сети провайдера. Данная функция может быть использована при построении сетей провайдеров.
Для просмотра окна, представленного ниже, нажмите **Security ⇨ Traffic Segmentation**:

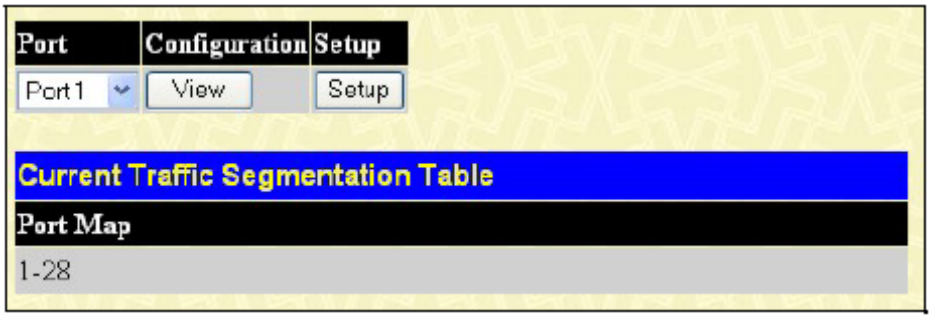


Рисунок 11.32 – Окно «Current Traffic Segmentation Table»

В этом окне можно посмотреть, какому порту разрешено направлять пакеты на другие порты данного коммутатора. С помощью выпадающего меню выберите номер порта и нажмите **View** для отображения портов, на которые будет направляться трафик. Для настройки новых портов, на которые будет направляться трафик с выбранного порта, выберите номер порта с помощью выпадающего меню и нажмите **Setup**. Откроется следующее окно:

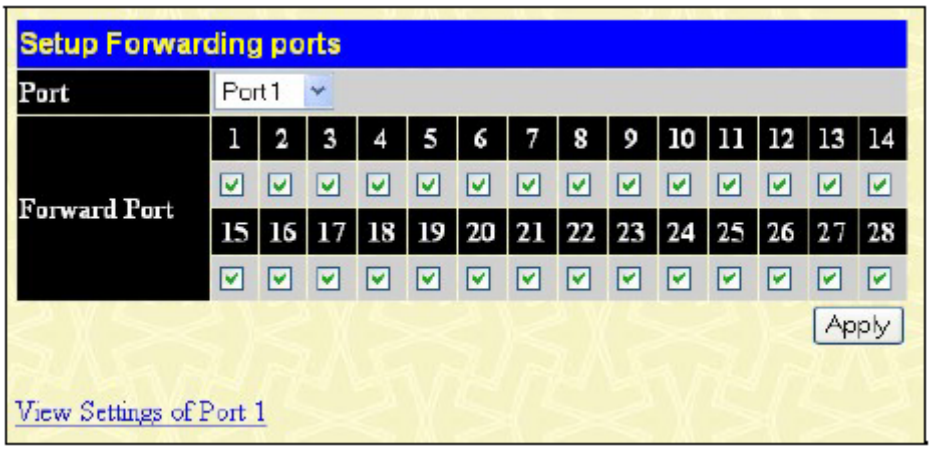


Рисунок 11.33 – Окно «Setup Forwarding Ports»

Пользователь может настроить следующие параметры:

Параметр	Описание
Port	Порт, с которого будет осуществляться передача пакетов.
Forward Port	Выберите порты коммутатора, которым будет разрешено получать пакеты с порта, определенного в предыдущем поле.

После нажатия на кнопку **Apply**, комбинация передающего и принимающих портов будет занесена в таблицу **Current Traffic Segmentation Table (Текущую таблицу сегментации трафика)**.

Secure Socket Layer (SSL)

Secure Sockets Layer (SSL) – протокол, обеспечивающий безопасную связь между хостом и клиентом с помощью установки подлинности, цифровых подписей и шифрования. Эти функции безопасности осуществлены с помощью *ciphersuite*, который является набором средств обеспечения безопасности, определяющим точные шифровальные параметры, определенные алгоритмы шифрования и длину ключей, которые используются для аутентификации. C*iphersuite* состоит из трех частей:

1. **Ключ обмена (Key Exchange)**: в первой части cyphersuite строки описывается алгоритм открытого ключа. Коммутатор использует Rivest Shamir Adleman (RSA)- алгоритм открытого ключа и Digital Signature Algorithm (DSA) – цифровую подпись, определённую здесь как DHE DSS Diffie-Hellman (DHE). Это первый процесс аутентификации между хостом и клиентом, таким образом, они "обмениваются ключами" в поиске подходящих и установления подлинности, для того чтобы перейти к шифрованию на следующем уровне.
2. **Шифрование (Encryption)**: вторая часть *cyphersuite* включает в себя шифрование сообщения посылаемого между хостом и клиентом. Коммутатор поддерживает два типа шифрования:
   - Steam Ciphers. В коммутаторе присутствует два типа Steam Ciphers RC4 с 40-битным ключом и RC4 со 128-битным ключом. Эти ключи используются для шифрования сообщений и должны быть постоянными для хоста и клиента.
   - CBC Block Cliphers означает, что часть предварительно зашифрованного блока зашифрованного текста используется в шифровании текущего блока. Коммутатор поддерживает 3 DES EDE шифрование, определённое стандартом Data Encryption Standart (DES) для создания зашифрованного текста.
3. **Hash Algoritm**. Эта часть *cyphersuite* позволяет создать из исходного сообщения дайджест, который определяет Message Authentification Code (сообщение кода аутентификации). Этот Message Authentification Code будет зашифрован вместе с передаваемым сообщением для того, чтобы обеспечить целостность сообщения и предотвратить взлом защиты путём замещения оригинала. Коммутатор поддерживает два типа Hash algorithm (алгоритма хеширования): MD5 (Message Diggest 5) и SHA (Secure Hash Algoritm).

Эти три параметра создают трёхуровневый алгоритм шифрования для безопасной коммуникации между сервером и хостом. Пользователь может выбрать один или комбинацию возможных cyphersuite, однако использование нескольких cyphersuite улучшат уровень безопасности и быстродействие безопасной связи. Информация, включённая в *cyphersuite*, отсутствует в коммутаторе и требует загрузки из источника в виде файла – сертификата. Данная функция коммутатора не может быть выполнена без файла сертификации и может быть загружена в коммутатор путём установки TFTP-сервера. Коммутатор поддерживает SSLv3 и TLSv1. другие версии SSL могут быть несовместимы с коммутатором и могут привести к возникновению казусов во время аутентификации и передачи сообщений между клиентом и хостом.

Загрузка сертификата

Это окно используется для загрузки файла сертификации для SSL функции с TFTP-сервера. Файл сертификации представляет из себя набор данных для определения устройства в сети. Он содержит информацию о владельце, ключи аутентификации и цифровую подпись. У клиента и сервера должны быть совместимые файлы сертификации для оптимального использования SSL функции. Коммутатор поддерживает только файлы сертификации типа .der. Хотя коммутатор поставляется с предустановленным сертификатом, пользователь может произвести дальнейшую загрузку.

Ciphersuite

Это окно позволит пользователю выбрать SSL на коммутаторе и выполнить один ciphersuite или их комбинацию. Ciphersuite является строкой безопасности, определяющей точные параметры шифрования, определенные алгоритмы шифрования и ключевые размеры, которые используются

для аутентификации. Чтобы использовать конкретный ciphersuite, дезактивируйте ненужные ciphersuite, оставив только нужный ciphersuite для аутентификации.

Когда выбрана SSL-функция, WEB будет неактивна. Для управления Коммутатором через web одновременно с выбранной SSL-функцией, WEB-браузер должен поддерживать SSL шифрование адрес (URL) должен начинаться с http// (например, http://10.90.90.90). Любые другие варианты приведут к ошибке и отказе в доступе при авторизации.

Для просмотра соответствующих окон для **Download Certificate** и **Ciphersuite**, нажмите **Security > SSL**:

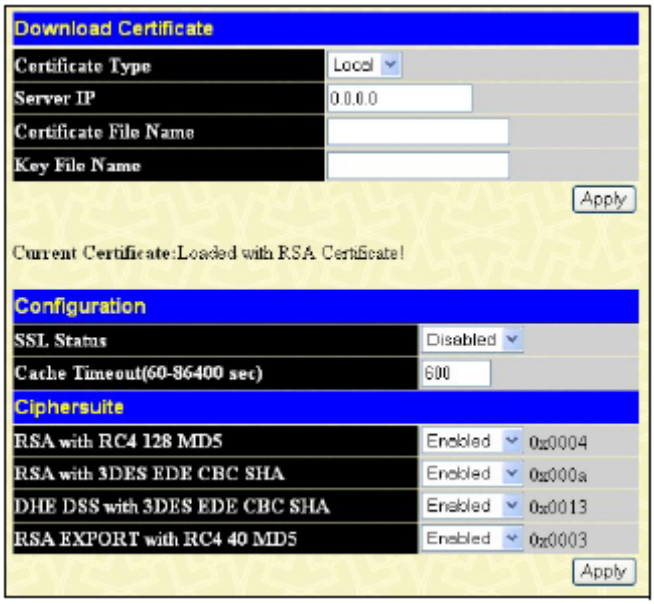


Рисунок 11.34 – Окно «Download Certificate and Cirphersuite»

Для загрузки сертификатов, установите следующие параметры и нажмите **Apply**.

Параметр	Описание
Certificate Type	Выберите тип загружаемого сертификата. Этот тип ссылается на сервер ответственный за выпуск сертификата. В данной реализации это поле может содержать только значение *local*
Server IP	Введите IP-адрес TFTP-сервера, где расположен файл сертификата.
Certificate File Name	Введите путь и имя загружаемого файла сертификата. Этот файл должен быть с расширением .der (например, c:/cert.der).
Key File Name	Введите путь и имя загружаемого файла ключа. Этот файл должен быть с расширением .der (например, c:/cert.der).

Для установки SSL функции на коммутаторе, настройте следующие параметры и нажмите **Apply**.

Параметр	Описание
Configuration	
SSL Status	С помощью выпадающего меню можно включать или отключать статус

	SSL. По умолчанию протокол SSL отключен *Disabled.*
Cache Timeout (60-86400)	Время обмена новым ключом между клиентом и хостом с помощью SSL – функции. Новая SSL-сессия устанавливается каждый раз, когда клиент и хост обмениваются ключами. Определение большего значение в данном поле позволит SSL-сессии повторно использовать мастер-ключ при будущих соединениях, однако ускоряет процесс согласования. По умолчанию, установлено значение в 600 секунд.
Ciphersuite	
RSA with RC4 128 MD5	Этот Ciphersuite комбинирует ключи обмена RSA, 128-битное шифрование RC4 и алгоритм шифрования MD5 Hash Algorithm. Используйте выпадающее меню для выбора или отмены Ciphersuite. По умолчанию установлено значение *Enabled*.
RSA with 3DES EDE CBC SHA	Этот Ciphersuite комбинирует ключи обмена RSA, шифрование CBC Block Cipher 3DES_EDE и алгоритм шифрования MD5 Hash Algorithm. Используйте выпадающее меню для выбора или отмены Ciphersuite. По умолчанию установлено значение *Enabled*.
DHS DSS with 3DES EDE CBC SHA	Этот Ciphersuite комбинирует ключи обмена DHS Diffie Hellman, шифрование CBC Block Cipher 3DES_EDE и алгоритм шифрования SHA Hash Algorithm. Используйте выпадающее меню для выбора или отмены Ciphersuite. По умолчанию установлено значение *Enabled*.
RSA EXPORT with RC4 40 MD5	Этот Ciphersuite комбинирует ключи обмена RSA, 40-битное шифрование RC4. Используйте выпадающее меню для выбора или отмены Ciphersuite. По умолчанию установлено значение *Enabled*.

Примечание: Определенное выполнение функции и конфигурации SSL не доступно через web в данном коммутаторе и должно осуществляться из командной строки. Для получения более подробной информации по SSL и его функциям читайте описание командной строки в руководстве по xStack DES-3800, находящееся на CD-диске.

Примечание: при выборе SSL-команды, переключатель управления через web будет неактивным. Для новой авторизации на Концентраторе адрес (URL) должен начинаться с http//. Введя что-то другое в поле адреса, Web-браузер выдаст ошибку и отказ в доступе при авторизации.

Secure Shell (SSH)

SSH – абревиатура от Secure Shell, программы, позволяющей удалённую безопасную авторизацию и безопасные сетевые сервисы по безопасной сети. Она позволяет удалённую авторизацию на удалённом хосте, безопасное выполнение команд на удалённом компьютере end node, и обеспечит безопасное шифрование и коммуникацию между двумя нетрастовыми (недоверительные отношения) хостами. SSH, с его множеством непревзойденных особенностей безопасности - существенный инструмент в сегодняшней компьютерной сети. Это - мощная защита от многочисленных существующих нарушений безопасности, которые теперь угрожают сетям.
Шаги, требующиеся выполнить для безопасной связи между удалённым PC (SSH-клиент) и коммутатором (SSH-сервер) следующие:

1. Создайте учётную запись пользователя с правами администратора, используя окно User Accounts в папке Security Management. Это идентично созданию любых других учётных записей пользователей с правами администратора на Коммутаторе, включая задачу пароля. Этот пароль используется для авторизации на Коммутаторе как только была установлена безопасная связь с использованием SSH-протокола.
2. Сконфигурируйте учётную запись, определив метод идентификации пользователей , которым можно устанавливать SSH-соединение с Коммутатором, используя окно SSH User Authentication. Существует три варианта авторизации пользователя Host Based, пароль и открытый ключ (public key).
3. Сконфигурируйте алгоритм шифрования, который будет использовать SSH для шифрования и дешифрования посылаемых сообщений между SSH-клиентом и SSh-сервером, используя окно SSH Algoritm.
4. в заключение установите SSH в Коммутаторе, используя окно SSH Configuration.

После завершения данных шагов, SSH-клиент на удалённом компьютере сконфигурирован для управления Коммутатором, используя безопасное соединение.

SSH Server Configuration

Окно **«SSH Server Configuration»** используется для настройки и просмотра настроек SSH сервера, для его открытия нажмите **Security ⇨ SSH ⇨ SSH Server Configuration:**

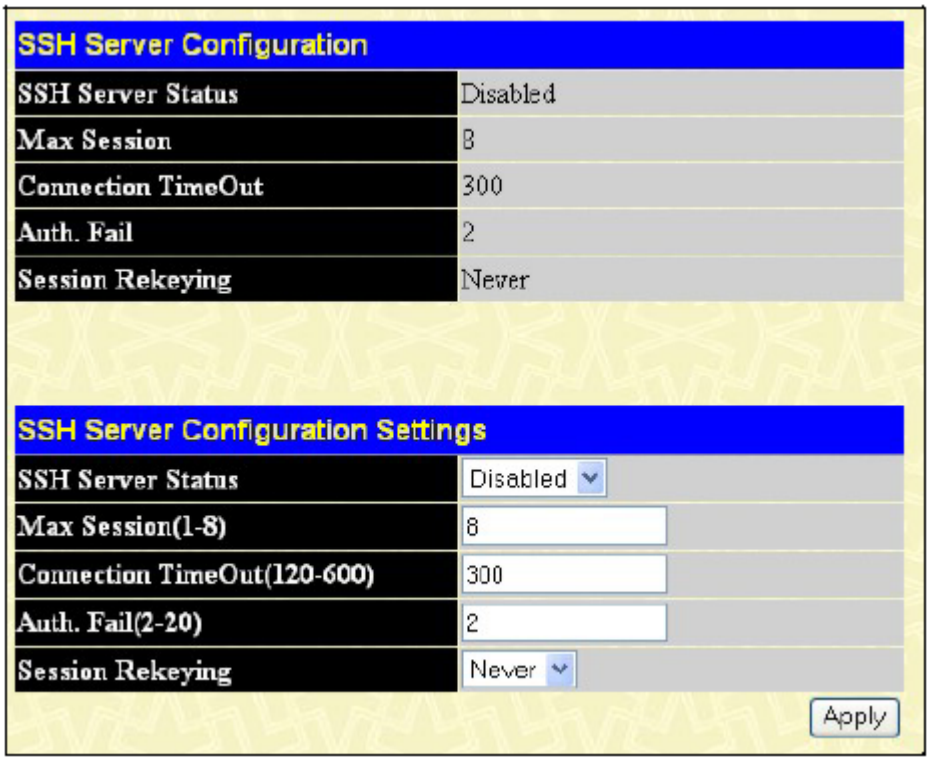


Рисунок 11.35 – Окно «SSH Server Configuration Settings»

Для настройки SSH сервера на коммутаторе, измените следующие параметры и нажмите **Apply**.

Параметр	Описание
SSH Server Status	Для включения или отключения SSH на коммутаторе воспользуйтесь выпадающим меню. По умолчанию SSH отключен *Disabled.*
Max Session (1-8)	Введите значение от 1 до 8 для установки количества пользователей, которые могут одновременно получать доступ к коммутатору. По умолчанию данный параметр равен 8.
Time Out (120-600)	Позволяет пользователю установить прерывание соединения по прошествии определенного времени. Возможно установить временной интервал между 120 и 600 секундами. По умолчанию этот параметр равен 300 секунд.
Auth/ Fail (2-20)	Позволяет администратору установить количество попыток пользователя авторизоваться на SSH-сервере, используя SSH-аутентификацию.
Session Rekeying	При помощи выпадающего меню этого поля установите период времени, по истечении которого коммутатор будет менять шифры программы безопасности. Доступны следующие опции: *Never*, *10 min, 30 min* и *60 min*. По умолчанию применяется настройка *Never*.

Настройка алгоритма и режима аутентификации SSH

Окно SSH Algorithm позволяет конфигурировать желаемые типы SSH-алгоритма, использующиеся для опознавательного шифрования. Существует четыре категории алгоритмов, и каждый из алгоритмов можно активировать или дезактивировать, используя выпадающее меню. Все алгоритмы выбраны по умолчанию. Для открытия данного окна нажмите **Security > SSH > SSH Authentication Mode and Algorithm Settings**:

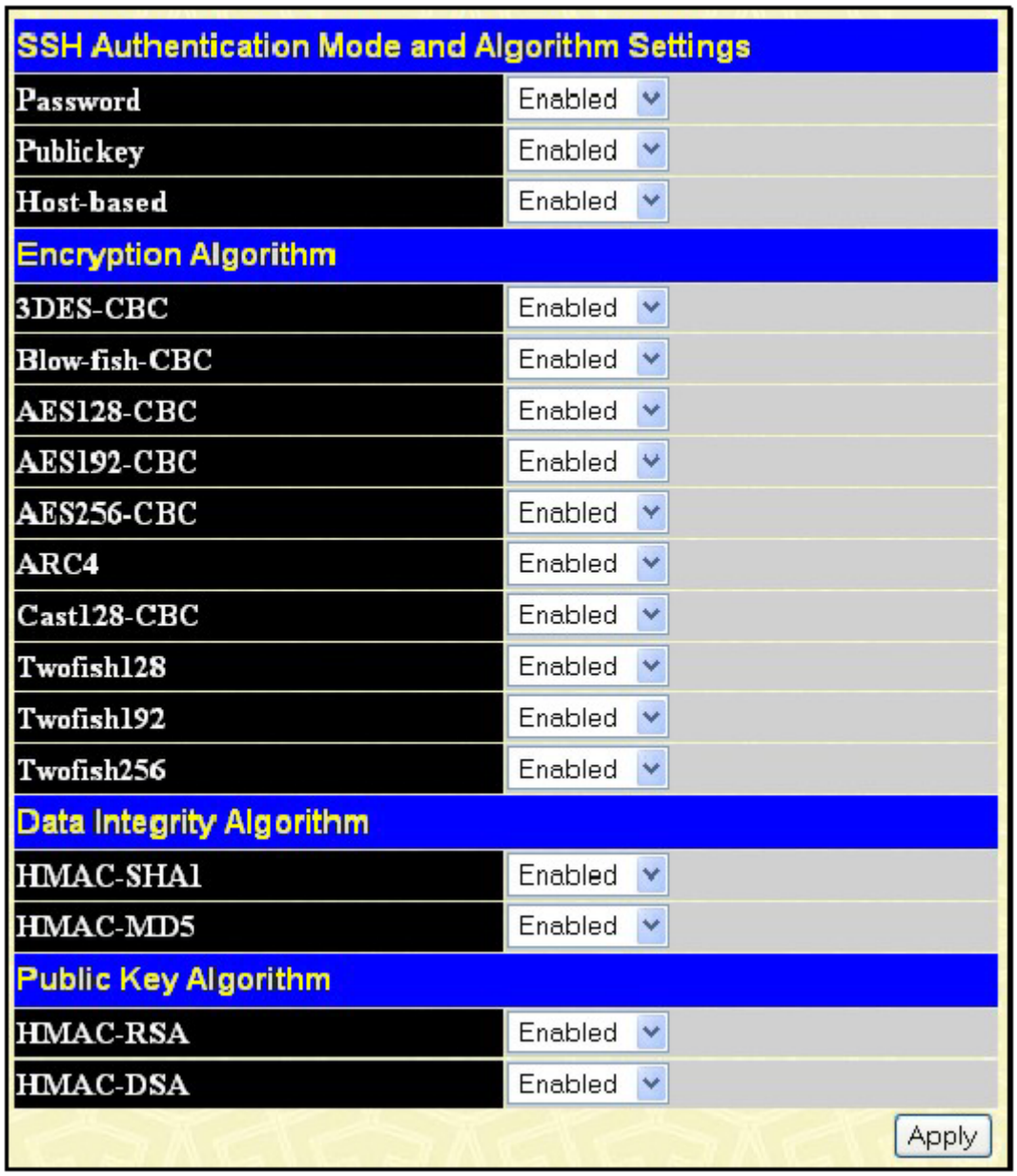


Рисунок 11.36. Encryption Algorithm окно

Следующие алгоритмы могут быть применены:

Параметр	Описание
	SSH Authentication Mode and Algorithm Settings
Password	Возможно использование этого параметра, если администратор желает использовать локально сконфигурированный пароль для аутентификации на коммутаторе. По умолчанию значение *Enabled*.
Public Key	Возможно использование этого параметра, если администратор желает использовать публичную конфигурацию на SSH-сервере для аутентификации на коммутаторе. По умолчанию значение *Enabled*.
Host-based	Возможно использование этого параметра, если администратор желает использовать хост-компьютер для аутентификации на коммутаторе. Этот параметр будет интересен в основном пользователям операционной системы Linux, где SSH-аутентификация необходима технически и хост, работающий в операционной системе Linux с предварительно установленной SSH-программой. По умолчанию значение *Enabled*.
Encryption Algorithm	
3DES-CBC	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования Triple Data Encryption Standard с Cipher Block Chaining. Значение по умолчанию Enabled.
Blow-fish CBC	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования Blowfish with Cipher Block Chaining. Значение по умолчанию *Enabled*.
AES128-CBC	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. Значение по умолчанию *Enabled*.
AES192-CBC	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. Значение по умолчанию *Enabled*.
AES256-CBC	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. Значение по умолчанию *Enabled*.
ARC4	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования Arcfour encryption algorithm with Cipher Block Chaining.Значение по умолчанию *Enabled*.
Cast128-CBC	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования Cast128 encryption algorithm with Cipher Block Chaining. Значение по умолчанию *Enabled*.
Twofish128	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования twofish128 encryption algorithm.Значение по умолчанию *Enabled*.
Twofish192	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования twofish192 encryption algorithm. Значение по умолчанию *Enable.*
Twofish256	Используйте выпадающее меню для активации или дезактивации алгоритма шифрования twofish256 encryption algorithm.Значение по умолчанию *Enabled*.
Data Integrity Algorithm	
HMAC-SHA1	Используйте выпадающее меню для активации или дезактивации HMAC (Hash for Message Authentication Code) – механизм utilizing the Secure Hash algorithm. Значение по умолчанию *Enabled*.

HMAC-MD5	Используйте выпадающее меню для активации или дезактивации HMAC (Hash for Message Authentication Code) – механизм utilizing MD5 Message Digest Значение по умолчанию *Enabled*.
Public Key Algorithm	
HMAC-RSA	Используйте выпадающее меню для активации или дезактивации HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. Значение по умолчанию *Enabled*.
HMAC-DSA	Используйте выпадающее меню для активации или дезактивации HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm encryption. Значение по умолчанию *Enabled*.
Authentication Algorithm	
Password	Этот параметр может быть выбран. Если администратор желает использовать пароль локальной конфигурации на Коммутаторе. Значение по умолчанию *Enabled*.
Public Key	Этот параметр может быть выбран, если пдминистратор желает использовать открытый ключ, сконфигурированный на SSH-сервере, для авторизации на Коммутаторе. Значение по умолчанию *Enabled*.
Host-based	Этот параметр может быть выбран. Если администратор желает использовать компьютер-хост для аутентификации. Этот параметр вводится для пользователей Linux с инсталляцией SSH. Значение по умолчанию *Enabled*.

Нажмите **Apply** для принятия изменений.

Аутентификация SSH-пользователя

Данное окно используется для конфигурирования параметров попыток подключения пользователей через SSH. Для получения доступа к следующему окну, нажмите **Security > SSH > SSH User Authentication Mode**.

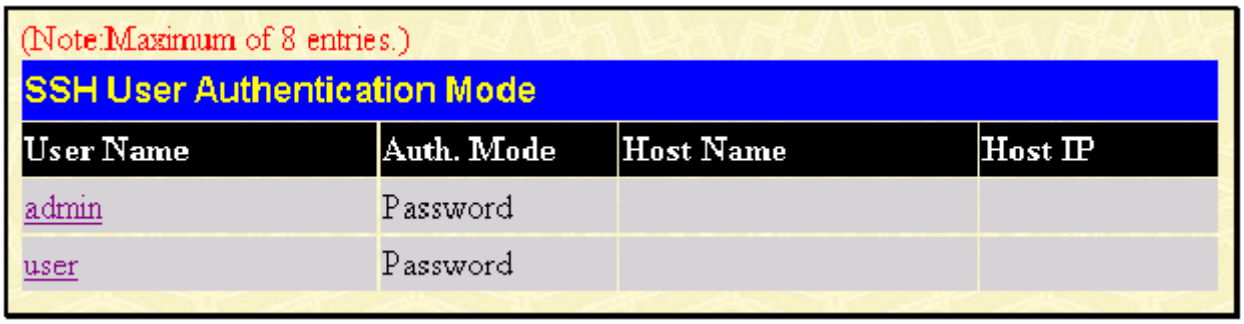


Рисунок 11. 37. Current Accounts окно

Ниже показан пример, User Account «admin» был установлен ранее в окне User Accounts в папке **Security Management**. User Account ДОЛЖЕН быть установлен для того чтобы установить параметры SSH-пользователя. Для конфигурирования параметров SSH-пользователя кликните по гиперссылке с именем пользователя в окне **Current Accounts**, затем откроется следующее окно конфигурации.

Рисунок 11.38. SSH User window для доступа к коммутатору.

Пользователь может задать следующие параметры:

Параметр	Описание
User Name	Для идентификации SSH-пользователя введите имя пользователя не более 15 символов. Это имя пользователя должно быть предварительно сконфигурировано на Коммутаторе как учётная запись пользователя.
Auth. Mode	Администратор может выбрать одну из следующих установок авторизации попыток пользователей при подключении к Коммутатору. *Host Based* – этот параметр должен быть выбран, если администратор желает использовать удалённый SSH-сервер для аутентификации пользователей. При выборе данного параметра у пользователя будет запрошена следующая информация для идентификации: • *Host Name* – введите цифробуквенную строку не более 31 символа для идентификации удалённого SSH-пользователя. • *Host IP* – введите соответствующий IP-адрес SSH-пользователя. *Password* – этот параметр должен быть выбран, если администратор желает использовать административный (administrator-defined) пароль. После ввода данного параметра, коммутатор запросит у администратора пароль и тогда напечатает пароль ещё раз для подтверждения. *Public Key* – этот параметр должен быть выбран, если администратор желает использовать для аутентификации на SSH-сервере открытый ключ.
Host Name	Введите цифробуквенную строку не боле 31 символа для идентификации удалённого SSH-пользователя. Этот параметр используется только при выборе Host Based в поле Auth. Mode.
Host IP	Введите соответствующий IP- адрес SSH-пользователя. Этот параметр используется только при выборе Host Based в поле Auth. Mode.

Нажмите **Apply** для принятия изменений.

Примечание: Для установки параметров аутентификации SSH-пользователя на коммутаторе, учётная запись пользователя должна быть сконфигурирована заранее. Для получения большей информации о конфигурации локальной учётной записи пользователя на Коммутаторе смотрите описание «Учетные записи пользователей» в данном руководстве, текущем разделе.

IP-MAC Binding (Связка IP-MAC)

На уровне IP используется адрес, состоящий из четырех байт, на уровне Ethernet адрес состоит из шести байт MAC-адреса. Связка этих двух адресов вместе позволяет осуществлять передачу данных между уровнями. Первостепенной целью связки IP-MAC является ограничение доступа пользователей к коммутатору. Только авторизованный клиент может получить доступ к порту коммутатора благодаря проверки пары адресов IP-MAC в ранее сконфигурированной базе данных.

Если неавторизованный пользователь пытается получить доступ к порту со связкой IP-MAC, происходит блокирование доступа путем удаления пакетов. Максимальное количество записей связок IP-MAC зависит от аппаратных возможностей коммутатора, для данной серии оно равно 500. Создание авторизованных пользователей можно производить вручную через интерфейс командной строки CLI или Web-интерфейс. Привязка IP-MAC к конкретному порту означает, что пользователь может включать и отключать данную функцию на интересующем его порту.

Порт IP-MAC Binding

Для включения или отключения связки IP-MAC на определенных портах, нажмите: **Security ⇨ IP-MAC Binding ⇨ IP-MAC Binding Port ⇨ IP-MAC Binding Ports Setting.** В полях **From** и **To** выберите порт или диапазон портов. Включение или отключение порта производится в поле **State**. Нажмите **Apply** для сохранения изменений.

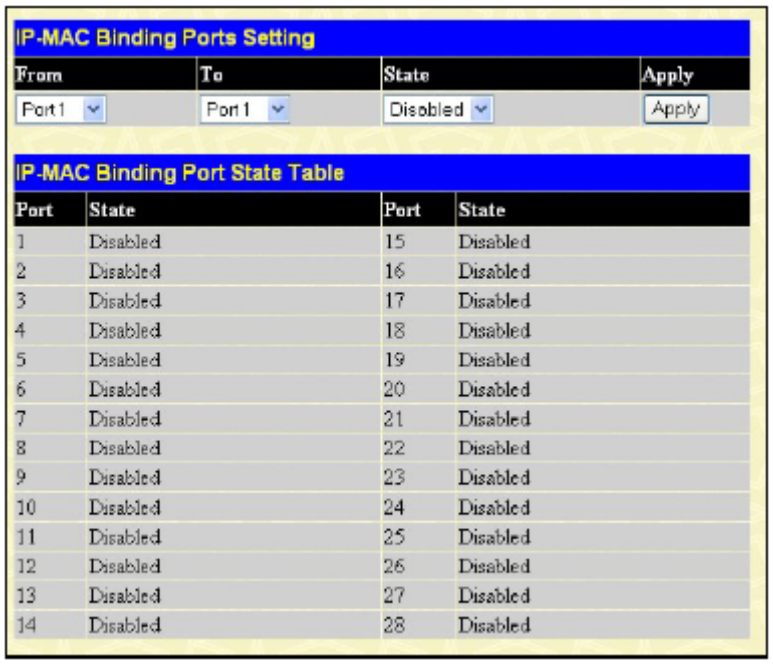


Рисунок 11.39 – Окно «IP-MAC Binding Ports»

IP-MAC Binding Table

Приведенное ниже окно можно использовать для создания записей связок IP-MAC. Для просмотра окна **IP-MAC Binding Setting** нажмите **Security ⇨ IP-MAC Binding ⇨ IP-MAC Binding Table.** Введите IP и MAC-адреса авторизованных пользователей в соответствующих полях и нажмите **Add**. Для преобразования IP-адреса или MAC-адреса в записи связки, внесите изменения в соответствующих полях, после чего нажмите **Modify**. Для поиска записи связки IP-MAC, введите IP – адрес и MAC-адрес и нажмите **Find**. Для удаления записи нажмите **Delete**. Для удаления всех записей из таблицы нажмите **Delete All**.

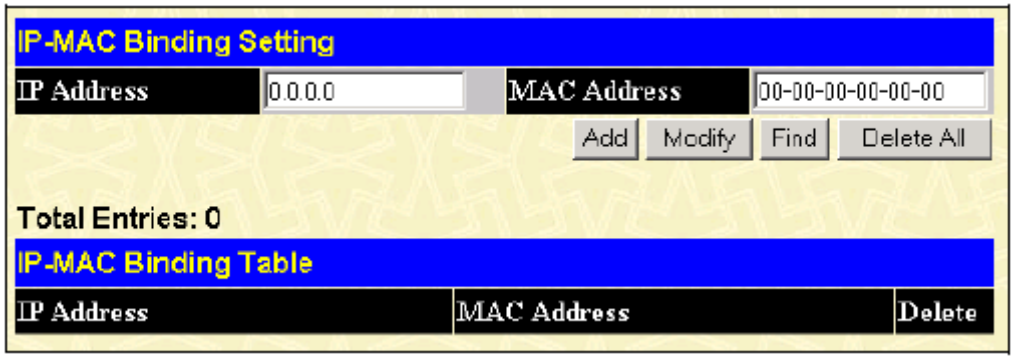


Рисунок 11.40 – Окно «IP-MAC Binding Table»

Блокировка IP-MAC Binding

Для просмотра неавторизованных устройств, которым был блокирован доступ из-за несоответствия связки IP-MAC, откройте окно **IP-MAC Binding Blocked,** для этого нажмите: **Security ⇨ IP-MAC Binding ⇨ IP-MAC Binding Blocked.** В данной таблице можно устанавливать и изменять следующие поля:

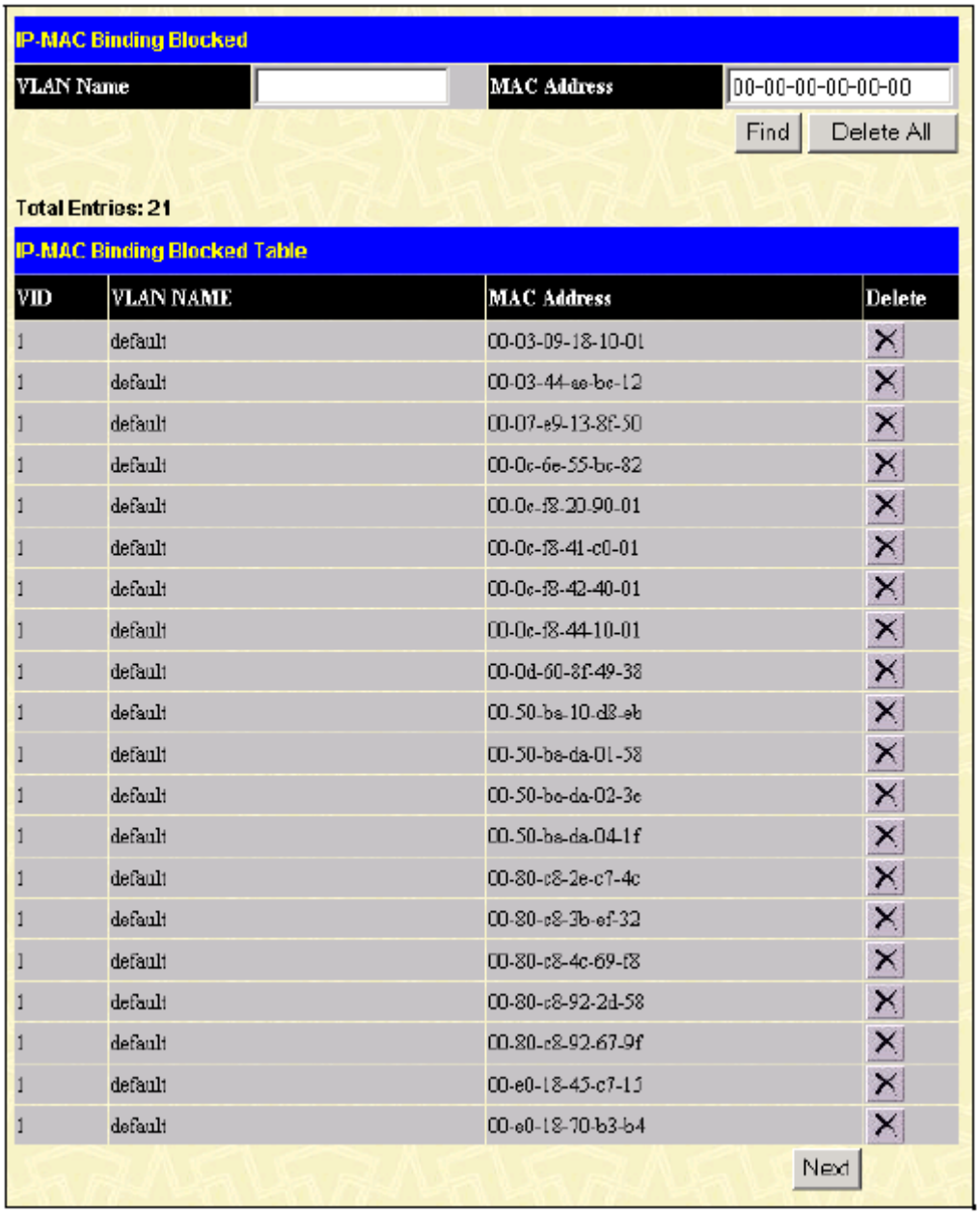


Рисунок 11.41 – Окно «IP-MAC Binding Blocked»

Для поиска неавторизованных устройств, которым был блокирован доступ из-за несоответствия связки IP-MAC, введите название виртуальной локальной сети **VLAN** и **MAC-адрес** в соответствующих полях и нажмите **Find**. Для удаления записи нажмите кнопку удалить , следующую вслед за записью MAC-адреса. Для удаления всех записей в таблице **IP-MAC Binding Blocked Table** нажмите **Delete All.**

Диапазон Limited IP Multicast

Окно **Limited IP Multicast Range** позволяет пользователю определить, какие многоадресные сообщения будут приняты на определённый порт коммутатора. Таким образом, эта функция ограничивает количество принятых сообщений и количество multicast-групп на коммутаторе. Пользователь может установить IP-адрес или диапазон IP-адресов, приходящих на определённые порты коммутатора, для приёма сообщений (Permit) или отказа (Deny).Для открытия окна **Limited IP Multicast Range**, показанного ниже, нажмите **Security ⇨ Limited IP Multicast Range Settings.**

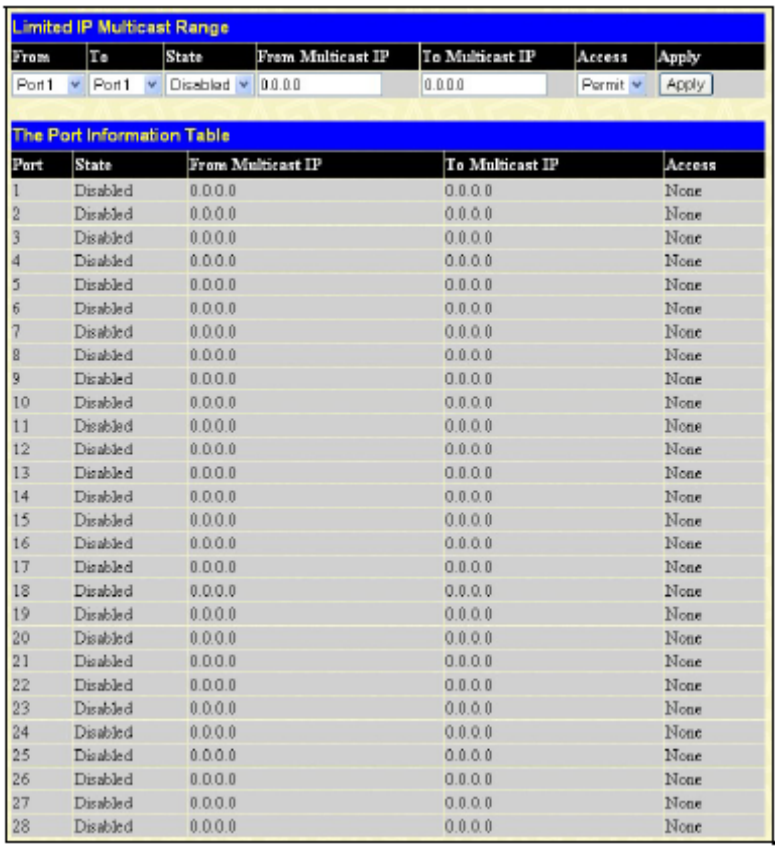


Рисунок 11.42 – Окно «Limited IP Multicast Range»

Для конфигурации Limited IP Multicast Range следует:

1. Выбрать порт или последовательность портов, используя выпадающее меню From…To…
2. с помощью других выпадающих меню можно сконфигурировать параметры описанные ниже:

Параметр	Описание
State	Переключатель **State** может принимать значения *Enabled* или *Disabled*. Передающий порт или группа портов будут принимать или отрицать.
From Multicast IP	Задаётся младший multicast IP-адрес диапазона.
To Multicast IP	Задаётся старший multicast IP-адрес диапазона.
Access	Переключатель **Access** может принимать значения *Enabled* или *Disabled*. Для ограничения или предоставления доступа к указанному диапазону Multicast-адресов на определённом порте или диапазоне портов.

Для того чтобы настройки вступили в силу, нажмите **Apply**.

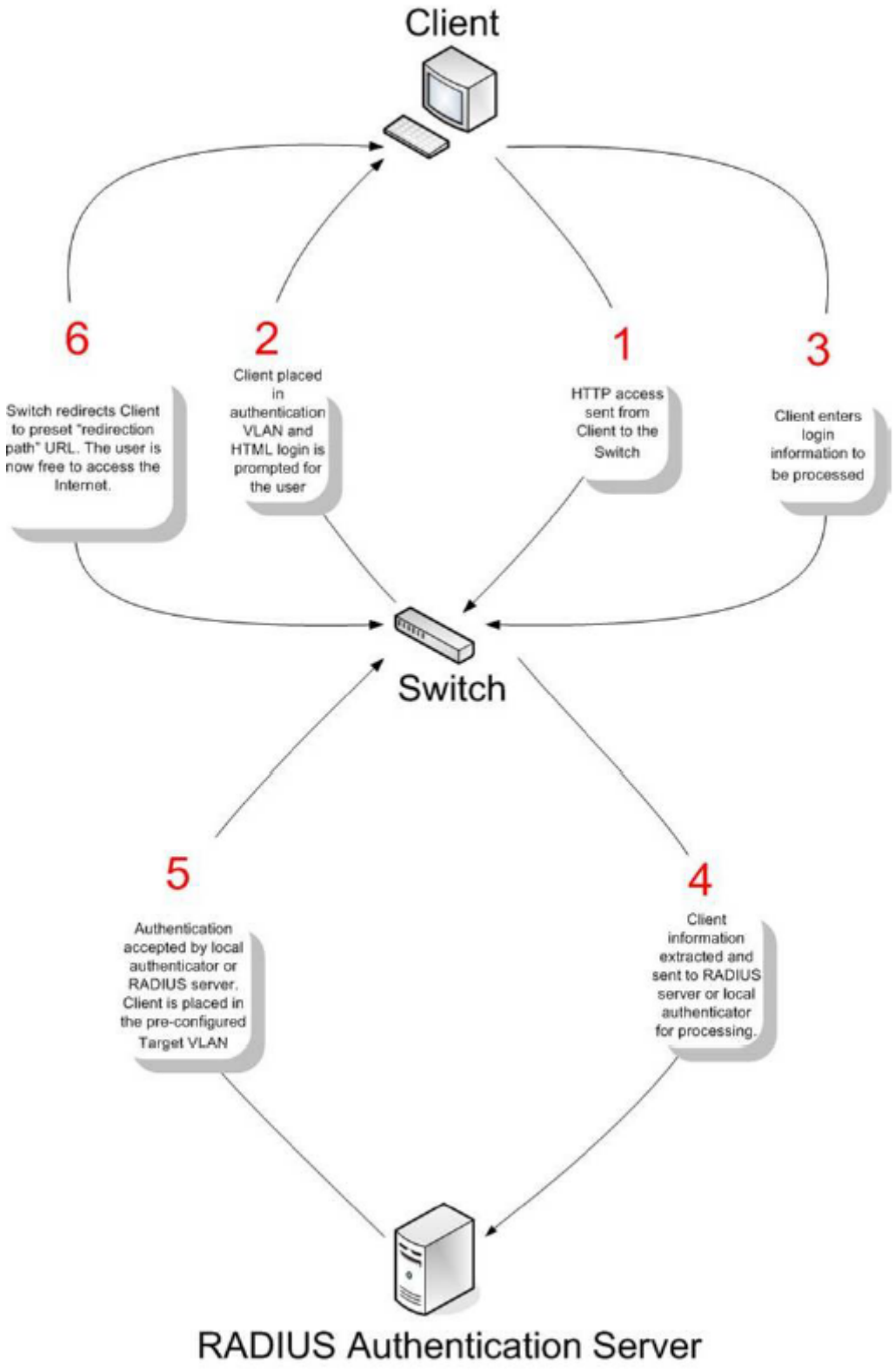
Web-based Access Control (WAC, Контроль доступа на базе Web)

Контроль доступа на базе Web – другой метод контроля доступа на базе порта, который легко совмещается с предварительно установленным контролем доступа 802.1x на базе порта. Эта функция позволит пользователям аутентифицироваться через RADIUS-сервер или с помощью локальной аутентификации, установленной на коммутаторе, если на порту, через который подключается пользователь, установлена данная функция.

Пользователю, пытающемуся получить доступ через Web, будет предложено ввести имя пользователя и пароль, и только после корректного ввода этих данных доступ будет разрешен. Когда клиент пытается получить доступ к Web-сайту, этот порт устанавливается в VLAN аутентификации пользователем. Все клиенты данной VLAN аутентификации будут ждать своей очереди для аутентификации локальным методом или с помощью RADIUS-сервера. Однажды авторизованный, пользователь помещается в target VLAN коммутатора и имеет необходимые права и привилегии для свободного доступа в Internet. Если доступ пользователю был запрещен, пакеты не будут передаваться от/к пользователю, и он будет возвращен в VLAN аутентификации, откуда он и пришел, и получит дополнительные попытки для аутентификации.

Когда клиент единожды прошел аутентификацию на определенном порту, этот порт будет расположен в предустановленную VLAN, и любые другие клиенты на этом порту будут автоматически аутентифицированы для доступа на определенную URL, как аутентифицированные клиенты.

Ниже приведен пример основных шести шагов, необходимых для успешного процесса **Web-based Access Control.**



Условия и ограничения

1. Подсеть IP-интерфейса VLAN аутентификации должна быть точно такая же, как у клиента. Если это не установлено особо, то аутентификатор будет постоянно запрещать аутентификацию.

2. Если клиент использует DHCP для достижения IP-адреса, то VLAN аутентификации должна обеспечивать функции DHCP-сервер или быть совместима с DHCP. Только при этом условии клиент может достигнуть IP-адрес.

3. VLAN аутентификации для этой функции должна быть установлена для доступа к DNS-серверу с целью увеличения производительности CPU и для разрешения DNS, UDP и HTTP пакетов.

4. На коммутаторе существуют определенные функции, которые отфильтровывают HTTP пакеты. Пользователю необходимо соблюдать особую осторожность при установке функции фильтрации для target VLAN, чтобы не запретить HTTP-пакеты на коммутаторе.

5. Путь маршрут переадресации (Redirection Path) должен быть установлен перед подключением Контроля доступа на базе Web.

6. Если для аутентификации будет использоваться RADIUS-сервер, пользователем первым делом должен установить соответствующие параметры RADIUS-сервера.

Для включения опции управления доступом на основе Web-интерфейса сначала откройте папку **Security** и нажмите **WAC Configuration**. После этого появится показанное ниже окно.

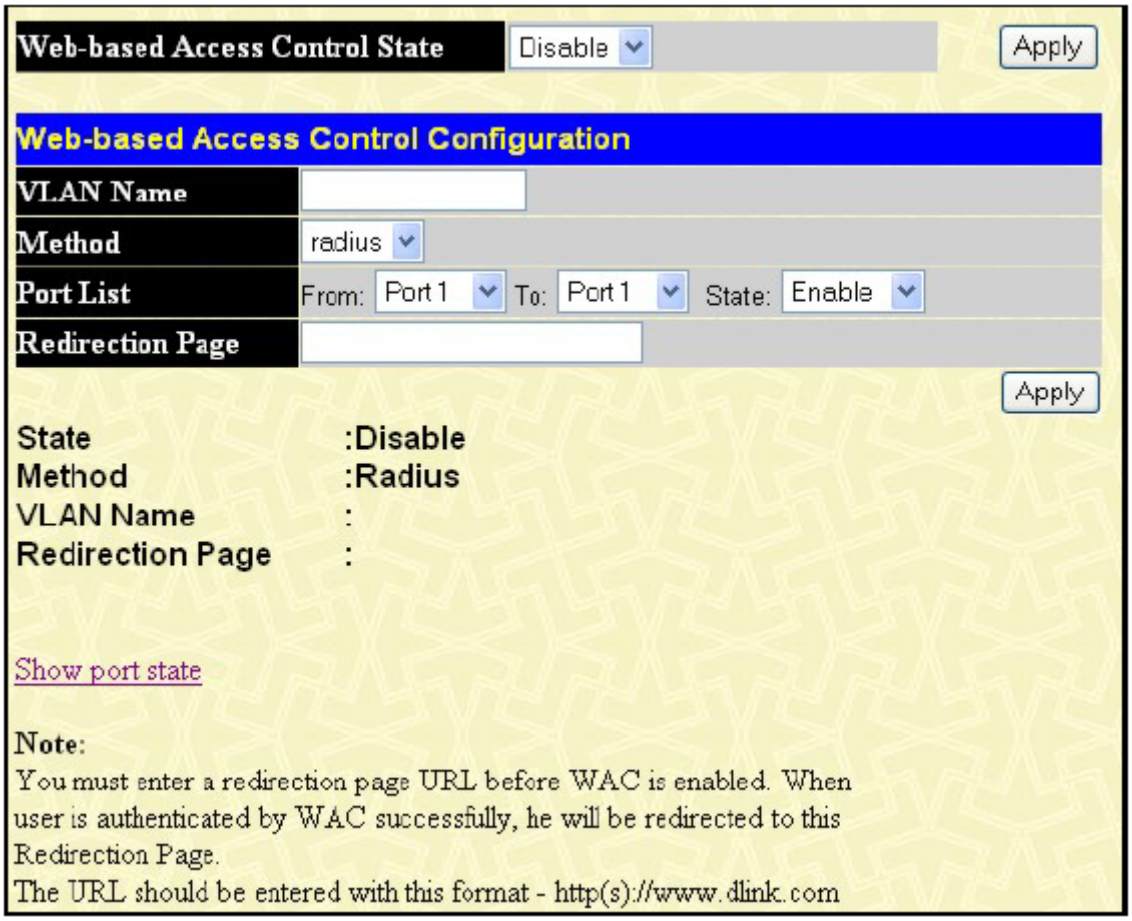


Рисунок 11.43. Web-based Access Control Configuration окно

Для включения опции управления доступа на основе Web заполните следующие поля:

Параметр	Описание
Web-based Access Control State	Позволяет включить (Enable) или выключить (Disable) управление доступом на основе Web.
VLAN Name	Введите имя VLAN, в которой пользователь будет располагаться, пока не будет аутентифицирован коммутатором или RADIUS-сервером. Эта VLAN должна быть предварительно сконфигурирована с ограниченными правами доступа пользователей, аутентифицированных на основе Web.
Method	Используя выпадающее меню, выберите аутентификатор для контроля доступа на основе Web: *Local* – выберите этот параметр для использования метода локальной аутентификации для пользователей, пытающихся получить доступ к сети через коммутатор. Это фактически имя пользователя и пароль для доступа к коммутатору, используя User Account окно, показанное ниже. Radius- выберите этот параметр для использования в качестве аутентификатора удаленного RADIUS-сервера для пользователей, пытающихся получить доступ к сети через коммутатор. RADIUS-сервер должен также быть предустановлен администратором, используя окно RADIUS Server, расположенное в разделе 802.1x.
Port List	Определите порты для подключения контроля доступа на базе Web. Только эти порты будут принимать параметры аутентификации от пользователей, желающих получить права ограниченного доступа через коммутатор. При аутентификации одного клиента на порту для управления доступа на основе Web остальные клиенты, работающие на базе того же порта также получают аутентификацию. Используйте выпадающее меню **State** для включения управления доступа на основе Web для определенных портов.
Redirection Page	Введите URL Web-сайта, на который направляются уже аутентифицированные однажды пользователи. Необходимо заполнить это поле до включения опции управления доступом на основе Web.

Нажмите **Apply** для применения выполненных настроек.

Примечание: Для подключения функции управления доступом на основе Web, в поле **Redirection page** необходимо указать URL Web-сайта, на который пользователь будет перенаправляться, однажды пройдя аутентификацию. Пользователь, нажавший **Apply**, не заполнив предварительно поле **Redirection page** будет сталкиваться с сообщениями об ошибке, и управление доступа на основе Web не будет работать. URL должна быть следующего вида http(s)://www.dlink.com

Примечание: Подсеть IP-адреса VLAN аутентификации должна быть точно такая же, как и у клиента, иначе клиент всегда будет получать отказ в аутентификации.

Примечание: Успешная аутентификация должна направлять клиента на определенную Web-страницу. Если клиент не достигает этой web-страницы, еще не получив **Fail!**-сообщения, то клиент будет уже аутентифицирован, и поэтому должен обновить текущее окно браузера или попытаться открыть другие Web-страницы.

Для просмотра статуса отдельных портов контроля доступа на основе Web, нажмите ссылку Show port state, чтобы открыть показанное ниже окно:

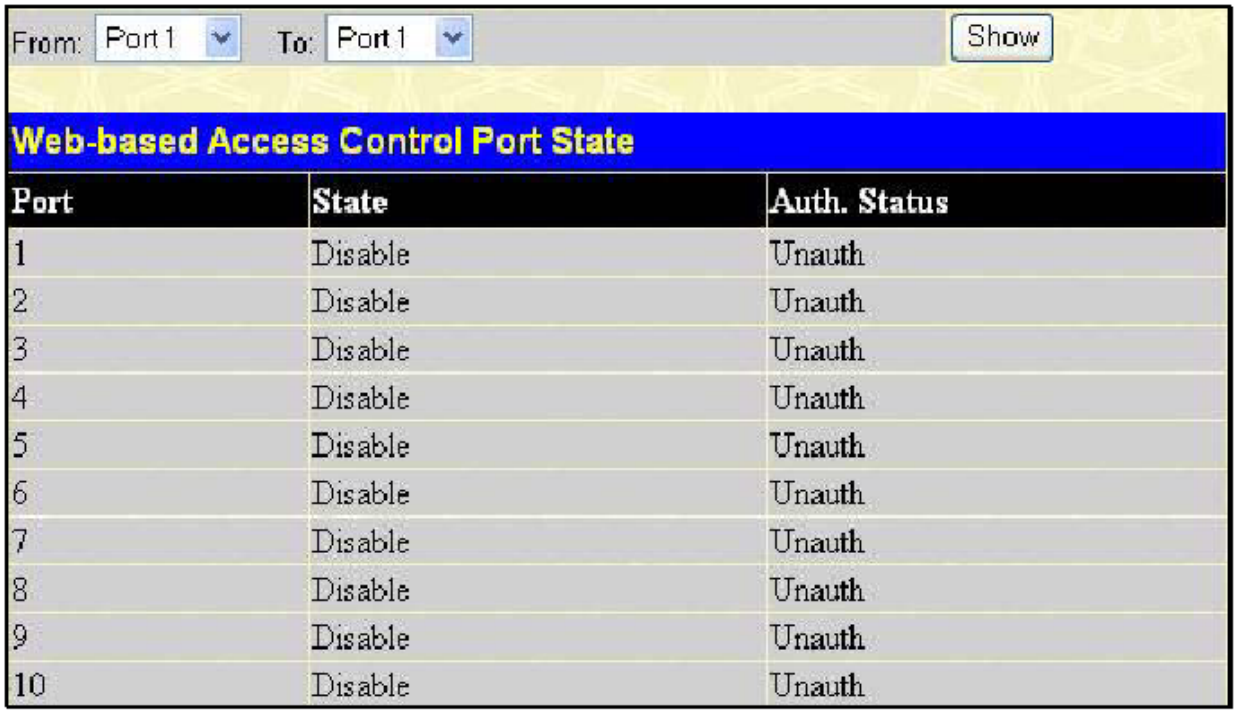


Рисунок 11.44. Web-based Access Control Port State окно

Используйте выпадающее меню в полях **From** и **To** для выбора порта или диапазона портов, для которых требуется просмотреть состояние контроля доступа на основе Web. В предыдущем окне, для просмотра выбраны порты 1-10.

Для просмотра учетных записей пользователей, настроенных для управления доступа на основе Web, нажмите **Security>User Account Management**, после чего появится следующее окно для настроек пользователя:

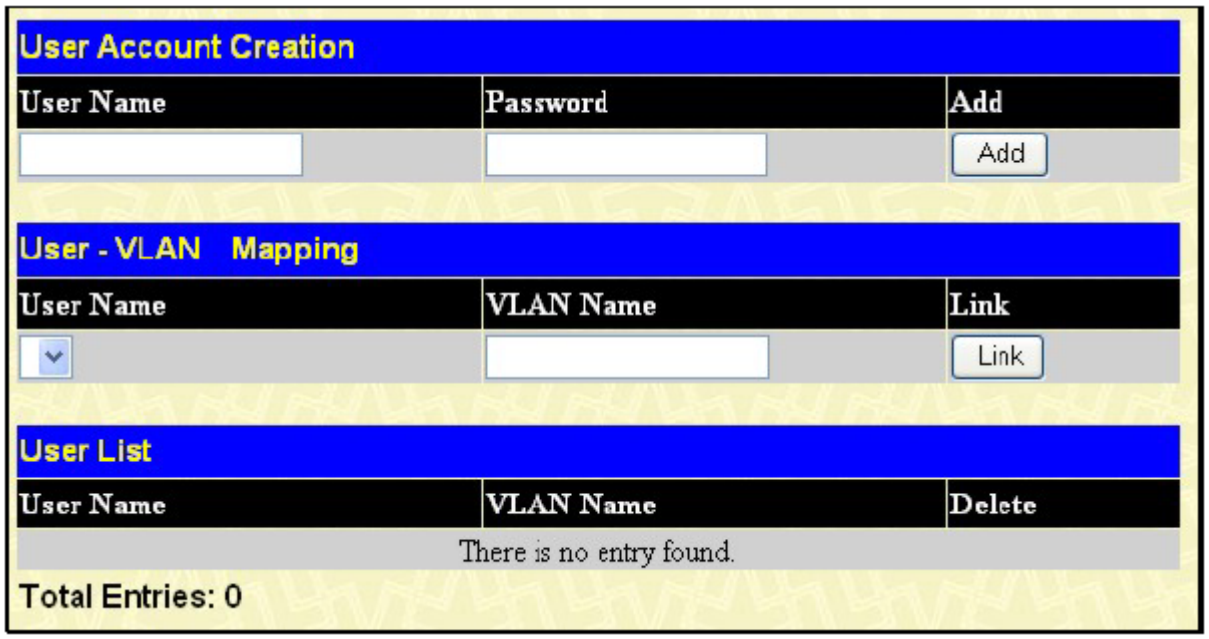


Рисунок 11.45. Web-based User Account Settings окно

Для установки учетной записи пользователя для контроля доступа на базе Web, заполните следующие поля:

Параметр	Описание
Создание учетной записи пользователя	
User Name	Введите имя пользователя до 15 буквенно-цифровых знаков, идентифицирующих пользователя, желающего получить доступ к Web с включенной опцией управления доступа на основе Web. Это поле для администраторов, выбравших поле *local* для аутентификатора на основе Web.
Password	Введите пароль, выбранный администратором для определенного пользователя. Это поле чувствительно к изменению регистра и представляет собой буквенно-цифровую последовательность без пробелов. Это поле для администраторов, выбравших поле *local* для аутентификатора на основе Web.
User-VLAN Mapping	
User Name	Введите имя гостевого пользователя, аутентифицированного с помощью данного процесса (WAC), чтобы быть нанесенным в предварительно установленной VLAN с ограниченными правами.
VLAN Name	Введите имя предварительно установленной VLAN, в которую будет занесен Web-пользователь, успешно прошедший аутентификацию.
Link	Нажмите кнопку Link, чтобы отметить имя пользователя и VLAN, установленные в двух предыдущих полях. Пользователи будут подключены непосредственно к VLAN после успешной аутентификации.
User List	Это поле отображает пользователей и соответствующие им VLAN, настроенные для WAC. Для удаления пользователя нажмите соответствующий значок «x».

Следующее окно отображает окна Authentication Login, которые получат гостевые пользователи при первой попытке обращения к WAC. Введите имя пользователя и пароль, установленные в предыдущем окне и нажмите Enter для успешной аутентификации.

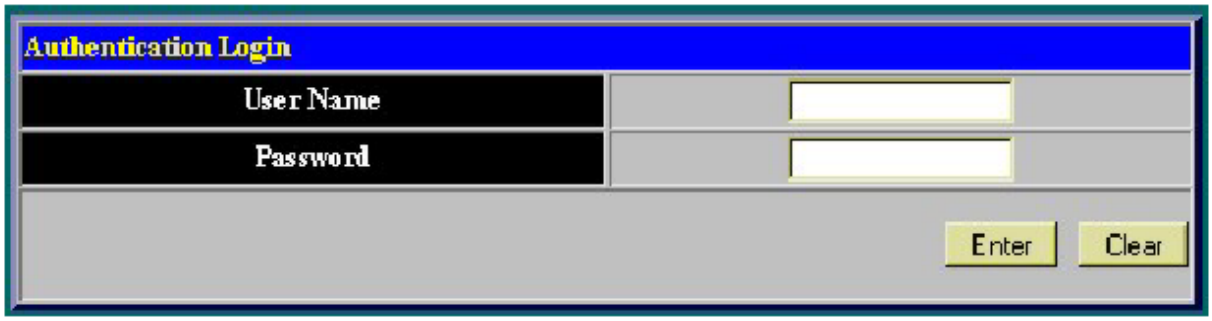


Рисунок 11.46. Web-based Access Control Authentication Login окно

Safeguard Engine

Периодически злоумышленные хосты на сети будут атаковать коммутатор, используя пакетный флудинг (от англ. flooding – наводнение, ARP-шторм) или другие способы. Без применения Safeguard Engine количество таких атак может значительно возрасти. Для уменьшения влияния этой проблемы, на программном обеспечении коммутатора была добавлена функция Safeguard Engine.

Safeguard Engine может оказаться полезным для достижения максимальной работоспособности коммутатора путем минимизации рабочей загрузки коммутатора при атаке, давая возможность пересылать важные пакеты по сети в ограниченном диапазоне. Когда коммутатор а) получает слишком много пакетов для обработки или б) использует слишком много памяти, он будет введен в режим **Exhausted (**истощенный режим). В этом режиме коммутатор будет отбрасывать все ARP-пакеты и все широковещательные IP-пакеты в течение определенного временного интервала. Каждые пять секунд коммутатор будет проверять, все так же ли много флудинг-пакетов поступает на коммутатор. Если пороговое значение преодолено, то коммутатор инициирует остановку всех поступающих на вход ARP-пакетов и всех широковещательных IP-пакетов на 5 секунд. По истечении еще 5 секунд, коммутатор снова проверит входящий поток пакетов. Если флуд приостановлен, коммутатор снова начинает принимать все пакеты. Если проверка показывает по-прежнему слишком много флудинг-пакетов, поступающих на коммутатор, то он перестает принимать все ARP- пакеты и все широковещательные IP-пакеты в течение удвоенного времени предыдущего периода остановки приема пакетов. Удвоение времени остановки приема всех ARP-пакетов и всех широковещательных IP-пакетов будет продолжаться до достижения максимального времени (320 секунд) и далее этот интервал уже не будет увеличиваться. Для лучшего понимания изучите следующий пример Safeguard Engine.

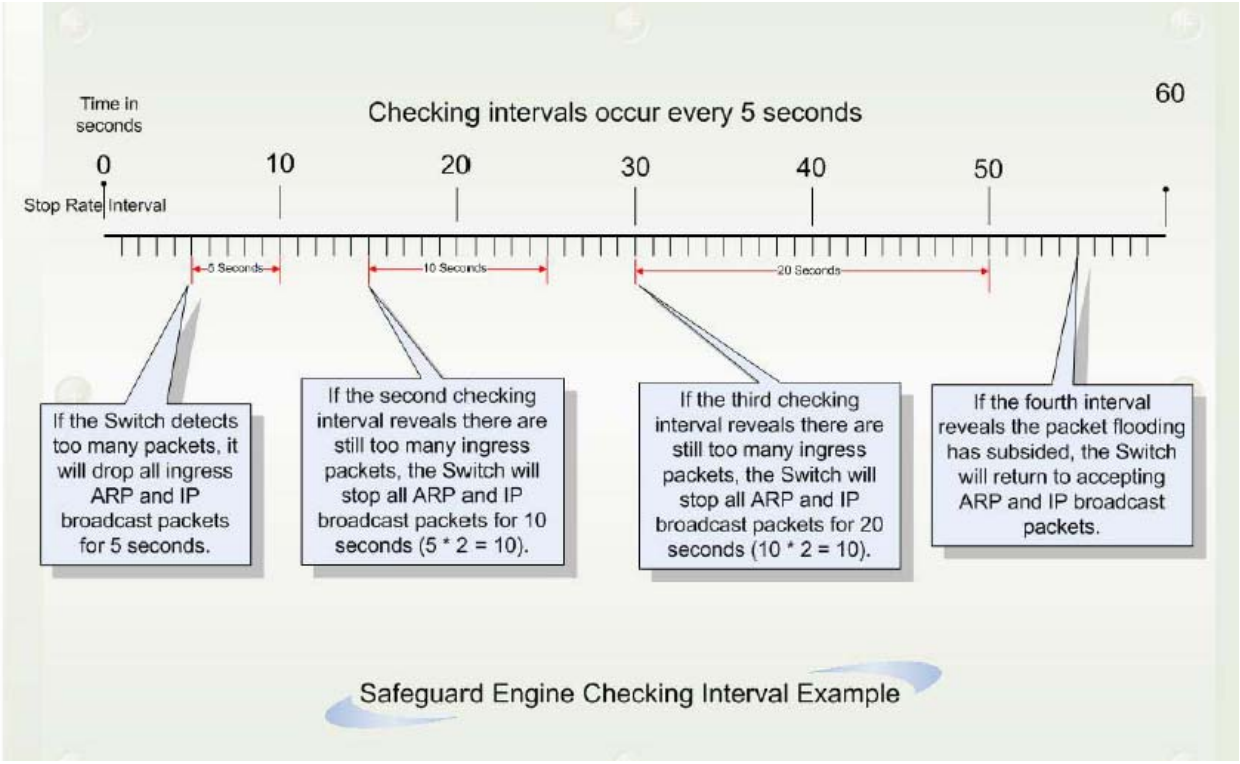


Рисунок 11.47. Пример Safeguard Engine

Для каждого последующего интервала проверки, при которой обнаруживается флудинг-пакетов, коммутатор будет удваивать время, в течение которого он будет отбрасывать ARP- пакеты и широковещательные IP-пакеты. В показанном выше примере коммутатор удваивает время отбрасывания ARP- пакетов и широковещательных IP-пакетов, когда в течение двух интервалов по 5 секунд были обнаружены флудинг-пакеты. (первая остановка = 5 секунд, вторая остановка = 10 секунд, третья остановка = 20 секунд). Когда флудинг-пакеты больше не обнаружены, период отбрасывания ARP- пакетов и широковещательных IP-пакетов возвращается к 5 секундам и при необходимости процесс может быть запущен вновь.

В истощенном режиме, поток пакетов будет уменьшаться наполовину по сравнению с уровнем, в котором находился коммутатор перед входом в истощенный режим. После того, как поток пакетов

стабилизируется, то сначала произойдет его увеличение на 25%, а затем он вернется в нормальный режим.

Для настройки Safeguard Engine на коммутаторе нажмите **Security> Safeguard Engine**, после чего откроется следующее окно:

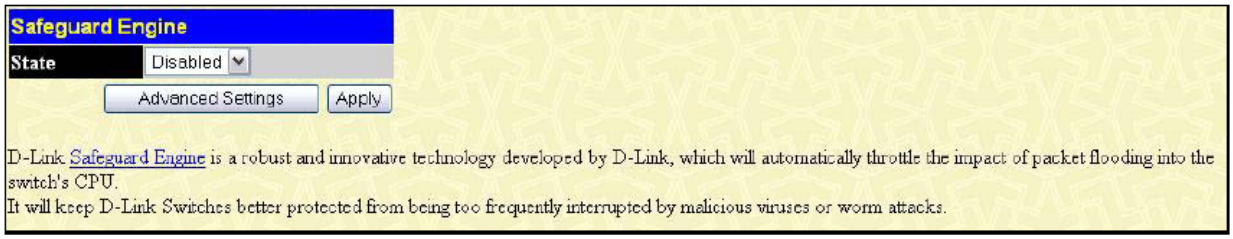


Рисунок 11.48. Safeguard Engine окно

В появившемся окне заполните следующие поля:

Параметр	Описание
State	Переключите данное поле между Enabled и Disabled для подключения/отключения на коммутаторе Safeguard Engine.
Rising Threshold	Используется для установки допустимого уровня загрузки CPU до запуска механизма Safeguard Engine. Когда загрузка CPU достигнет данного процентного соотношения, коммутатор перейдет в **Exhausted** режим.
Falling Threshold	Используется для установки допустимого уровня загрузки CPU, когда коммутатор выйдет из **Exhausted** режима и вернется к нормальному режиму работы.
Trap/Log	Используйте выпадающее меню для включения или отключения посылки сообщений на SNMP-агент устройства и в журнал коммутатора об активации Safeguard Engine.

Раздел 12 – Мониторинг устройства

Статус устройства
Использование CPU
Статус Safeguard Engine
Использование порта
Пакеты
Ошибки
Размер пакетов
Просмотр порта маршрутизатора
Контроль Port Access
Таблица MAC-адресов
Таблица IP-адресов
Просмотр таблицы маршрутизации
Просмотр ARP-таблицы
Просмотр таблицы IP Multicast Forwarding
Группа IGMP Snooping
IGMP Snooping Forwarding
Просмотр таблицы IGMP-групп
Мониторинг DVMRP
Мониторинг OSPF
Просмотр статуса PoE
Настройки просмотра WRED
Системный журнал коммутатора

Статус устройства (Device Status)

Окно **«Device Status»** отображает информацию о состоянии внутреннего и внешнего источников питания, вентиляторов на боковой и задней панелях коммутатора.

Device Status

ID	Internal Power	External Power	Side Fan	Back Fan
1	Active	Fail	Fail	OK

Рисунок 12.1 – Окно «Device Status»

Использование CPU

Окно **«CPU Utilization»** позволяет получить процентное соотношение использования процессора CPU. Для работы с данным окном нажмите: **Monitoring ⇨ CPU Utilization.**

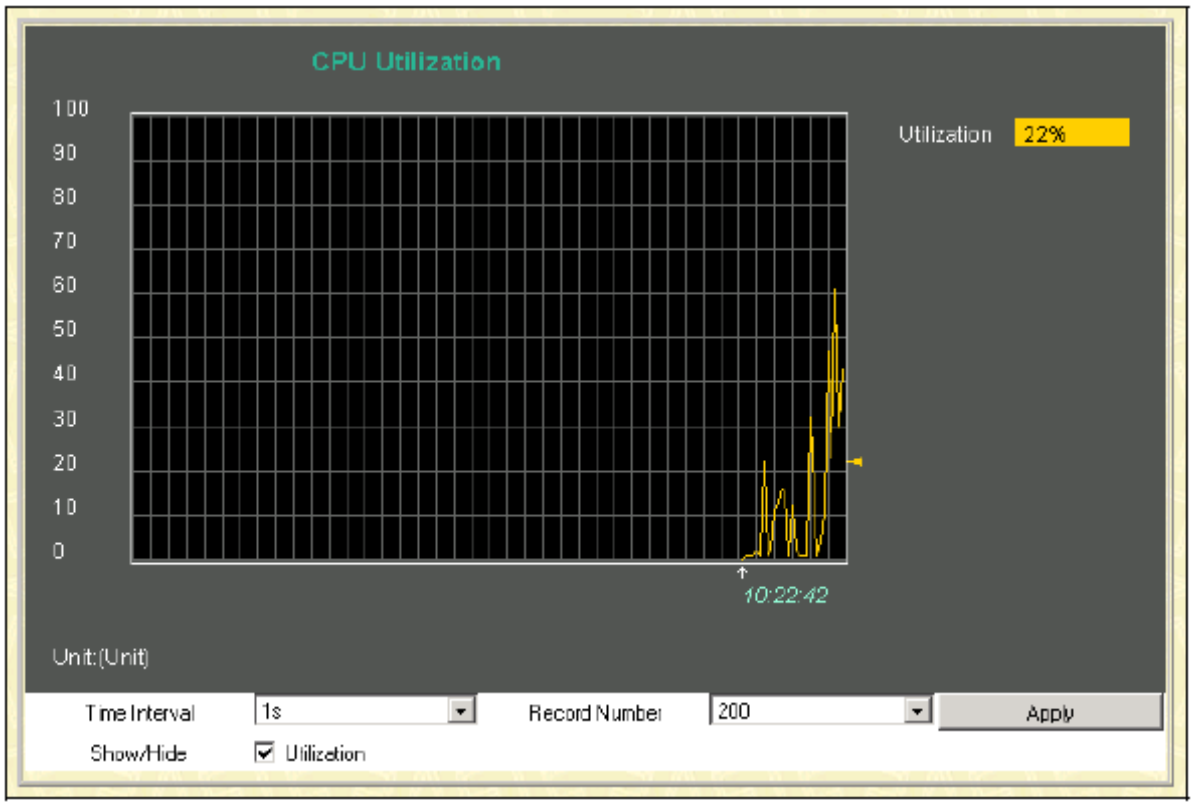


Рисунок 12.2 – Окно CPU Utilization (Использование CPU)

В появившемся окне существует возможность ввести следующие параметры:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с. Этот параметр указывает временной интервал, через который будет проводиться измерение использования CPU.
Record Number	В этом поле необходимо указать значение от 20 до 200 (по умолчанию указано 200). Этот параметр задает, сколько раз будет измеряться значение использования CPU с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка.
Utilization	Отметив это поле, пользователь получает возможность просмотреть среднее использование CPU (значение простого среднего на основании полученной выборки значений использования CPU в различное время). Если же достаточно лишь графического отображения информации, то это поле можно не отмечать.

Ввод указанных параметров и нажатие на **Apply** приведет к обновлению информации.

Статус Safeguard Engine

Окно «Safeguard Engine» отображает параметры настройки функции Safeguard Engine, которая является средством защиты процессора CPU. CPU коммутатора предназначен для обработки управляющей информации, такой как STP, SNMP, доступ по WEB-интерфейсу и т.д. Также CPU обрабатывает некоторый специфичный трафик, такой как ARP-широковещание, пакеты с неизвестным IP-адресом назначения, IP-широковещание и т.д. Но в современных сетях достаточно много вирусов и вредоносного трафика. Обычно они генерируют много «интересного» для CPU трафика (такого как ARP-широковещание например). Поэтому очень важно обеспечить защиту CPU. D-Link Safeguard Engine позволяет идентифицировать и приоритезировать этот «интересный» для CPU трафик с целью отбрасывания ненужных пакетов для сохранения функциональности коммутатора.

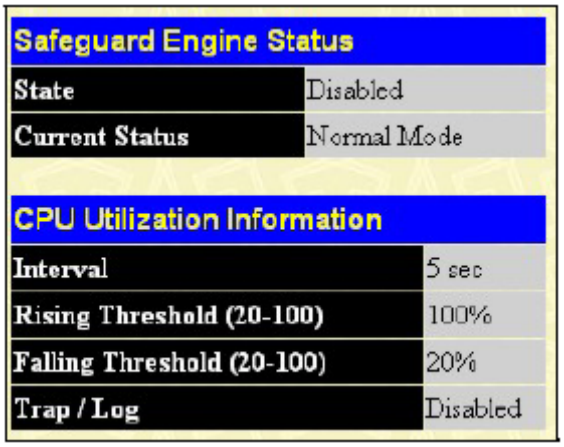


Рисунок 12.3 – Окно «Safeguard Engine Status» и «CPU Utilization Information»

Параметр	Описание
State	В данном поле отображается текущее состояние функции Safeguard Engine: включена (Enabled) или выключена (Disabled).
Current Status	В данном поле отображается текущий режим работы CPU.
Interval	Отображает временной интервал, через который каждый раз будет проверяться загрузка CPU и сравниваться со значениями порогов **Rising Threshold** и **Falling Threshold**. По умолчанию составляет 5 секунд.
Rising Threshold	Пользователь может установить значение в процентах <20-100> верхнего порога загрузки CPU, при котором включается механизм Safeguard Engine. Если загрузка CPU достигнет этого значения, механизм Safeguard Engine начнёт функционировать.
Falling Threshold	Пользователь может установить значение в процентах <20-100> нижнего порога загрузки CPU, при котором выключается механизм Safeguard Engine. Если загрузка CPU снизится до этого значения, механизм Safeguard Engine перестанет функционировать.
Trap/log	Позволяет включить/выключить отправку сообщений об активации механизма Safeguard Engine в журнал коммутатора / SNMP.

Использование порта

Функция Port Utilization (Использование порта) является еще одним важным инструментом мониторинга состояния сети. Окно **«Utilization»** отображает процентное соотношение общей доступной полосы пропускания к полосе, приходящейся на порт. Для просмотра процентного соотношения использования портов откройте: **Monitoring ⇨ Port Utilization.**

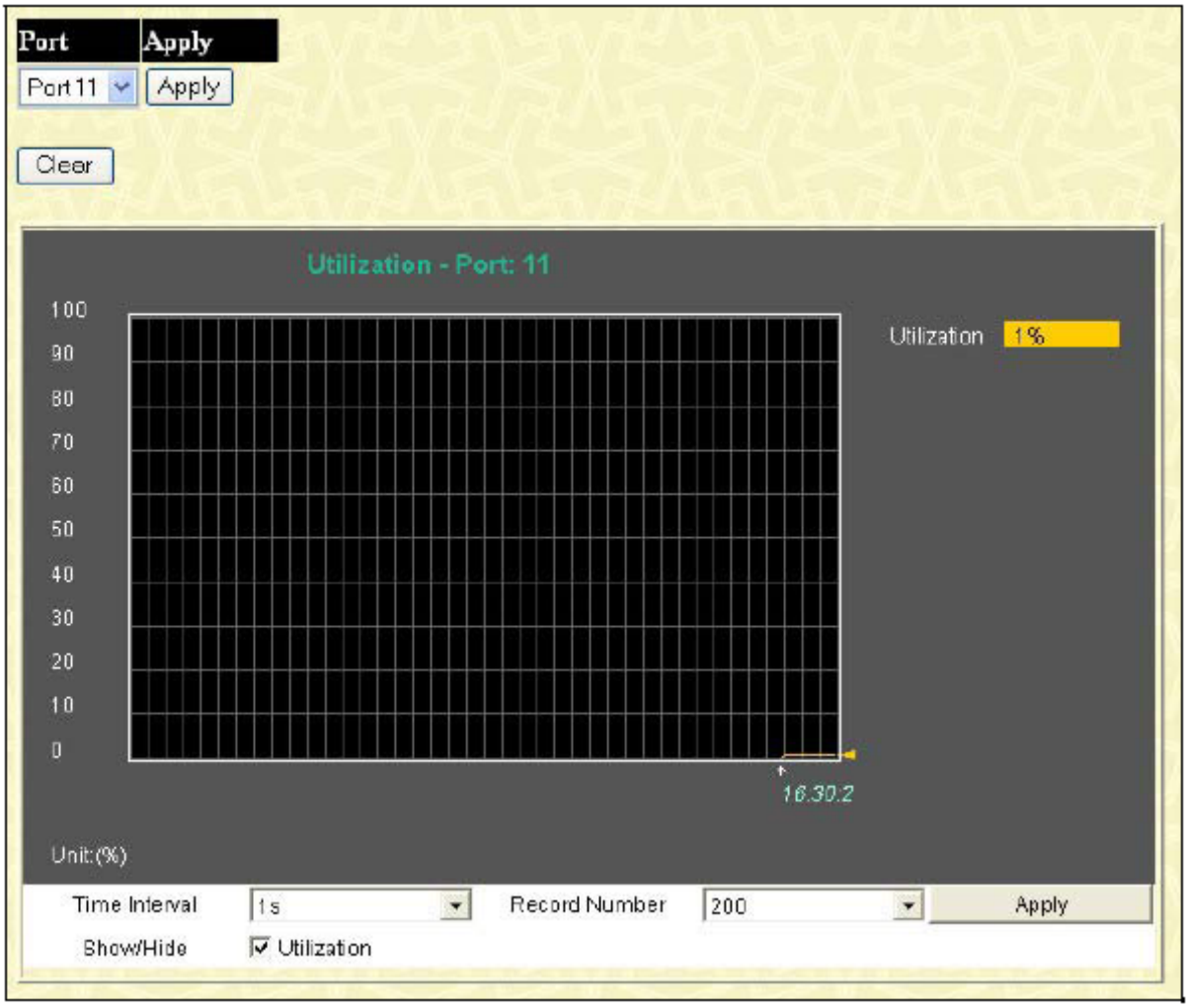


Рисунок 12.4 – Окно «Utilization Port»

Выберите номер порта в выпадающем меню и кликните по **Apply** для отображения диаграммы использования выбранного порта.

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с. Этот параметр указывает временной интервал, через который будет проводиться измерение использования порта.
Record Number	В этом поле необходимо указать значение от 20 до 200 (по умолчанию указано 200). Этот параметр задает, сколько раз будет измеряться значение использования порта с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка

Кликните по **Clear** для очистки поля. Кликните по **Apply** для того, чтобы изменения вступили в силу.

Пакеты

Web-интерфейс управления позволяет просматривать различные статистики по пакетам, как в графическом виде, так и в виде таблицы. Так, пользователь может просмотреть статистику по полученным пакетам, отправленным пакетам, а также многоадресным, одноадресным и широковещательным пакетам, полученным коммутатором. Ниже данные статистики будут рассмотрены более подробно.

Полученные пакеты(RX)

Для просмотра статистики по пакетам, полученным коммутатором, нажмите: **Monitoring ⇨ Packets ⇨ Received (RX).**

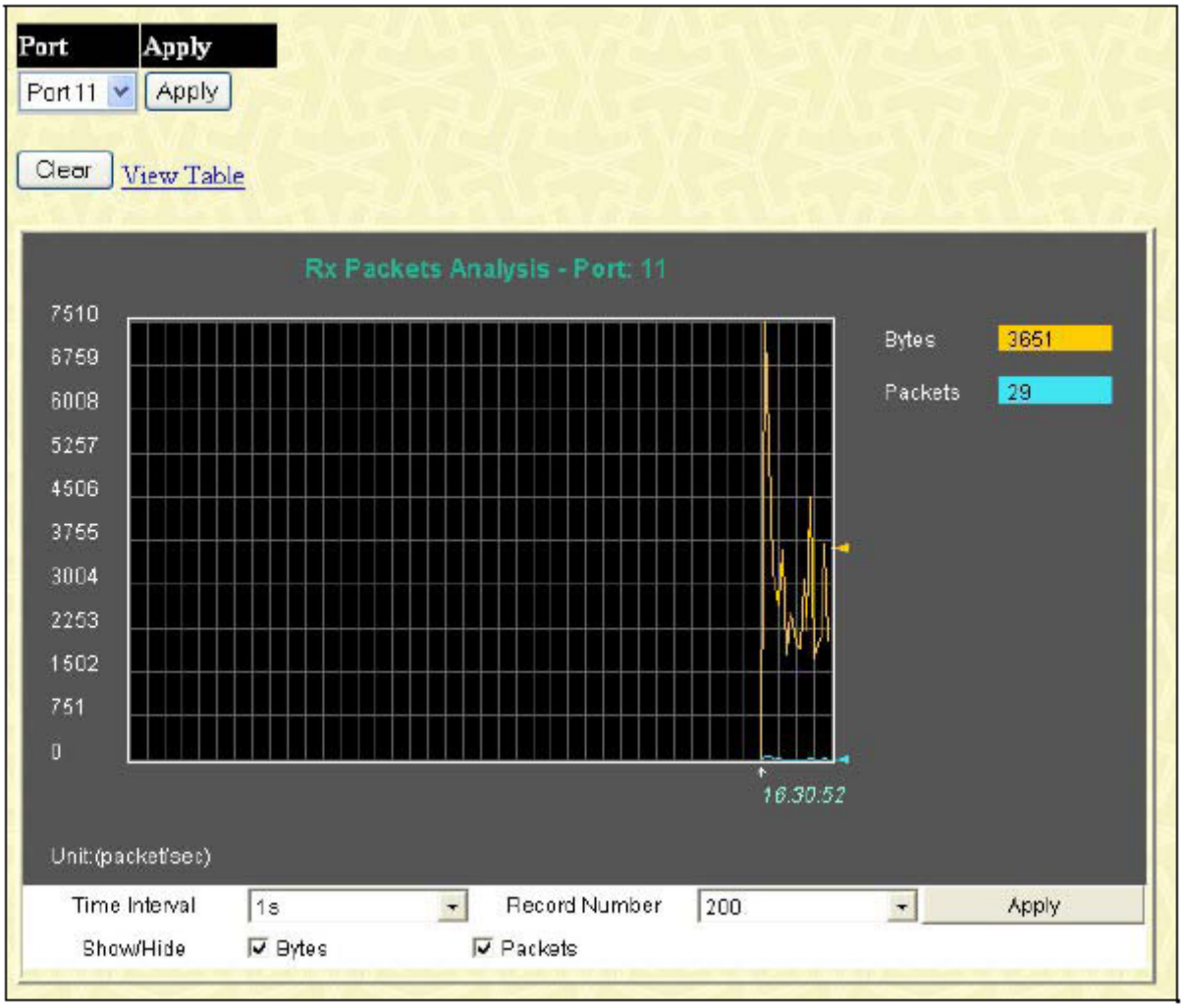


Рисунок 12.5 – Окно «Rx Packets Analysis» (график зависимости количества байт и количества переданных пакетов)

В выпадающем меню выберите номер порта и кликните по **Apply** для отображения статистики по полученным пакетам на выбранном порту. Для просмотра таблицы **Received Packets Table**, кликните по ссылке View Table:

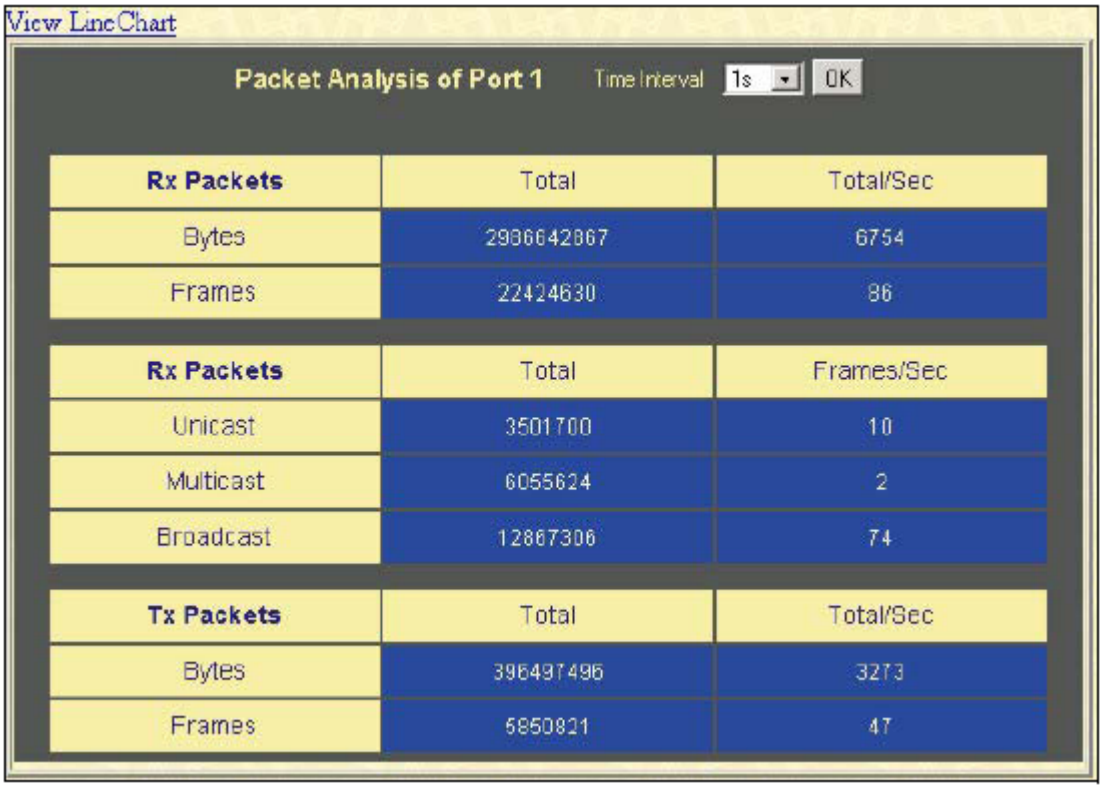


Рисунок 12.6 – Окно «Rx Packets Analysis» (таблица зависимости количества байт и количества переданных пакетов)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с. Через данный временной интервал каждый раз будет измеряться количество пакетов.
Record Number	Этот параметр задает, сколько раз будет измеряться количество пакетов с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка. Данное значение по умолчанию равно 20.
Bytes	Подсчитывает число байт, полученных на порту.
Packets	Подсчитывает число пакетов, полученных на порту.
Show/Hide	Отметьте, нужно ли отображать байты и пакеты или нет.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

UMB Cast (RX)

Для просмотра графика пакетов UMB cast, полученных коммутатором, нажмите: **Monitoring ⇨ Packets ⇨ UMB Cast (RX).**

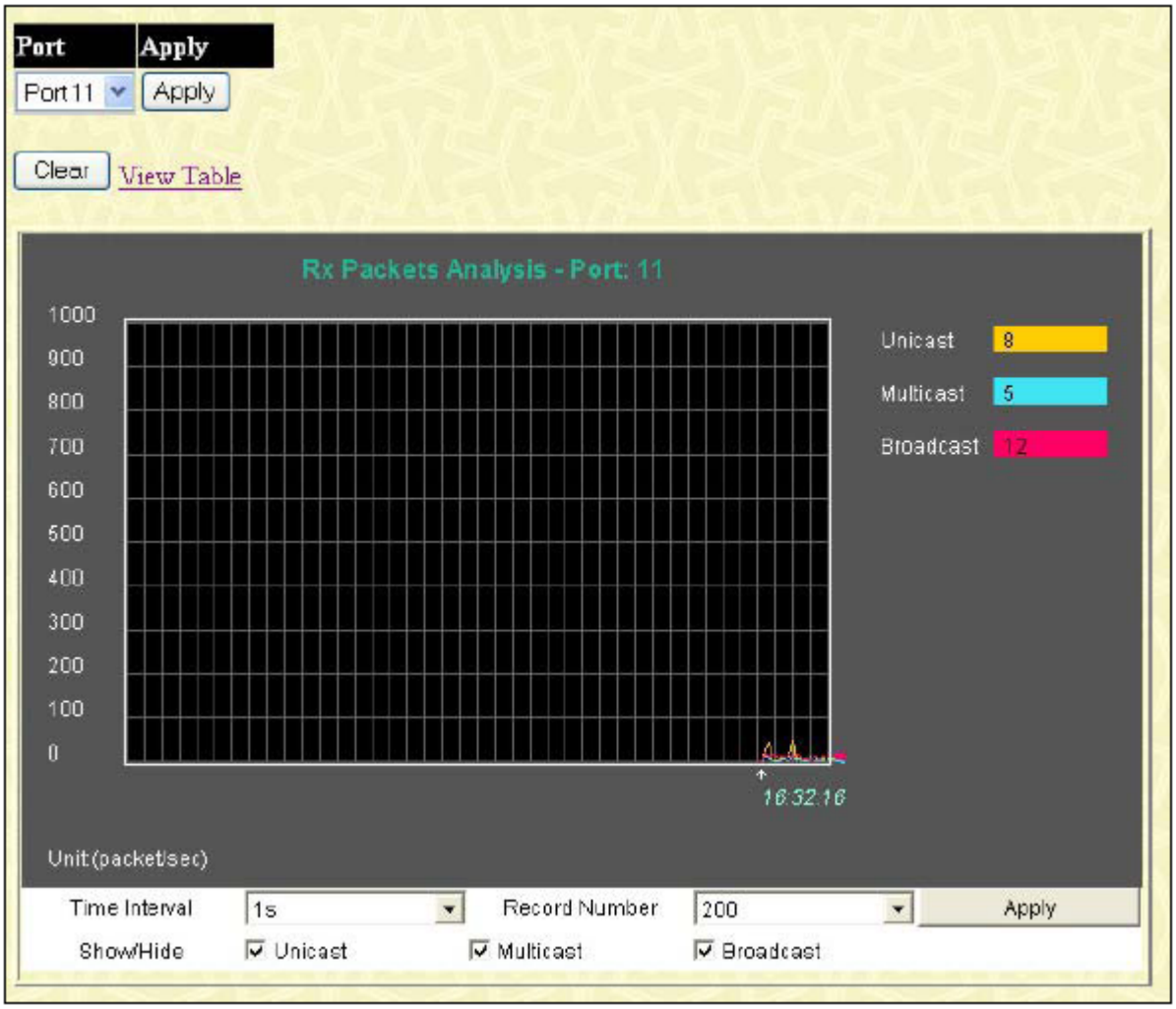


Рисунок 12.7 – Окно «Rx Packets Analysis» (график зависимости Unicast-, Multicast- и Broadcast- пакетов)

Для просмотра таблицы **UMB Cast Table**, нажмите ссылку View Table:

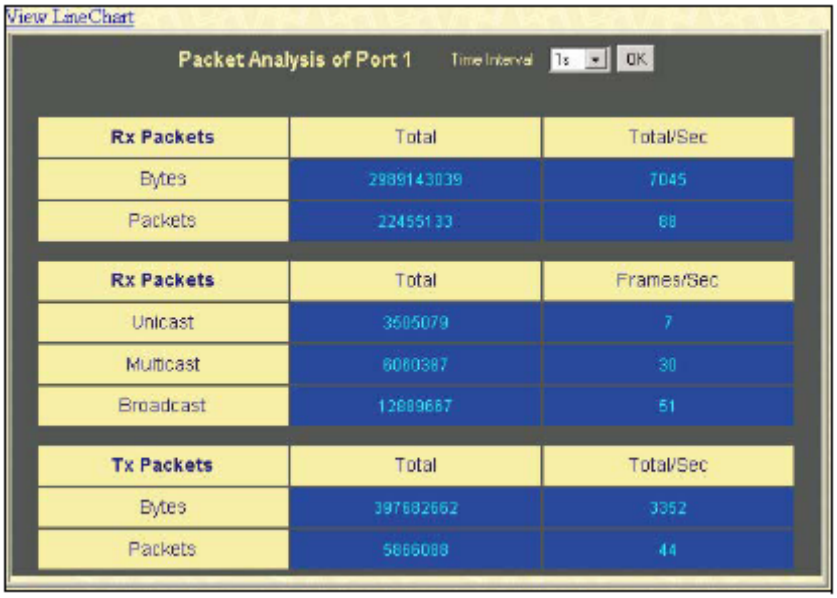


Рисунок 12.8 – Окно «Rx Packets Analysis» (таблица зависимости одноадресных, многоадресных и широковещательных пакетов)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1сек. Через данный временной интервал каждый раз будет измеряться количество пакетов.
Record Number	Этот параметр задает, сколько раз будет измеряться количество пакетов с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка. Данное значение по умолчанию равно 20.
Unicast	Счетчик, отображающий количество пакетов, полученных портом, предназначенных для данного узла.
Multicast	Счетчик, отображающий количество пакетов, полученных данным портом, предназначенных для многоадресной группы, в которой он состоит.
Broadcast	Счетчик, отображающий количество широковещательных пакетов, полученных данным портом.
Show/Hide	Позволяет выбрать, какой тип пакетов будет отображаться: многоадресные (Multicast), широковещательные (Broadcast) и/или одноадресные (Unicast).
Clear	Кликните по этой кнопке для сброса значения всех счетчиков.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Отправленные пакеты (TX)

Для просмотра статистики по пакетам, отправленным коммутатором, нажмите: **Monitoring ⇨ Packets ⇨Transmitted (TX).**

Рисунок 12.9 – Окно «Tx Packets Analysis» (график зависимости количества байт и количества переданных пакетов)

Для просмотра количества переданных коммутатором пакетов TX в виде таблицы, кликните по ссылке View Table:

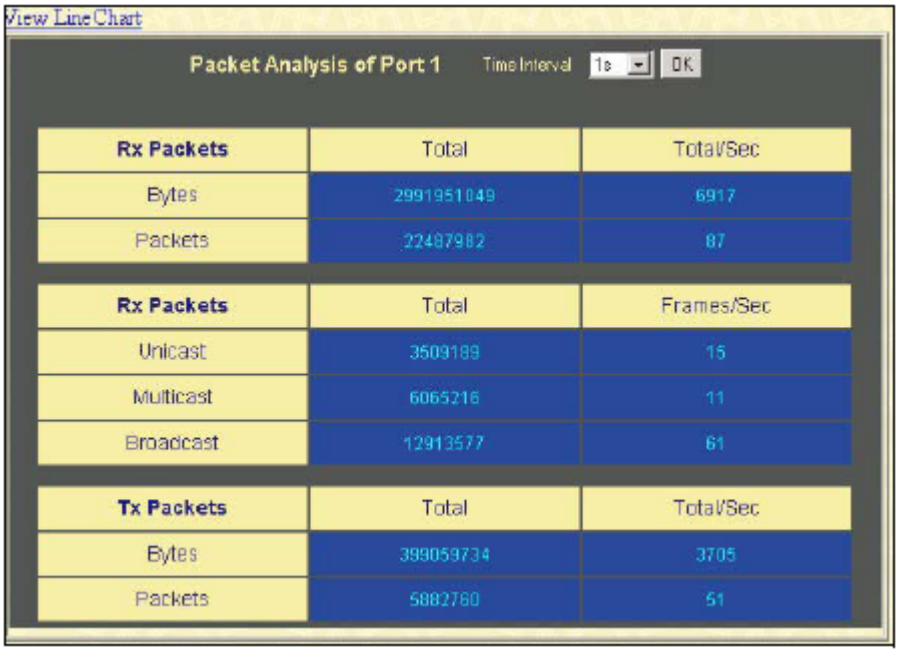


Рисунок 12.10 – Окно «Tx Packets Analysis» (таблица зависимости количества байт и количества переданных пакетов)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с. Через данный временной интервал каждый раз будет измеряться количество пакетов.
Record Number	Этот параметр задает, сколько раз будет измеряться количество пакетов с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка. Данное значение по умолчанию равно 20.от 20 до 200. Данное значение по умолчанию равно 20.
Bytes	Подсчитывает число байт, отправленных с данного порта.
Packets	Подсчитывает число пакетов, отправленных с данного порта.
Show/Hide	Отметьте, нужно ли отображать байты и пакеты или нет.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Ошибки

Web-интерфейс управления позволяет просматривать статистику ошибок по порту, собранную агентом управления коммутатора, как в графическом виде, так и в виде таблицы. Далее остановимся на этом более подробно.

Ошибки в полученных коммутатором пакетах (RX)

Для просмотра следующего графика, отражающего количество ошибок в полученных коммутатором пакетах, нажмите: **Monitoring ⇨ Error ⇨ Received (RX).**

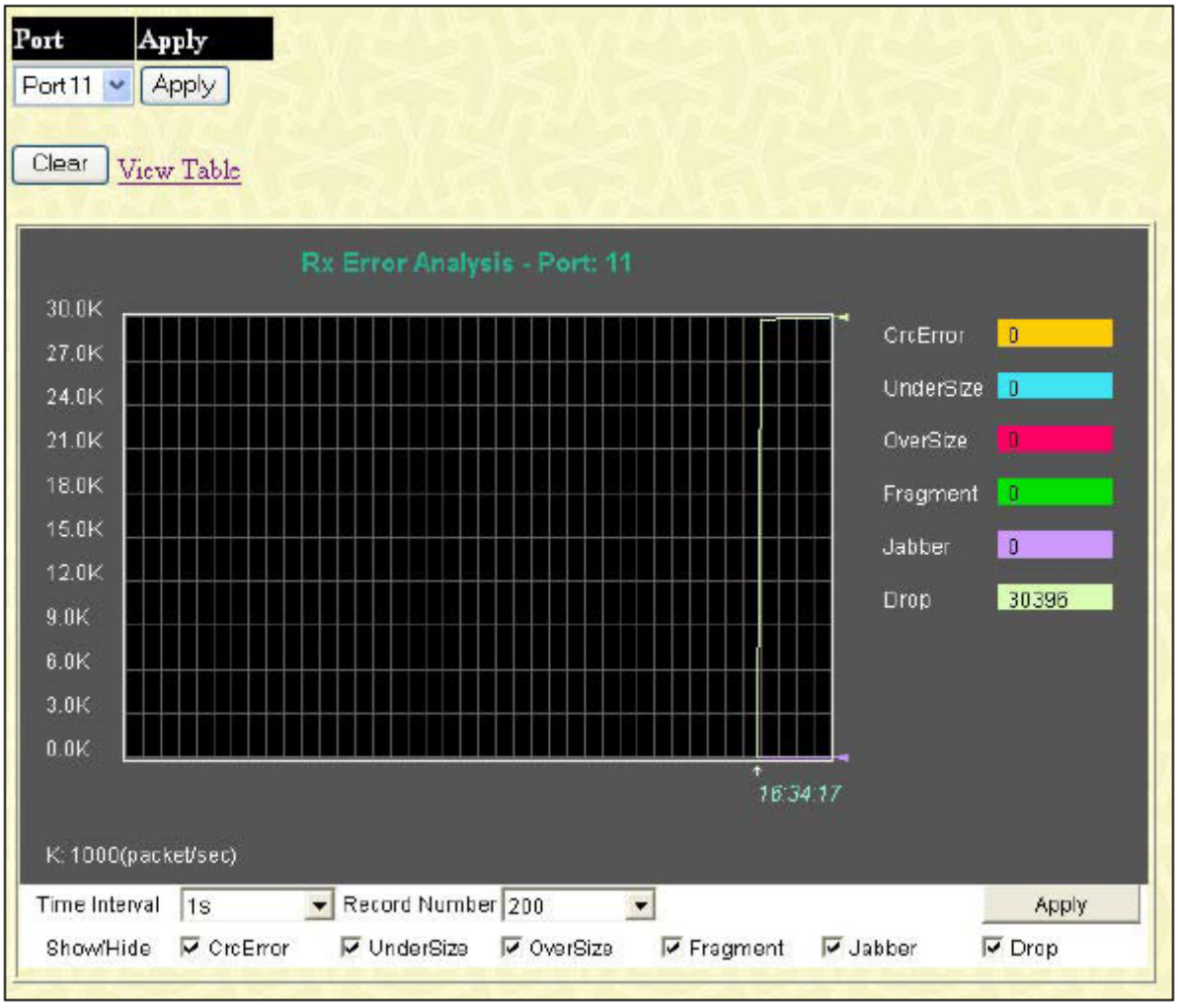


Рисунок 12.11 – Окно «Rx Error Analysis» (график зависимости)

Чтобы увидеть табличное отражение данной зависимости, кликните по ссылке View Table**:**

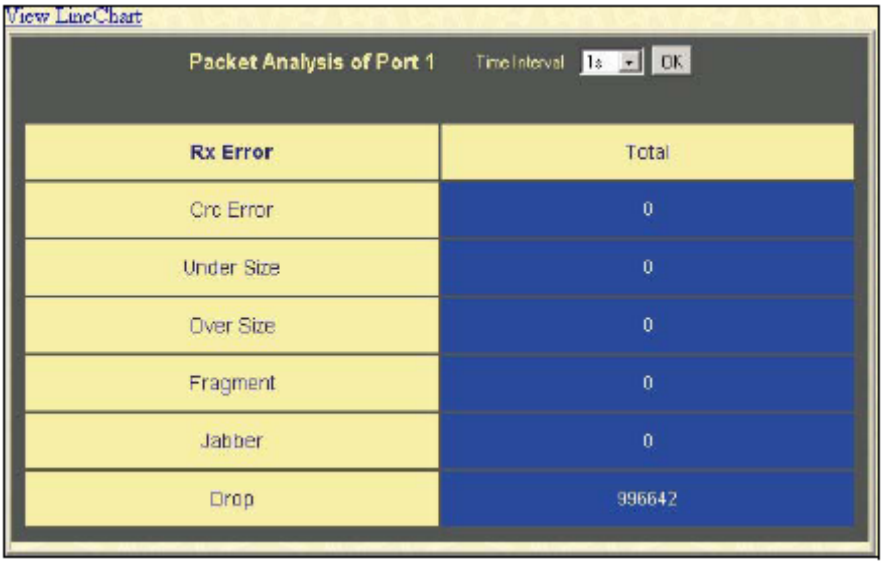


Рисунок 12.12 – Окно «Rx Error Analysis» (таблица)

Следующие поля доступны для настройки:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с.
Record Number	Этот параметр задает, сколько раз будет измеряться количество ошибок с заданным временным интервалом (Time Interval). Данное значение по умолчанию равно 20.
Crc Error	Подсчитывает количество пакетов, не прошедших проверку с помощью циклического избыточного кода.
Under Size	Количество обнаруженных пакетов длиной меньше, чем минимально допустимый размер пакета в 64 байт и верным значением CRC последовательности. Пакеты недостаточной длины обычно указывают на наличие коллизии.
Over Size	Количество пакетов, длиной более 1518 байт, или в случае фрейма VLAN, длиной менее значения MAX_PKT_LEN, равного 1522 байт.
Fragment	Количество пакетов, длиной меньше 64 байт, а также или неправильным значением CRC, что обычно свидетельствует о коллизиях.
Jabber	Количество пакетов, длиной более значения MAX_PKT_LEN, равного 1522 байт.
Drop	Количество пакетов, удаленных данным портом с момента последнего перезапуска коммутатора.
Show/Hide	Отметьте, нужно ли отображать или нет ошибки Crc Error, Under Size, Over Size, Fragment, Jabber и Drop.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Ошибки в отправленных коммутатором пакетах (TX)

В следующем окне отображается график зависимости ошибок в отправленных коммутатором пакетов, для работы с данным окном нажмите: **Monitoring ⇨ Error ⇨Transmitted (TX).**

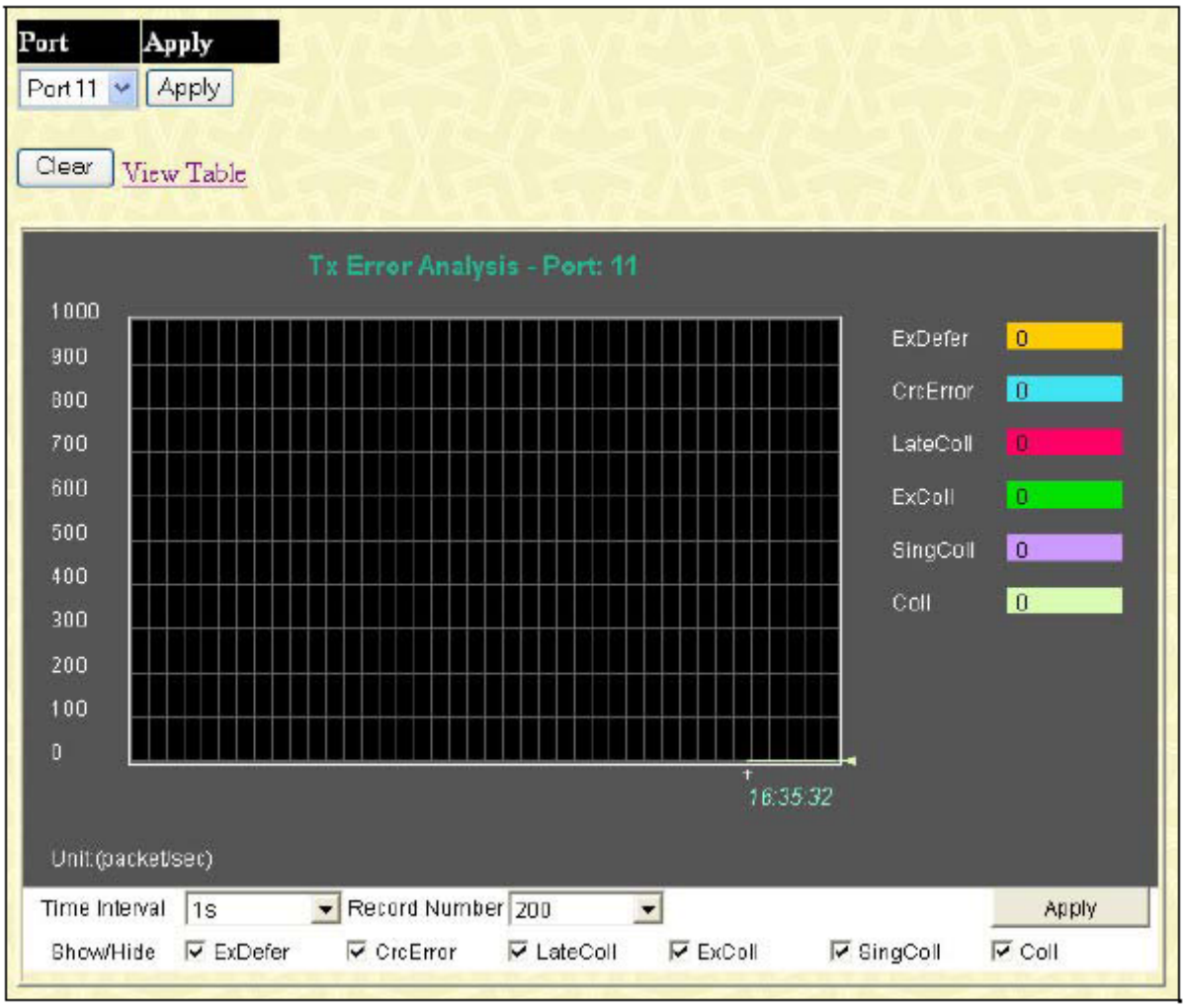


Рисунок 12.13 – Окно «Tx Error Analysis» (график зависимости)

Чтобы увидеть статистику по ошибкам в отправленных коммутатором пакетах в виде таблице, кликните по ссылке View Table**:**

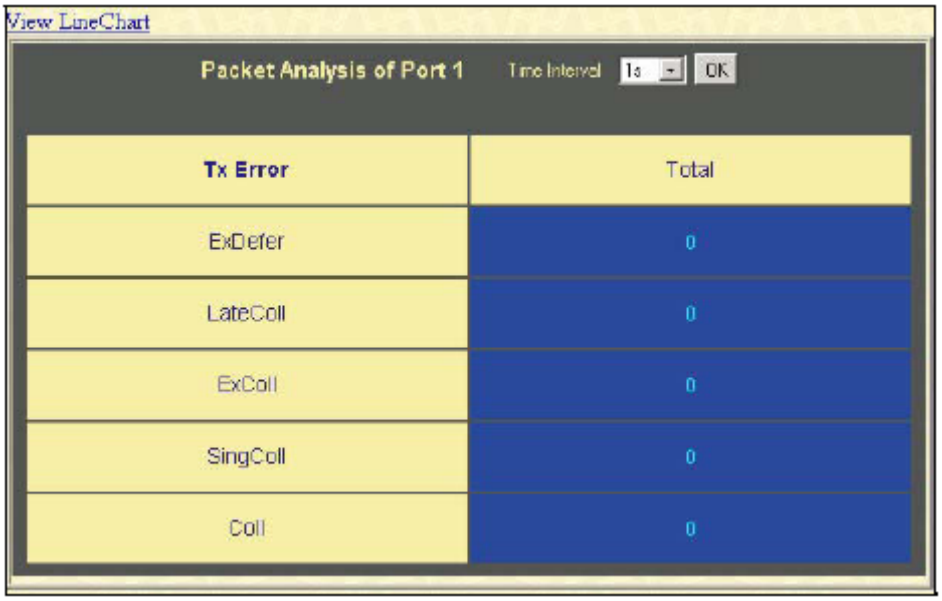


Рисунок 12.14 – Окно «Tx Error Analysis » (таблица)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с.
Record Number	Этот параметр задает, сколько раз будет измеряться количество ошибок с заданным временным интервалом (Time Interval). Данное значение по умолчанию равно 20.
ExDefer	Счетчик, отображающий количество пакетов, которые были задержаны во время первой попытки передачи по определенному интерфейсу из-за того, что среда была занята.
LateColl	Счетчик, отображающий количество раз, когда коллизия при передаче пакета была обнаружена позже, чем за 512 битовых интервала.
ExColl	Excessive Collisions – чрезмерные коллизии. Количество пакетов, не переданных из-за чрезмерных коллизий
SingColl	Single Collision Frames – кадры с одиночными коллизиями. Количество успешно отправленных пакетов, которые были задержаны во время передачи из-за более, чем одной коллизии.
Coll	Оценка общего числа коллизий в данном сегменте сети.
Show/Hide	Отметьте, нужно ли отображать или нет значение соответствующих счетчиков ExDefer, LateColl, ExColl, SingColl и Coll.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Размер пакета

Web-интерфейс управления позволяет просматривать как в графическом виде, так и в виде таблицы, статистику по размеру полученных коммутатором пакетам. При этом в зависимости от размера пакетов выделяется 6 групп.

Рисунок 12.15 – Окно «Rx Size Analysis»(график зависимости)

Чтобы просмотреть ту же статистику в табличном виде, кликните по ссылке **View Table:**

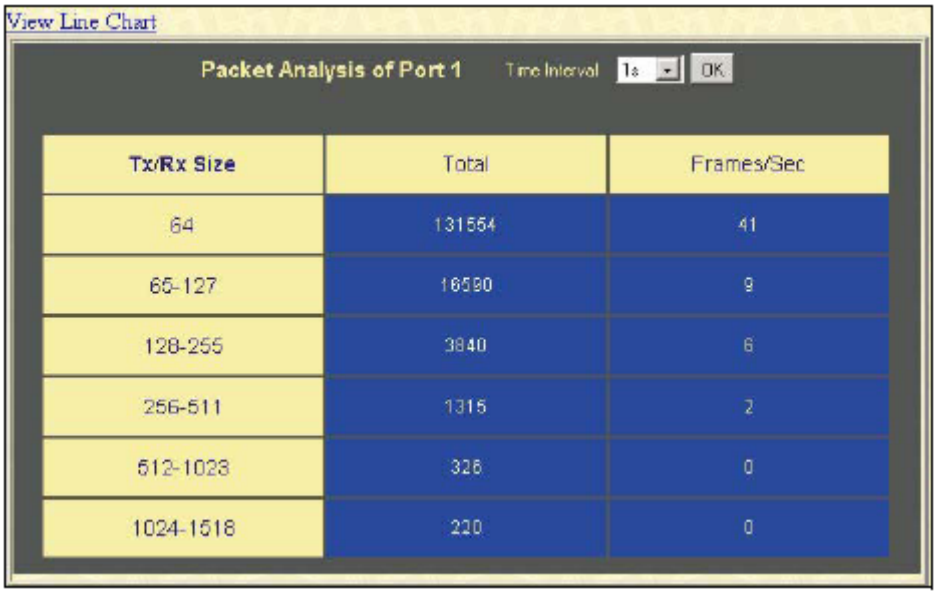


Рисунок 12.16 – Окно «Tx/Rx Packet Size Analysis (таблица)»

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 20.
64	Общее число полученных пакетов (включая «битые» пакеты), длиной 64 байт (исключая биты синхронизации, но включая байты FCS).
65-127	Общее число полученных пакетов (включая «битые» пакеты), длиной от 65 до 127 байт (исключая биты синхронизации, но включая байты FCS).
128-255	Общее число полученных пакетов (включая «битые» пакеты), длиной от 128 до 255 байт (исключая биты синхронизации, но включая байты FCS).
256-511	Общее число полученных пакетов (включая «битые» пакеты), длиной от 256 до 511 байт (исключая биты синхронизации, но включая байты FCS).
512-1023	Общее число полученных пакетов (включая «битые» пакеты), длиной от 512 до 1023 байт (исключая биты синхронизации, но включая байты FCS).
1024-1518	Общее число полученных пакетов (включая «битые» пакеты), длиной от 1024 до 1518 байт (исключая биты синхронизации, но включая байты FCS).
Show/Hide	Отметьте, по пакетам какой длины необходимо получить статистику: 64, 65-127, 128-255, 256-511, 512-1023 и 1024-1518 байт.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Просмотр статуса порта маршрутизатора

Окно «Browse Router Port» отображает порты коммутатора, которые подключены к маршрутизатору. Если такой порт настроен пользователем с помощью интерфейса командной строки или Web-интерфейса управления, то он является статическим портом и обозначается буквой S (от англ. «Static»). Буквой D (от англ. «Dynamic») обозначается порт, подключенный к маршрутизатору и настройки которого динамически изменяются коммутатором. Для просмотра следующей таблицы зайдите: **Monitoring ⇨ Browse Router Port.**

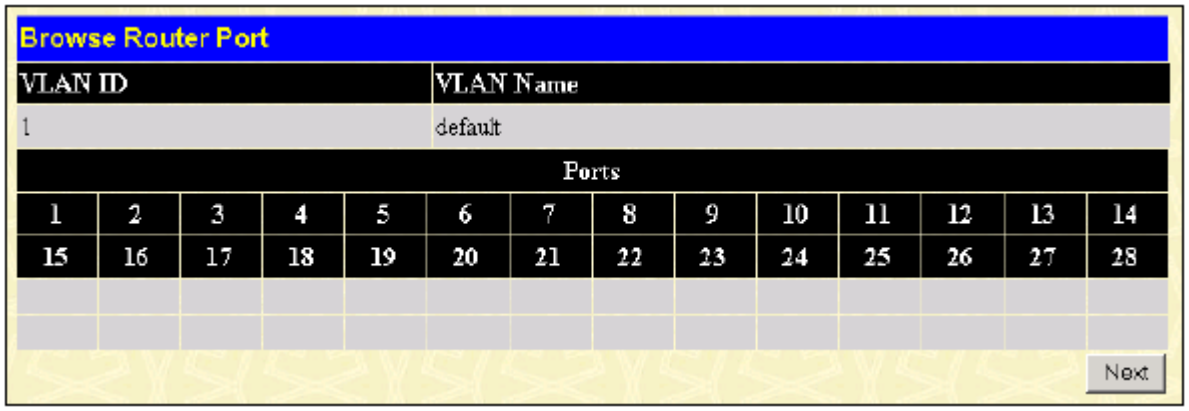


Рисунок 12.17 – Окно «Router Port»

Управление доступом к порту (Port Access Control)

Управление статистикой аутентификации 802.1x на основе портов осуществляется с помощью опций окна «Port Access Control». Для работы с указанной статистикой откройте: **Monitoring ⇨ Port Access Control.**

Примечание: Состояние аутентификатора **Authenticator State** не будет отображаться до тех пор, пока не будет включена аутентификация 802.1x на основе портов или на основе MAC-адресов. Для включения опции аутентификации 802.1x обратитесь к меню Web Management Tool Menu коммутатора DES-3800.

Аутентификация с помощью внешнего сервера RADIUS

Таблица **«RADIUS Authentication»** содержит информацию по аутентификации со стороны клиента. В данной таблице каждой строке соответствует сервер аутентификации RADIUS, содержащий секретную информацию клиента.

Для просмотра соответствующей таблицы нажмите: **Monitoring ⇨ Port Access Control ⇨ RADIUS Authentication.**

Рисунок 12.18 – Окно «RADIUS Authentication»

Пользователь может выбрать значение временного интервала для обновления статистики в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1c. Для обнуления статистики нажмите кнопку *Clear* в верхнем левом углу. До 90 одновременных звонков

Параметр	Описание
ServerIndex	Идентификационный номер, назначенный каждому серверу аутентификации RADIUS, которому пользователи сообщают свою секретную информацию.
InvalidServerAddr	Количество пакетов доступ-ответ RADIUS, полученных от неизвестных адресов.
Identifier	NAS-идентификатор RADIUS клиента. (Необязательно такой же как sysname в MIB II)
AuthServerAddr	Таблица, показывающая серверы RADIUS-аутентификации, получающие секретную информацию пользователей.
SeverPortNumber	UDP-порт, используемый клиентом для посылки запросов на этот сервер.
RoundTripTime	Временной интервал (в сотнях секунд) между последними «доступ-ответ»/ «Доступ-вызов», в течение которого необходимо отметиться на этом сервере аутентификации RADIUS.
AccessRequests	Количество пакетов запроса доступа RADIUS, отправленных на этот сервер, не учитывая количество повторных передач.
AccessRetrans	Количество повторных передач пакетов запроса доступа RADIUS, отправленных на этот сервер.

AccessAccepts	Количество (действительных и недействительных) пакетов разрешения доступа RADIUS, полученных от данного сервера.
AccessRejects	Количество (действительных и недействительных) пакетов отклонения доступа RADIUS, полученных от данного сервера.
AccessChallenges	Количество пакетов RADIUS отклик-доступ, полученных от данного сервера.
AccessResponses	Количество искаженных пакетов RADIUS запроса доступа. Искаженные пакеты включают в себя пакеты неправильной длины, плохие аутентификаторы или атрибуты подписи не включаются в число искаженных пакетов
BadAuthenticators	Количество пакетов «отклик-доступ», содержащих неверные аутентификаторы или атрибуты подписи, полученные от этого сервера.
PendingRequests	Количество пакетов запроса доступа, предназначенных для этого сервера, которые не получают ответа
Timeouts	Количество аутентификаций просроченного времени к этому серверу. По истечении времени клиент может попытаться повторно подключиться к данному серверу, послать запрос на аутентификацию другому серверу или прекратить попытки. Повторная попытка подключиться к тому же серверу считается повторной передачей, как и таймаут.
UnknownTypes	Количество пакетов RADIUS неизвестного типа, полученные с данного сервера на аутентификационный порт.
PacketsDropped	Количество пакетов RADIUS, полученных с этого сервера на аутентификационный порт и удаленные по некоторым другим причинам.

Учетные записи RADIUS

Это окно показывает управляемые объекты, используемые для управления учетных записей клиентов RADIUS, и текущую статистику, соответствующую им. Каждая строка в данном окне соответствует RADIUS серверу аутентификации, содержащему секретную информацию пользователя. Для просмотра **RADIUS Accounting**, нажмите **Monitoring > Port Access Control > RADIUS Accounting**.

Рисунок 12.18 – Окно «RADIUS Accounting»

Пользователь может выбрать значение временного интервала для обновления статистики в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1сек. Для обнуления статистики нажмите кнопку *Clear* в верхнем левом углу.

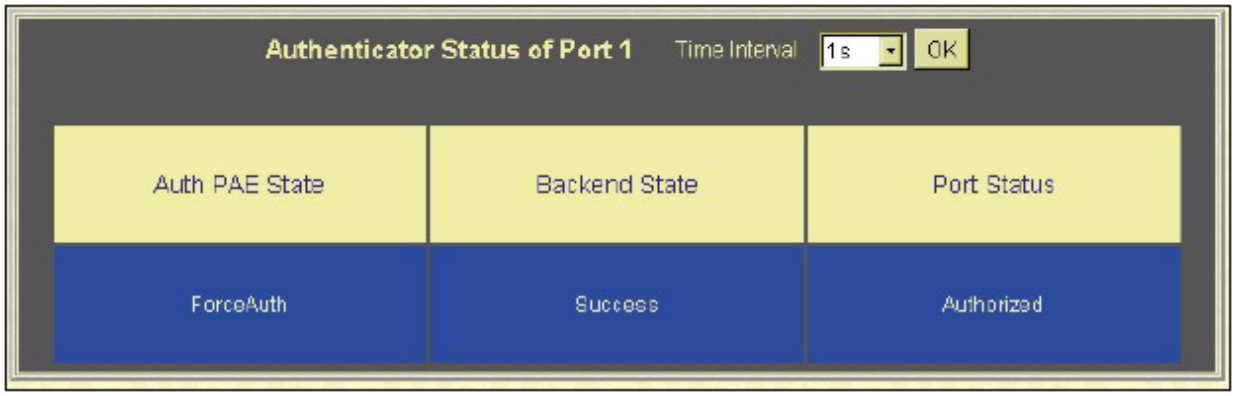
Следующие поля доступны для просмотра:

Параметр	Описание
ServerIndex	Идентификационный номер, назначенный каждому серверу аутентификации RADIUS. (необязательно такой, как SysName в MIB II)
InvalidserverAddr	Количество пакетов ответа учетной записи RADIUS, полученных от неизвестных адресов.
Identifier	Идентификатор NAS клиента учетных записей RADIUS (необязательно такой, как SysName в MIB II)
ServerAddress	Общая таблица, содержащая серверы учетных записей RADIUS, содержащие секретную информацию пользователей.
SeverPortNumber	Порт UDP, используемый клиентом для посылки запросов на этот сервер.
RoundTripTime	Временной интервал между самым последним запросом учетной записи и ответом на данный запрос, данный временной интервал отсчитывается на данном сервере учетных записей пользователя.
Requests	Количество пакетов запроса учетной записи RADIUS. В это поле не включается количество повторных передач
Retransmissions	Количество пакетов запроса учетной записи пользователя RADIUS
Responses	Количество пакетов RADIUS, полученных на порт учетных записей сервера.
MalformedResponses	Количество искаженных пакетов запроса учетной записи RADIUS, полученных от этого сервера. Искаженные пакеты включают в себя пакеты неправильной длины, плохие аутентификаторы или атрибуты подписи не включаются в число искаженных пакетов
BadAuthenticators	Количество пакетов «отклик- учетная запись», содержащих неверные аутентификаторы или атрибуты подписи, полученные от этого сервера.
PendingRequests	Количество пакетов запроса доступа, предназначенных для этого сервера, которые не получают ответа. Эта переменная возрастает, когда послан запрос учетной записи пользователя, и убывает по мере получения отклика учетной записи пользователя, таймаута или повторной передачи.
Timeouts	Количество просроченного времени учетных записей пользователя к этому серверу. По истечении времени клиент может попытаться повторно

	подключиться к данному серверу, послать запрос на аутентификацию другому серверу или прекратить попытки. Повторная попытка подключиться к тому же серверу считается повторной передачей, как и таймаут. Попытка подключиться к другому серверу рассматривается как запрос учетной записи пользователя точно также, как и таймаут.
Unknown Types	Количество пакетов неизвестного типа RADIUS, полученых с данного сервера на порт учетной записи пользователя.
PacketsDropped	Количество пакетов RADIUS, полученных с этого сервера на порт учетной записи пользователя и удаленных по некоторым другим причинам.

Состояние аутентификатора

В данном пункте описывается состояние коммутатора согласно протоколу 802.1x**.** Для просмотра таблицы «**Authenticator State**»: **Monitoring ⇨ Port Access Control ⇨Authenticator State.**



Представленное окно отображает состояние аутентификатора для конкретного порта Authenticator State

Интервал между опросами может быть от 1 до 60 сек., он устанавливается в выпадающем меню в верхней части таблицы, после чего следует нажать **OK.**

Информация, представленная в данном окне, описывается в таблице:

Параметр	Описание
Auth PAE State	Значение коммутатора (аутентификатора) Authenticator PAE State может быть *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth* или *N/A*. N/A (Not available – не доступен) свидетельствует о том, что возможность аутентификации портов отключена.
Backend State	Состояние выходного буфера аутентификации может быть *Request, Response, Success, Fail, Timeout, Idle, Initialize* или *N/A*. N/A (Not available – не доступен) свидетельствует о том, что возможность аутентификации портов отключена.
Port Status	Состояние порта может быть авторизованное *Authorized*, неавторизованное *Unauthorized* или не доступно *N/A*.

Таблица MAC-адресов

Динамические MAC-адреса можно просмотреть в таблице, представленной ниже. Когда коммутатор узнает связь между MAC-адресом и номером порта, он делает запись в данной таблице. Эти записи используются при пересылке пакетов через коммутатор.

Для просмотра таблицы с MAC-адресами нажмите: **Monitoring ⇨ MAC Address Table.**

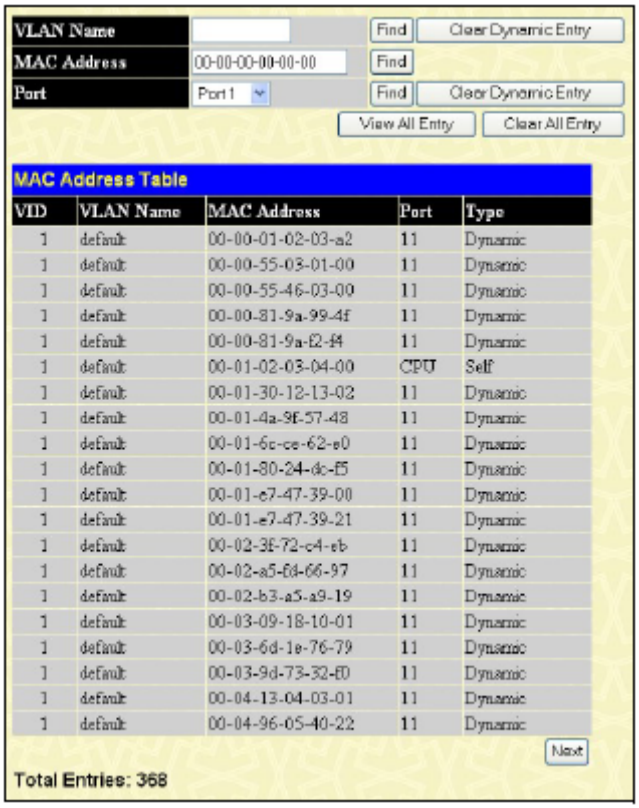


Рисунок 12.19 – Окно «MAC Address Table»

Можно настроить или просмотреть следующие поля:

Параметр	Описание
VLAN Name	Введите имя виртуальной локальной сети VLAN для поиска в таблице.
MAC Address	Введите MAC-адрес для поиска в таблице.
Find	Позволяет пользователю перейти к той области базы данных, которая соответствует определенным пользователем портом, VLAN или MAC-адресом.
VID	VLAN ID виртуальной сети VLAN, членом которой является данный порт.
MAC Address	MAC-адрес, занесенный в таблице.
Port	Порт, которому соответствует MAC-адрес, указанный в поле MAC Address.
Type	Показывает, каким образом коммутатор узнает MAC-адрес. Возможны следующие записи: Dynamic, Self, Static.
Next	Нажмите данную кнопку для просмотра следующей страницы таблицы адресов.
Clear Dynamic Entry	При нажатии на эту кнопку будут удалены динамические записи, выученные коммутатором. Это может быть установлено благодаря имени VLAN или порту.
View All Entry	При нажатии на эту кнопку пользователь может просмотреть все записи таблицы адресов.
Clear All Entry	При нажатии на эту кнопку пользователь может удалить все записи таблицы адресов.

Таблица IP-адресов

Таблицу IP-адресов можно найти в меню **Monitoring**. Таблица **«IP Address Table»** доступна только для чтения: пользователь может просмотреть IP-адреса, занесенные коммутатором. Для поиска определенного IP-адреса, введите его в поле **IP Address**, расположенное в верхней части окна, и нажмите **Find**.

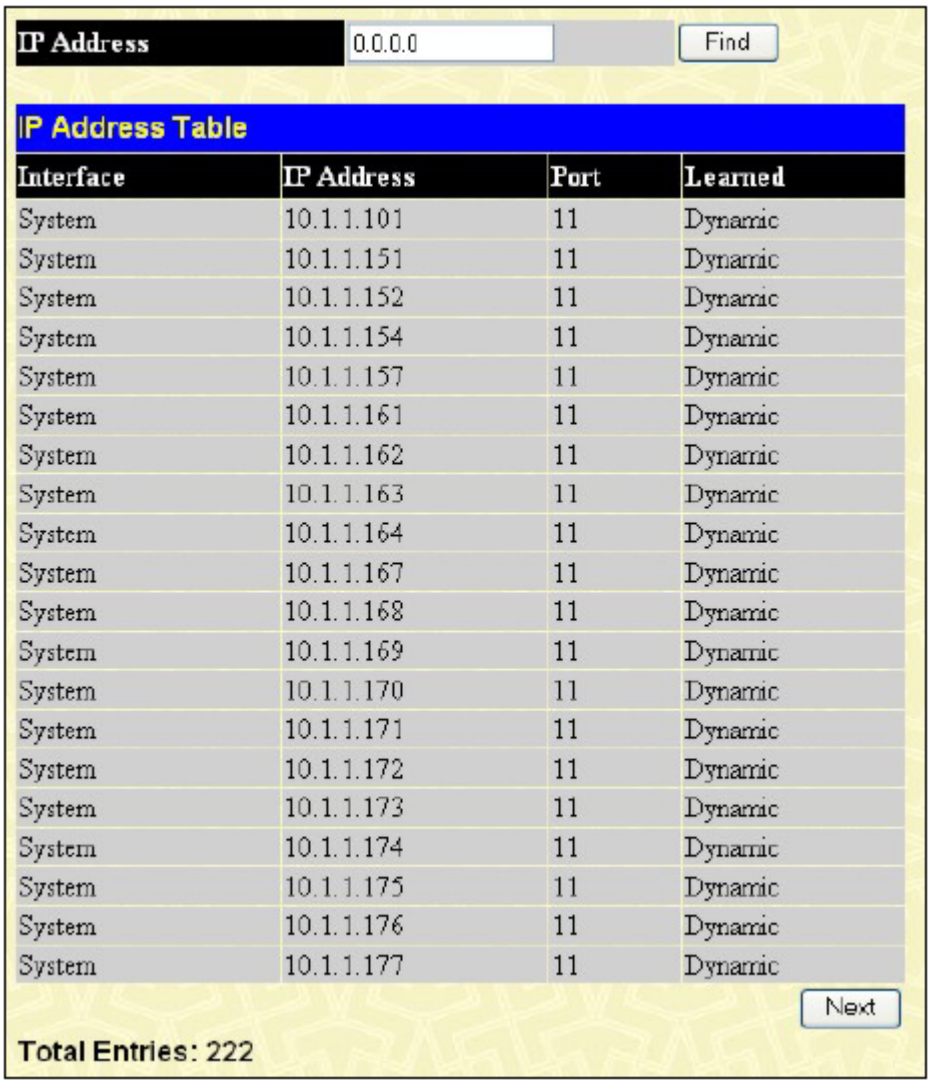


Рисунок 12.20 – Окно «IP Address Table»

Просмотр таблицы маршрутизации

Окно **«Browse Routing Table»** можно найти в меню **Monitoring**. В данном окне представлена таблица IP маршрутизации коммутатора. Для поиска определенного IP-маршрута, введите IP-адрес в поле Destination Address и маску подсети в поле **Netmask** и нажмите **Find**.

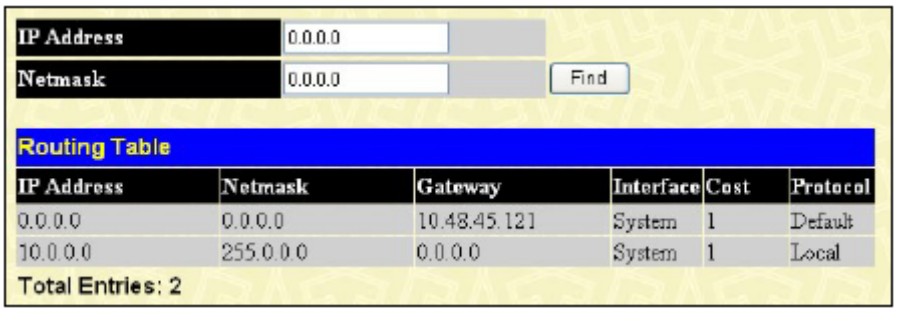


Рисунок 12.21 – Окно «Browse Routing Table»

Окно **«Browse ARP Table»** можно найти в меню **Monitoring**, в нем показаны текущие ARP-записи коммутатора. Для поиска определенной ARP-записи, введите имя интерфейса в поле **Interface Name** или **IP Address** и нажмите **Find**. Для очистки таблицы ARP, нажмите **Clear All**.

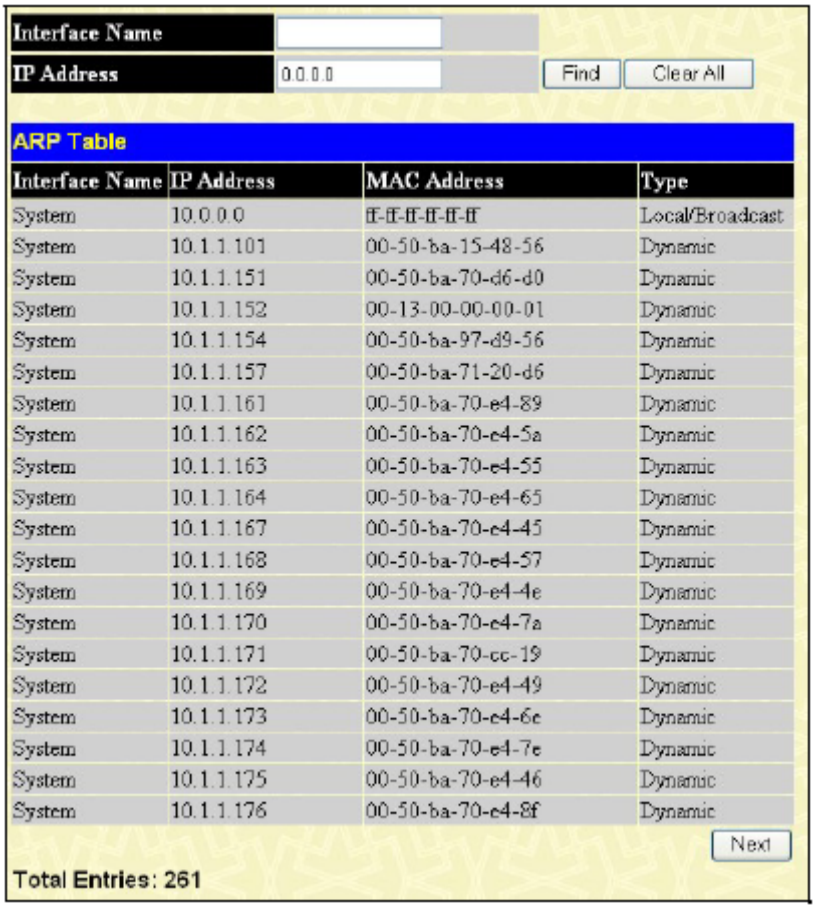


Рисунок 12.22 – Окно «Browse ARP Table»

Просмотр таблицы IP Multicast Forwarding

Окно **«Browse IP Multicast Forwarding Table»** можно найти в меню **Monitoring**. В данном окне представлена информация по многоадресным группам коммутатора. Для поиска определенной записи введите IP-адрес многоадресной группы в поле **Multicast Group** или **Source IP Address** и нажмите **Find**.

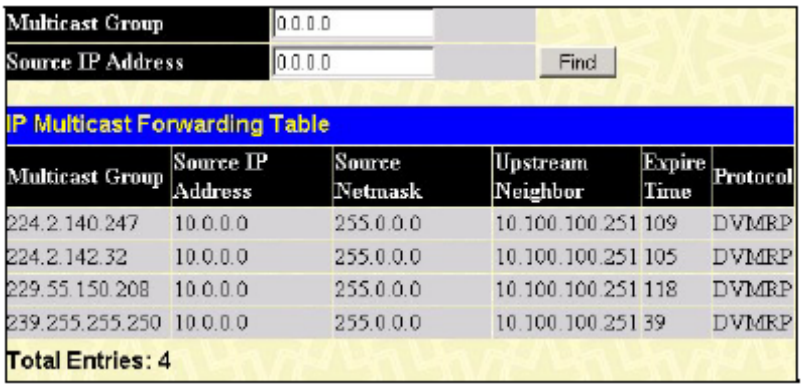


Рисунок 12.23 – Окно «Browse IP Multicast Forwarding Table»

Группа IGMP Snooping

IGMP Snooping позволяет коммутатору считывать IP-адрес многоадресной группы и соответствующий MAC-адрес IGMP-пакетов, проходящих через коммутатор. Количество IGMP-отчетов, которые были «подсмотрены» отображаются в поле Reports. Для просмотра таблицы **IGMP Snooping Group Table**, нажмите: **Monitoring ⇨ IGMP Snooping Group.**

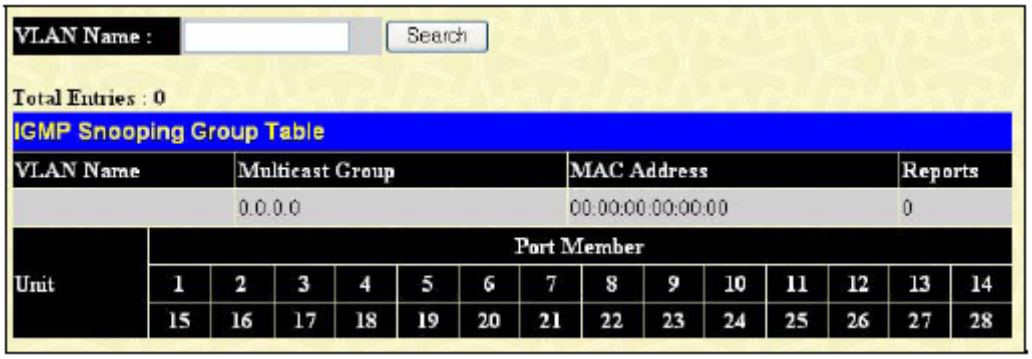


Рисунок 12.24 – Окно «IGMP Snooping Group Table»

Пользователь может найти IGMP Snooping Table по имени VLAN путем его введения в соответствующее поле **VLAN Name** в верхнем левом углу и нажатием на **Search**.

Примечание: Коммутатор поддерживает до 256 групп IGMP Snooping.

Можно просмотреть следующие поля:

Параметр	Описание
VLAN Name	Введите имя виртуальной локальной сети VLAN многоадресной группы
Multicast Group	IP-адрес многоадресной группы.

MAC Address	MAC-адрес многоадресной группы.
Reports	Общее количество отчетов, полученных данной группой.
Port Member	Отображаются порты, на которых были «подсмотрены» пакеты.

IGMP Snooping Forwarding

Ниже приведенное окно отображает текущие записи в таблице IGMP Snooping Forwarding Table, для ее просмотра нажмите: **Monitoring ⇨ IGMP Snooping Forwarding. 192.168.100.228**

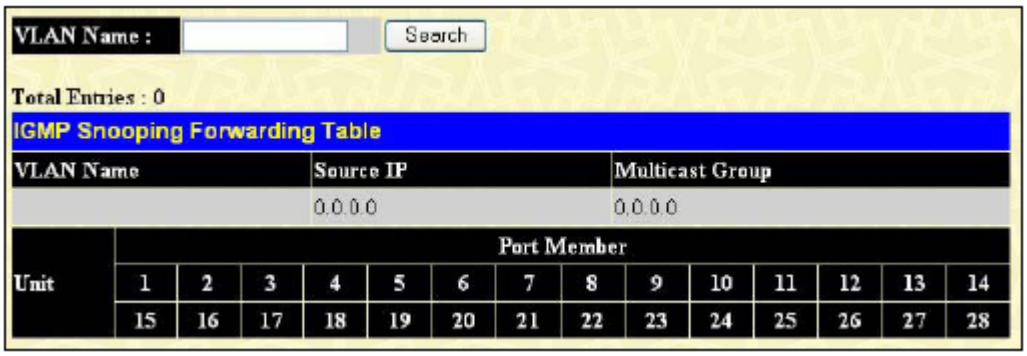


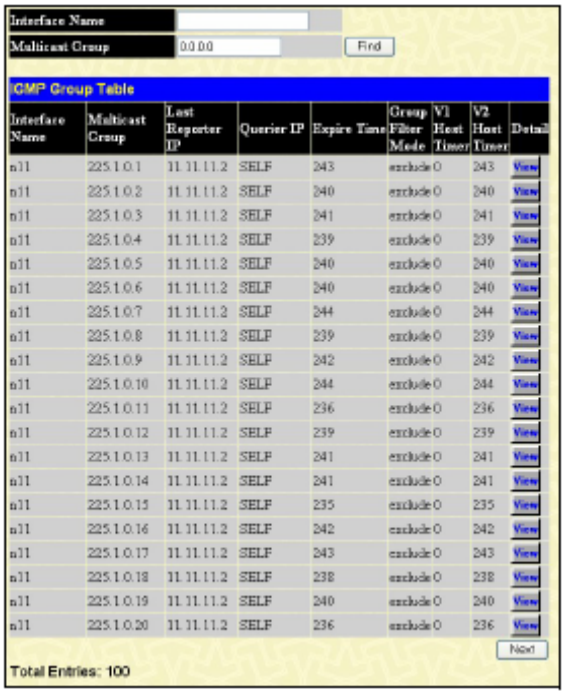
Рисунок 12.25 – Окно «IGMP Snooping Forwarding Table»

Пользователь может найти **IGMP Snooping Forwarding Table** по имени VLAN, введя его в поле VLAN Name в верхнем левом углу и нажав на **Search**.
Можно просмотреть следующие поля:

Параметр	Описание
VLAN ID	Имя VLAN многоадресной группы.
Source IP	IP-адрес многоадресной группы.
Multicast Group	MAC-адрес многоадресной группы.
Port Member	Отображаются порты, на которых были «подсмотрены» IGMP пакеты.

Просмотр таблицы IGMP-групп

Для просмотра текущих записей IGMP-группы откройте окно **Browse IGMP Group**, для этого нажмите: **Monitoring ⇨ Browse IGMP Group Table.** Для поиска определенной записи IGMP группы введите имя интерфейса в поле **Interface Name** или **Multicast Group** и нажмите **Find**.



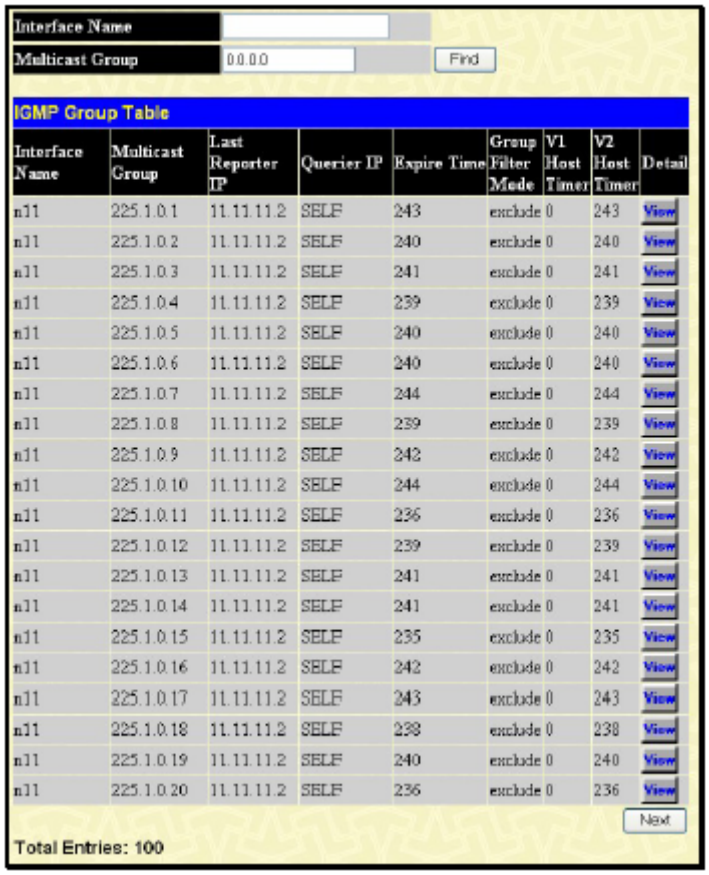


Рисунок 12.26 – Окно «Browse IGMP Group Table»

Для просмотра подробной информации по определенной IGMP-группе, нажмите соответствующую кнопку View, после чего появится следующее окно:

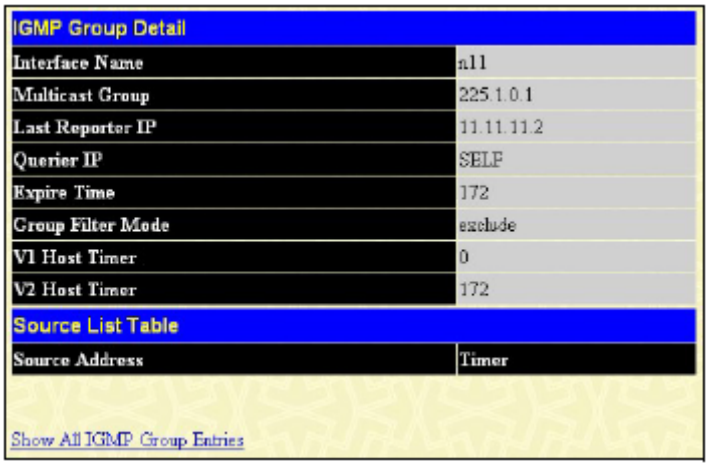


Рисунок 12.27 – Окно «IGMP Group Detail»

Мониторинг протокола DVMRP

Это меню позволяет наблюдать статус DVMRP для каждого IP-интерфейса коммутатора. Оно находится в папке **Monitoring** и содержит следующие таблицы: **Browse DVMRP Routing Table, Browse DVMRP Neighbor Address Table, Browse DVMRP Routing Next Hop Table** и **Browse PIM Neighbor Table**.

Просмотр таблицы маршрутизации DVMRP

Широковещательная информация маршрутизации собирается и хранится DVMRP в **DVMRP Routing Table** (таблице маршрутизации DVMRP), которую можно найти в папке **Monitoring**, под заголовком **Browse DVMRP Monitoring,** содержащей по одной строке для каждого порта в режиме DVMRP. Каждая запись маршрутизации содержит информацию об источнике и широковещательной группе, входящих и исходящих интерфейсов. В поля верхней части этой страницы возможно ввести **Source IP Address(**источник IP-адреса) и его маску подсети:

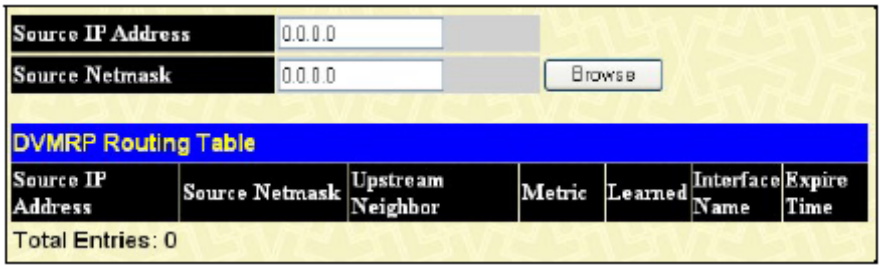


Рисунок 12.28. DVMRP Routing Table

Просмотр таблицы DVMRP-соседей

Эта таблица, находящаяся в меню **Monitoring** по адресу **DVMRP Monitor > Browse DVMRP Neighbor Table,** содержит информацию о DVMRP-соседях коммутатора. Для поиска этой таблицы, введите **Interface Name** или **Neighbor Address** в соответствующее поле и нажмите кнопку **Find**. DVMRP-соседи этой записи появятся в **DVMRP Neighbor Table,** показанной ниже.

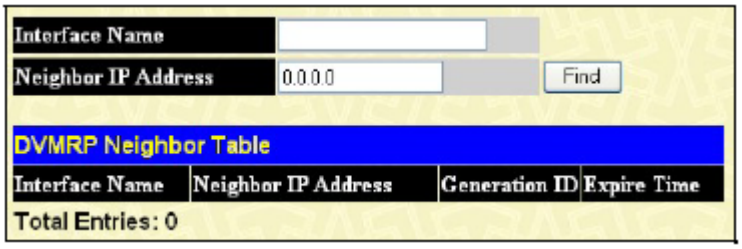


Рисунок 12.29 – Окно «DVMRP Neighbor Table»

Просмотр таблицы DVMRP Routing Next Hop

Таблица **DVMRP Routing Next Hop Table** содержит информацию, относящуюся к следующему хопу для пересылки многоадресных пакетов на исходящие интерфейсы. Каждая запись в таблице **DVMRP Routing Next Hop Table** относится к следующему хопу от специфического источника до специфической широковещательной группы адресов. Эта таблица находится в меню **Monitoring> DVMRP Monitoring,** под заголовком **BrowseDVMRP Routing Next Hop Table.** Для поиска этой таблицы, введите **Interface Name** или **Source IP Address** в соответствующее поле и нажмите кнопку **Find**. Следующий хоп для данной записи DVMRP Routing появится в таблице **DVMRP Routing Next Hop,** показанной ниже.

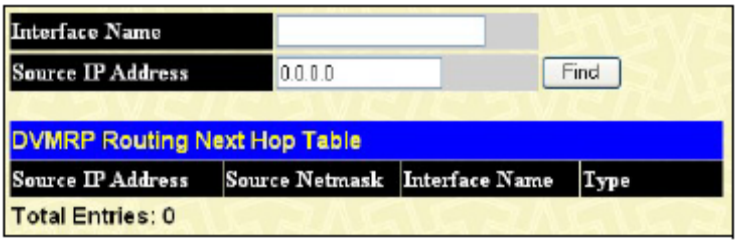


Рисунок 12.30. Таблица DVMRP Routing Next Hop Table

Просмотр таблицы PIM-соседей

Многоадресные маршрутизаторы используют протокол **Protocol Independent Multicast (PIM),** определяющий, какие еще многоадресные маршрутизаторы получат многоадресные пакеты. Таблица **PIM Neighbor Address Table** содержит информацию, относящуюся ко всем PIM-соседям маршрутизатора. Это окно можно найти в папке **Monitoring** под заголовком **PIM Monitor**. Для поиска этой таблицы, введите **Interface Name** или **Neighbor Address** в соответствующее поле и нажмите кнопку **Find**. PIM-соседи данной записи появятся в таблице **PIM Neighbor Table,** показанной ниже.

Рисунок 12.31 – Окно «PIM Neighbor Table»

Мониторинг OSPF

Этот раздел предлагает пользователям ознакомиться с опциями, относящимися к статистике протокола OSPF (Open Shortest Path First) на коммутаторе, включая **OSPF LSDB Table**, **OSPF Neighbor Table** и **OSPF Virtual Neighbor Table**. Для просмотра этих таблиц, откройте папку **Monitoring** и нажмите **OSPF Monitoring**.

Просмотр таблицы OSPF LSDB

Эта таблица, находящаяся в папке **Monitoring**, может быть найдена в папке **OSPF Monitor**, путем нажатия на ссылку **Browse OSPF LSDB Table**. Таблица **OSPF Link-State Database Table** отображает текущее состояние базы данных о состоянии каналов при помощи OSPF протокола маршрутизации на база OSPF-областей.

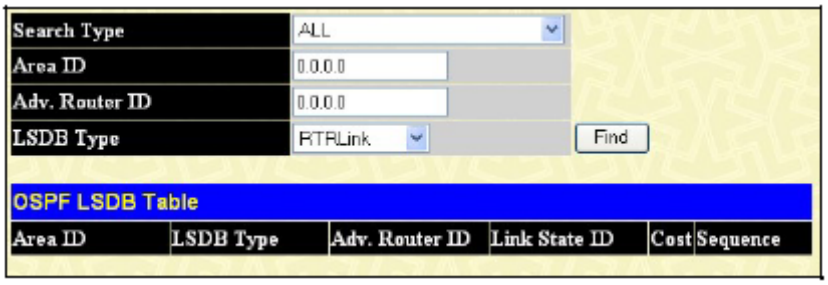


Рисунок 12.32. Таблица Browse OSPF LSDB

Пользователь может найти конкретную запись путем введения следующей информации в поля в верху экрана:
Для просмотра **OSPF LSDB Table**, сначала необходимо выбрать, какой метод просмотра будет использоваться, в поле **Search Type**. Возможны следующие варианты: *All*, *Area ID*, *Advertise Router ID*, *LSDB*, *Area ID & Advertise Router ID*, *Area ID & LSDB*, и *Advertise Router ID & LSDB*.
При выборе *Area ID* в качестве метода просмотра необходимо ввести IP-адрес в поле **Area ID** и затем нажать *Find*.
При выборе *Adv. Router ID*, необходимо ввести IP-адрес в поле **Adv. Router ID** и затем нажать *Find*.
Если выбрано *LSDB*, Вам необходимо выбрать тип состояния канала(*RtrLink*, *NetLink, Summary*, *ASSummary* и *ASExtLink*) в поле **LSDB Type** и затем нажать *Find*.
В таблице **OSPF LSDB Table** отображаются следующие поля:

Параметр	Описание
Area ID	Позволяет ввести идентификатор области OSPF. Этот идентификатор будет затем использоваться для поиска таблицы и отображает запись при условии ее существования.
LSDB Type	Отображает, какой из восьми типов объявлений о состоянии канала используется для этой линии на коммутаторе: Router link (*RTRLink*), Network link (*NETLink*), Summary link(*Summary*), Autonomous System link (*ASSummary*), Autonomous System external link(*ASExternal)*, MCGLink (*Multicast Group*), и NSSA (*Not So Stubby Area*)
Adv.Router ID	Отображает идентификатор объявляемого маршрутизатора.
Link State ID	Содержание этого поля зависит от типа объявления о состоянии канала. LS Type — Link State ID 1 — Оригинальный идентификатор маршрутизатора 2 — Адрес IP-интерфейса сетевого маршрутизатора Designated

	Router 3 IP-адрес сети назначения 4 Идентификатор маршрутизатора описываемого граничащего с автономной системой маршрутизатора
Cost	Отображает стоимость записи таблицы
Sequence	Отображает число раз изменения состояния канала.

Просмотр таблицы OSPF Neighbor

Эту таблицу можно найти в папке **OSPF Monitoring** путем нажатия на ссылку **Browse OSPF Neighbor Table**. Маршрутизаторы, подключенные к одной и той же области или сегменту, становятся соседями в этой области. Соседние маршрутизаторы выбираются с помощью Hello-протокола. IP-широковещание используется для отправки Hello-пакетов другим маршрутизаторам сегмента. Маршрутизаторы становятся соседями, когда они видят друг друга в списке Hello-пакета, отправленного другим коммутатором того же сегмента. В этом случае возможна гарантированная двусторонняя связь между любыми двумя соседними маршрутизаторами. Эта таблица отображает OSPF-соседей на коммутаторе.

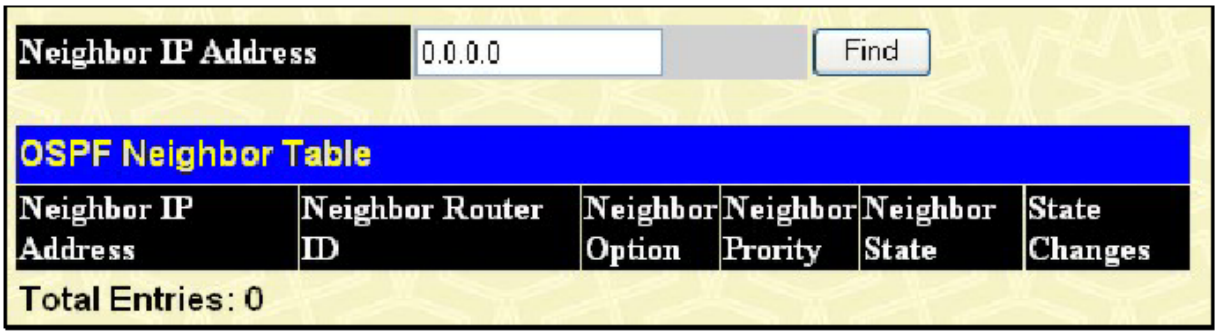


Рисунок 12.33. OSPF Neighbor Table

Для нахождения OSPF-соседей, введите IP-адрес и нажмите **Find.** Реальные OSPF-соседи появятся в **OSPF Neighbor Table** ниже**.**

Просмотр таблицы OSPF Virtual Neighbor (виртуальные соседи)

Эта таблица может быть найдена в папке **Monitoring** путем нажатия на ссылку **Browse OSPF Virtual Neighbor Table** в папке **OSPF Monitoring**. Эта таблица отображает список **Virtual OSPF Neighbors** (соседи) коммутатора. Пользователь может выбрать специальный поиск виртуальных соседей, используя одну из двух опций поиска в верху экрана, как:

Параметр	Описание
Transit Area ID	Позволяет ввести идентификатор области OSPF, предварительно установленной на коммутаторе, что позволяет удаленным областям (remote area) взаимодействовать с магистралью (area 0). Транзитная область не может быть тупиковой областью (Stub area) или магистралью (Backbone area).
Virtual Neighbor Router ID	Идентификатор OSPF-маршрутизатора для удаленного маршрутизатора. Этот IP-адрес однозначно определяет область пограничного маршрутизатора (Area Border Router) удаленной области.

Transit Area ID	0.0.0.0	
Virtual Neighbor Router ID	0.0.0.0	Browse

OSPF Virtual Neighbor Table

Transit Area ID	Virtual Neighbor Router ID	Virtual Neighbor IP Address	Virtual Neighbor Option	Virtual Neighbor State	Events

Total Entries: 0

Рисунок 12.34.OSPF Virtual Neighbor Table

Просмотр статуса PoE (только для DES-3828P)

Эта таблица может быть найдена в папке **Monitoring** путем нажатия на **Browse PoE Status**. Она отображает текущее состояние системы PoE и настроек портов PoE.

PoE System Status

Power Limit (W)	372
Power Consumption (W)	0
Power Remained (W)	372
Power Disconnection Method	Deny next port

PoE Port Status

Port	State	Priority	Power Limit (mW)	Class	Power (mW)	Voltage (decivolt)	Current (mW)	Status
1	Enabled	Low	15400	0	0	0	0	OFF : Improper Capacitor Detection results
2	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
3	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
4	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
5	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
6	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
7	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
8	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
9	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
10	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
11	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
12	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
13	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
14	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
15	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
16	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
17	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
18	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
19	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
20	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
21	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
22	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
23	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection
24	Enabled	Low	15400	0	0	0	0	OFF : Interim state during line detection

Рисунок 12.35. Browse PoE Status окно

Просмотр настроек WRED

Следующее окно отображает текущие настройки WRED на коммутаторе. Для просмотра этого окна, нажмите **Monitoring >Browse WRED Settings**.

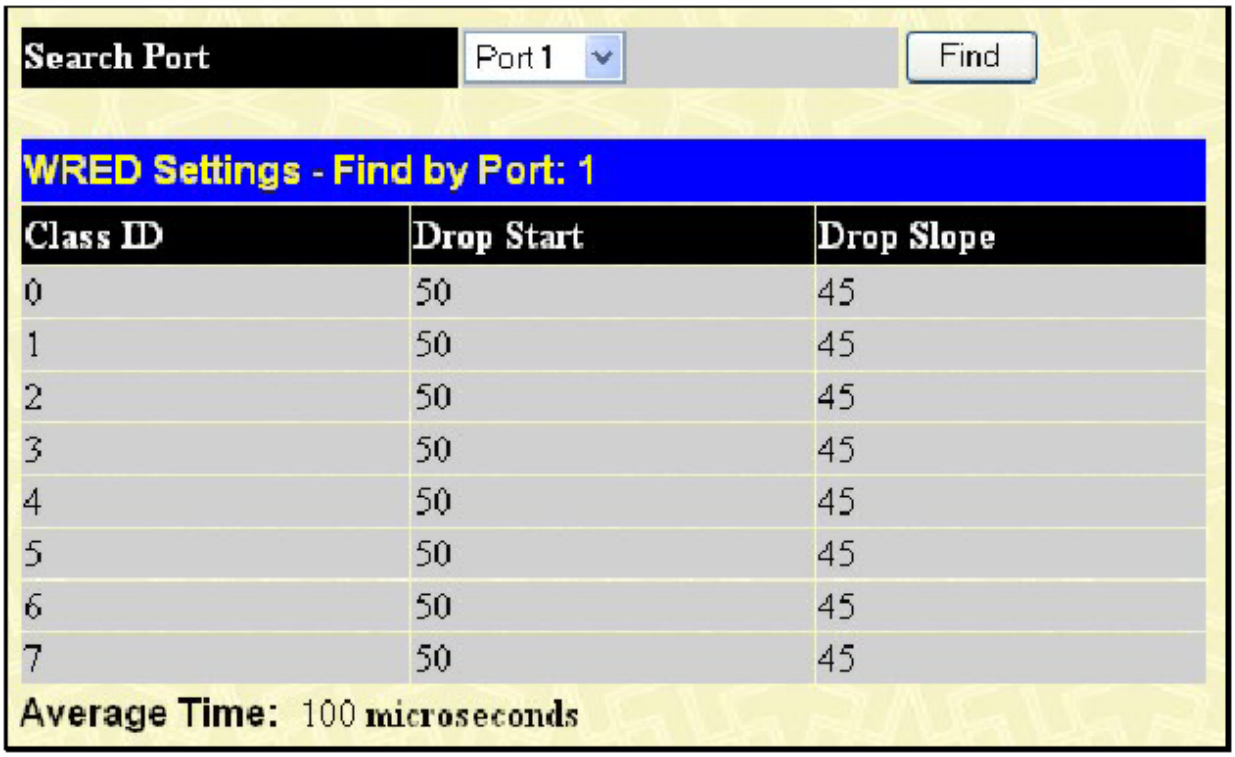


Рисунок 12.36. WRED Settings окно

Выше отображены следующие параметры:

Параметр	Описание
Search port	Используя выпадающее меню, выберите порт для WRED.
Class ID	Отображает идентификатор класса на просматриваемом порту.
Drop Start	Отображает Drop start (начало отбрасывания) в процентном соотношении. Может принимать значение от 1 до 100.
Drop Slope	Отображает Drop Slope, принимает значение от 0 до 90.
Average Time	Отображает среднее время, в течение которого WRED-механизм проверяет пакеты очередей QoS в зависимости от скорости возрастания количества пакетов.

Журнал коммутатора (Switch Log)

Web-интерфейс управления коммутатора позволяет просмотреть журнал коммутатора, созданный агентом управления коммутатора. Для просмотра архива журнала, откройте папку **Monitoring** и нажмите на ссылку **Switch Log**.

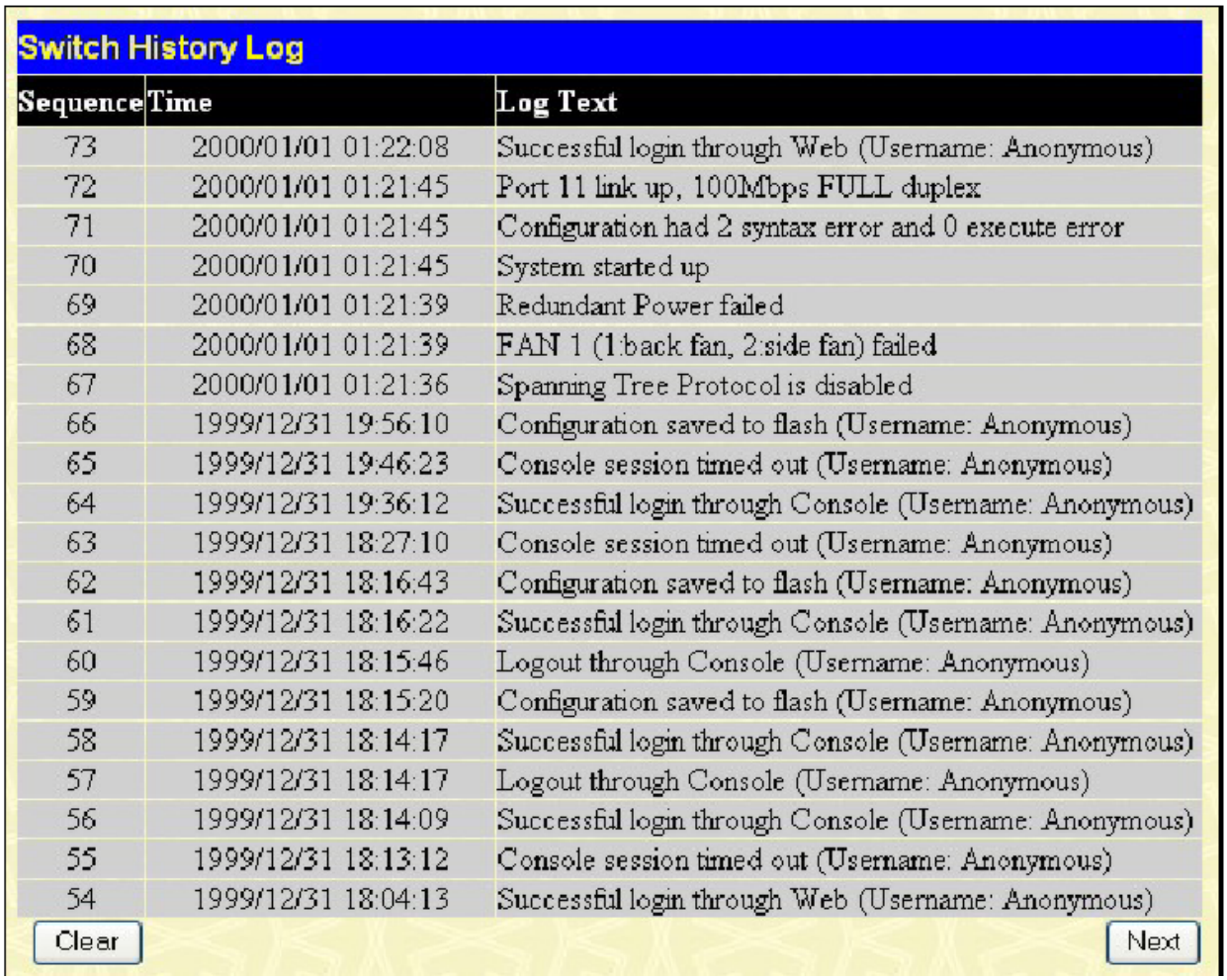


Рисунок 12.37. Switch History окно

Коммутатор может записывать информацию о событиях в своем собственном журнале на условленном SNMP трапе принимающей станции и на персональном компьютере, присоединенном к консоли. Нажмите **Next** для перехода к следующей странице архива журнала коммутатора. Нажатием **Clear** пользователь очистит архив журнала коммутатора.

Информация описывается следующими параметрами:

Параметр	**Описание**
Sequence	Счетчик, увеличивающийся на 1 каждый раз, когда появляется новая запись в журнале коммутатора. В таблице записи с большим номером отображаются первыми.
Time	Отображает время в формате кол-во дней, часов, минут с момента последнего перезапуска коммутатора.
Log Text	Описание события.

Раздел 13 – Техническая эксплуатация коммутатора

Сброс настроек коммутатора (Reset)
Перезапуск коммутатора
Сохранение изменений
Выход из системы (Logout)

Сброс настроек коммутатора (Reset)

Окно Reset позволяет сбросить настройки коммутатора. Однако очень важно выбрать нужную опцию:

- Опция **Reset** – выбор этой опции с последующим нажатием на кнопку **Apply** позволяет сохранить информацию об учетных записях пользователей, журнал событий и информацию о стеке. Все другие настройки будут сброшены к заводским установкам по умолчанию.

- Опция **Reset Config** – выбор этой опции с последующим нажатием на кнопку **Apply** позволяет сохранить только информацию о стеке. Все другие настройки будут сброшены к заводским установкам по умолчанию.

- Опция **Reset System** – Только выбор опции **Reset System** с последующим нажатием на кнопку **Apply** вводит в энергонезависимую память коммутатора заводские параметры по умолчанию, после чего происходит автоматический перезапуск устройства, и коммутатор получает те самые настройки, которые у него были после выпуска с завода.

При этом, очень важно отметить, что первые две опции (Reset и Reset Config) вносят заводские параметры только в память RAM, но не сохраняют ее в энергонезависимой памяти NV-RAM (более подробная информация о различии между памятью RAM и NV-RAM приводится ниже в разделе «Сохранение изменений»). Поэтому после сброса настроек с использованием первых двух опций в дальнейшем при перезапуске коммутатора устройство вернется к последней сохраненной в энергонезависимой памяти конфигурации.

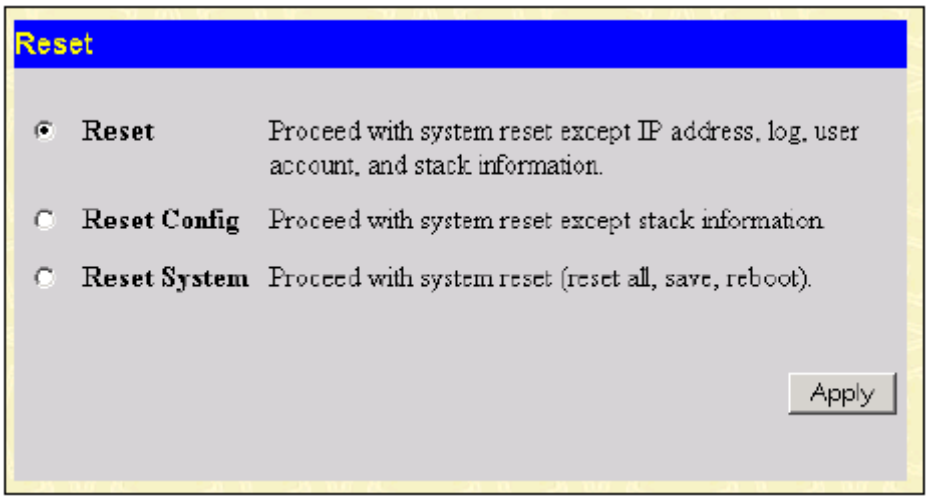


Рисунок 13.1 – Окно «Reset»

Перезапуск коммутатора

Следующее окно используется для перезапуска коммутатора. Все настройки, не сохраненные в энергонезависимой памяти коммутатора, будут утрачены (более подробная информация приводится в главе «Сохранение изменений»). Зайдите в окно **Reboot System** и кликните по кнопке **Restart** для перезапуска коммутатора.

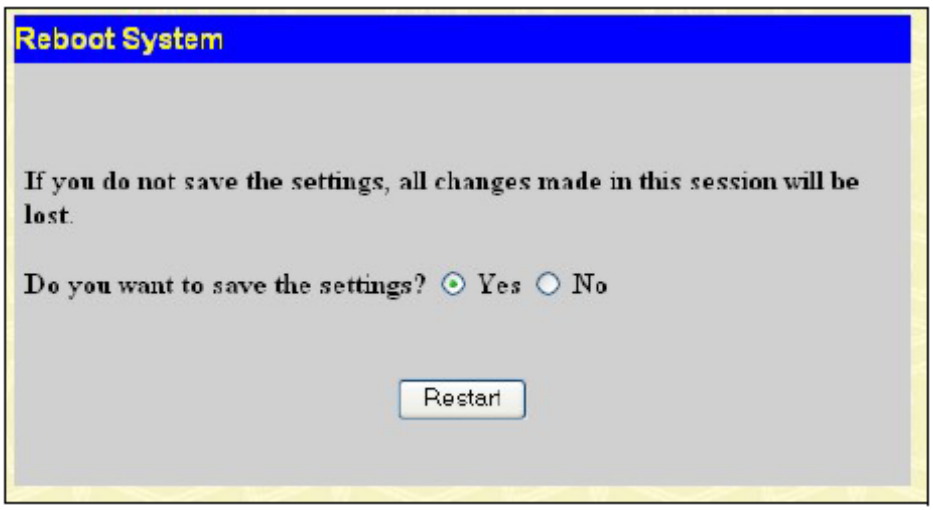


Рисунок 13.2 – Окно «Reboot System»

Сохранение изменений

Коммутатор обладает двумя видами памяти: оперативная RAM и постоянная (энергонезависимая) NV-RAM. Выполняемые настройки записываются в RAM и вступают в силу после нажатия на кнопку **Apply** (Применить).

Если настройки не были сохранены в памяти NV-RAM, то во время перезапуска коммутатора они сотрутся, и коммутатор вернется к настройкам, сохраненным в NV-RAM.

Для сохранения выполненных изменений в настройках в энергонезависимой памяти NV-RAM кликните по **Save Changes.** Далее появится следующее окно.

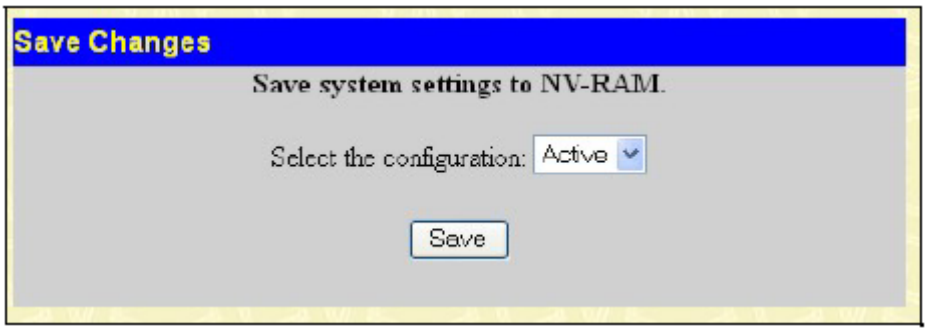


Рисунок 13.3 – Окно «Save Changes»

Коммутатор поддерживает два варианта сохранения конфигурационных настроек в его внутренней памяти, обозначенные как *1* и *2* в выпадающем меню. Также пользователь может сделать текущие настройки активными на коммутаторе, выбрав в поле **Select the configuration** (Выбор конфигурации) – *Active.* В этом случае данные настройки будут использоваться каждый раз после перезапуска коммутатора. Для сохранения настроек кликните по Save. Следующее диалоговое окно сообщит о сохранении настроек.

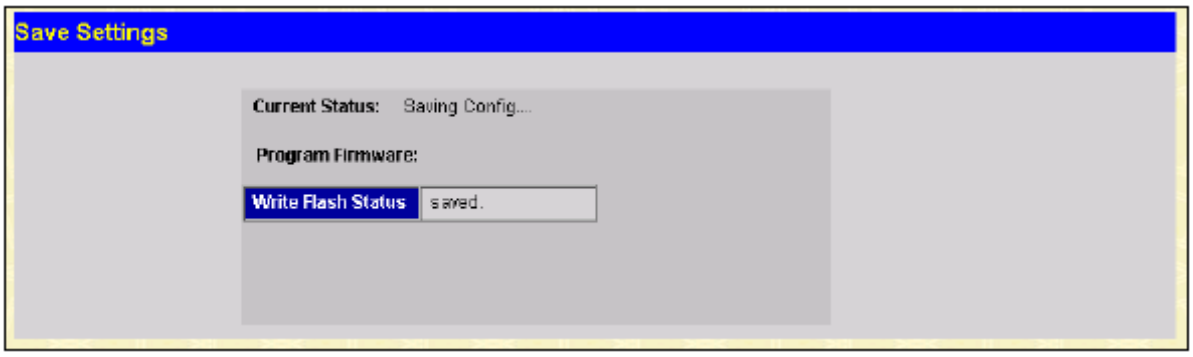


Рисунок 13.5 - Диалоговое окно «Save Settings»

Выход из системы (Logout)

Воспользуйтесь страницей завершения работы Web-интерфейса управления коммутатором, нажав кнопку **Log Out**.

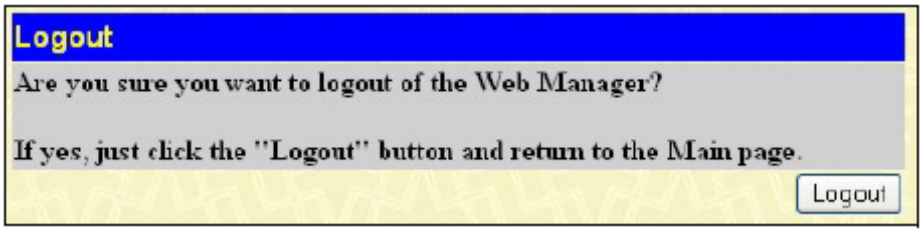


Рисунок 13.6 – Окно «Logout Web Setup»

Приложение А

Техническая спецификация

Основные	
Стандарты	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”) IEEE 802.1D Spanning Tree IEEE 802.1W Rapid Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.1p очередь приоритетов IEEE 802.3ad Link Aggregation Control IEEE 802.3x управление потоком для полнодуплексного режима IEEE 802.3 поддержка автосогласования Nway IEEE 802.3af Power over Ethernet
Протоколы	CSMA/CD
Канал связи **Ethernet** **Fast Ethernet** **Gigabit Ethernet** **Fiber Optic**	Полудуплекс / Дуплекс 10 Мбит/с / 20 Мбит/с 100 Мбит/с / 200 Мбит/с n/a / 2000 Мбит/с Поддержка SFP (Mini GBIC) IEEE 802.3z 1000BASE-LX (трансивер DEM-310GT) IEEE 802.3z 1000BASE-SX (трансивер DEM-311GT) IEEE 802.3z 1000BASE-LH (трансивер DEM-314GT) IEEE 802.3z 1000BASE-ZX (трансивер DEM-315GT)
Топология	Звезда
Сетевые кабели	Расширенный 5 категории для 1000BASE-T UTP 5 категории, расширенный 5 категории для 100BASE-TX UTP 3, 4, 5 категории для 10BASE-T EIA/TIA-568 100 Ом STP (100м)
Количество портов	24 порта 10/100 Мбит/с (48 для DES-3852) 2 комбо-порта 1000BASE-T/SFP 2 1000Base-T медных порта

Физические параметры и условия эксплуатации	
Внешнее устройство питания	**DES-3828 и DES-3852** Входное напряжение переменного тока: 100 – 240 В, 1А, с частотой 50/60 Гц Выходное напряжение 12В, 5А (макс.) **DES-3828P** Входное напряжение переменного тока: 100 -240В, 10А, с частотой 50/60 Гц Выходное напряжение: 50 В, 7.5 А (макс);12 В, 10,5 А (макс) **PoE** Выходная мощность всей системы 370 Ватт На порт 15,4 Ватт (по умолчанию) или 1-16,8 Ватт (устанавливается заказчиком) **DES-3828DC DC** Питание на входе DC 48В
Потребляемая мощность	24 Вт (макс.) для DES-3828/DES-3828DC 395,2 Вт (макс.) для DES-3828P 47 Вт (макс.) для DES-3852
DC вентиляторы	Один вентилятор(15см) для DES-3828/DES-3828DC/ DES-3828P/ DES-3852 Два вентилятора (8,3 см) для DES-3852 Один дополнительный вентилятор (27см) для DES-3828P
Рабочая температура	От 0 до 40С
Температура хранения	От -40 до 70С
Влажность	От 5% до 95% без конденсата

Размеры	для DES-3828/DES-3828DC/ DES-3852: 441 мм x 310 мм x 44 мм для DES-3828P: 441 мм x 369 мм x 44 мм
Масса	DES-3828/DES-3828DC: 4.24 кг DES-3828P: 6.02 кг DES-3852:4,25 кг
Электромагнитное излучение (EMI)	CE class A, FCC Class A, C-Tick
Безопасность	CSA International, CB report

Производительность	
Метод коммутации	Store-and-forward
Буферизация пакетов	32 MB на устройство
Скорость фильтрации/продвижения пакетов	14,881 pps на порт (для 10Мбит/с) 148,810 pps на порт (для 100Мбит/с 1,488,100 pps на порт (для 1 Гбит/с)
Изучение MAC -адресов	Автоматическое обновление. Поддержка 16K MAC-адресов
Приоритезация очередей	4 приоритезации очередей на порт.
Время жизни таблицы MAC-адресов	Максимальный помежуток: 10-1000000 с. По умолчанию 300 с.

Приложение B
Кабели и коннекторы

При подключении коммутатора к другому коммутатору, мосту или концентратору необходим обычный кабель. Пожалуйста, проверьте, подходят ли pin-контакты устройств. Нижеприведённые рисунок и таблица демонстрируют стандартный разъём RJ-45 с распределением его pin-контактов.

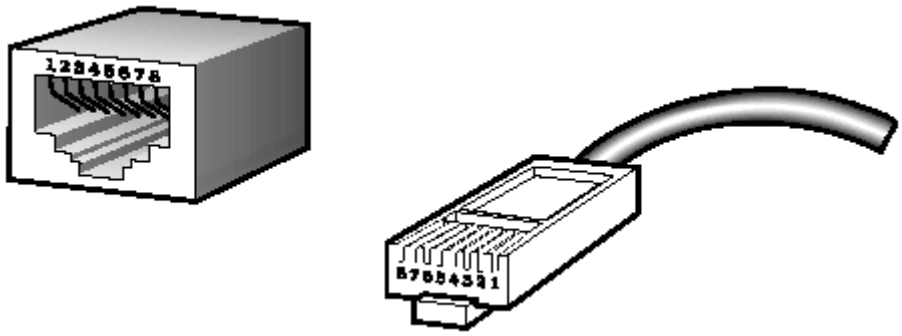


Рисунок B-1. Стандартный RJ-45 разъём с вилкой

Контакты разъёма RJ-45		
Контакты	MDI-X Port	MDI-II Port
1	RD+ (прием)	TD+ (передача)
2	RD- (прием)	TD- (передача)
3	TD+ (передача)	RD+ (прием)
4	не используется	не используется
5	не используется	не используется
6	TD- (передача)	RD- (прием)
7	не используется	не используется
8	не используется	не используется

Таблица B-1. Стандартный разъём RJ-45

Приложение C
Длина кабелей

Используйте данную таблицу как руководство при использовании кабеля максимальной длины.

Стандарт	Тип	Максимальная протяжённость
Mini-GBIC	1000BASE-LX, модуль с поддержкой одномодового оптического кабеля 1000BASE-SX, модуль с поддержкой многомодового оптического кабеля 1000BASE-LHX, модуль с поддержкой одномодового оптического кабеля 1000BASE-ZX, модуль с поддержкой многомодового оптического кабеля	10 км 550 м 40 км 80 км
1000BASE-T	UTP кабель 5 категории UTP кабель 5 категории (1000 Мбит/с)	100 м
100BASE-TX	UTP кабель 5 категории (1000 Мбит/с)	100 м

Глоссарий

1000BASE-LX: технология Gigabit Ethernet, использует многомодовое волокно, дальность прохождения сигнала без повторителя до 550 м.

1000BASE-SX: технология Gigabit Ethernet, использует многомодовое волокно, дальность прохождения сигнала без повторителя до 10 км.

100BASE-FX: Fast Ethernet с помощью оптоволоконного кабеля.

100BASE-TX: Часть спецификации IEEE 802.3u Ethernet для скорости 100 Мбит/с с использованием 2-пар неэкранированного медного кабеля категории 5.

10BASE-T: Спецификация IEEE 802.3i для сетей Ethernet с использованием неэкранированного кабеля на основе скрученных пар ("витая пара").

aging: Автоматическое удаление из базы данных Коммутатора записей, которые устарели или утратили свою актуальность.

ATM: Asynchronous Transfer Mode (асинхронный режим передачи). Протокол передачи, ориентированный на соединение и основанный на использовании пакетов (ячеек) фиксированной длины. ATM рассчитан на передачу различных типов трафика, включая голос, данные и видео.

Автоматическое согласование (auto-negotiation): функция порта, которая позволяет ему сообщать свои параметры скорости, режима и управление потока. При соединении со станцией, также поддерживающей автоматическое согласование, оптимальные установки определяются автоматически.

Магистральный порт (**backbone port):** порт, который не распознает адреса устройств, получает все фреймы с нераспознанными адресами. Этот порт используется для соединения Коммутатора с магистралью сети. Магистральные порты также известны как назначенные downlink-порты.

Магистраль сети (backbone): Часть сети, по которой передается основной трафик между сегментами сети.

Полоса пропускания (bandwidth): характеризует количесво информации, которое может передать канал, измеряется в битах в секунду. Полоса пропускания для технологии Ethernet равна 10Мбит/с, для Fast Ethernet – 100Мбит/с.

baud rate: скорость коммутации в линии, скорость линии между сегментами сети.

BOOTP: Протокол BOOTP позволяет автоматически назначать IP-адрес соответствующему MAC-адресу при запуске устройства. Кроме того, протокол позволяет назначить маску подсети и шлюз по умолчанию для данного устройства.

Мост (bridge): Устройство, соединяющее локальные или удаленные сети при использовании протоколов высоких уровней модели OSI.

Широковещание (broadcast): Отправка сообщений на все устройства назначения в сети.

Широковещательный шторм (broadcast storm): Множество одновременных широковещательных рассылок в сети, которые, как правило, поглощают доступную полосу пропускания сети и могут вызвать отказ сети.

Консольный порт (console port): Порт на коммутаторе, к которому подключается терминальное или модемное соединение. Он преобразует параллельное представление данных на последовательное, которое используется при передаче данных. Этот порт чаще используется для выделенного локального управления.

CSMA/CD: Carrier sense multiple access/collision detection. Метод канального доступа, использующий стандарты Ethernet и IEEE 802.3, где устройства передают данные только тогда, когда канал передачи данных не занят в течение некоторого периода времени. Когда два устройства передают данные одновременно, возникает коллизия. В этом случае конфликтующие устройства передают информацию повторно через выбранный случайным образом временной интервал.

Коммутация центра обработки данных (data center switching): точка агрегации в корпоративной сети, где коммутатор предоставляет высокопроизводительный доступ к серверной ферме, высокоскоростное соединение и контрольную точку для обеспечения управления сетью и безопасности.

Ethernet: Стандарт организации локальных сетей (LAN) совместно разработанный Xerox, Intel и Digital Equipment Corporation. Ethernet обеспечивает скорость 10Мбит/с и использует протокол CSMA/CD для передачи данных.

Fast Ethernet: 100Мбитная технология, разработанная на основе Ethernet. Использует тот же протокол CSMA/CD для передачи данных.

Управление потоком (Flow Control): (IEEE 802.3z). Методы, используемые для управления передачей данных между двумя точками сети и позволяющие избегать потери данных в результате переполнения приемных буферов.
Продвижение (forwarding): Процесс продвижения пакета к месту его назначения посредством сетевого устройства**.**
Полный дуплекс (full duplex): Возможность одновременной передачи и приема пакетов, и в результате удвоение потенциальной пропускной способности канала.
Полудуплекс (half duplex): Возможность передачи и приема пакетов, но не одновременно, в отличие от режима полного дуплекса.
IP-адрес (IP address): Уникальный идентификатор устройств, подключенных к сети с помощью протокола TCP/IP. Адрес записывается как 4-х байтовое значение с разделением точками, включает номер сети, а также может дополнительно включать номера подсети и номер хоста.
IPX: Протокол, обеспечивающий взаимодействие в сети NetWare
Локальная сеть (LAN): Сеть, соединяющая такие устройства как компьютеры, принтеры, сервера, покрывающая относительно небольшую площадь (часто не больше этажа или здания). Характеризуется высокой скоростью передачи данных и маленким количеством ошибок.
Задержка (latency): Временная задержка между моментом, когда устройство получило пакет, и моментом, когда пакет был отправлен на порт назначения.
Скорость линии (line speed): смотри baud rate.
Основной порт (main port): Основной порт отказоустойчивой линии, обычно используемый для продвижения трафика в нормальных эксплуатационных режимах.
MDI - Medium Dependent Interface: Порт Ethernet, где передатчик одного устройства напрямую соединён с приёмником другого.
MDI-X - Medium Dependent Interface Cross-over: Порт Ethernet, где линии передатчика и приёмника пересекаются.
База управляющей информации (MIB): База данных, в которой хранятся параметры и характеристики управления устройством. Эта база данных ведется протоколом сетевого управления SNMP. Каждый коммутатор ведет совю собсвенную базу MIB.
Многоадресная рассылка (multicast): Передача пакета заданному подмножеству сетевых адресов. Эти адреса задаются в поле адреса приемника (Destination address field).
Протокол (protocol): набор правил, используемый для соединения устройств в сети. Эти правила задают формат пакета, временные интервалы, последовательность и контроль ошибок.
Отказоустойчивый канал (resilient link): пара портов, настроенные таким образом, что при выходе одно из них из строя, его функции принимает на себя другой порт. Смотрите также Основной порт (main port) и standby port.
RJ-45: стандартный 8-пиновый разъём для IEEE 802.3 10BASE-T
Удаленный мониторинг (RMON): Модуль SNMP MIB II, который позволяет мониторить и управлять устройством, обрабатывая до 10 различных потоков информации.
Резервный источник питания (RPS): устройство, подключаемое к коммутатору для обеспечения резервного питания.
SLIP - Serial Line Internet Protocol: протокол, позволяющий передвать IP-информацию поверх последовательных соединений.
SNMP - Simple Network Management Protocol: Простой протокол сетевого управления, изначально использовавшийся только в сетях TCP/IP. Сейчас SNMP широко используется в компьютерах и сетевом оборудовании и позволяет управлять многими параметрами сети и конечными станциями.
Spanning Tree Protocol (STP): Проткол покрывающего дерева, позволяющий избежать образование петель в сетях. При использовании проткола STP обеспечиваются резервные пути для прохождения трафика, в то же время, в сети не образуются петли.
Стек (stack): Группа сетевых устройств, которые объединены в группу, образуя единое логическое устройство.
standby port: порт в отказоустойчивом канале, который возьмет на себя передачу данных в случае выхода из строя основного порта.
Коммутатор (switch): устройство, которое фильтрует, продвигает и рассылает пакеты, основываясь на адресе их доставки. Коммутатор изучает адреса, связанные с каждым своим портом, и заносит полученные данные в таблицы. Продвижение пакетов происходит на основе данных, представленных в данной таблице.

TCP/IP: стек протоколов связи, обеспечивающий эмуляцию терминала Telnet, передачу по FTP и другие сервисы для связи в компьютерной сети.
telnet: приложение протокола TCP/IP, который предоставляет сервис виртуального терминала, позволяя пользователю авторизоваться на другом компьютере и разрешая доступ к хосту так, как если бы пользователь был напрямую соединён с ним.
FTP - Trivial File Transfer Protocol: протокол, позволяющий передавать файлы (такие как обновление программного обеспечения) с удалённого устройства, используя возможности управления коммутатора.
UDP - User Datagram Protocol: протокол Интернета, позволяющий программному приложению на одном устройстве отправлять датаграммы программному приложению другого устройства.
VLAN (Виртуальная LAN): объединение устройств в логическую группу независимо от размещения устройства и топологии сети. При этом взаимодействие устройств практически идентично взаимодействию в обычной сети LAN.
Канал виртуальный LAN (VLT): соединение Коммутатор-коммутатор, которое передаёт трафик всех VLAN-ов на каждый коммутатор.
VT100: тип терминала, который использует символы ASCII. VT100-терминалы представляют информацию в текстовом виде.