

D-Link™ DES-3010F / DES-3010FL / DES-3010G / DES-3018 /
DES-3026

Управляемый коммутатор с 8/16/24 портами Fast Ethernet
10/100 Мбит/с и дополнительными слотами

Версия III

Руководство пользователя

Информация в этот документ не может быть внесена без предварительного уведомления.

© 2006 D-Link Corporation. Все права защищены.

Воспроизведение материалов любым способом без письменного разрешения D-Link Corporation строго запрещается.

Торговые марки, использованные в данном тексте: D-Link и логотип D-LINK являются торговыми марками корпорации D-Link; Microsoft и Windows являются зарегистрированными торговыми марками корпорации Microsoft Corporation.

Другие торговые марки и названия могут использоваться в этом документе для ссылок как к заголовкам заявленных марок и названий, так и к их продуктам.

Корпорация D-Link не заявляет прав на патентованные торговые марки и названия, кроме своих собственных.

Май 2006 P/N 651ES3026035G

Введение

Руководство пользователя DES-3010F/DES-3010FL/DES-3010G/DES-3018/DES-3026 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.

Раздел 3, Подключение коммутатора – Описывает, как подключить коммутатор к сети 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, Введение в управление коммутатором на основе Web-интерфейса – Рассматривается управление устройством с помощью Web-интерфейса.

Раздел 6, Управление коммутатором – 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, Свойства 2 уровня – Обсуждение свойств 2 уровня коммутатора, включая VLAN, создание агрегированных каналов, IGMP Snooping, и Spanning Tree.

Раздел 8, Безопасность – Детальное обсуждение функций безопасности коммутатора, включая управление трафиком, Port Security, 802.1X, доверенный хост и сегментацию трафика.

Раздел 9, CoS – Подробное обсуждение функций Quality of Service (QoS) на коммутаторе.

Раздел 10, Контроль – Обсуждаются графические интерфейсы, используемые для управления свойствами и пакетами коммутатора.

Приложение А, Технические спецификации – Технические спецификации коммутаторов DES-3010F, DES-3010FL, DES-3010G, DES-3018 и DES-3026.

Приложение В, Кабели и коннекторы – Описание гнезд RJ-45 /коннекторов, одноходовых и пересекающихся кабелей и стандартного контактного распределения.

Приложение С, Длина кабеля – Информация о типах кабеля и их максимальной длине.

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

Предполагаемые читатели

Руководство пользователя **DES-3010F/DES-3010FL/DES-3010G/DES-3018/DES-3026** 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 .
<i>Курсив</i>	Курсивом указывается название окна или области, а также переменные или параметры, которые необходимо заменить соответствующим словом или строкой. Например: фраза «напечатайте <i>имя файла</i> » 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 Кореи 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 силовую 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 разворачиванием 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

Технология Ethernet
Описание коммутатора
Технические характеристики
Порты
Компоненты передней панели
Описание боковой панели
Описание задней панели
Гигабитные комбо-порты
Технология Ethernet
Технология Fast Ethernet

В данном руководстве рассматриваются вопросы установки, технической эксплуатации и настройки группы коммутаторов DES-3010F/DES-3010FL/DES-3010G/DES-3018/DES-3026. Эти коммутаторы идентичны как в настройках, так и в части основных аппаратных средств, поэтому 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, однако настройки для других коммутаторов группы будут идентичны, за исключением количества портов. В дальнейшем для пояснения, примеров и настроек в основном будет использоваться коммутатор DES-3018.

Описание коммутатора

Коммутаторы DES-3010F/DES-3010FL/DES-3010G/DES-3018/DES-3026 являются высокопроизводительными коммутаторами с 8/16/24 портами Fast Ethernet. Благодаря портам под неэкранированную витую пару (UTP) и автоматическому определению полярности MDI-X/MDI-II, а также портам uplink и выделенной полосе пропускания 10/100 Мбит/с, эти коммутаторы идеально подходят для сегментации сетей на небольшие группы и обеспечивают лучшую производительность для мультимедийных и фото/видео сетевых приложений. Порты Fast Ethernet могут быть использованы для подключения ПК, принтеров, серверов, концентраторов, маршрутизаторов, коммутаторов и другого сетевого оборудования, каждый порт может обеспечить пропускную способность до 200 Мбит/с в полнодуплексном режиме. Открытый слот, доступный на моделях DES-3018 / DES-3026, гигабитный порт на DES-3010G и оптический порт на DES-3010F и DES-3010FL позволяют обеспечить линию связи к серверу или магистрали сети. Встроенный консольный интерфейс может использоваться для настроек параметров коммутатора (таких, как приоритет очередей, VLAN и группы агрегированных каналов, зеркалирование портов и скорость портов).

Технические характеристики

- Поддержка IEEE 802.3z
- Управление потоком IEEE 802.3x для полнодуплексного режима
- Поддержка IEEE 802.3u

- Поддержка IEEE 802.3ab
- Приоритезация очередей IEEE 802.1p
- Поддержка протокола управления IEEE 802.3ad Link Aggregation
- Управление доступом на основе портов и MAC-адресов IEEE 802.1x
- IEEE 802.1Q VLAN
- IEEE 802.1D Spanning Tree и IEEE 802.1W Rapid Spanning Tree
- Поддержка управления через единый IP-адрес
- Поддержка протокола SNTP (простой протокол синхронизации времени)
- Поддержка системы и использования порта
- Поддержка системного журнала
- Неблокируемая схема коммутации store-and-forward с автоматическим определением скорости и протокола передачи
- Поддержка управления скоростью входа/выхода порта
- Поддержка разблокировки и блокировки на основе порта
- Адресная таблица: поддерживает до 8 К MAC-адресов на устройстве
- Trunking порт с гибким распределением нагрузки и функцией обработки отказов
- Поддержка IGMP Snooping
- Поддержка SNMP
- Поддержка SMTP
- Списки контроля доступа (ACL) CPU
- Поддержка зеркалирования портов
- Поддерживает MIB для:
 - RFC1213 MIB II
 - RFC1493 Bridge
 - RFC1757 RMON
 - RFC1643 Ether-like MIB
 - RFC2233 Interface MIB
 - RFC2358 Ether-like MIB
 - IF MIB
 - Private MIB
 - RFC2674 for 802.1p
 - IEEE 802.1x MIB
- Консольный порт RS-232 DCE для управления коммутатором через консоль
- Индикаторы, отображающие состояние портов(link/act, speed и т.д.).

Технология Ethernet Fast Ethernet

С ростом локальных сетей и сложности компьютерных приложений требуются более высокопроизводительные сети. Технология 100BASE-T (Fast Ethernet) предоставляет экономически эффективное и высокопроизводительное решение для малых сетей, сетей SMB (Small to Medium Business, малого и среднего бизнеса) и других сетей, обеспечивая высокую полосу пропускания для приложений, требовательных к полосе пропускания. Технология Fast Ethernet работает на скорости в 10 раз большей, чем традиционная технология Ethernet, предлагая высокую производительность и расширенные возможности для существующих сетей Ethernet. Технология 100 Мбит/с Fast Ethernet определена стандартом IEEE 802.3. Это расширение стандарта 10 Мбит/с Ethernet с возможностью передачи и приема данных на скорости 100 Мбит/с, оставаясь при этом в рамках протокола Ethernet CSMA/CD.

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, контроль потока и объекты управления, но характеризуется десятикратным увеличением теоретической пропускной способности по сравнению с 100Мб/с Fast Ethernet и стократным увеличением по сравнению с 10 Мб/с Ethernet. Gigabit Ethernet обеспечивает усовершенствование характеристик сети без дополнительных инвестиций в аппаратные средства, программное обеспечение и обучение персонала.

Увеличенная скорость и расширенная пропускная способность, предоставляемые технологией Gigabit Ethernet, необходимы пользователям, работающим с более скоростными приложениями, генерирующими большое количество трафика. Одновременное улучшение магистрали и серверов до Gigabit Ethernet, может значительно сократить время отклика сервера, а также увеличить скорость передачи данных между подсетями.

Gigabit Ethernet дает возможность организовать скоростные соединения по оптическому волокну для поддержки видеоконференции, систем формирования изображений и приложений, требующих обработки большого количества данных. Поскольку передача данных происходит в 10 раз быстрее, чем в технологии Fast Ethernet, серверы снабжаются 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, делает экономически эффективным использование преимуществ данной технологии в рамках быстро развивающихся на сегодняшний день технологий коммутации и маршрутизации сетей.

Технология коммутации

Коммутация – это экономически эффективный способ увеличения производительности сети для пользователей LAN. Коммутатор увеличивает пропускную способность сети и уменьшает ее загрузку путем разделения всей локальной сети на несколько сегментов. Разделение локальной сети на множество сегментов является самым распространенным способом увеличения пропускной способности. При правильном сегментировании сети большая часть сетевого трафика будет передаваться в пределах одного сегмента, используя полную пропускную способность данного сегмента.

Если в сети Ethernet появляются признаки перегрузки, низкой пропускной способности, увеличивается время отклика и повышается количество коллизий, то установка в сети коммутатора может сохранить большую часть кабельной структуры и сетевых адаптеров на рабочих станциях при одновременном увеличении выделенной для пользователей пропускной способности. Коммутатор окажется жизнеспособным решением, даже если планируется использовать чувствительные к задержкам мультимедийные приложения или видеоконференции в сети. Еще одно преимущество, наряду с сохранением вложенных инвестиций, состоит в том, что в сети возможно установить несколько коммутаторов Ethernet.

Коммутатор обеспечивает для каждого соединения работу на полной скорости канала связи и выделенную пропускную способность. Это прямая противоположность концентратору, который использует традиционную сетевую топологию – общий разделяемый сегмент, и подключенные к нему узлы совместно используют одну и ту же полосу пропускания. Когда между собой взаимодействуют два коммутируемых узла, то они соединяются через выделенный канал связи, поэтому конкуренции с другими узлами за пропускную способность сети не возникает. Как следствие, коммутатор значительно снижает вероятность перегрузки сети.

Для сетей Ethernet коммутатор является эффективным решением проблемы последовательного соединения концентраторов свыше «предела двух повторителей». Коммутатор может быть использован для выделения частей сети в отдельные домены коллизий, делая возможным расширение сети Ethernet на больший диаметр, чем ограничение для сетей 100BASE-TX в 205 метров. Поддержка коммутатором как сетей 10 Мбит/с Ethernet, так и 100 Мбит/с Fast Ethernet идеально подходит для использования его в качестве моста между существующими сетями 10 Мбит/с и новыми сетями 100 Мбит/с.

Технология коммутации локальных сетей является заметным улучшением предыдущего поколения сетевых концентраторов и мостов, которые характеризовались большой задержкой в работе. Маршрутизаторы также использовались для сегментирования локальных сетей, но стоимость маршрутизатора, его установка и обслуживание делали такое решение относительно непрактичным. На сегодняшний день коммутаторы являются идеальным решением большинства проблем с перегрузкой локальных сетей.



ПРИМЕЧАНИЕ: За дополнительной информацией по программному обеспечению SNMP-управления от D-Link Corporation и загрузкой ПО и руководства пользователя, пожалуйста, обратитесь на Web-страницу D-Link (www.dlink.ru).

Компоненты передней панели и индикаторы

Передняя панель коммутатора содержит индикаторы (Power, Console, Link/Act и Speed), 8/16/24 портов FastEthernet, 2 дополнительных слота для подключения модулей (только для DES-3018/3026), медный гигабитный порт 1000BASE-T (DES-3010F/G), порт 100BASE-FX Ethernet (DES-3010F, DES-3010FL), порт SFP Gigabit Ethernet (DES-3010G). Также на передней панели находится консольный порт RS-232.

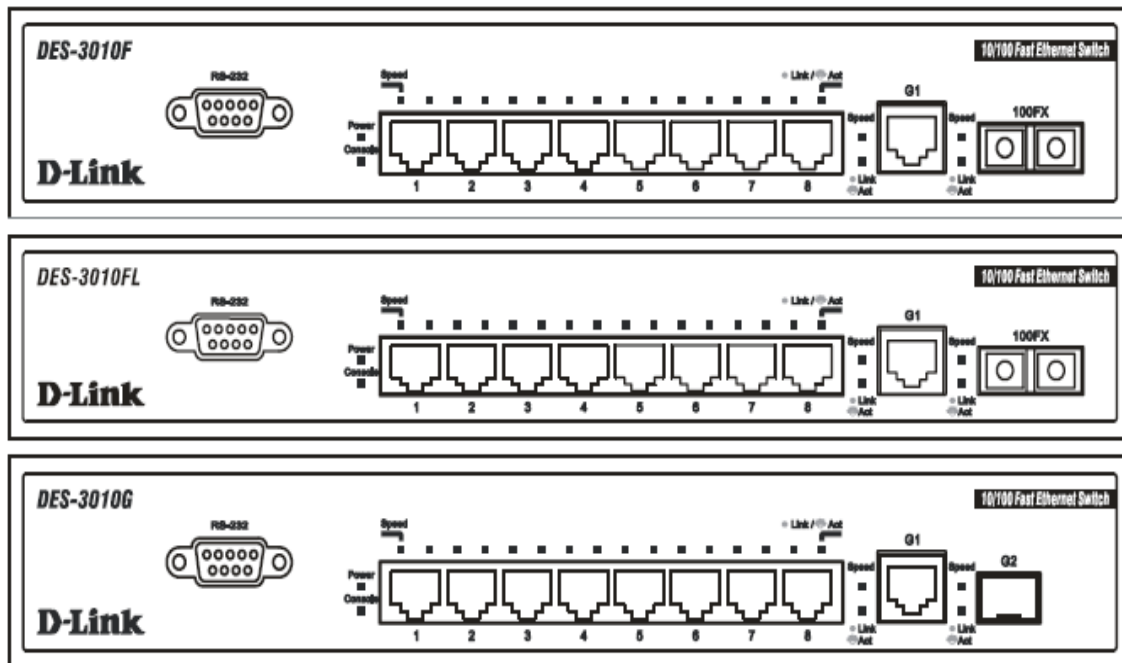


Рисунок 1.1 – Вид передней панели коммутаторов DES-3010F/FL/G

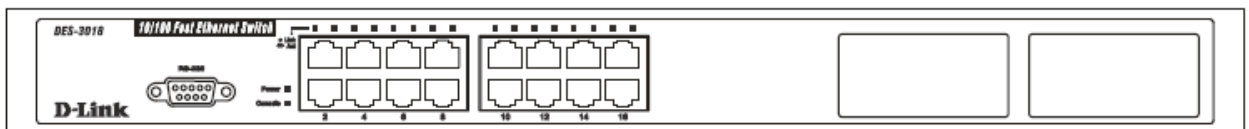


Рисунок 1.2 – Вид передней панели коммутаторов DES-3018

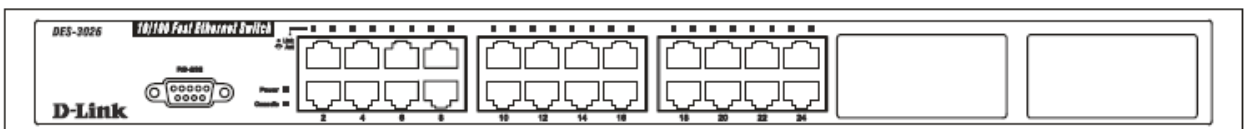


Рисунок 1.3 – Вид передней панели коммутаторов DES-3026

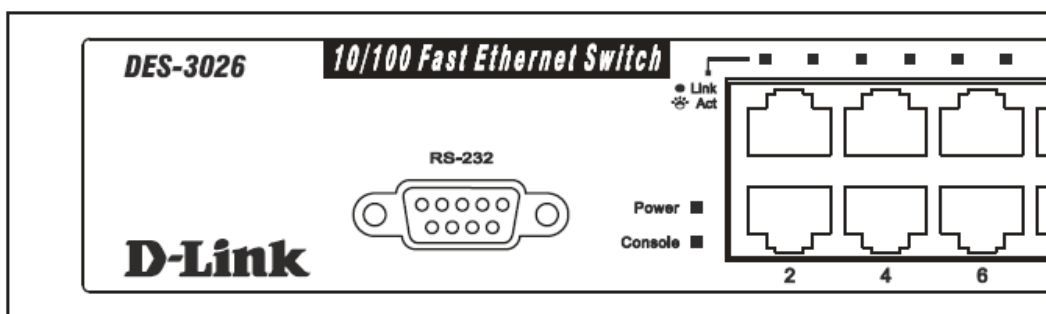


Рисунок 1.4 – индикаторы на коммутаторе DES-3026

Индикаторы отображают состояние коммутатора и сети.

Светодиодный индикатор	Описание
Power	После включения коммутатора индикатор питания будет гореть зеленым светом, показывая готовность устройства к работе. В случае отключения питания индикатор погаснет.
Console	Данный индикатор будет мигать во время самотестирования при включении питания Power-On Self Test (POST). После того, как самотестирование будет завершено, индикатор погаснет. Индикатор будет гореть постоянным зеленым светом в случае удаленного или локального управления коммутатором через консольный порт RS-232 с помощью «прямого» последовательного кабеля.
Link/Act	Постоянный зеленый свет данного индикатора свидетельствует об установленном соединении на порту. Мигающий индикатор свидетельствует о текущей активности на порту.
Speed	<p>Справа от каждого индикатора Link/Act расположен индикатор Speed, соответствующий каждому порту. В зависимости от модели коммутатора, индикаторы могут означать различное состояние порта. DES-3010F/FL/G – постоянный зеленый цвет индикатора указывает на передачу данных на порту на скорости 100 Мбит/с, при погасшем индикаторе – со скоростью 10 Мбит/с.</p> <p>Порт 9 – индикатор этого порта, который горит постоянным зеленым светом, указывает на передачу данных со скоростью 1000 Мбит/с. Погасший индикатор указывает на передачу данных со скоростью 10/100 Мбит/с.</p> <p>Порт 10 – для 3010F и 3010FL постоянный зеленый цвет индикатора указывает на скорость передачи данных со скоростью 100 Мбит/с, и погасший индикатор указывает на отсутствие соединения. Для 3010G – постоянный зеленый цвет индикатора указывает на передачу данных со скоростью 1000 Мбит/с, а погасший индикатор указывает на отсутствие соединения.</p> <p>DES-3018/DES-3026 – постоянный зеленый цвет индикатора указывает на установленное соединение на скорости 100 Мбит/с, и мигающий индикатор указывает на передачу данных через этот порт в настоящее время. Постоянный желтый цвет индикатора означает установленное соединение на скорости 10 Мбит/с, и мигающий индикатор указывает на передачу данных через этот порт в настоящее время.</p>

Описание задней панели

На задней панели коммутатора расположен разъем питания переменного тока.

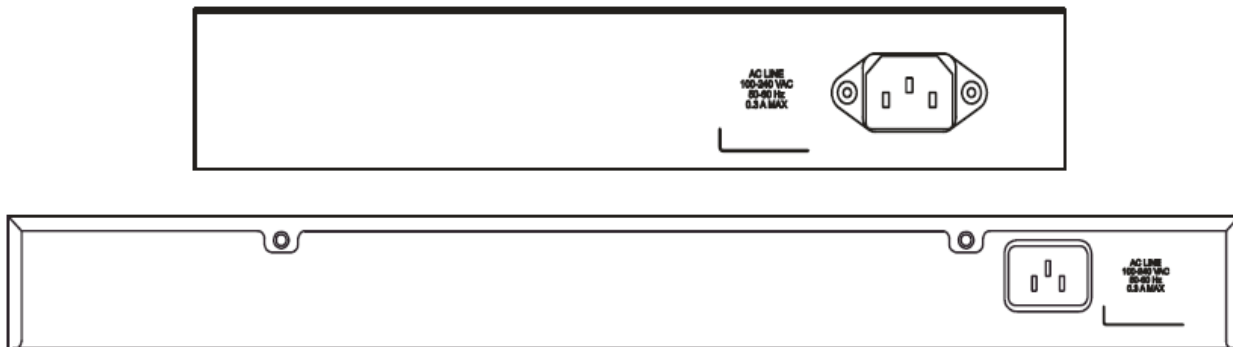


Рисунок 1.5 – Вид задней панели коммутаторов DES-3010F/FL/G и DES-3018/ DES-3026

Описание боковой панели

Обе панели коммутатора содержат вентиляторы, используемые 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 для обеспечения надлежащей вентиляции. Напоминаем, что без правильно организованного теплового рассеивания и циркуляции воздуха, компоненты системы могут перегреться, что, в свою очередь, может привести к нарушению работы устройства.

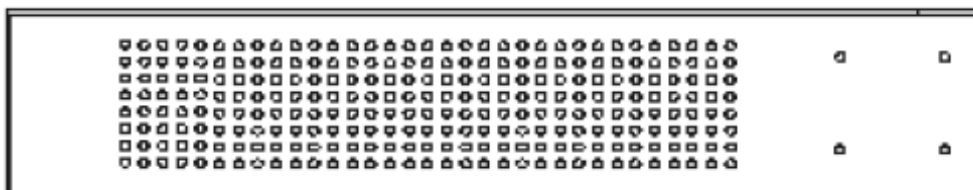


Рисунок 1.6 – Боковые панели коммутатора

Раздел 2 - Установка

Комплект поставки
Перед подключением к сети
Установка коммутатора вне стойки
Монтаж коммутатора в стойку
Включение электропитания
Дополнительные модули
Резервная система питания

Комплект поставки

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

- Один коммутатор DES-3010F, DES-3010FL, DES-3010G, DES-3018 или DES-3026 Fast Ethernet
- Монтажный комплект для крепления в стойку (две скобы и винты)
- Четыре резиновые ножки с клейкой подложкой
- Один шнур питания переменного тока (AC)
- Консольный кабель RS-232
- Один компакт-диск, содержащий руководство пользователя/ CLI/ модуль D-View/ модуль SNMP
- Данное руководство пользователя с регистрационной карточкой

Если любой из элементов отсутствует или поврежден, пожалуйста, обратитесь к поставщику D-Link для замены.

Перед подключением к сети

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

- Установите коммутатор на прочную горизонтальную поверхность, которая может выдержать вес коммутатора. Не помещайте тяжелые предметы на коммутатор.
- Электрическая розетка должна быть не далее 1,82м от коммутатора.
- Проверьте, чтобы шнур питания был плотно подсоединен к разъему питания переменного тока.
- Убедитесь, что обеспечиваются надлежащие теплоотвод и вентиляция для работы коммутатора. Оставьте по 10 см свободного пространства перед передней и задней панелями коммутатора для вентиляции.
- Установите коммутатор в довольно прохладном и сухом месте с допустимым значением температуры и влажности.
- Установите коммутатор таким образом, чтобы он не находился под воздействием источников сильного электромагнитного поля (таких как двигатели), вибрации, пыли и прямых солнечных лучей.
- При установке коммутатора на горизонтальную поверхность, прикрепите резиновые ножки к основанию устройства. Резиновые «ножки» коммутатора предохранят корпус от царапин.

Установка коммутатора вне стойки

Прежде чем установить коммутатор на стол или полку, прикрепите сначала прилагающиеся к коммутатору резиновые «ножки», служащие для амортизации, в углы основания устройства. Обеспечьте достаточное вентиляционное пространство между коммутатором и другими предметами, находящимися по близости.

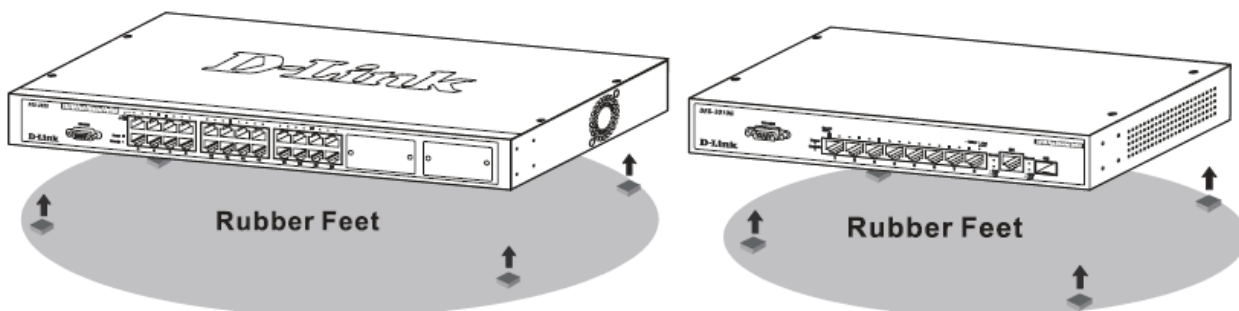


Рисунок 2.1 – Подготовка коммутатора к установке на стол или полку

Монтаж коммутатора в стойку

Коммутатор может быть вмонтирован в стандартную 19” стойку. Используйте следующие рисунки в качестве руководства.

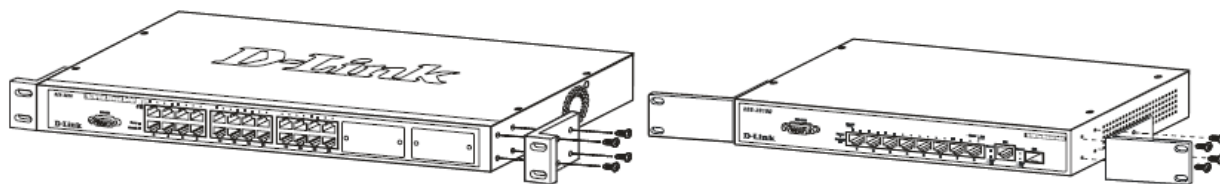


Рисунок 2.2 – Прикрепление монтажных уголков к коммутатору

Прикрепите монтажные уголки к коммутатору с помощью прилагающихся винтов. Благодаря аккуратно прикрепленным петлям, можно монтировать коммутатор в стойку, как это показано ниже на рисунке 2.3.

Монтаж коммутатора в стандартную 19” стойку

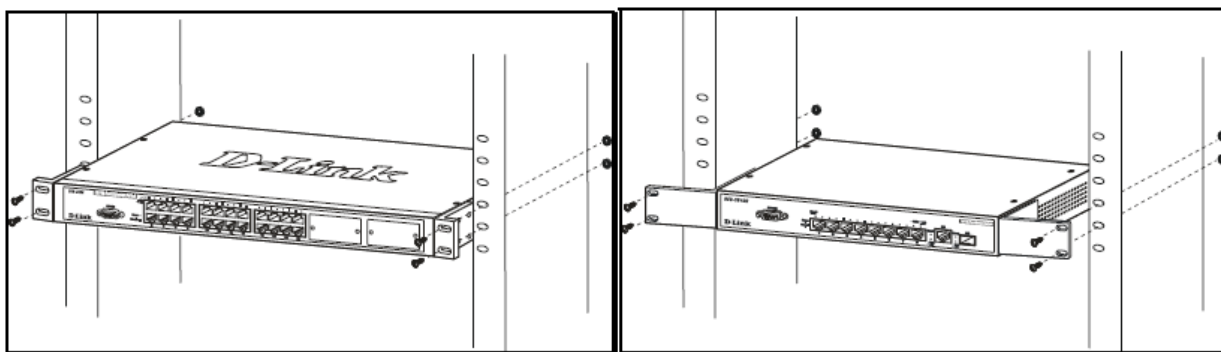


Рисунок 2.3 – Монтаж коммутатора в стойку

Включение питания

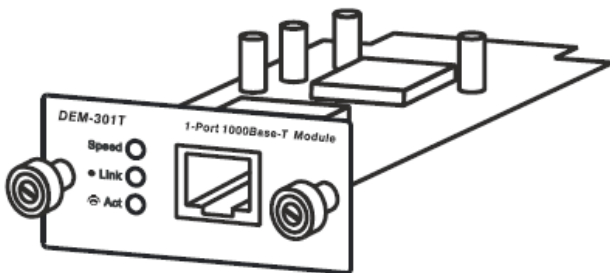
Подключите один конец шнура питания с переменным током к разъему питания коммутатора, а другой конец подключите в ближайшую розетку.

После включения коммутатора сразу же замигают светодиодные индикаторы. Подобное мигание означает сброс настроек системы.

При сбое питания необходимо выключить коммутатор. Включите коммутатор снова при восстановлении питания.

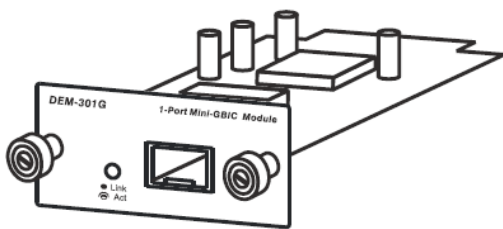
Дополнительные модули

На передней панели DES-3018 и DES-3026 расположены слоты для дополнительных модулей. Модули, специально разработанные для этой серии коммутаторов, могут использоваться как uplink-порты для подключения к серверу или коммутатору ядра сети. Этот слот может быть оснащен однопортовым Uplink-модулем, продающимся отдельно. Дополнительная информация по модулям приведена ниже.



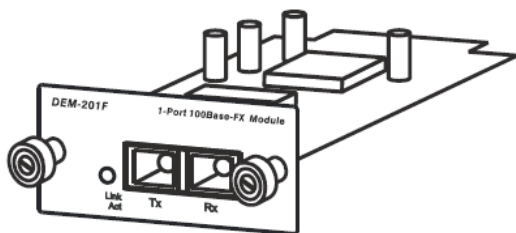
- Uplink-модуль с одним портом 1000BASE-T GigabitEthernet
- Совместимый с IEEE802.3, IEEE802.3u, IEEE802.3ab
- Комплексные индикаторы для Speed, Link и Act(ivity)
- Поддержка автосогласования скорости 10/100/1000 Мбит/с, полнодуплексного режима, управление потоком в полудуплексном / полнодуплексном режиме методом обратного давления IEEE802.3x

Рисунок 2- 4. Дополнительный модуль DEM-301T



- Гигабитный uplink-модуль с одним портом SFP
- Совместим с IEEE802.3z
- Индикаторы Link и Act(ivity)
- Поддержка автосогласования скорости в полнодуплексном режиме и управления потоком IEEE802.3x в полнодуплексном режиме
- Поддерживает модули DEM-310GT, DEM-311GT, DEM-314GT, DEM-315GT

Рисунок 2- 5. Дополнительный модуль DEM-301G



- Uplink-модуль с одним портом 100BASE-FX Fast Ethernet
- Совместим с IEEE802.3u
- Индикаторы Link и Act(ivity)
- Поддержка скорости 100 Мбит/с, полнодуплексного режима и управления потоком IEEE802.3x в полнодуплексном режиме
- Разъем SC для кабеля с максимальной длиной 2 км

Рисунок 2- 6. дополнительный модуль DEM-201F

Для установки модулей следуйте несложным шагам, описанным ниже:



ПРЕДОСТРЕЖЕНИЕ: Перед установкой дополнительного модуля, убедитесь, что все источники питания, подключенные к коммутатору, отключены. Пренебрежение данным правилом может привести к поражению электрическим током, которое может привести к повреждению устройства и нанести вред человеку.

На передней панели коммутатора справа расположены слоты для дополнительных модулей, как показано на рисунке 2-7 и 2-8. Эти слоты закрыты лицевыми панелями. При необходимости использования слотов, необходимо открутить винты и снять панели.

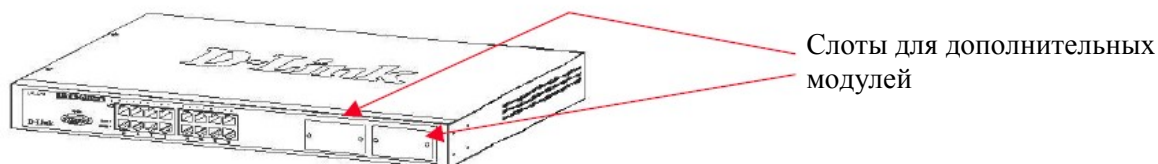


Рисунок 2- 7. Слоты для дополнительных модулей на передней панели DES-3018

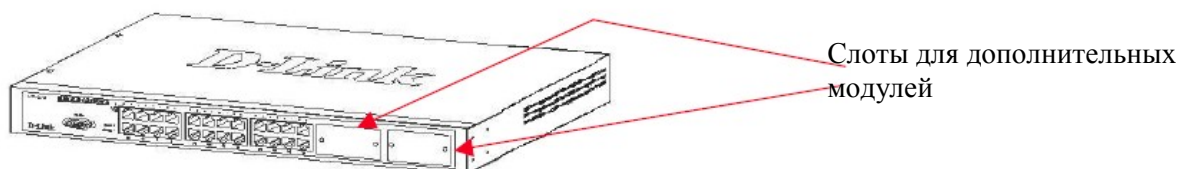


Рисунок 2- 8. Слоты для дополнительных модулей на передней панели DES-3026

Возьмите модуль и вставьте его в свободный слот на передней панели коммутатора до упора, как показано на следующем рисунке. Модуль должен быть подключен к задней панели слота. Осторожно, но с усилием введите модуль в коммутатор. Необходимо, чтобы модуль был надежно закреплен в соответствующем слоте.

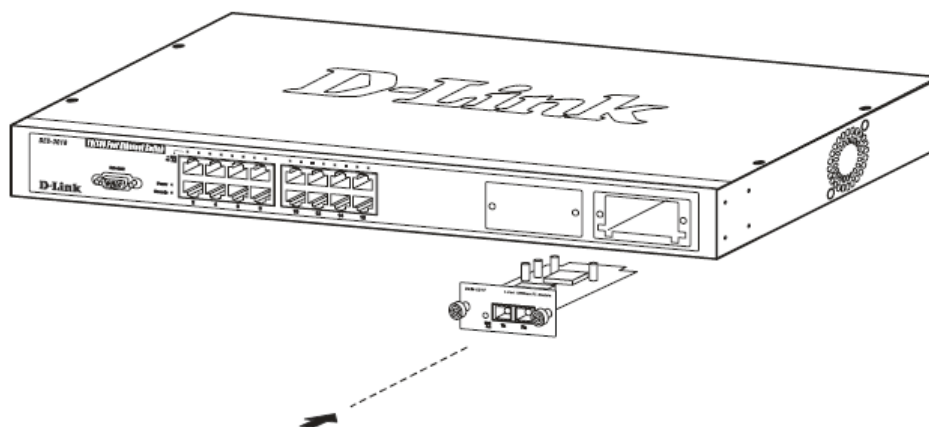


Рисунок 2- 9. Установка дополнительного модуля в коммутатор

Теперь установка модуля в коммутатор завершена, и DES-3018 / DES-3026 готов к использованию.

Раздел 3 - Подключение коммутатора

Подключение коммутатора к конечному узлу

Подключение коммутатора к концентратору или коммутатору

Подключение коммутатора к магистрали сети или серверу



Примечание: Все высокопроизводительные порты NWay Ethernet коммутатора могут поддерживать как MDI-II, так и MDI-X соединения.

Подключение коммутатора к конечному узлу

Под конечным узлом подразумевается ПК (PC) с сетевыми адаптерами Ethernet/Fast Ethernet 10/100/1000 Мбит/с и 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. Конечный узел может быть подключен к любому порту 10/100BASE-T коммутатора.

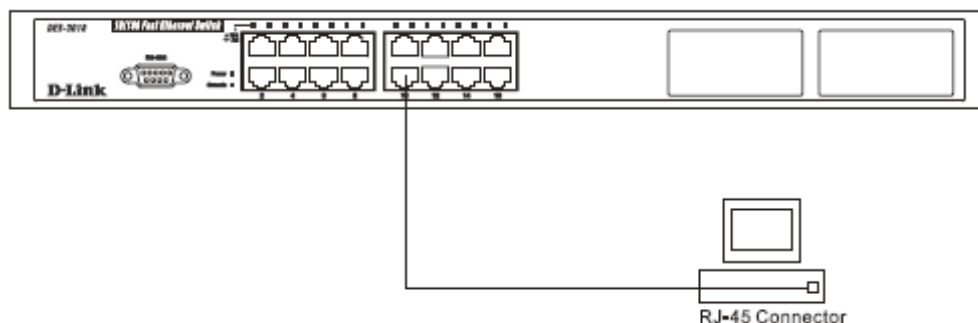


Рисунок 3.1 – Подключение коммутатора к конечному узлу

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

Подключение коммутатора к концентратору или коммутатору

Данное подключение может быть выполнено различными способами с помощью обычного кабеля.

- 10 Base-T - концентратор или коммутатор может быть подключен к коммутатору по витой паре неэкранированного/экранированного (UTP/STP) кабеля категории 3, 4 или 5.
- 100Base-TX - концентратор или коммутатор может быть подключен к коммутатору по витой паре неэкранированного/экранированного (UTP/STP) кабеля категории 5.
- 1000BASE-T коммутатор может быть подключен к коммутатору по витой паре неэкранированного/экранированного (UTP/STP) кабеля категории 5е.
- Коммутатор поддерживает оптоволоконный uplink-кабель и может быть подключен к порту SFP другого коммутатора по оптоволоконному кабелю.

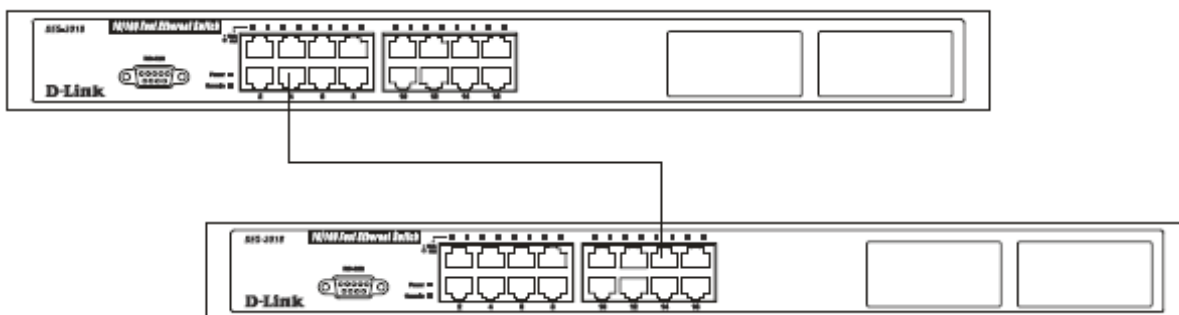


Рисунок 3.2 – Коммутатор, подключенный к концентратору или коммутатору с помощью прямого или кроссового кабеля

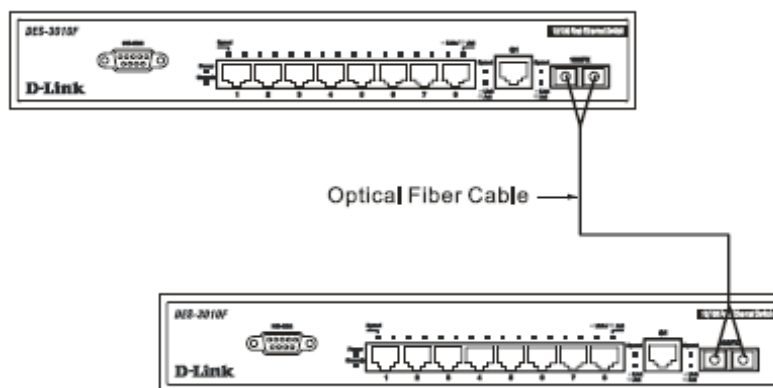


Рисунок 3- 3. Коммутатор, подключенный к коммутатору с помощью оптоволоконного кабеля

DES-3010F/FL/G, DES-3018 или DES-3026 в качестве магистрали сети

DES-3018 может применяться в качестве магистрали сети для офисов или зданий, требующих множество Ethernet соединений внутри закрытых зон. Включив в DES-3018 высокоскоростную линию провайдера, возможно обеспечить соединение для различных конечных узлов, включая компьютеры, принтеры, концентраторы, маршрутизаторы или другие коммутаторы. Количество топологий огромное количество, однако, во избежание «узких мест» в сети, убедитесь, что скорость соединения от DES-3018 является эквивалентной или меньшей, чем скорость uplink провайдера.

Медные порты могут работать на скорости 100 Мбит/с или 10 Мбит/с в режимах полного или полудуплекса. Порты 100BASE-FX могут работать на скорости 100 Мбит/с только в полудуплексном режиме. Медный гигабитный порт может работать на скорости 1000 Мбит/с

только в полнодуплексном режиме. Гигабитный порт SFP может работать на скорости 1000 Мбит/с только в полнодуплексном режиме.

Подключения к портам Gigabit Ethernet осуществляются в зависимости от типа порта по волоконно-оптическому кабелю или по медному кабелю категории 5е. Активность индикатора Link свидетельствует о правильном подключении.

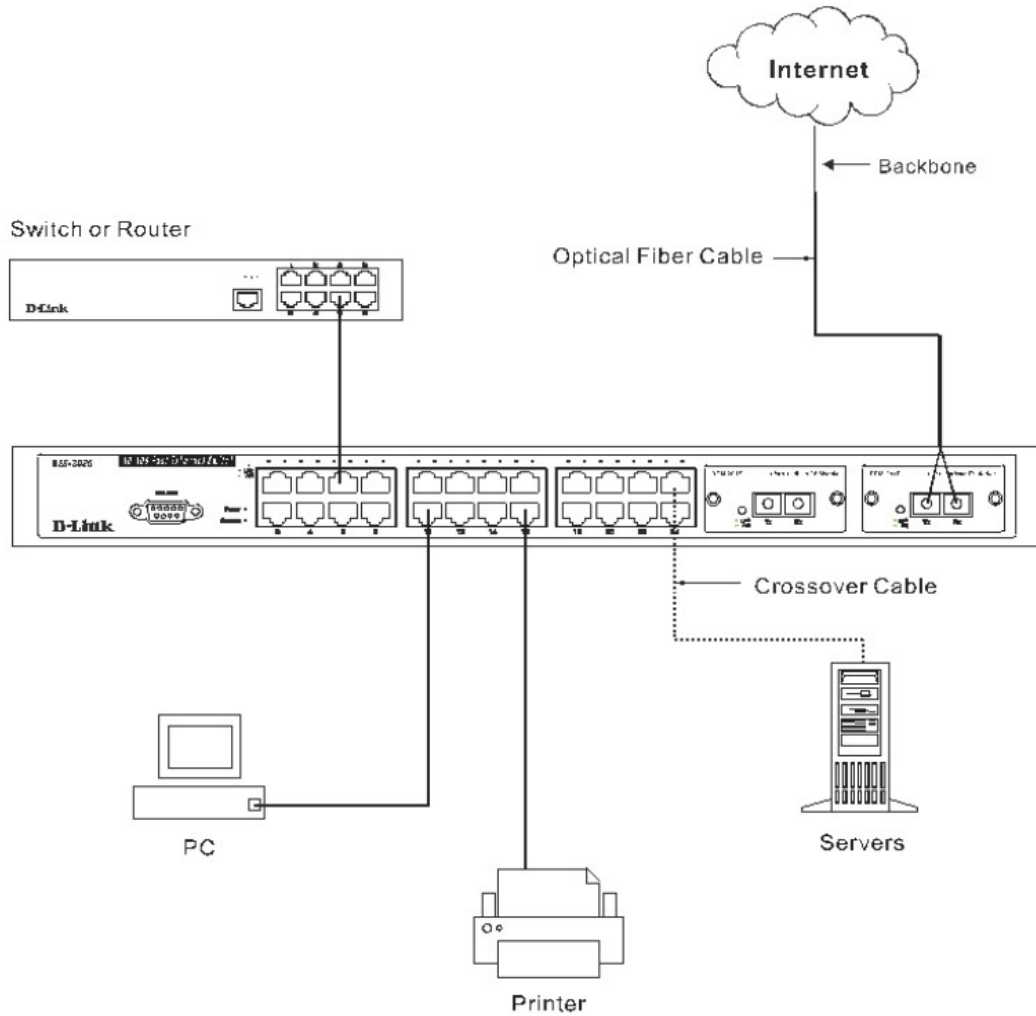


Рисунок 3- 4. Uplink-подключение к серверу, компьютеру или стеку коммутаторов.

Раздел 4 - Введение в управление коммутатором

Функции управления

Web-интерфейс управления

Управление через SNMP-протокол

Интерфейс командной строки через последовательный порт

Подключение к консольному порту коммутатора (RS-232 DCE)

Первое подключение к коммутатору

Защита паролем

Настройка SNMP

Назначение IP- адреса

Подключение устройств к коммутатору

Функции управления

Коммутатор поддерживает как удаленное управление через консольный порт на передней панели, так и локальное через Telnet. Пользователь также может управлять коммутатором через Web-интерфейс посредством Web-браузера.

Web-интерфейс управления

После успешной установки коммутатора, можно настраивать его, проверять его состояние по индикаторам на панели и просматривать графическую статистику, используя Web-браузер, например, Netscape Navigator (версии 6.2 и выше) или Microsoft Internet Explorer (версия 5.0).

Управление через SNMP- протокол

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

Интерфейс командной строки через последовательный порт

Можно подключить компьютер или терминал к последовательному порту консоли для доступа к коммутатору. Интерфейс командной строки обеспечивает полный доступ ко всем функциям управления коммутатора.

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 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:

1. Выберите подходящий последовательный порт (COM порт 1 или COM порт 2).
2. Установите скорость передачи данных 9600 бод.
3. Установите формат данных: 8 бит данных, 1 стоповый бит и отсутствие контроля по четности.
4. Установите отсутствие управление потоком.
5. В **Propertys** следует выбрать режим *VT 100* для запуска режима эмуляции.
6. Необходимо выбрать терминальные клавиши для функций, стрелок и Ctrl. Убедитесь, что выбранные клавиши, не совпадают с «горячими клавишами» Windows.



Примечание: При использовании HyperTerminal с операционной системой Microsoft® Windows® 2000, следует убедиться, что установлен Windows 2000 Service Pack 2 или более поздняя версия. Windows 2000 Service Pack 2 позволяет использовать клавиши со стрелками в эмуляторе HyperTerminal VT100. Получить информацию по Windows 2000 Service Pack можно на сайте www.microsoft.com

7. После правильной установки терминала следует подключить кабель питания в гнездо питания на задней панели коммутатора. На терминале отобразится процесс загрузки.
8. После завершения процесса загрузки, появится окно console login.
9. Если регистрация в программе интерфейса командной строки (CLI) еще не произведена, следует нажать клавишу Enter в полях Имя пользователя (User name) и Пароль (Password), т.к. по умолчанию они не заданы. Администратор, прежде всего, должен создать имя пользователя и пароль. Если учетные записи пользователей были установлены ранее, следует зарегистрироваться и продолжить настройку коммутатора.
10. 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 DES-3018, где приведен список всех команд и дополнительная информация по использованию CLI.
11. После того, как задачи выполнены, необходимо закрыть сессию с помощью команды завершения сеанса или закрыть программу эмулятора.

Необходимо убедиться, что терминал или ПК, который используется для подключения, настроен в соответствии с данными настройками.

Если возникли проблемы с созданием данного соединения на ПК, необходимо убедиться, что при эмуляции был установлен режим *VT100*.

Можно установить режим эмуляции, нажав в окне Hyper Terminal **File** □ **Properties** □ **Settings** □ **Emulation**. Если нет никаких изменений, следует попытаться 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 имя пользователя и пароль отсутствуют, таким образом, для доступа к интерфейсу командной строки необходимо будет дважды нажать Enter.

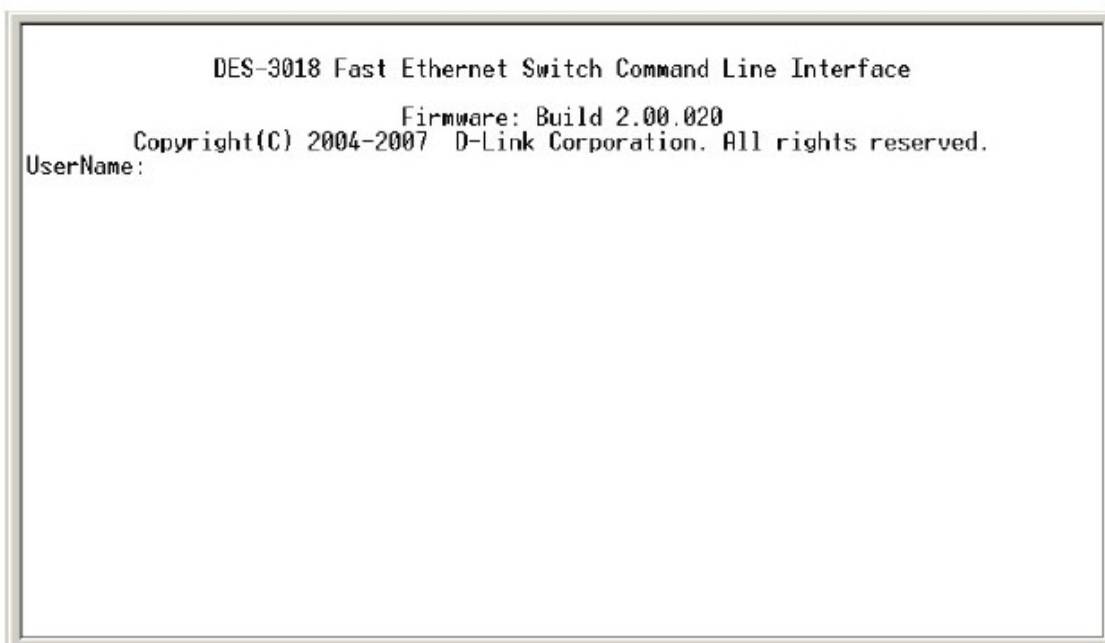


Рисунок 4.1 – Вид окна при первом подключении

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 разделе рассказывается, как зарегистрироваться на коммутаторе.



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

Во время первого подключения к коммутатору появится регистрационное окно (показано ниже).



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.

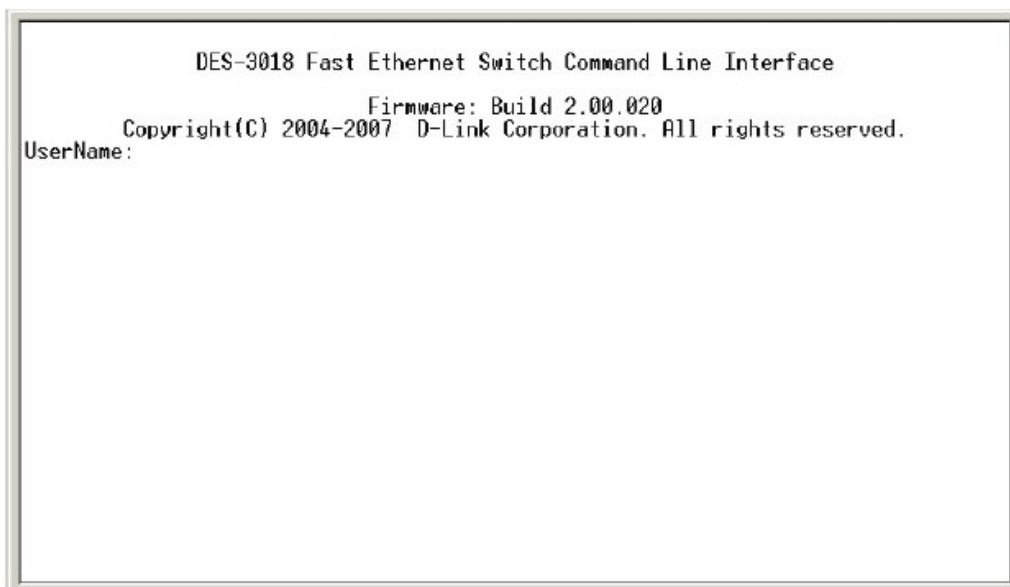


Рисунок 4- 2. Исходный экран при первом подключении к коммутатору

Нажмите Enter в обоих полях Username (Имя пользователя) и Password (Пароль). После чего будет предоставлен доступ к командной строке **DES-3018:4#**, как это показано ниже.

Изначально имя пользователя и пароль не установлены. Поэтому оставьте поля Username (Имя пользователя) и Password (Пароль) пустыми.

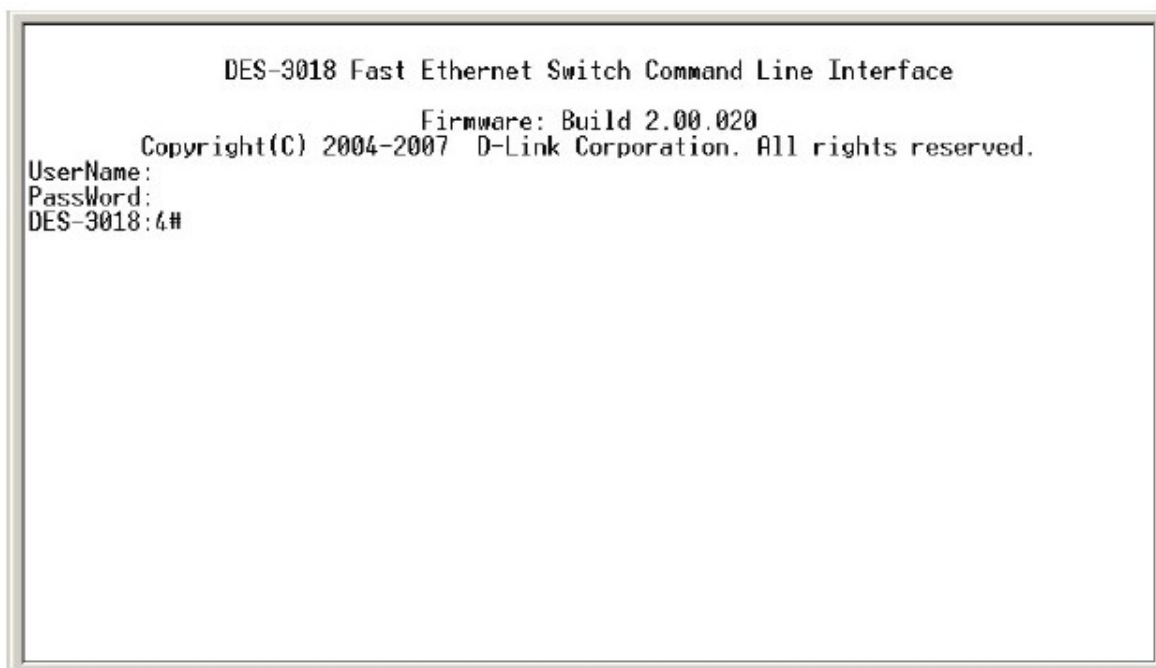


Рисунок 4.3 – Командная строка



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

Защита паролем

В коммутаторе DES-3018 по умолчанию не настроены имя пользователя и пароль. Одной из первых задач при настройке коммутатора является создание учетных записей пользователей. Если регистрация произведена с использованием предписанного имени пользователя уровня администратора, то будет предоставлен привилегированный доступ к программному обеспечению управления коммутатором.

После первоначальной регистрации, для предотвращения доступа к коммутатору неавторизованных пользователей задайте новые пароли для каждого имени пользователя.

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

- В командной строке CLI введите созданную учетную запись администратора после `<user name>` и нажмите клавишу Enter.
- Вас попросят ввести пароль. Введите `<password>`, заданный 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.
- Успешное создание новой учетной записи администратора будет подтверждено сообщением.



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

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

```
DES-3018:4#create account admin newmanager
Command: create account admin newmanager

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

Success.

DES-3018:4#
```



Примечание: Изменение настроек коммутатора при помощи интерфейса командной строки всего лишь изменяет 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.

Настройка 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.

DES-3018 поддерживает протокол SNMP версий: 1, 2с 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 значимыми, как например, изменение статуса порта. Коммутатор создает сообщения «traps» и отправляет их получателю аварийных сообщений (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.

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. Можно изменить этот адрес в соответствии со схемой адресов в сети.

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:

```
Command: show switch

Device Type       : DES-3018 Ethernet Switch
Module 1 Type     : None
Module 2 Type     : None
MAC Address       : 00-11-95-EB-83-32
IP Address        : 10.53.13.33 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.01.003
Firmware Version  : Build 2.00.020
Hardware Version  : 0A1
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
IGMP Snooping     : Disabled
802.1X           : Disabled
TELNET            : Enabled(TCP 23)
WEB               : Enabled(TCP 80)
RMON              : Disabled

DES-3018:4#
```

Рисунок 4.4 – Команда «show_switch»

MAC-адрес коммутатора можно также найти через управляющую Web-программу в окне **Switch Information (Basic Settings)** в меню **Configuration**.

Перед началом управления коммутатором необходимо задать его IP-адрес с помощью Web-менеджера. IP-адрес коммутатора может быть автоматически установлен с помощью протоколов BOOTP или DHCP. В данном случае необходимо знать текущий адрес, назначенный коммутатору. IP-адрес может быть установлен с помощью интерфейса 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, связанный с IP-интерфейсом (System); y – текущая маска подсети.

Также можно ввести команду: **config ipif System ipaddress xxx.xxx.xxx.xxx/z**

Где x – IP-адрес, связанный с IP-интерфейсом (System); z – соответствующее количество подсетей в CIDR-нотации.

IP- интерфейс, называемый System, на коммутаторе может быть связан с IP-адресом и маской подсети. Затем обычно управляющая станция соединяется с Telnet или управляемым Web-агентом коммутатора.

```
DES-3018 Fast Ethernet Switch Command Line Interface
                               Firmware: Build 2.00.020
                               Copyright(C) 2004-2007 D-Link Corporation. All rights reserved.
UserName:
Password:
DES-3018:4#config ipif System ipaddress 10.53.13.33/255.0.0.0
Command: config ipif System ipaddress 10.53.13.33/8

Success.
DES-3018:4#
```

Рисунок 4.5 – Назначение IP-адреса коммутатору

В приведенном выше примере коммутатору назначен IP-адрес 10.53.13.33 с маской подсети 255.0.0.0. Системное сообщение **Success** свидетельствует о том, что команда успешно выполнена. Настройка и управление коммутатором может осуществляться через Telnet и CLI или через Web-интерфейс управления.

Подключение устройств к коммутатору

После назначения IP-адреса можно подключать устройства к коммутатору.

Для подключения устройства к порту SFP-передатчика:

- Выберите соответствующий тип SFP-передатчика в соответствии с требованиями к кабелю.
- Вставьте SFP- модуль в слот для SFP- передатчика.
- Используйте соответствующий сетевой кабель для подключения устройства к SFP-передатчику.



Предупреждение: При установке соединения SFP- передатчиком, порт 10/100/1000 Base-T будет отключен.

Раздел 5 - Настройка коммутатора через Web-интерфейс

Введение
Регистрация в Web-менеджере
Пользовательский Web-интерфейс
Основные настройки
Перезагрузка
Основные настройки коммутатора
Сетевое управление
Утилиты коммутатора
Мониторинг сети
Состояние IGMP Snooping

Введение

Все программные функции коммутатора DES-3018 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 позволяет с помощью HTTP протокола подключаться к коммутатору.

Модуль управления через Web-интерфейс и консольная программа (Telnet) – это всего лишь различные способы для доступа и настройки одного и того же внутреннего программного обеспечения коммутатора. Таким образом, все настройки, встречающиеся в Web-интерфейсе, идентичны тем, которые представлены в консольной программе.

Регистрация в Web-менеджере

Для того чтобы начать настройку вашего коммутатора, просто запустите браузер, установленный на вашем компьютере и введите IP-адрес устройства. URL в адресной строке должен выглядеть следующим образом: <http://123.123.123.123>, где числа 123 представляют IP-адрес коммутатора.



Примечание: Заводской IP-адрес коммутатора по умолчанию 10.90.90.90.

На открывшейся странице нажмите **Login**:



Рисунок 5.1 - Кнопка регистрации

Откроется окно аутентификации пользователя, как показано ниже:

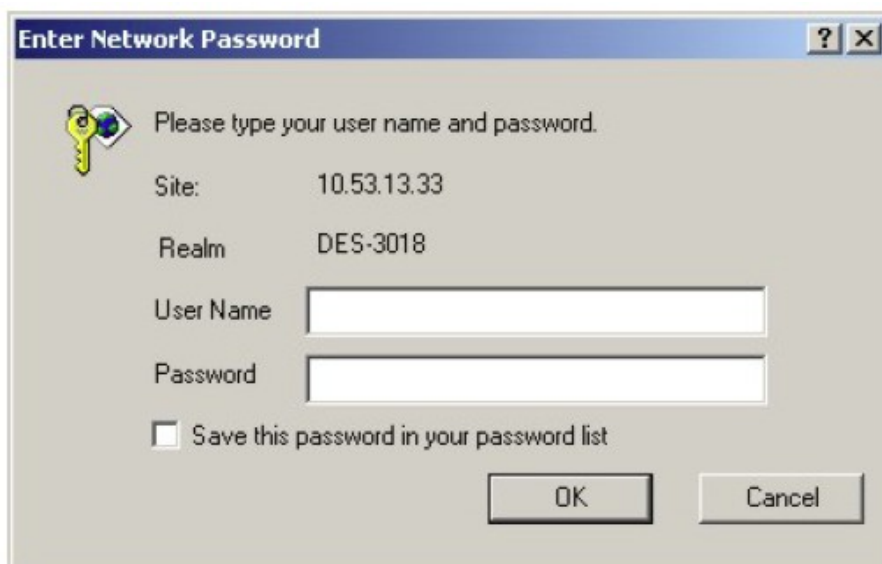


Рисунок 5.2 – Окно «Enter Network Password»

Оставьте поля **User Name** и **Password** незаполненными и нажмите **OK**. 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 опциям управления, позволяет видеть статистические данные и контролировать состояние системы с помощью удобного графического интерфейса.

Поля пользовательского интерфейса

На Рисунке, показанном ниже, представлено окно пользовательского интерфейса. Визуально экран поделен на три области, описание каждой из которых представлено в таблице ниже.

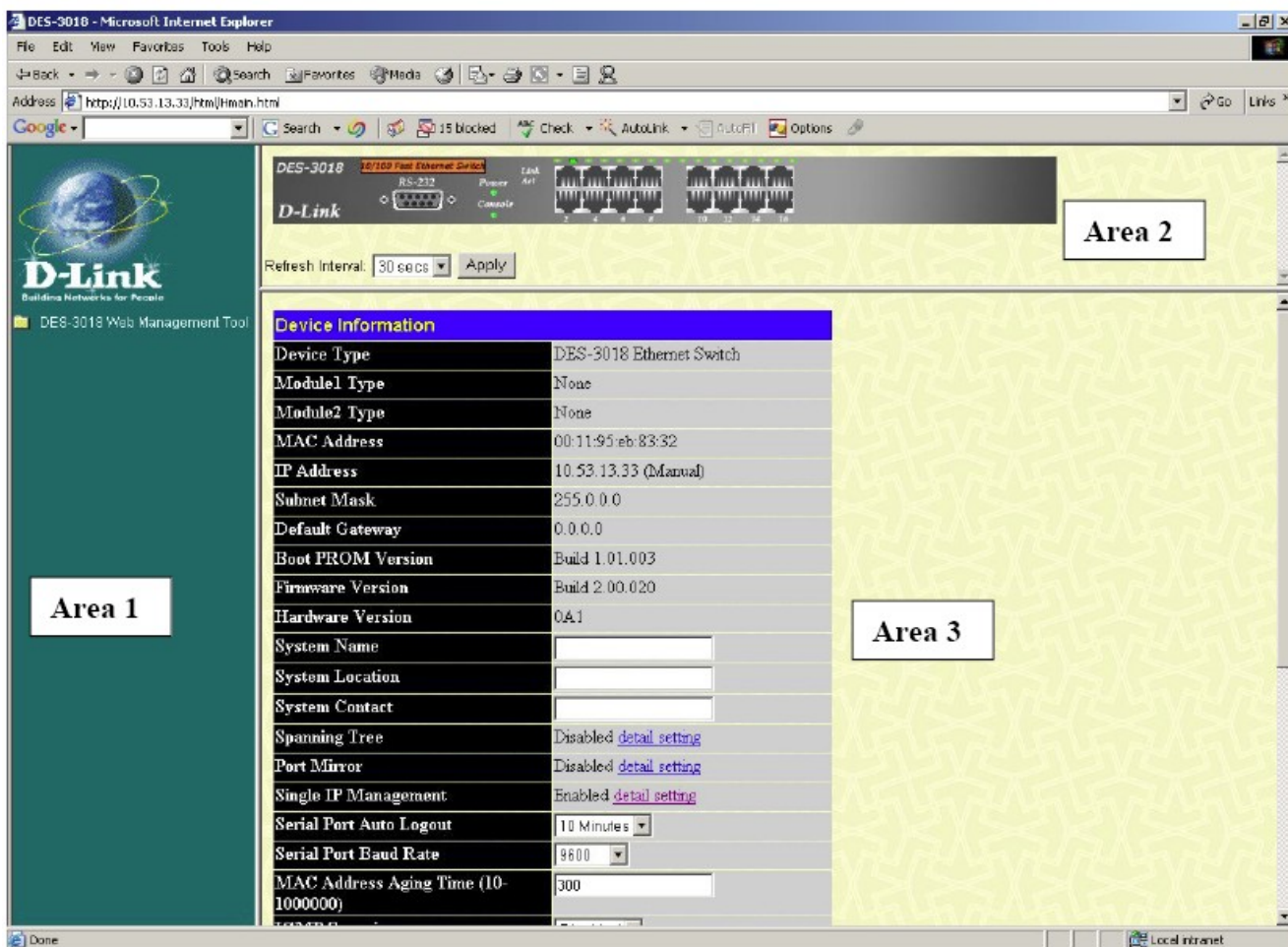


Рисунок 5.3 – Главная страница Web-менеджера

Область	Функция
Area 1	Выберите форму для отображения: меню или окна. Иконка папки должна быть открыта для отображения кнопок с гиперссылками меню и подпапок, содержащихся в них. Нажмите на логотип D-Link для перехода на сайт D-Link.
Area 2	Графически отображает переднюю панель коммутатора почти в реальном времени. Данная область отображает порты коммутатора и модули расширения, показывая активность портов, дуплексный режим или управление потоком в зависимости от заданного режима. Можно выбирать различные области для представления различных функций управления, включая конфигурацию портов.
Area 3	Представленная здесь информация по коммутатору основана на выбранных и введённых конфигурационных данных.



Примечание: Любые изменения, произведенные в настройках коммутатора во время текущей сессии, должны быть сохранены при помощи Web-меню Save Changes (которое будет описано ниже) или команды Save через интерфейс командной строки CLI.

Web-страницы

При подключении к режиму управления коммутатором через Web-браузер, появляется окно регистрации. Следует ввести 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, информацию о коммутаторе, расширенные настройки, конфигурация порта, IGMP, Spanning Tree, Forwarding Filtering, VLANs, полосу пропускания порта, настройки SNTP, Port Security, QoS, MAC Notification, LACP, Access Profile Table, System Log Servers, PAE Access Entity, Layer 3 IP Networking.

Layer 2 Features – содержит опции, позволяющие настроить Static VLAN Entry, Trunking, IGMP Snooping и Spanning Tree.

CoS – содержит опции, позволяющие настроить полосу пропускания порта, приоритет по умолчанию 802.1p, приоритет пользователя 802.1p, CoS Scheduling Mechanism и CoS Output Scheduling

CPU Interface Filtering - содержит опции, позволяющие настроить CPU Interface Filtering State и CPU Interface Filtering Table.

Security - содержит опции, позволяющие настроить управление трафиком, Port Security, Port Lock Entries, 802.1X, Trusted Host и сегментацию трафика.

Monitoring - содержит опции, позволяющие настроить мониторинг коммутатора, использование CPU, использование порта, пакеты, ошибки пакетов, размер пакетов, MAC-адрес, журнал коммутатора, группу IGMP Snooping, Browse Router Port, ARP-таблицу поиска, таблицу сессий и управление доступом на основе портов.



Примечание: Перед подключением коммутатора к сети, убедитесь, что в меню учетных записей пользователей настроены имя пользователя и пароль.

Раздел 6 - Управление коммутатором

Информация о коммутаторе
IP-адрес
Конфигурирование портов
Учетные записи пользователей
Зеркалирование портов
Настройки системного журнала
Настройки SNTP
Сервисы TFTP
Ping Test
Управление SNMP
Настройка единого IP-адреса
Продвижение и фильтрация пакетов
Сервис SMTP

получит
информацию
системы.
настроен
файла в

Для

Параметры настройки нажмите **Apply**.

Установка IP-адреса коммутатора с использованием интерфейса консоли

У каждого коммутатора может быть свой IP-адрес, который используется для связи с сетевым управлением SNMP или другими протоколами TCP/IP (например, BOOTP, TFTP). IP-адрес коммутатора по умолчанию 10.90.90.90. Зная схему сетевых адресов, можно изменить IP-адрес коммутатора по умолчанию.

IP-адрес коммутатора должен быть установлен до того, как он будет управляться Web-менеджером. IP-адрес коммутатора может быть автоматически установлен с помощью протоколов

BOOTP и DHCP, в этом случае текущий адрес коммутатора должен быть известен. IP-адрес может быть установлен из командной строки (CLI) следующим образом:

- Запустите командную строку, введите команду **config ipif System ipaddress xxx.xxx.xxx.xxx/ ууу.ууу.ууу.ууу**. Где x - IP-адрес, связанный с IP- интерфейсом (System), у – соответствующая маска подсети.
- Также можно ввести команду **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Где x – IP-адрес, связанный с IP-интерфейсом (System); z – соответствующее количество подсетей в нотации CIDR

IP- интерфейс, называемый System, на коммутаторе может быть связан с IP-адресом и маской подсети. Затем обычно управляющая станция соединяется с Telnet или управляемым Web-агентом коммутатора.

Конфигурирование портов

Данный раздел содержит информацию для настройки различных функций и свойств индивидуально для каждого физического порта, включая скорость на порту и управление потоком. Для открытия окна нажмите: **Administration** **Port Configuration** **Port Settings**.

Port Configuration					
From	To	State	Speed/Duplex	Flow Control	Apply
Port 1	Port 1	Enabled	Auto	Disabled	Apply

The Port Information Table					
Port	State	Speed/Duplex	Flow Control	Connection/Duplex/FlowCtrl	Learning
1	Enabled	Auto	Disabled	100M/Full/None	Enabled
2	Enabled	Auto	Disabled	LinkDown	Enabled
3	Enabled	Auto	Disabled	LinkDown	Enabled
4	Enabled	Auto	Disabled	LinkDown	Enabled
5	Enabled	Auto	Disabled	LinkDown	Enabled
6	Enabled	Auto	Disabled	LinkDown	Enabled
7	Enabled	Auto	Disabled	LinkDown	Enabled
8	Enabled	Auto	Disabled	LinkDown	Enabled
9	Enabled	Auto	Disabled	LinkDown	Enabled
10	Enabled	Auto	Disabled	LinkDown	Enabled
11	Enabled	Auto	Disabled	LinkDown	Enabled
12	Enabled	Auto	Disabled	LinkDown	Enabled
13	Enabled	Auto	Disabled	LinkDown	Enabled
14	Enabled	Auto	Disabled	LinkDown	Enabled
15	Enabled	Auto	Disabled	LinkDown	Enabled
16	Enabled	Auto	Disabled	LinkDown	Enabled
17	Enabled	Auto	Disabled	LinkDown	Enabled
18	Enabled	Auto	Disabled	LinkDown	Enabled

Рисунок 6.3. Окна Port Configuration и The Port Information Table

Для настройки портов коммутатора:

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

Параметр	Описание
State	В данном поле можно включить или выключить выбранный порт или группу портов.
Speed/Duplex	В данном поле вы можете выбрать скорость и дуплексный/полудуплексный режим передачи порта. Режим <i>Auto</i> обеспечивает согласование устройств на скоростях от 10 до 100 Мбит/с как в дуплексном, так и полудуплексном режимах. Настройки <i>Auto</i> позволяют автоматически определять на порту максимально возможную скорость подключения и использовать ее. Кроме <i>Auto</i> возможны следующие режимы работы: 10M/Half, 10M/Full, 100M/Half, 100M/Full и 1000M/Full_M, 1000M/Full_S, однако они не обеспечивают автоматическую регулировку настроек. Пользователь может установить на коммутаторе три вида гигабитных

	<p>соединений: 1000M/Full, 1000M/Full_M, 1000M/Full_S. Гигабитные соединения поддерживаются только при дуплексном режиме, и для них должны быть установлены соответствующие характеристики.</p> <p>Параметры режимов 1000M/Full_M и 1000M/Full_S относятся к соединениям по кабелю 1000Base-T между портом коммутатора и другим устройством, поддерживающим гигабитное соединение. Настройка master (1000M/Full_M, ведущий) определяет отношение ведущий (master) – ведомый (slave) между двумя физическими уровнями.</p> <p>Это необходимо для установки синхронизации между двумя физическими уровнями. Настройка slave (1000M-Full/S) предполагает использование loop-синхронизации, которая работает в соответствии с данными, полученными от управляющего коммутатора. Если одна из сторон соединения установлена в режим 1000M/Full_M, то другая сторона соединения обязательно должна быть установлена в режим 1000M/Full_S. Какие-либо другие установки приведут к отказу в работе (статус «link down») обоих портов.</p> <p>Оптические порты установлены статически в положение 1000 Мбит/с, дуплексный режим. При настройке данных портов пользователь может выбрать из двух режимов (<i>Auto</i> или <i>1000M/Full</i>).</p>
Flow Control	<p>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.</p>

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

Описание портов

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

Port Description			
From	To	Description	Apply
Port 1 ▾	Port 1 ▾	<input type="text"/>	Apply
Port Description Table			
Port	Description		
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			

Рисунок 6.4. «Port Description Setting» и «Port Description Table»

Для выбора порта или диапазона портов для описания используйте выпадающее меню **From** и **To**, и введите описание порта (-ов).

Нажмите **Apply** для размещения описания в таблице описания порта **Port Description Table**. Для удаления описания выберите соответствующий порт, очистите поле описания и нажмите **Apply**.

Port Err-Disabled

В следующем окне представлена информация о портах, которые в данный момент являются отключенными по причинам обнаружения петли при работе протокола STP. Чтобы увидеть следующее окно, откройте папку **Administration** и нажмите на ссылку **Port Error Disabled**.

Port Error Disabled Table				
Port	State	Connection	Reason	Description
17	Enabled	Err-Disabled	STP LBD	Port17
19	Enabled	Err-Disabled	STP LBD	
26	Enabled	Err-Disabled	STP LBD	

Рисунок 6.4 – Окно «Err-disabled ports»

В этом окне доступна для просмотра следующая информация:

Параметр	Описание
Port	Отображает номер отключенного порта коммутатора.
State	Отображает текущее состояние данного порта (отключен или подключен порт).
Connection	Описывает текущее состояние данного порта. В этом поле можно прочитать «err-disabled», когда порт отключен по причине ошибок соединения.
Reason	Описывает причину ошибки в текущем состоянии порта(STP LBD, обнаружение петель при помощи протокола STP).
Description	Отображает предварительно установленное пользователем описание порта.

Учетные записи пользователей

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

User Accounts		
User Name	Access Right	Add
Trinity	Admin	Modify

Рисунок 6.6 – Окно «User Accounts»

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

пользователя.

User Account Modify Table	
User Name	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
Access Right	Admin ▾
Apply	
Show All User Account Entries	

Рисунок 6.7. – 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*).

User Account Modify Table	
User Name	Darren
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
Access Right	Admin
Apply Delete	
Show All User Account Entries	

Рисунок 6.8 –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*) указан в поле **Access Right**.

Привилегии Admin(Администратор) и User (Пользователь)

Выделяют два уровня привилегий пользователя, **Admin** (Администратор) и **User** (Пользователь). Не все настройки, доступные для пользователей с привилегиями **Admin**, доступны для пользователей с привилегиями **User**.


В следующей таблице представлены в обобщенном виде привилегии **Admin** и **User**:

Функция управления	Admin (Администратор)	User (Пользователь)
Установки	Да	Только чтение
Мониторинг сети	Да	Только чтение
Строки имени и пароля, traps	Да	Только чтение
Обновление прошивки и файлов конфигурации	Да	Нет
Системные утилиты	Да	Нет
Сброс к заводским установкам	Да	Нет
Управление учетными записями пользователей		
Добавление/обновление/удаление учетных записей пользователей	Да	Нет
Просмотр учетных записей пользователей	Да	Нет

Таблица 6.1. Привилегии Admin (Администратор) и User (Пользователь)

После установки учетной записи пользователя с уровнем привилегий Admin, сохраните выполненные изменения, открыв окно **Save Changes** в главном меню и нажав кнопку **Save Configuration**.

Зеркалирование портов

Благодаря зеркалированию портов Вы сможете копировать переданные и полученные кадры на порту и перенаправлять их 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**.

Port Mirroring																		
Target Port	Port 1																	
Status	Disabled																	
Source Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ingress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Both	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply																		
Note(1):The "Source Port" and "Target Port" should be different, or the setup will be invalid.																		
Note(2):The target port should be a non-trunked port.																		

Рисунок 6.9 – Окно «Port Mirroring»

Для настройки зеркального порта:

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



ПРИМЕЧАНИЕ. 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 системного журнала (System Log)

С помощью **System Log Server** коммутатор может отправлять сообщения **Syslog** назначенным серверам (до четырех), используя окно **Current System Log Host**. Для просмотра окна, представленного ниже, нажмите: **Administration** **System Log Settings**.

System Log Host			
Index	Server IP	Status	Delete
1	10.1.2.3	Enabled	<input type="button" value="X"/>

Рисунок 6.10– Окно «System Log Host»

Параметры, настраиваемые для создания и для редактирования **System Log Server**, одинаковы. Для создания нового Syslog Server, нажмите кнопку **Add**. Чтобы изменить существующую запись, нажмите на гиперссылку номера сервера в поле **Index**. В результате появится приводимое ниже окно для установок, описание параметров которого приведены в таблице.

System Log Host Add	
Index(1-4)	<input type="text" value="1"/>
Host IP	<input type="text" value="0.0.0.0"/>
Severity	<input type="text" value="Warning"/>
Facility	<input type="text" value="Local0"/>
UDP Port(514 or 5000-65535)	<input type="text" value="514"/>
Status	<input type="text" value="Disabled"/>

Рисунок 6.11 – Окно «Configure System Log Server-Add»

Могут быть установлены следующие параметры:

Параметр	Описание
Index	Настройка индекса сервера Syslog (1-4).
Server IP	IP-адрес сервера Syslog.
Severity	В выпадающем меню выберите тип отсылаемых сообщений: <i>Warning</i> (предупреждающее), <i>Informational</i> (информационное) и <i>All</i> (все типы).
Facility	Некоторые процессы и демоны определяются значениями 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: <ul style="list-style-type: none"> 0- сообщения ядра 1- сообщения пользовательского уровня 2- почтовая система 3- системные демоны 4- сообщения безопасности/авторизации 4- сообщения, генерируемые внутри системы

	<p>подсистемой syslog line printer</p> <p>7- подсистема сетевых новостей</p> <p>8- подсистема UUCP</p> <p>9- демон часов</p> <p>10- сообщения безопасности/авторизации</p> <p>11- FTP-демон</p> <p>12- подсистема NTP</p> <p>13- Аудит журнала регистрации</p> <p>14- Предупреждение журнала регистрации</p> <p>15- демон часов</p> <p>16- локальное использование 0(local0)</p> <p>17- локальное использование 1(local1)</p> <p>18- локальное использование 2(local2)</p> <p>19- локальное использование 3(local3)</p> <p>20- локальное использование 4(local4)</p> <p>21- локальное использование 5(local5)</p> <p>22- локальное использование 6(local6)</p> <p>23- локальное использование 7(local7)</p>
UDP Port (514 или 6000- 65535)	Введите номер UDP-порта, который используется для передачи сообщений Syslog.
Status	Для активации/деактивации выберите <i>Enabled/Disabled</i>



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

Для установки конфигурации сервера System Log нажмите **Apply**. Чтобы отменить ввод из окна **System Log Host** нажмите соответствующий знак «x» для удаления записи. Для возвращения в окно **System Log Host** нажмите на ссылку [Show All System Log Server](#).

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.

Time Settings-Current Time	
Current Time	0 days 00:32:36
Time Source	System Clock
SNTP Settings	
SNTP State	Disabled
SNTP Primary Server	0.0.0.0
SNTP Secondary Server	0.0.0.0
SNTP Poll Interval in Seconds	720
Apply	
Time Settings: Set Current Time	
Year	
Month	
Day	
Time in HH MM SS	
Apply	

Рисунок 6.12 – Текущее окно «Time Settings»

Следующие параметры доступны для просмотра и отображения:

Параметр	Описание
Current Time	Отображает текущее время, которое установлено на коммутаторе.
Time Source	Отображает время источника.
SNTP Settings	
SNTP State	При помощи выпадающего меню включите (Enabled) или выключите (Disabled) SNTP
SNTP Primary Server	В этом поле указывается IP-адрес первичного сервера, с которого будет получена SNTP-информация.
SNTP Secondary Server	В этом поле указывается IP-адрес вторичного сервера, с которого будет получена SNTP-информация
SNYP Poll Interval in Seconds	Интервал времени в секундах между запросами на обновление SNTP-информации
Time Settings - 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** **Time Zone and DST**.

Time Zone and DST	
Daylight Saving Time State	Disabled <input type="button" value="v"/>
Daylight Saving Time Offset in Minutes	60 <input type="button" value="v"/>
Time Zone Offset from GMT in +/-HH:MM	- <input type="button" value="v"/> 06 <input type="button" value="v"/> 00 <input type="button" value="v"/>
DST Repeating Settings	
From Which Week of the month	First <input type="button" value="v"/>
From Which Day of the Week	Sunday <input type="button" value="v"/>
From Which Month	April <input type="button" value="v"/>
From What Time HH:MM	00 <input type="button" value="v"/> 00 <input type="button" value="v"/>
To Which Week	Last <input type="button" value="v"/>
To Which Day	Sunday <input type="button" value="v"/>
To Which Month	October <input type="button" value="v"/>
To What Time HH:MM	00 <input type="button" value="v"/> 00 <input type="button" value="v"/>
DST Annual Settings	
From What Month	April <input type="button" value="v"/>
From What Date	29 <input type="button" value="v"/>
From What Time	00 <input type="button" value="v"/> 00 <input type="button" value="v"/>
To What Month	October <input type="button" value="v"/>
To What Date	12 <input type="button" value="v"/>
To What Time	00 <input type="button" value="v"/> 00 <input type="button" value="v"/>
<input type="button" value="Apply"/>	

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 выключения настроек DST (перехода на летнее время).
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 (Настройки ежегодного режима DST)	
Использование ежегодного режима позволяет отрегулировать установку сезонного времени. Данный режим требует точного задания 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 путем клика по линку **MAC Notification Settings** в папке **Administration**.

MAC Notification Global Settings

State	Disabled
Interval (1-2147483647 sec)	1
History size (1-500)	1

New MAC Notification Global Settings

State	Disabled ▾
Interval (1-2147483647 sec)	<input style="width: 100%;" type="text" value="1"/>
History size (1-500)	<input style="width: 100%;" type="text" value="1"/>

MAC Notification Port Settings

From	To	State	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	<input type="button" value="Apply"/>

MAC Notification Port State Table

Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled

Рисунок 6.14. MAC Notification Settings

Глобальные настройки

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.

Следующие параметры доступны для просмотра и изменения:

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 чтобы позволить MAC Notification.
State	Установка MAC Notification 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 версией программного обеспечения с TFTP-сервера на коммутатор и наоборот. Используя выпадающее меню, выберите нужный сервис. **Download Firmware** используется для передачи файла прошивки от внешнего источника на Коммутатор с помощью протокола TFTP. **Download Configuration** применяется для передачи конфигурационного файла с внешнего источника на Коммутатор с помощью протокола TFTP. **Upload Configuration** используется для передачи конфигурационного файла с коммутатора на внешний источник с помощью протокола TFTP. **Upload Log** используется для передачи log-файла от коммутатора ко внешнему источнику с помощью протокола TFTP. Выбрав нужный сервис, введите **Server IP Address**, путь к необходимому имени файла и нажмите **Start** для инициирования передачи файла.

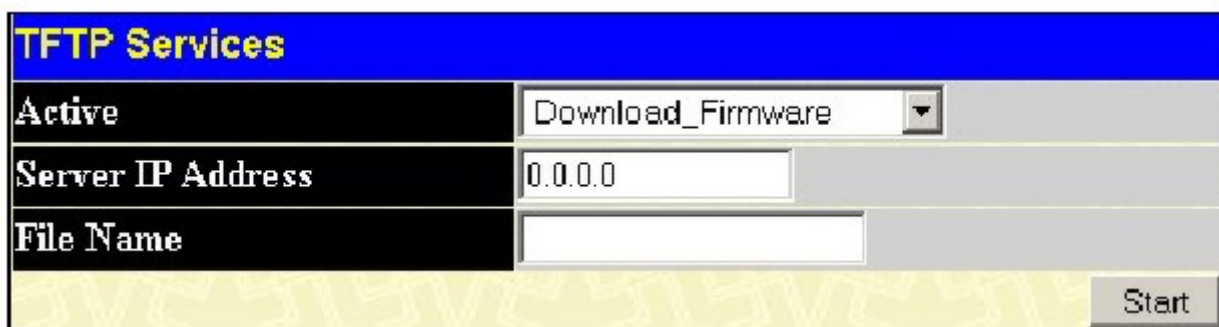


Рисунок 6.15 – Окно «TFTP Services»

Ping test

Ping test – 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.

Ping Test

Enter the IP Address of the device or station you want to ping, then click **Start**.

Target IP Address:

Repeat Pinging for: Infinite times
 times (1 - 255)

Time Out: seconds(1~99)

Start

Рисунок 6.16 – 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 передачи ping на указанный IP-адреса путем ввода числа от 1 до 255. Нажмите **Start** для начала запуска программы ping.

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 программное обеспечение SNMP (называемое агентом), работающее локально на оборудовании. Определенный набор управляемых объектов обслуживается протоколом 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-3000 поддерживают протокол SNMP версий: 1, 2с 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 версиях 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.

Базы управляющей информации MIB

Коммутатор хранит в базе управляющей информации MIB управляющую информацию и значения счетчиков. 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 DES-3000 поддерживают протокол SNMP версий: 1, 2c и 3. Администратор может выбрать версию протокола SNMP для контроля над работой коммутатора и управления им. Три версии протокола SNMP различаются в уровне обеспечиваемой безопасности между станцией управления и сетевым оборудованием.

Настройки SNMP 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**.

Add			
Total Entries: 1 (Note: It is allowed insert 10 entries into the table only.)			
SNMP User Table			
User Name	Group Name	SNMP Version	Delete
initial	initial	V3	<input type="checkbox"/>

Рисунок 6.17 – 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:

SNMP User Table Display	
User Name	initial
Group Name	initial
SNMP Version	V3
Auth-Protocol	None
Priv-Protocol	None
Show All SNMP User Table Entries	

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	Это поле используется для обозначения, какая созданная SNMP-группа 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**.

SNMP User Table Configuration	
User Name	<input type="text"/>
Group Name	<input type="text"/>
SNMP V3 Encryption	<input type="checkbox"/> encrypted
Auth-Protocol	MD5 <input type="text"/> Password <input type="text"/>
Priv-Protocol	DES <input type="text"/> Password <input type="text"/>
<input type="button" value="Apply"/>	
Show All SNMP User Table Entries	

Рисунок 6.19 – 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 пользователей SNMP.
Group Name	Это поле используется для обозначения, какая созданная SNMP-группа может запрашивать SNMP -сообщения.
SNMP Encryption	Отметьте encrypted для подключения шифрования для протокола SNMP. Это свойство предназначено для пользователей, использующих протокол SNMP V3 версии. Пользователь может установить шифрование в последующих двух полях.
SNMP Version	<i>V1</i> – свидетельствует о том, что используется SNMP версии 1. <i>V2</i> – свидетельствует о том, что используется SNMP версии 2. <i>V3</i> – свидетельствует о том, что используется SNMP версии 3.
Auth-Protocol	<i>MD5</i> – 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. <i>SHA</i> – 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.
Priv-Protocol	<i>None</i> – определяет, что протокол аутентификации не используется. <i>DES</i> – Определяет, что используется 56-битное шифрование DES, основанное на стандарте CBC-DES (DES-56). Данное поле доступно, когда в поле SNMP Version выбрана версия V3 и подключено шифрование в поле Encryption. Пользователя попросят ввести пароль, состоящий из 8-16 буквенно-цифровых знаков.

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**.

Add

Total Entries:8 (Note: It is allowed insert 30 entries into the table only.)

SNMP View Table

View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	X
restricted	1.3.6.1.2.1.11	Included	X
restricted	1.3.6.1.6.3.10.2.1	Included	X
restricted	1.3.6.1.6.3.11.2.1	Included	X
restricted	1.3.6.1.6.3.15.1.1	Included	X
CommunityView	1	Included	X
CommunityView	1.3.6.1.6.3	Excluded	X
CommunityView	1.3.6.1.6.3.1	Included	X

Рисунок 6.20 - 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.

SNMP View Table Configuration

View Name

Subtree OID

View Type

Apply

[Show All SNMP View Table Entries](#)

Рисунок 6.21 – 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 в виде буквенно-цифровой последовательности длиной не более 32 символов. Параметр используется для идентификации нового объекта SNMP.
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](#).

Таблица SNMP-группы

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:

SNMP Group Table			
Group Name	Security Model	Security Level	Delete
gl	SNMPv3	NoAuthNoPriv	<input type="checkbox"/>
public	SNMPv1	NoAuthNoPriv	<input type="checkbox"/>
public	SNMPv2	NoAuthNoPriv	<input type="checkbox"/>
initial	SNMPv3	NoAuthNoPriv	<input type="checkbox"/>
private	SNMPv1	NoAuthNoPriv	<input type="checkbox"/>
private	SNMPv2	NoAuthNoPriv	<input type="checkbox"/>
ReadGroup	SNMPv1	NoAuthNoPriv	<input type="checkbox"/>
ReadGroup	SNMPv2	NoAuthNoPriv	<input type="checkbox"/>
WriteGroup	SNMPv1	NoAuthNoPriv	<input type="checkbox"/>
WriteGroup	SNMPv2	NoAuthNoPriv	<input type="checkbox"/>

Рисунок 6.22 – 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**.

SNMP Group Table Display	
Group Name	public
Read View Name	CommunityView
Write View Name	
Notify View Name	CommunityView
Security Model	SNMPv1
Security Level	NoAuthNoPriv
Show All SNMP Group Table Entries	

Рисунок 6.23 – 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 6.24 – Окно «SNMP Group Table Configuration- Add»

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 SNMP-пользователей новой SNMP-группы.
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 trap-сообщения SNMP, создаваемые SNMP-агентом коммутатора.
Security Model	<i>SNMP v1</i> – свидетельствует о том, что будет использоваться SNMP версии 1. <i>SNMP v2</i> – 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 управляющей информации (Structure of Management Information, SMI), а также добавлены некоторые функции безопасности. <i>SNMP v3</i> – 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. <i>NoAuthNoPriv</i> – свидетельствует о том, что будет отсутствовать авторизация, а также шифрование пакетов, отправляемых между коммутатором и удаленным SNMP-менеджером. <i>AuthNoPriv</i> – свидетельствует о том, что будет затребована авторизация, но будет отсутствовать шифрование пакетов, отправляемых между коммутатором и удаленным SNMP-менеджером. <i>AuthPriv</i> – 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 менеджером и агентом SNMP. «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.
- Просмотр 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**.

Community Name	View Name	Access Right
<input type="text"/>	<input type="text"/>	Read_Only

Apply

Total Entries: 2 (Note: It is allowed insert 10 entries into the table only.)

Community Name	View Name	Access Right	Delete
public	CommunityView	Read_Only	<input type="checkbox"/>
private	CommunityView	Read_Write	<input type="checkbox"/>

Рисунок 6.25 – Окно «SNMP Community Table»

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 хоста SNMP

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.

Add			
Total Entries: 1 (Note: It is allowed insert 10 entries into the table only.)			
SNMP Host Table			
Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete
10.1.1.1	V1	public	X

Рисунок 6.26 – Окно «SNMP Host Table»

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**.

SNMP Host Table Configuration	
Host IP Address	0.0.0.0
SNMP Version	V1
Community String / SNMPv3 User Name	
Apply	
Show All SNMP Host Table Entries	

Рисунок 6.27 – 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. <i>V3-Auth-Priv</i> – 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 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.

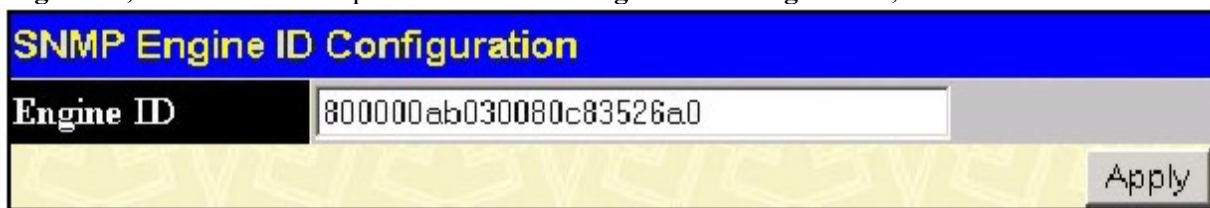


Рисунок 6.28 – Окно «SNMP Engine ID Configuration»

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

Связка IP-МАС (IP-МАС Binding)

На уровне IP используется адрес, состоящий из четырех байт. На уровне Ethernet адрес (MAC-адрес) состоит из шести байт. Связка этих двух адресов вместе позволяет осуществлять передачу данных между уровнями. Первостепенной целью связки IP-МАС является ограничение доступа пользователей к коммутатору. Только авторизованный клиент может получить доступ к порту коммутатора благодаря проверке пары адресов IP-МАС в ранее сконфигурированной базе данных. Если неавторизованный пользователь пытается получить доступ к порту с установленной связкой IP-МАС, происходит блокирование доступа путем удаления пакетов. Максимальное количество записей связок IP-МАС 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-МАС к конкретному порту означает, что пользователь может включать и отключать данную функцию на интересующем его порту.

Связка IP-МАС на базе портов (IP-МАС Binding Port)

Меню IP-МАС Ports Settings применяется для включения связки IP-МАС на базе портов. На портах с включенной данной функцией будет производиться проверка IP-МАС поступающих на порт пакетов. База данных IP-МАС, применяемая для проверки, должна быть настроена со страницы **IP-МАС Binding Table** (приведена ниже).

Для включения или отключения связки IP-МАС на определенных портах, нажмите: **Configuration** **IP-МАС Binding** **IP-МАС Binding Port**. В полях **From** и **To** выберите порт или диапазон портов. Включение или отключение порта производится в поле **State**. Нажмите **Apply** для сохранения изменений.

IP-MAC Binding Ports Setting			
From	To	State	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	Apply

IP-MAC Binding Port State Table	
Port	State
1	Enabled
2	Enabled
3	Enabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Рисунок 6.29 – Окно «IP-MAC Binding Ports»

После включения функции IP-MAC Binding Ports воспользуйтесь меню IP-MAC Binding для настройки IP-MAC binding для включенных портов.

Таблица связей IP-МАС (IP-MAC Binding Table)

Приведенное ниже окно можно использовать для создания записей связей IP-МАС. Для просмотра окна **IP-MAC Binding Setting** нажмите **IP-MAC Binding** **IP-MAC Binding Table**. Введите IP и МАС-адреса авторизованных пользователей в соответствующих полях и нажмите **Add**. Для использования связки IP-МАС для определенных портов, эти порты должны сначала быть подключенными в меню **IP-MAC Binding Ports** (указано выше). Порты определяются в поле **Port** как диапазон целых чисел (например, “1-3”) или выбором опции **All** для применения данной функции ко всем портам.

IP Address	MAC Address	Port
0.0.0.0	00-00-00-00-00-00	All <input type="checkbox"/>

Total Entries: 1

IP Address	MAC Address	Ports	Delete
10.41.44.254	00-0c-6e-7b-71-df	1-26	

Рисунок 6.30 – Окно «IP-MAC Binding Table»

Для изменения IP-адреса или МАС-адреса в записи связки, внесите изменения в соответствующих полях, после чего нажмите **Modify**. Для поиска записи связки IP-МАС, введите IP – адрес и МАС-адрес и нажмите **Find**. Для удаления записи нажмите **Delete**. Для удаления всех записей из таблицы нажмите **Delete All**.

Блокировка по связкам IP-МАС

Для просмотра списка неавторизованных устройств, которым был заблокирован доступ из-за несоответствия связки IP-МАС, откройте окно **IP-MAC Binding Blocked**. Для этого нажмите: **Security** **IP-MAC Binding** **IP-MAC Binding Blocked**.

IP-MAC Binding Blocked

VLAN Name MAC Address

Find Delete All

Total Entries: 21

IP-MAC Binding Blocked Table

VID	VLAN NAME	MAC Address	Delete
1	default	00-03-09-18-10-01	X
1	default	00-03-44-ae-bc-12	X
1	default	00-07-e9-13-8f-50	X
1	default	00-0c-6e-55-bc-82	X
1	default	00-0c-f8-20-90-01	X
1	default	00-0c-f8-41-c0-01	X
1	default	00-0c-f8-42-40-01	X
1	default	00-0c-f8-44-10-01	X
1	default	00-0d-60-8f-49-38	X
1	default	00-50-ba-10-d8-eb	X
1	default	00-50-ba-da-01-58	X
1	default	00-50-ba-da-02-3e	X
1	default	00-50-ba-da-04-1f	X
1	default	00-80-c8-2e-c7-4c	X
1	default	00-80-c8-3b-ef-32	X
1	default	00-80-c8-4c-69-f8	X
1	default	00-80-c8-92-2d-58	X
1	default	00-80-c8-92-67-9f	X
1	default	00-e0-18-45-c7-15	X
1	default	00-e0-18-70-b3-b4	X

Next

Рисунок 6.31 – Окно «IP-MAC Binding Blocked»

Для поиска неавторизованных устройств, которым был заблокирован 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 **X**, следующую вслед за записью MAC-адреса. Для удаления всех записей в таблице **IP-MAC Binding Blocked Table** нажмите **Delete All**.

Технология 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, масштабируя сеть и увеличивая полосу пропускания.
2. SIM может сократить число необходимых в сети IP-адресов.
3. SIM позволяет 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 выключена через интерфейс командной строки или Web-интерфейс. Стекирование коммутаторов по технологии SIM не будет влиять на стандартную работу коммутатора в сети пользователя.
- Существует следующая классификация 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 *default*.

Технология SIM может использоваться в сетях, содержащих устройства, не поддерживающие SIM. Это позволяет пользователю контролировать работу коммутаторов, которые находятся на расстоянии более одного hop (перехода) 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 функция SIM включена, приложения управляющего коммутатора будут перенаправлять пакеты вместо их обработки.

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 принадлежал 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.

Подключение функции SIM через Web-интерфейс

Все коммутаторы настроены как коммутаторы CaS согласно заводским настройкам по умолчанию, а функция Single IP Management отключена. Для того чтобы подключить функцию SIM через Web-интерфейс, нажмите: **Administration** **Single IP Management** **SIM Settings**, после чего появится следующее окно.



Рисунок 6.32 – Окно «SIM Settings» (disabled – выключено)

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

SIM Settings	
SIM State	Enabled ▾
Role State	Candidate ▾
Discovery Interval	30 (30..90 sec)
Holdtime	100 (100..255 sec)
Apply	

Рисунок 6.33 – Окно «SIM Settings» (enabled – включено)

Можно настроить следующие параметры:

Параметр	Описание
SIM State	Используйте выпадающее меню для изменения SIM-состояния коммутатора. <i>Disabled</i> переведет все функции SIM коммутатора в нерабочее состояние.
Role State	Используйте выпадающее меню для изменения роли коммутатора в SIM-группе. Возможно два варианта: <i>Candidate</i> – Candidate Switch (CaS) не является членом SIM-группы, но подключен к управляемому коммутатору Commander Switch (CS). Данная роль коммутатора в SIM-группе является настройкой по умолчанию. <i>Commander</i> – Выберите данный вариант, чтобы коммутатор выполнял роль управляющего CS. Пользователь может подключить другие коммутаторы к управляемому поверх Ethernet, чтобы они стали членами этой SIM-группы. При выборе данной роли для коммутатора, становится возможным настройка SIM.
Discovery Interval	Пользователь может установить интервал посылки Коммутатором обнаруживающих пакетов (discovery packets) в секундах. В ответ коммутатор CS получит информацию о других коммутаторах, подключенных к нему (например, MS, CaS). Пользователь может установить Discovery Interval от 30 до 90 секунд.
Holdtime	Данный параметр может быть установлен разово; Коммутатор будет хранить информацию, посланную от других коммутаторов в течение данного интервала времени. Пользователь может установить holdtime равным от 100 до 255 секунд.

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 компьютере.

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

Device name	Local port	Speed	Remote port	Mac Address	Model name
(default:eb-03-32)	-	-	-	00-11-95-eb-03-32	DES-3010 L2 Switch
(default:30-10-01)	1	100-Full	2	00-50-ba-30-10-01	DES-3010G L2 Swit...
(default:10-24-04)	45	100-Full	4	00-35-50-10-24-04	DES-3550 L2 Switch
xyz	1	100-Full	4	00-90-c8-05-55-00	DES-3020 L3 Switch

Рисунок 6.34 – 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).

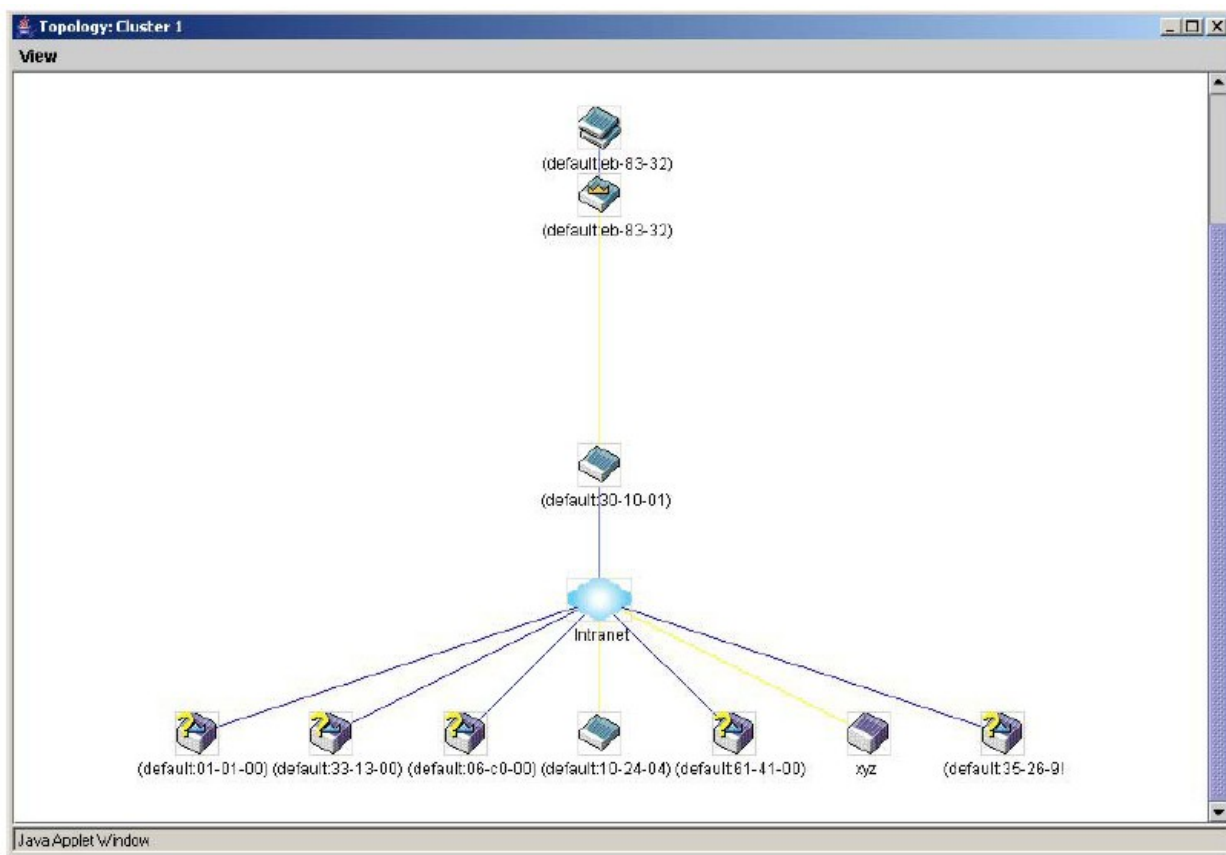


Рисунок 6.35 – Окно «Topology View»

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.

Значки устройств

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 ниже приведено окно.

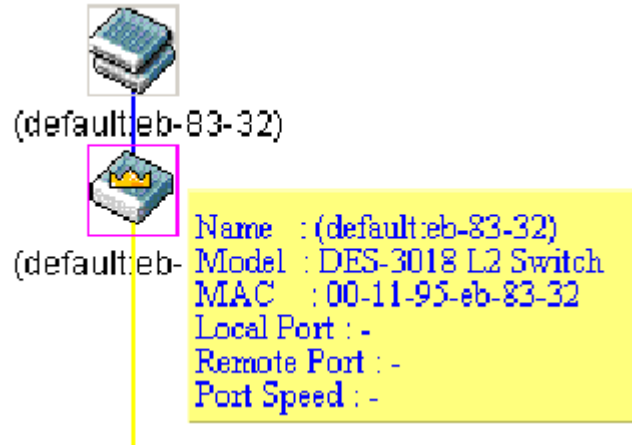


Рисунок 6.36 – Получение информации об устройстве, используя **Tool Tips**

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

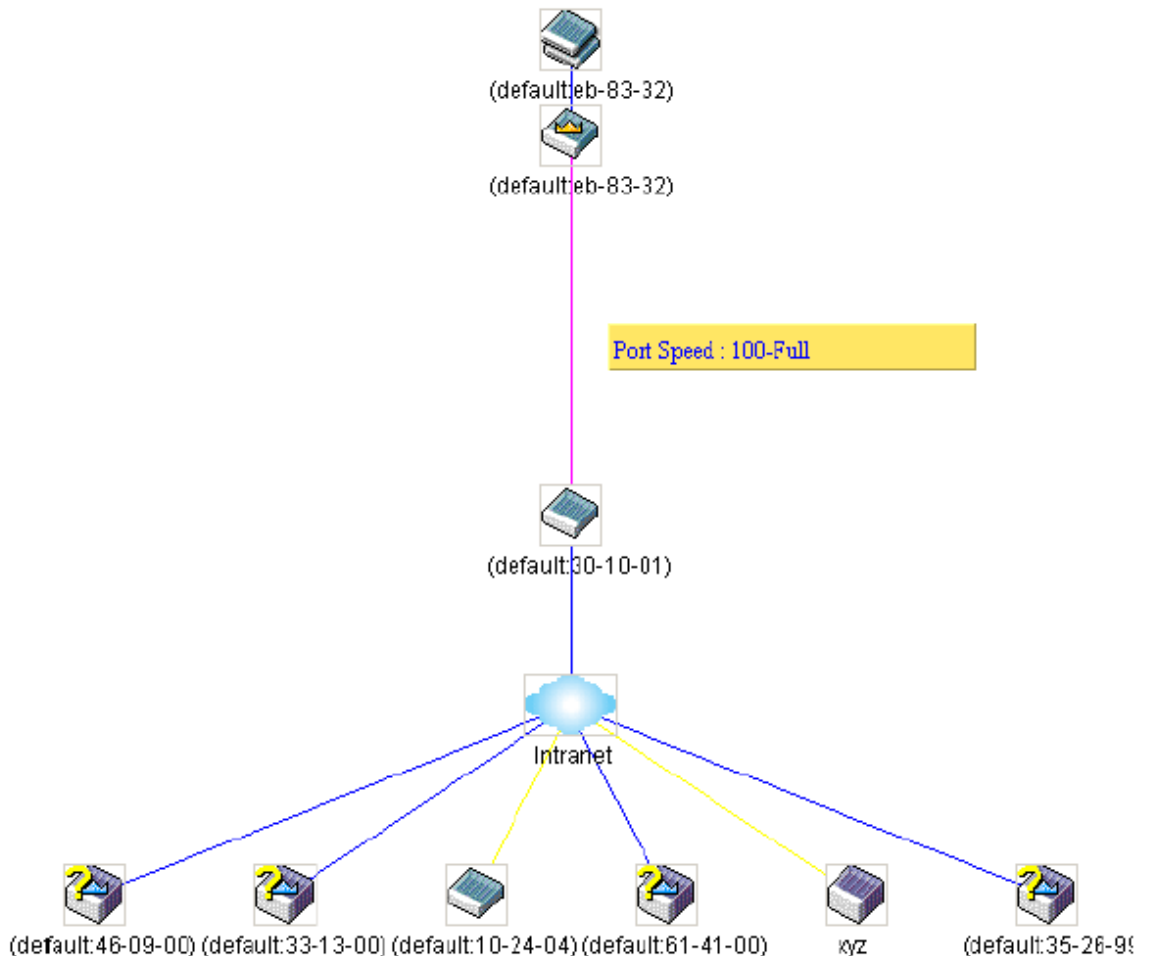


Рисунок 6.37 – Получение информации о скорости порта, используя значки устройств

Нажатие правой кнопки мышки

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

Значок группы



Рисунок 6.38 – Нажатие правой кнопкой мышки на значок 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.

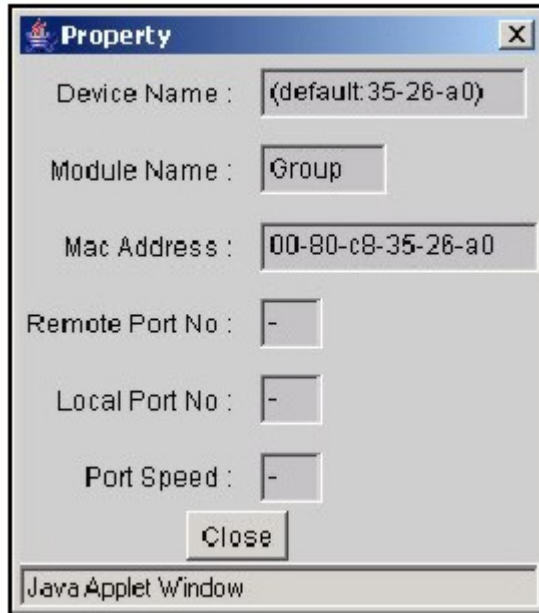


Рисунок 6.39 – Окно «Property»

Значок управляющего коммутатора

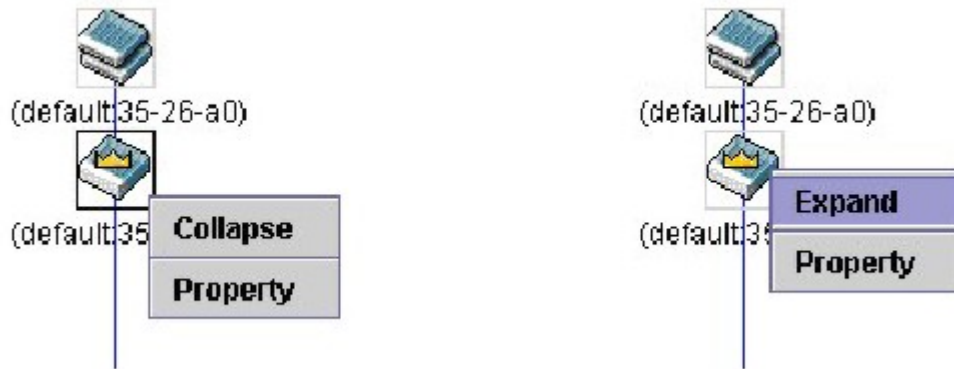


Рисунок 6.40 – Нажатие правой кнопкой мыши по значку управляющего коммутатора

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.

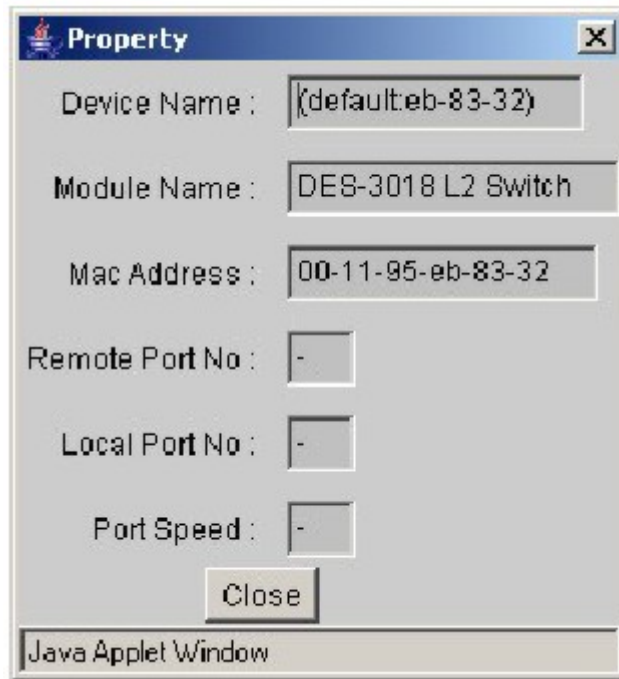


Рисунок 6.41 – Окно «Property»

Значок члена группы

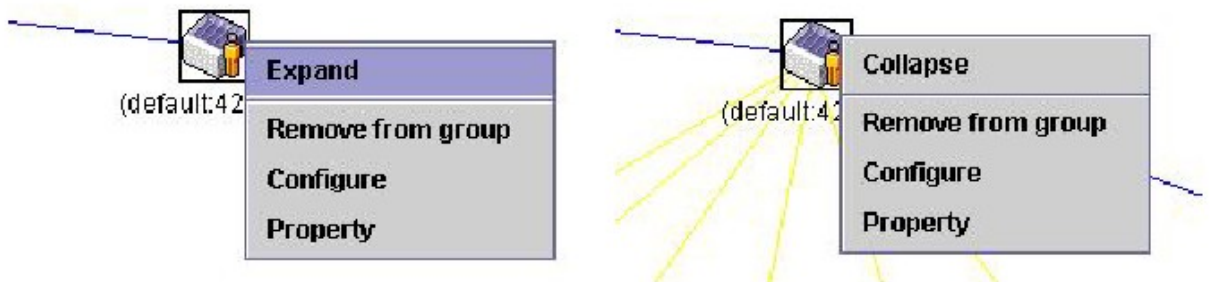


Рисунок 6.42 – Нажатие правой кнопки мышки по значку члена группы

Следующие опции могут быть доступны пользователю при настройке:

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

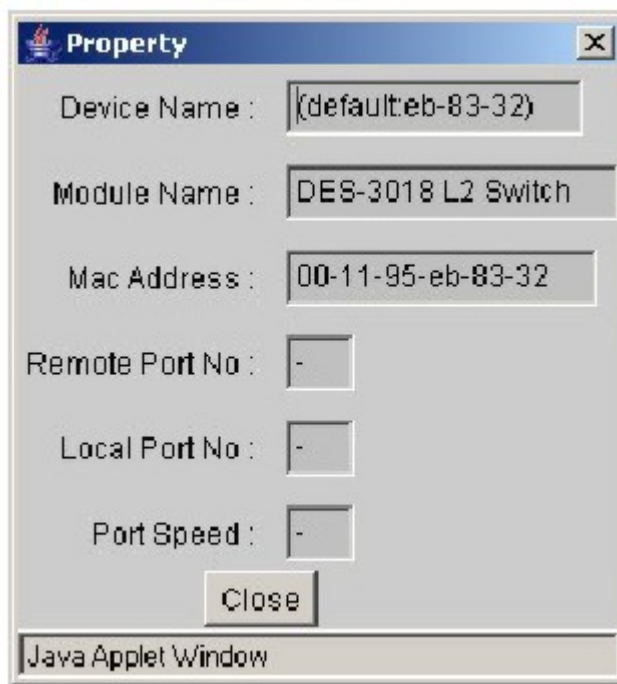


Рисунок 6.43 – Окно «Property»

Значок коммутатора CaS

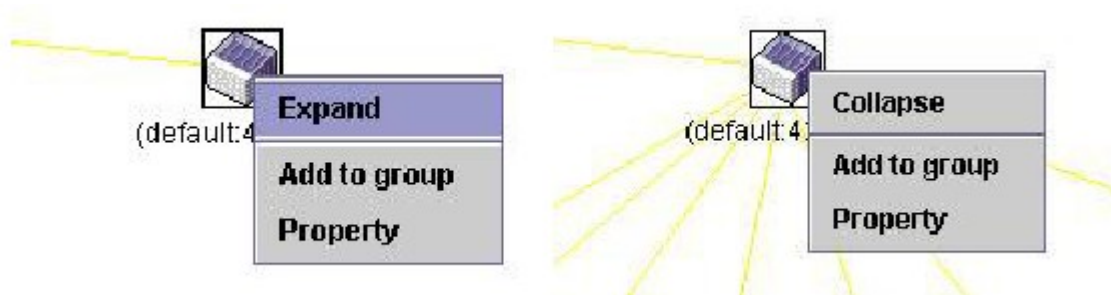


Рисунок 6.44 – Нажатие правой кнопки мыши по значку CaS

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 6.45 – Диалоговое окно «Input password»

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

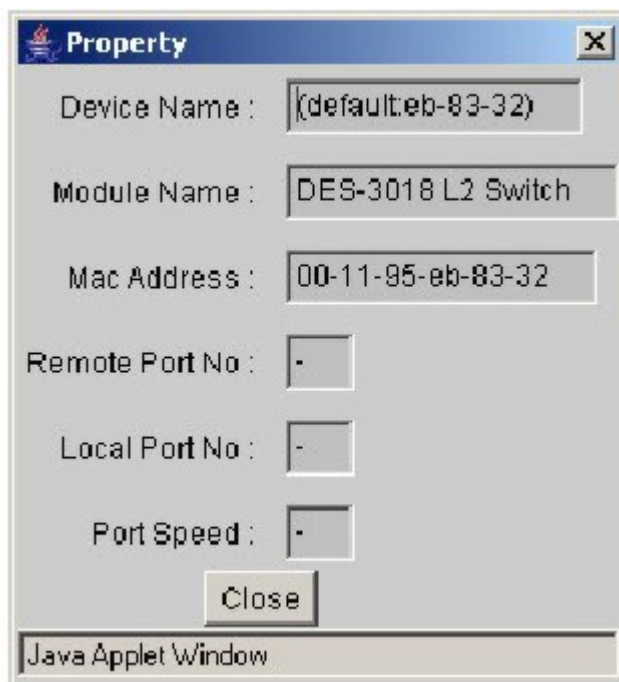


Рисунок 6.46 - Окно «Property»

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 управляемому 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 6.47 – 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 6.48 - 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-30xx 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**.

Firmware Upgrade																			
Port	MAC Address	Model Name	Version																
<table border="1"> <tr> <td>Server IP Address</td> <td>0</td> <td>.</td> <td>0</td> <td>.</td> <td>0</td> <td>.</td> <td>0</td> </tr> <tr> <td>Path \ Filename</td> <td colspan="7"><input type="text"/></td> </tr> </table>				Server IP Address	0	.	0	.	0	.	0	Path \ Filename	<input type="text"/>						
Server IP Address	0	.	0	.	0	.	0												
Path \ Filename	<input type="text"/>																		
			Download																

Рисунок 6.49 – Окно «Firmware Upgrade»

Сохранение /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.

Configuration File Backup/Restore			
Port	MAC Address	Model Name	Version
Server IP Address		0	0
Path \ Filename			
		Upload	Download

Рисунок 6.50 – Окно «Configuration File Backup/Restore»

Рассылка и фильтрация

Рассылка Unicast

Откройте папку **Forwarding & Filtering** в меню **Administration** и нажмите на ссылку **Unicast Forwarding**, чтобы открыть показанное ниже окно **Setup Static Unicast Forwarding Table**.

Setup Static Unicast Forwarding Table				
VID	MAC Address	Allow to go port		
	00:00:00:00:00:00	Port 1		
		Add/Modify		
Static Unicast Forwarding Table				
Mac Address	VID	VLAN Name	Port	Delete
End of data!				

Рисунок 6. 51. Окно Unicast Forwarding Table и Static Unicast Forwarding Table

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 Unicast MAC address.
MAC Address	MAC-адрес, на который будут пересылаться пакеты. Это должен быть unicast MAC address.
Allowed to Go Port	Позволяет выбрать номер порта, на который будет ссылаться вышеупомянутый MAC-адрес.

Нажмите **Apply** для применения выполненных изменений. Текущие записи могут быть просмотрены в **Static Unicast Forwarding Table**, как показано в нижней части рисунка, рассмотренного выше.

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

Многоадресная рассылка

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

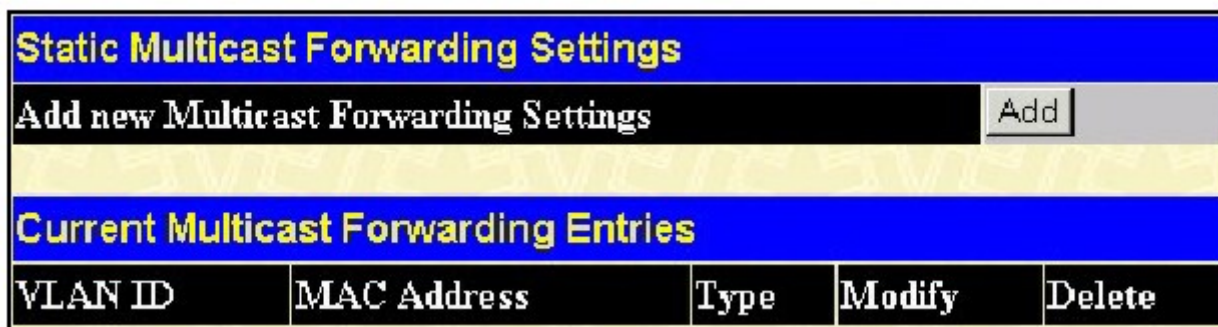


Рисунок 6.52. Static Multicast Forwarding Settings окно

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:

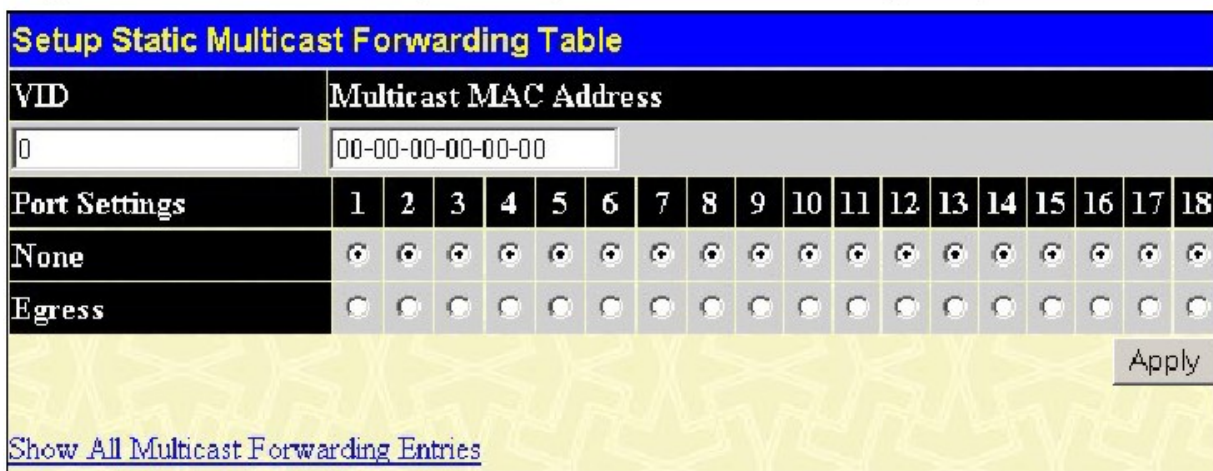


Рисунок 6.53. Setup Static Multicast Forwarding Table окно

Могут быть установлены следующие параметры:

Параметр	Описание
VID	Идентификатор VLAN, к которой принадлежит соответствующий MAC-адрес.
Multicast MAC Address	MAC-адрес источника multicast-пакетов. Это должен быть MAC-адрес multicast.
Port Settings	Позволяет выбрать порты, которые будут членами multicast-группы. Существуют значения: <i>None</i> – нет ограничений на порт, динамически присоединяющийся к multicast-группе. Когда выбрано значение <i>None</i> , порт не может быть членом <i>Static Multicast Group</i> . <i>Egress</i> – 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**, необходимо нажать на ссылку **Show All Multicast Forwarding Entries**.

Фильтрация широковещательных пакетов

Используйте меню **Multicast Filtering Mode Setting** (настройка режима широковещательной фильтрации) для выбора одной из двух опций фильтрации для широковещательных пакетов:

- **Forward unregistered groups** – Эта настройка (задана по умолчанию) будет пересылать все широковещательные пакеты.
- **Filter unregistered groups** – Эта настройка будет пересылать широковещательные пакеты только к зарегистрированным широковещательным группам. Широковещание для незарегистрированных групп заблокировано.



Рисунок 6.54. Configure Multicast Filtering Mode

Выберите наиболее подходящие настройки режима широковещательной фильтрации и нажмите **Apply** для вступления изменений в силу.

Сервис SMTP

SMTP (Simple Mail Transfer Protocol, простой протокол передачи электронной почты) – это функция коммутатора, которая позволяет пересылать события на коммутаторе на e-mail адреса, введенные при помощи команд, указанных ниже. Коммутатор будет установлен как SMTP-клиент,

в то время как сервер (удаленное устройство, которое будет получать сообщения от коммутатора) помещает соответствующую информацию в e-mail и доставляет ее получателям, установленным на коммутаторе. Это очень выгодно для администратора коммутатора из-за упрощения управления малыми рабочими группами или серверными комнатами, увеличивая скорость обработки аварийных сигналов коммутатора и безопасность посредством записи сомнительных событий, обнаруженных на коммутаторе.

Коммутатор играет четыре важные роли как SMTP-клиент:

- Для функционирования должным образом, сам сервер и его виртуальный порт должны быть корректно настроены для этой функции. Это достигается путем настройки полей *SMTP Server Address* и *SMTP Server Port* в окне **SMTP Service Settings**.
- Получатели сообщений e-mail настраиваются на коммутаторе. Эта информация отсылается на сервер, затем обрабатывается и отправляется по e-mail установленным получателям. На коммутаторе может быть установлено до 8 e-mail получателей в поле *Mail Receiver Address* в окне **SMTP Service Settings**.
- Администратор может установить mail-адрес источника, от которого сообщения доставляются установленным получателям. Это позволяет администратору получить больше информации о функциях коммутатора и обнаруженных проблемах. Персональный e-mail может быть установлен при помощи окна **SMTP Service Settings** и настройки поля *Self Mail Address*.
- Коммутатор может быть настроен для отсылки тестовых mail-сообщений, чтобы убедиться, что получатель получит сообщения e-mail от SMTP-сервера, относящегося к коммутатору. Для настройки тестовых сообщений test mail, функция SMTP сначала должна быть подключена путем установки состояния SMTP State в окне **SMTP Service Settings** и затем путем отправки e-mail при помощи окна **SMTP Service**. Все получатели с установленной функцией SMTP будут получать образец тестового сообщения от SMTP-сервера, гарантируя надежность данной функции.

Коммутатор будет отправлять e-mail сообщения получателям, когда произойдет одно или несколько следующих событий:

- Когда произойдет холодный запуск коммутатора.
- Когда порт входит в состояние отказа (link down).
- Когда порт входит в рабочее состояние (link up).
- Когда аутентификация SNMP запрещена коммутатором.
- Когда запись конфигурации коммутатора сохранена в памяти NVRAM коммутатора.
- Когда обнаружена аномальность TFTP в процессе загрузки прошивки. Это событие включает *in-process, invalid-file, violation, file-not-found, complete* и *time-out* сообщения от TFTP-сервера.
- Когда произошел сброс системы на коммутаторе.

Информация, приходящая по e-mail от SMTP-сервера, относящегося к коммутатору, включает:

- Имя устройства и IP-адрес источника.
- Временная метка, показывающая идентичность SMTP-сервера и клиента, отправившего сообщение, точно так же, как время и дата получения сообщения от коммутатора. Переданные сообщения будут иметь временные метки для каждой передачи.
- Событие, произошедшее на коммутаторе, следствием которого явилась отправка e-mail-сообщения.
- Когда это событие было вызвано пользователем, как, например, сохранение обновления прошивки, IP-адрес, MAC-адрес и имя пользователя User Name, по завершении задачи, сообщение об имевшем месте событии будет отправлено.
- Когда одно и то же событие происходит более одного раза, второе и каждое последующее mail-сообщения будет иметь тему «the system's error message».

Относительно доставки сообщений необходимо иметь в виду следующее:

- Срочное mail-сообщение будет иметь высокий приоритет и будет немедленно отправлено получателем, в то время как обычное mail-сообщение будет размещено в очереди для будущей передачи.
- Максимальное количество непереданных mail-сообщений, расположенных в очереди, не может превышать 30 сообщений. Любые новые сообщения будут отброшены, если очередь переполнена.
- Если первое сообщение, отправленное получателю, не доставлено, оно будет размещено в очереди ожидания и затем будет предпринята повторная попытки передачи сообщения.
- Максимальное количество попыток доставок mail-сообщений получателем равно трем. Попытки доставить mail-сообщения будут повторяться каждые пять минут, пока не будет достигнуто максимальное количество попыток. Если после этого сообщение не было успешно доставлено, оно удаляется и получателю не доставляется.

Если коммутатор выключается или перезапускается, mail-сообщения в очереди ожидания будут потеряны.

Настройки SMTP-сервера

Следующее окно применяется для настройки соответствующих полей для SMTP-сервера коммутатора, наряду с установкой e-mail адресов, на которые могут быть отправлены log-файлы коммутатора, когда на коммутаторе появляются проблемы. Чтобы открыть следующее окно, откройте папку **Administration**, затем папку **SMTP Service** и нажмите ссылку **SMTP Server Settings**.

SMTP Service Settings

SMTP State	Enabled ▾
SMTP Server Address	172.19.3.32
SMTP Server Port(1-65535)	25
Self Mail Address	me@switch.com

SMTP Mail Receiver

Mail Receiver Address	<input style="width: 90%;" type="text"/>
------------------------------	--

Mail Receiver Address Table

Index	Mail Receiver Address	Delete
1	darren_tremblett@nhl.com	<input type="checkbox"/>
2	dubya@moron.com	<input type="checkbox"/>
3	mryder@canadiens.com	<input type="checkbox"/>
4		
5		
6		
7		
8		

Рисунок 6.55. Окно SMTP Service Settings и Mail Receiver Address Table

Следующие параметры могут быть установлены.

Параметр	Описание
SMTP State	Используя выпадающее меню, включите или выключите сервис SMTP для этого устройства
SMTP Server Address	Введите IP-адрес SMTP-сервера, с которого будут отправляться mail-сообщения.
SMTP Server Port	Введите номер виртуального порта, через который коммутатор будет подключаться к SMTP-серверу. Как правило, порт для SMTP -25. Однако значение этого поля может иметь значение от 1 до 65535.
Self Mail Address	Введите e-mail адрес, с которого будут отправляться mail-сообщения. Этот адрес будет в поле «from» e-mail-сообщения, отправленного получателю. Можно настроить только один mail-адрес. Его длина не может превышать 64 буквенно-цифровых знака.
Mail Receiver Address	Введите список e-mail адресов получателей, которые будут получать e-mail сообщения о функциях коммутатора. Возможно установить до 8 e-mail адресов. Для удаления соответствующего адреса нажмите соответствующий значок X под заголовком Delete в таблице Mail Receiver Address Table.

Нажмите **Apply** для применения выполненных изменений.

Сервис SMTP

Следующее окно применяется для отправки тестовых сообщений всем получателям mail, установленным на коммутаторе. Это позволяет провести тестирование настроек и надежность SMTP-сервера. Для доступа к следующему окну, откройте папку **Administration**, затем **SMTP Service Folder** и нажмите ссылку **SMTP Service**.



Рисунок 6.56. SMTP Mail Service

Следующие параметры могут быть установлены:

Параметр	Описание
Subject	Введите тему тестового сообщения e-mail.
Content	Введите содержимое тестового сообщения e-mail.

Когда Ваше сообщение готово, нажмите Send для отправки этого сообщения всем получателям SMTP-сообщений, установленным на коммутаторе.

Раздел 7 – Опции второго уровня

VLAN

Агрегирование каналов

IGMP Snooping

Spanning Tree

Виртуальные локальные сети (VLAN)

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 улучшить производительность за счет сохранения полосы пропускания, а также 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.

Некоторые замечания относительно сетей VLAN , построенных на базе коммутаторов

Неважно, по какому принципу происходит однозначная идентификация конечных узлов и объединение этих узлов в VLAN, пакеты не могут проходить через VLAN без сетевого устройства, выполняющего функции маршрутизации между сетями VLAN.

Коммутаторы DES-3000 серии поддерживают VLANs на основе стандарта IEEE 802.1Q. 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 VLAN на основе порта могут перекрываться, если это необходимо.

Сети VLAN IEEE 802.1Q

Некоторые тематические термины:

- **Tagging** – добавление маркера в заголовок пакета (802.1Q VLAN).
- **Untagging** – удаление маркера 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. VLAN IEEE 802.1Q доставляет пакеты только между станциями одной VLAN.

Любой порт может быть сконфигурирован как **tagging**(tagged), так и **untagging**(untagged). Функция **untagging**(untagged) IEEE 802.1Q VLANs позволяет VLANs работать с коммутаторами, не поддерживающими распознавание тегов VLAN в заголовках пакетов. Функция **tagging**(tagged) 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 продвижение 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 одноуровневого тегирования.

- 802.1Q VLAN Packet Forwarding.
- Решение о продвижении 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

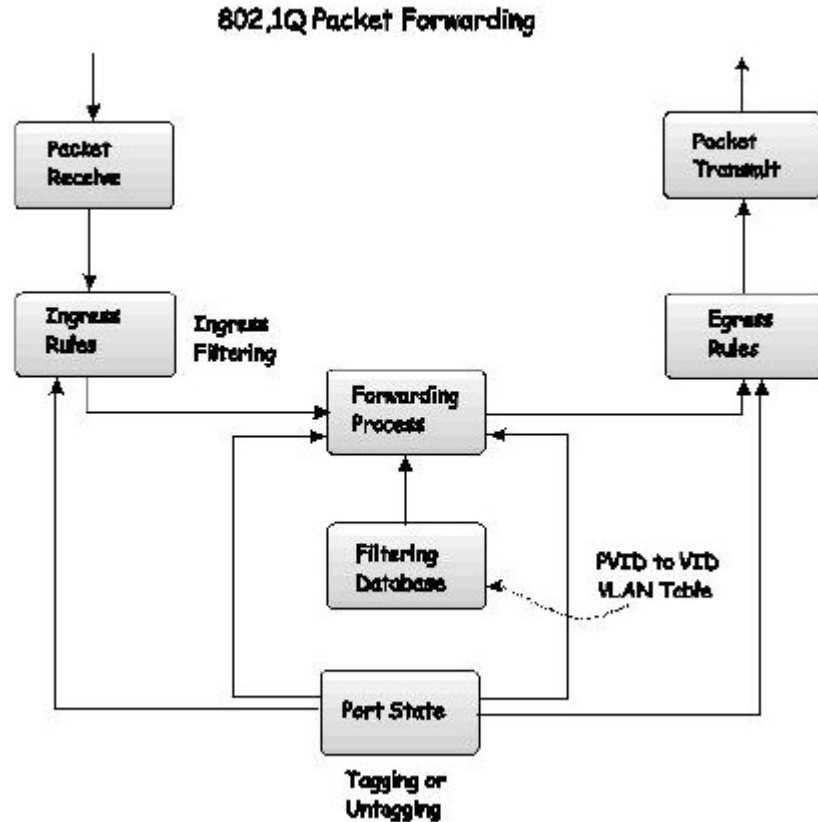


Рисунок 7.1 – Продвижение пакетов согласно IEEE 802.1Q

Метки 802.1Q VLAN

Рисунок, представленный ниже, отображает тег 802.1Q VLAN. 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.

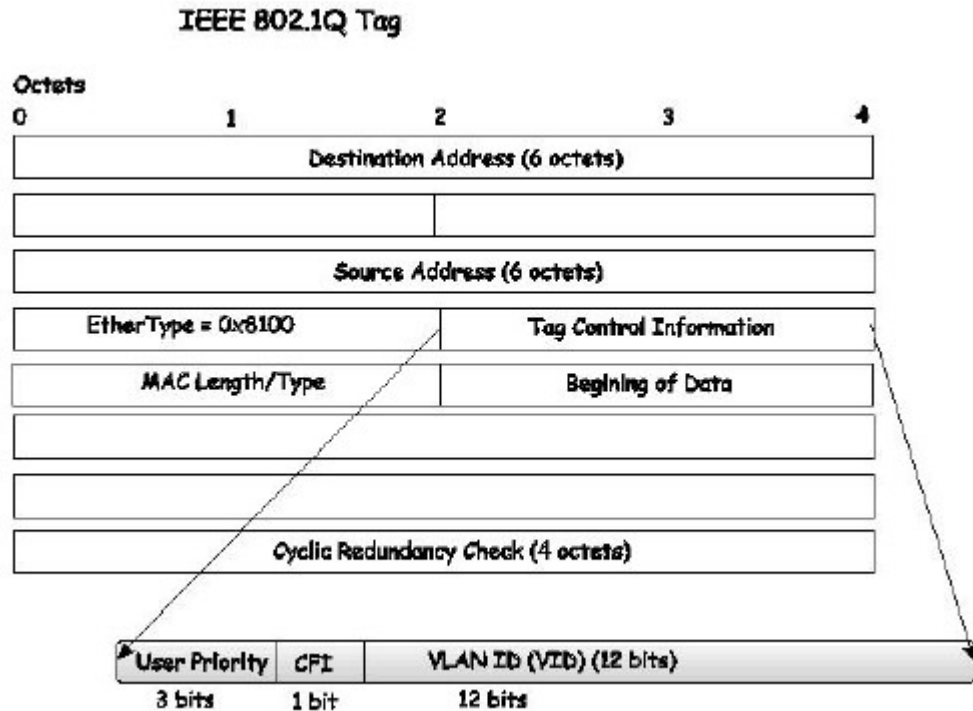


Рисунок 7.2 – Метка IEEE 802.1Q

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

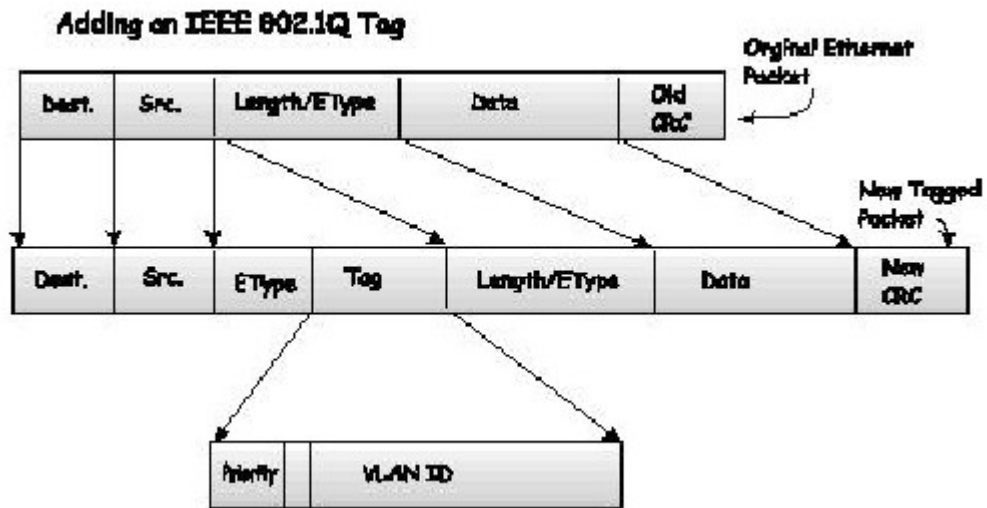


Рисунок 7.3. Добавление тега IEEE 802.1Q

Тегированные (tagged) и нетегированные (untagged) порты

Каждый порт, поддерживающий 802.1Q, может быть сконфигурирован как тегированный (tagged) или нетегированный (untagged).

Тегированные 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 продвижении пакетов, используют эту VLAN-информацию.

Нетегированный порт неспособен считывать тег 802.1Q из проходящих через него пакетов. Если у пакета нет тега 802.1Q VLAN, порт не изменит пакет. Таким образом, пакеты, принятые или переданные через нетегированный порт, не содержат информации 802.1Q VLAN. (Следует помнить, что PVID используется только внутри коммутатора). Удаление тегов из заголовков пакетов используется для отправки пакетов с устройств поддерживающих 802.1Q, на несоответствующие сетевые устройства.

Входящая фильтрация

Порт Коммутатора, на который приходят пакеты, 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 тегированный 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 перенаправляться на все порты. Широковещательные и многоадресные пакеты также будут перенаправляться на 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.

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 продвижения), 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. Эта выборочное продвижение пакетов базируется на таком свойстве VLAN, как сетевые сегменты VLAN. Таким образом, порт 1 может только осуществлять передачу на VLAN 2.

VLAN и группы агрегированных каналов

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

Запись статической VLAN

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

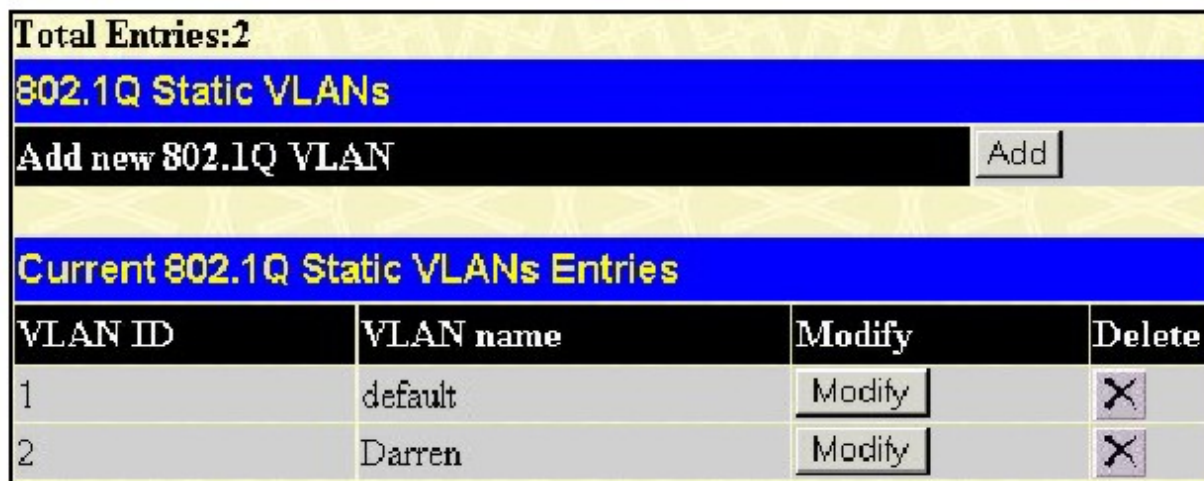


Рисунок 7.7. Окно 802.1Q Static VLANs

Окно **802.1Q Static VLANs** показывает все сконфигурированные сети VLAN (имя и ID). Для удаления 802.1Q VLAN следует кликнуть по соответствующему знаку 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, показанной ниже.

802.1Q Static VLANs																		
VID	VLAN Name																	
<input type="text"/>	<input type="text"/>																	
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Tag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
																	<input type="button" value="Apply"/>	
Show All Static VLAN Entries																		

Рисунок 7.5. Окно 802.1Q Static VLANs - Add (добавить)

Для возвращения в окно **Current 802.1Q Static VLANs Entries** следует кликнуть по линку [Show All Static VLAN Entries](#). Чтобы изменить уже существующую 802.1Q VLAN, необходимо кликнуть по соответствующей кнопке **Modify**. Появится новое меню для конфигурирования настроек порта и связи уникального имени и номера с новым VLAN. Описание параметров представлено в таблице ниже.

802.1Q Static VLANs																		
VID	VLAN Name																	
<input type="text" value="2"/>	<input type="text" value="Darren"/>																	
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Tag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
																	<input type="button" value="Apply"/>	
Show All Static VLAN Entries																		

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. VLANs идентифицируются по имени или VID.
VLAN Name	Позволяет ввести имя нового VLAN в окне Add или редактировать имя VLAN в окне Modify .
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 определить 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 так же тегирующими или нетегирующими.

Для применения настроек нажмите **Apply**. Нажмите ссылку [Show All Static VLAN Entries](#) для возврата к окну **802.1Q Static VLANs**.

Агрегирование каналов

Понятие магистральной группы каналов связи

Магистральная группа каналов связи (Port trunk groups) используется для объединения портов в одну высокоскоростную магистраль. DES-30xx поддерживает до тридцати двух магистральных групп каналов связи с количеством портов от 2 до 8 на группу. Может быть достигнута потенциальная скорость передачи данных до 8000Мбит/с.

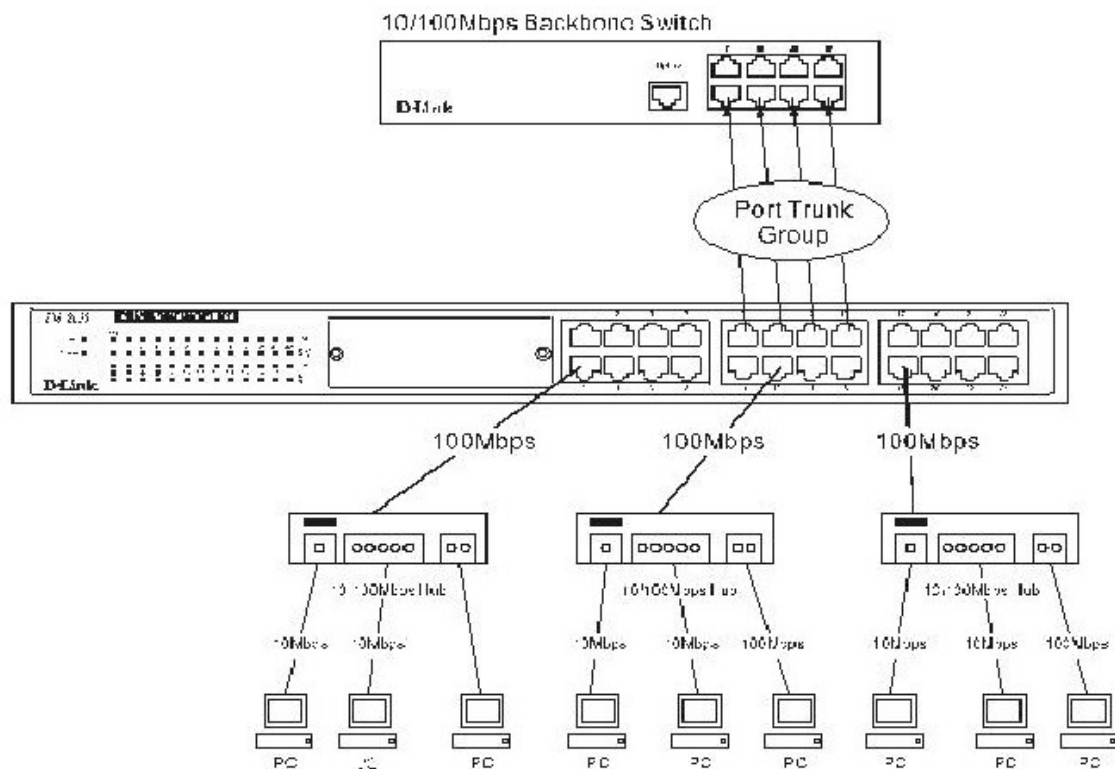


Рисунок 7.7. Пример Port Trunk Group

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 трех 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.

Для конфигурирования агрегирования портов нажмите **L2 Features > Trunking > Link Aggregation**, откроется окно **Port Trunking Group**:

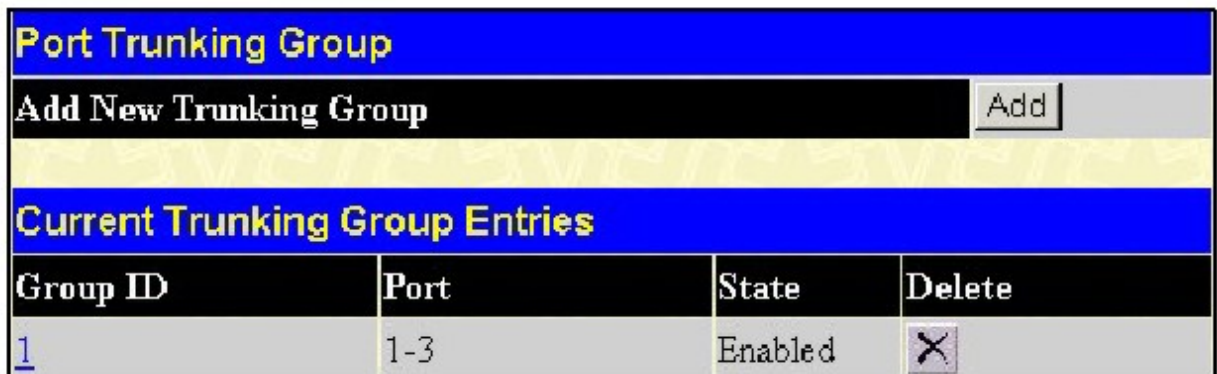


Рисунок 7.8. Port Trunking Group окно

При настройке магистральной группы каналов связи нажмите кнопку **Add**, чтобы добавить новую группу. Меню **Port Trunking Configuration** (показано ниже) используется для настройки групп. Чтобы изменить группу нажмите Hyperlinked Group ID. Чтобы удалить группу нажмите значок **X** под надписью **Delete**, в таблице **Current Trunking Group Entries**.

Port Trunking Configuration																																					
Group ID	1																																				
State	Disabled																																				
Type	Static																																				
Master Port	Port 1																																				
Port Map	<table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td> </tr> <tr> <td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18																				
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																				
Active Port																																					
Flooding Port	None																																				
<input type="button" value="Apply"/>																																					
<p>Note: It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Port Trunking Group Entries</p>																																					

Рисунок 7.9. Окно Link Aggregation Group Configuration – Add(добавить)

IGMP Snooping

IGMP (Internet Group Management Protocol) snooping 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 на основе IGMP-сообщений, проходящих через Коммутатор.

Чтобы использовать IGMP Snooping, необходимо сначала определить это глобально в настройках Коммутатора (см. **Advanced Settings**). Затем можно сделать тонкую настройку для каждой VLAN, нажав на ссылку **IGMP Snooping** в папке **L2 Features**. Когда IGMP snooping включён, коммутатор может открыть или закрыть порт для определённого члена группы широковещательной рассылки на основе IGMP-сообщений, проходящих через коммутатор. Коммутатор отслеживает IGMP – сообщения и прекращает посылать широковещательные пакеты, когда больше нет хостов, запрашивающих продолжение рассылки.

Окно **IGMP Snooping Group Entry Table** используется для просмотра настроек **IGMP Snooping**. Для изменения настроек, надо кликнуть по кнопке **Modify** соответствующего VLAN ID.

IGMP Snooping Settings				
VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	<input type="button" value="Modify"/>

Рисунок 7.10. Текущие записи IGMP Snooping Group

После нажатия на кнопку **Modify** откроется окно **IGMP Snooping Settings**, представленное ниже:

IGMP Snooping Settings	
VLAN ID	<input type="text" value="1"/>
VLAN Name	<input type="text" value="default"/>
Query Interval (1-65535)	<input type="text" value="125"/>
Max Response Time (1-25)	<input type="text" value="10"/>
Robustness Value (1-255)	<input type="text" value="2"/>
Last Member Query Interval (1-25)	<input type="text" value="1"/>
Host Timeout (1-16711450)	<input type="text" value="260"/>
Router Timeout (1-16711450)	<input type="text" value="260"/>
Leave Timer (1-16711450)	<input type="text" value="2"/>
Querier State	Disabled ▾
Querier Router Behavior	Non-Querier
State	Disabled ▾
Multicast fast leave	Disabled ▾
<input type="button" value="Apply"/>	
Show All IGMP Group Entries	

Рисунок 7.11. Окно IGMP Snooping Settings-Edit (редактировать)

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 отправки 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.
Router 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 <i>Enabled</i> – для включения IGMP-запросов, <i>Disabled</i> – для отключения. Значение по умолчанию – <i>Disabled</i> .
Querier Router Behavior	Это поле доступно только для чтения. Оно описывает поведение маршрутизатора при посылке IGMP-пакетов. <i>Querier</i> будет означать, что маршрутизатор уже отослал IGMP-пакеты. <i>Non-Querier</i> будет означать, что маршрутизатор еще не отослал IGMP-пакеты. Это поле будет доступно для чтения только при нахождении полей <i>Querier State</i> и <i>State</i> в состоянии <i>Enabled</i> (Включено).
State	Значение <i>Enabled</i> – для применения IGMP snooping. Значение по умолчанию – <i>Disabled</i> .
Multicast Fast Leave	Этот параметр позволяет пользователю подключить функцию Fast Leave. При подключении этой функции, членам широковещательной группы будет разрешено покинуть группу немедленно (а не в соответствии с настройкой <i>Last Member Query Interval</i>) после получения коммутатором пакета Leave. По умолчанию эта функция отключена (<i>Disabled</i>).

Нажмите Apply для применения настроек. Для возврата в окно **IGMP Snooping Group Settings** нажмите [Show All IGMP Snooping Entries](#).



Примечание: Функция Fast Leave предназначена для пользователей IGMP версии 2, которые желают покинуть широковещательную группу, и лучше всего адаптирована для VLAN, содержащих только один хост на каждом порту. Когда же эту функцию использует один хост из группы, это может послужить причиной непреднамеренного применения этой функции и для других хостов группы.

Создание записи о статических портах маршрутизатора

Статический порт маршрутизатора – это порт, к которому прикреплен маршрутизатор многоадресной рассылки. У этого маршрутизатора будет соединение с WAN или Интернет. Назначение порта маршрутизатора позволит многоадресным пакетам, получаемым от маршрутизатора распространяться по сети, а многоадресным сообщениям (IGMP), поступающим из сети, распространяться через маршрутизатор.

Порт маршрутизатора обладает следующими свойствами:

- Все IGMP-пакеты будет перенаправлены на порт маршрутизатора.

- IGMP-ответы от маршрутизатора направляются ко всем портам.
- Все UDP-пакеты будут перенаправлены на порт маршрутизатора. Поскольку маршрутизаторы не посылают IGMP-пакетов или не используют IGMP snooping, широковещательный маршрутизатор, связанный с портом маршрутизатора 3-го уровня, не способен принимать UDP-данные, если широковещательные UDP-пакеты не были перенаправлены на порт маршрутизатора.

Порт маршрутизатора будет динамически сконфигурирован, когда определятся пришедшие на порт IGMP-запросы, многоадресные пакеты RIPv2, DVMRP или PIM-DM.

Для открытия окна **Current Static Router Ports Entries** (показано ниже) следует открыть папку **IGMP Snooping**, нажать на ссылку **Static Router Ports Settings**.

Total Entries:2		
Static Router Port Settings		
VLAN ID	VLAN Name	Modify
1	default	Modify
2	Darren	Modify

Рисунок 7.12. Окно Static Router Ports Settings

Данное окно отображает текущие настройки статического порта маршрутизатора. Для изменения настроек кликните кнопку **Modify**. Откроется окно **Static Router Ports Settings-Edit**, как показано ниже:

Static Router Ports Settings																	
VID	2																
VLAN Name	Darren																
Member Ports																	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Apply																	
Show All Static Router Ports Entries																	

Рисунок 7.13. Окно Static Router Ports Settings - Edit

Могут быть установлены следующие параметры:

Параметр	Описание
VID (VLAN ID)	Это идентификатор (ID) VLAN, наряду с именем VLAN, определяющий, куда прикреплен маршрутизатор многоадресной рассылки.
VLAN Name	Это имя VLAN, куда прикреплен маршрутизатор многоадресной рассылки.
Member Ports	Порты на Коммутаторе, к которым будут прикреплены маршрутизаторы многоадресной рассылки.

Для применения настроек необходимо кликнуть **Apply**. Чтобы вернуться в окно **Static Router Ports Settings**, надо нажать на ссылку [Show All Static Router Port Entries](#).

Spanning Tree (Алгоритм покрывающего дерева)

Коммутатор поддерживает две версии Spanning Tree (протокол покрывающего дерева): 802.1d STP, 802.1w Rapid STP. 802.1d STP знаком большинству сетевых профессионалов. Однако поддержка 802.1w Rapid STP также была недавно реализована на управляемых коммутаторах Ethernet D-link. Ниже представлено краткое введение в технологию и настройку 802.1d STP, 802.1w Rapid STP.

802.1w Rapid Spanning Tree

В Коммутаторе используются две версии протокола Spanning Tree: 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 функциям новых коммутаторов, одни из них – функции 3-го уровня, которые всё чаще и чаще исполняются коммутаторами Ethernet. 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 продвижения пакетов и механизме этого перехода, относящегося к роли порта (пересылающий или не пересылающий) в топологии. RSTP комбинирует продвижение 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 создаётся статус Discarding. Таким образом, нет функциональных различий. Порт остаётся неработающим. В Таблице 7-1 показано сравнение port state transition двух протоколов.

Все два 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 регулированию топологии. Недостатком 802.1d является отсутствие непосредственной обратной связи между смежными мостами.

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

**Таблица 7-1.
Сравнение
статусов портов**

RSTP способен к более быстрому переходу к статусу продвижения – 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 продвижения. Для того чтобы быстро позволить этот переход, протокол вводит два новых понятия: edge port (пограничный порт) и point-to-point (P2P) порт.

Пограничный порт

Пограничный порт (Edge port) - порт, напрямую соединяемый 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 продвижения 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 эта настройка не была отключена вручную.

Совместимость 802.1d/802.1w

RSTP совместим с устаревшим оборудованием и при необходимости может автоматически корректировать BPDU-пакеты в формат 802.1d. 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 - настройки осуществлены глобально.
2. На уровне порта - настройки осуществлены в определенной пользователем группе портов.

STP LoopBack Detection (Обнаружение петель)

При подключению к коммутатору, STP - основной параметр в конфигурации при доставке пакетов на порт и может значительно улучшить производительность коммутатора. Всё же данная функция может работать со сбоями, с появлением STP BPDU-пакеты иногда возвращались на Коммутатор (loopback), таким образом, получалась обратная петля от неуправляемого коммутатора, связанного с DES-30xx. Для достижения хорошей производительности сейчас DES-30xx снабжён функцией STP loopback.

Когда функция STP LoopBack Detection включена, Коммутатор предотвращает образование петель между коммутаторами. Если BPDU-пакет вернулся на Коммутатор, данная функция определит и установит на принимающем порте статус ошибки-занятости. Сообщение «BPDU Loop Back on Port» будет записано в системный журнал коммутатора.

Установка таймера LoopBack

На следующем шаге таймер LoopBack играет ключевую роль при решении проблемы обнаружения петель. Выбирая не нулевое значение таймера, включается механизм Auto-Recovery. Когда время по таймеру истекает, коммутатор будет искать возвращённые BPDU-пакеты на том же порте. Если нет возвращённых пакетов, Коммутатор поменяет статус порта с Discarding на Designated. Если были приняты возвращённые BPDU-пакеты, порт остаётся с заблокированным статусом, таймер сбрасывается и процесс начинается заново.

Если данная функция не используется, значение таймера устанавливается 0. В этом случае, когда BPDU-пакеты возвращаются на Коммутатор, порт переводится в заблокированное состояние и в системный журнал коммутатора записывается сообщение. Для разблокирования порта

администратор должен поменять статус порта, сделав его активным. Это только один вариант. Как перевести порт в рабочее состояние, если таймер установлен 0.

Инструкции и ограничения для функции LoopBack Detection

- Все три версии STP (STP, RSTP and MSTP) должны быть включены
- Можно сделать глобальную конфигурацию (STP Global Bridge Settings), или индивидуально для каждого порта (MSTP Port Information).
- Соседние с DES-3018 коммутаторы должны быть способными пересылать BPDU-пакеты. Коммутаторы, не удовлетворяющие данным требованиям, будут отключать функцию данного коммутатора DES-3018.
- Значение по умолчанию для этой функции – Disabled
- Значение по умолчанию LoopBack таймера 60 сек.
- Данные установки доступны только, когда интерфейс STP выбран.

Функция LoopBack Detection может только предотвратить петли на определяемых портах DES-30xx. Она может определить условие возникновения петли на стороне пользователя, связанной с пограничным портом. Но не может обнаружить условие петли на выбранном корневом порту STP другого коммутатора.

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**.

Switch Spanning Tree Settings	
Spanning Tree Protocol	Disabled ▾
Bridge Max Age (6-40 Sec)	20
Bridge Hello Time (1-10 Sec)	2
Bridge Forward Delay (4-30 Sec)	15
Bridge Priority (0-61440)	32768
Default Path Cost	802.1T
STP Version	RSTP ▾
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled ▾
LBD	Disabled ▾
LBD Recover Time(0:Disable)	60
Apply	
Designated Root Bridge	--
Root Priority	--
Cost to Root	--
Root Port	--
Time Topology Change(Sec)	--
Topology Changes Count	--
Protocol Specification	--
Max Age	--
Hello Time	--
Forward Delay	--
Hold Time	--
<p>Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$, $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$</p>	

Рисунок 7.14. STP Bridge Global Settings окно



Примечание: Hello Time не может быть больше, чем Max. Age. Т.к. в этом случае возникнет ошибка конфигурации. Следует придерживаться следующего формата при установке параметров:

Max. Age = 2 x (Forward Delay - 1 сек)

Max. Age = 2 x (Hello Time + 1 сек)

Можно установить следующие параметры:

Параметр	Описание
Spanning Tree Protocol	В выпадающем меню можно выбрать или отменить функцию STP на коммутаторе. Значение по умолчанию <i>Disabled</i> .
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 Bridge 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 следующие значения: <i>STPCompatibility</i> – выберите этот параметр для глобальной установки на коммутаторе Spanning Tree Protocol (STP) <i>RSTP</i> - 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 <i>Enabled</i> или <i>Disabled</i> . Когда данный параметр выбран, это разрешает продвижение STP BPDU-пакетов от других сетевых устройств. Значение по умолчанию <i>Enabled</i> .
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 означать, 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 статуса STP. 0 означает, что LBD не будет автоматически перезапускаться, а администратор будет менять его состояние вручную. Пользователь может установить значение от 60 до 1000000 секунд. Значение по умолчанию 60 секунд.

Нажмите **Apply** для применения сделанных настроек.

STP Port Settings (Настройки STP-порта)

STP можно настроить на основе порта. Для просмотра следующего окна необходимо нажать **L2 Features > Spanning Tree > STP Port Settings**:

From	To	State	Cost(0=Auto)	Priority	Migration	Edge	P2P	BPDU	LBD
Port 1	Port 1	Enabled	0	128	No	False	Auto	Disabled	Disabled

Apply

Port	Connection	State	Cost	Priority	Edge	P2P	STP Status	Role	Port Forward	LED
1	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
2	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
3	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
4	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
5	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
6	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
7	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
8	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
9	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
10	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
11	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
12	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
13	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
14	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
15	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
16	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
17	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
18	Link Down	Yes	*2000000	128	No	Yes	Disabled	Disabled	Enabled	No
19	100M/Full/None	Yes	*2000000	128	No	Yes	Forwarding	NonStp	Enabled	No

Рисунок 7.15. Окно STP Port Settings and Table

В дополнение к установкам параметров Spanning Tree, используемым на уровне коммутаторов, на коммутаторе можно настроить также группы портов. Каждая группа портов будет обладать своим Spanning Tree, со своими конфигурационными настройками. STP-группа будет использовать параметры уровня коммутаторов, заданные ранее, а также приоритет порта и стоимость порта. Spanning tree группы STP работает так же, 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 избыточные 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 задать следующие настройки 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 продвижения пакетов на порт(ы). Значения Port Cost по умолчанию: для 100Мбит/с порта=200000; для Gigabit порта=20000 Значение от 1 до 200000000 – определяет внешнюю стоимость. Чем меньше значение, тем выше приоритет порта.
Priority	Приоритет порта может принимать значение от 0 до 240. Чем меньше это число, тем больше вероятность, что этот порт будет выбран как корневой порт.
Migration	При установке значения «yes» порты будут посылать BPDU-пакеты на порты, запрашивая параметры STP. Если на коммутаторе настроен RSTP, порт может менять свое состояние с 802.1d STP на 802.1w RSTP и обратно. Если на коммутаторе настроен MSTP, порт может менять свое состояние между 802.1d STP и 802.1s MSTP. RSTP и MSTP совместимы со стандартом STP, однако, при этом преимущества RSTP и MSTP не реализуются на порте, где идёт соединение 802.1d с 802.1w или 802.1s. «Миграция» должна быть настроена как «yes» на портах, подключённых к сетевым рабочим станциям или сегментам, которые позволяют изменять протоколы на 802.1w RSTP или 802.1s MSTP во всех или некоторых листах сегмента.
Edge	Выбор значения <i>True</i> 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 <i>False</i> означает, что порт не является пограничным портом.
P2P	Логика работы этих портов похожа на edge-порты. Линк переходит в режим P2P, если он перешел в режим полного дуплекса. Как и для пограничных портов, для портов P2P переход в состояние продвижения пакетов происходит быстрее, чем для обычных портов. Значение <i>False</i> означает, что порт не является P2P-портом. Значение <i>Auto</i> позволяет порту быть со статусом P2P всегда, когда возможно и оперировать так, как если бы значение P2P-статуса было <i>True</i> . Если порт не может поддерживать этот статус (например, если порт был принудительно поставлен в режим полудуплекса), значение P2P – статуса изменится на <i>False</i> . Значение по умолчанию для данного параметра <i>True</i> .
Forward BPDU	Значение <i>True</i> позволит продвижение BPDU-пакетов с сетевых устройств на назначенные порты. Для этого STP должен быть глобально отключён, а продвижение BPDU-пакетов глобально разрешена (глава Глобальные настройки STP-моста). Значение по умолчанию <i>False</i> , в этом случае BPDU

Руководство по настройке коммутатора Cisco Catalyst 3010FL/DES-3026 c портами Fast Ethernet

Для принятия настроек нажмите **Apply**.



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

Раздел 8 – Качество обслуживания (QoS)

Управление полосой пропускания
Приоритет по умолчанию 802.1P
Приоритет пользователя 802.1P
Работа по расписанию QoS
QoS Output Scheduling

CoS

Коммутаторы серии DES-30xx поддерживают приоритезацию трафика согласно протоколу 802.1p. В данном разделе обсуждается реализация качества обслуживания QoS и преимущества использования приоритезации трафика 802.1p.

Приоритезация 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, видеоконференция, могут 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 – указывает на низший приоритет данных, а 7 – на 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 незадаанным 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 (Strict mode) и взвешенный циклический алгоритм (round robin), 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.

Преимущества QoS

QoS представляет собой реализацию стандарта IEEE 802.1p, предоставляющего 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-30xx.

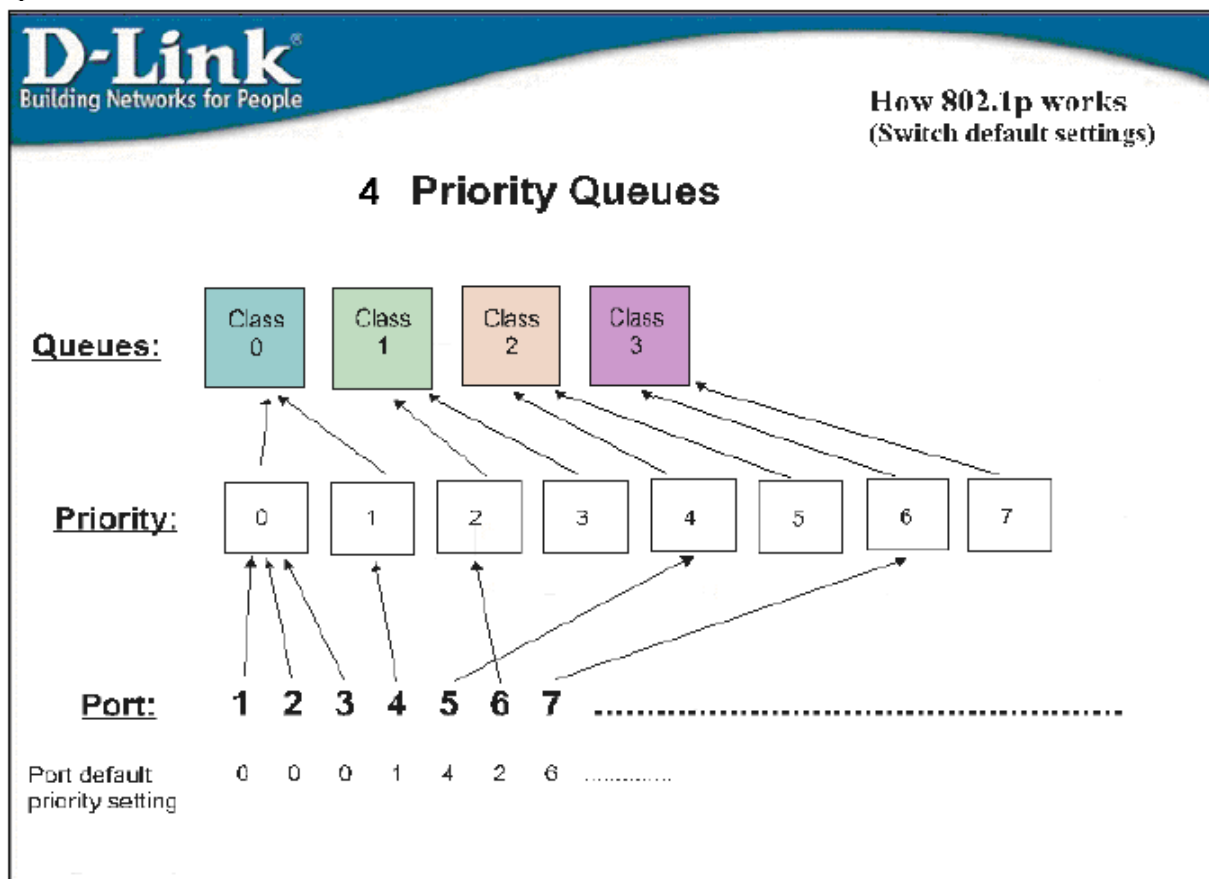


Рисунок 8.1 – Распределение пакетов по очередям приоритетов

Вышеприведённый рисунок показывает установки приоритезации Коммутатора по умолчанию. Class-3 обладает наивысшим приоритетом среди четырёх очередей Коммутатора. Для того, чтобы использовать QoS, Коммутатор проверяет заголовок пакета на наличие тега. Тегированные пакеты будут отправлены в соответствующую их приоритету очередь Коммутатора.

Например, рассмотрим случай, когда пользователь хочет установить видеоконференцию между двумя удалёнными компьютерами. Администратор, используя команды Access Profile, может добавить приоритет в видеопакеты, которые должны быть переданы. Тогда на принимающей стороне администратор проверяет пакеты на наличие тегов и ставит пакет в очередь соответствующую приоритету пакета. Затем администратор устанавливает для этой очереди такой приоритет, при котором пакеты уходят быстрее, чем приходят. Таким образом, пользователь получает пакеты настолько быстро, насколько это возможно. Такое расположение по приоритетам очереди и учёт непрерывного потока пакетов оптимизирует использование полосы пропускания, доступной для видеоконференции.

Понятие QoS

В коммутаторе DES-30xx поддерживаются очереди приоритетов 802.1p. Коммутатор имеет 4 класса приоритетов. Эти классы приоритетов нумеруются, начиная с 3 (Class 3, самый высокий приоритет класса обслуживания) до 0 (Class 0, самый низкий приоритет класса обслуживания). В IEEE 802.1p определено восемь очередей приоритетов, наивысший приоритет закреплен за 7, а самый низкий за 0. Восемью приоритетам, описанным в IEEE 802.1p, ставятся в соответствие следующие приоритетные классы обслуживания:

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

Возможно назначение приоритетов в соответствие с двумя методами: строгий приоритет (strict priority) и циклический приоритет (round-robin priority). По умолчанию, используется строгий порядок приоритетов.

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. Если строгий порядок установлен для CoS, самый высокий класс обслуживания будет работать в строгом режиме, и другие классы будут оставаться в режиме weight fair. Пакеты с более высоким приоритетом всегда получают преимущество, несмотря на пакеты с более низким приоритетом в буфере и время, прошедшее с отправки какого-либо пакета с более низким приоритетом. По умолчанию, коммутатор настроен на работу в строгом режиме.



Предупреждение: По умолчанию механизм CoS установлен для работы в строгом режиме приоритетов, что означает, что коммутатор будет рассматривать только пакеты с наивысшим классом обслуживания для соблюдения строгого режима, в то время как другие очереди также опустошаются при циклическом методе. Ознакомьтесь с командой **config scheduling_mechanism** в этом разделе для более детальной информации по данному вопросу.

Применяя циклические (взвешенные) приоритеты, четыре класса обслуживания коммутатора могут быть установлены для сокращения информации в буфере в циклическом режиме – начиная с наивысшего приоритета класса обслуживания и заканчивая наименьшим приоритетом класса обслуживания, а затем вновь возвращаясь к наивысшему приоритету класса обслуживания.

Механизм на базе взвешенных приоритетов компенсирует главные недостатки механизма на базе строгих приоритетов (при котором пакеты с более низким приоритетом класса обслуживания загружают полосу пропускания) путем обеспечения минимальной полосы пропускания для всех классов обслуживания при передаче. Это достигается путем установки максимального количества пакетов, которым разрешено быть переданными с данным приоритетом класса обслуживания, и максимального времени, в течение которого данный приоритет класса обслуживания должен ждать до передачи накопленных пакетов. При этом устанавливается класс обслуживания Class of Service (CoS) для каждого аппаратного обеспечения коммутатора.

Возможный диапазон значений параметра **weight** (вес) составляет: от 1 до 55 пакетов.

В сетевых средах, использующих альтернативные протоколы приоритезации, CoS коммутатора может быть установлен для подстройки к DSCP приоритету и Type of Service (ToS) приоритету. CoS может быть также установлен для определения MAC-адресов назначения или портов коммутатора.

Команды CoS в интерфейсе командной строки Command Line Interface (CLI) представлены (вместе с соответствующими параметрами) в следующей таблице.

Полоса пропускания порта

Параметры управления полосой пропускания используются, чтобы установить норму при передаче и получении данных для выбранного порта. Для просмотра таблицы «**Port Bandwidth Control**», нажмите **L2 Features> QoS > Bandwidth Control**.

Bandwidth Settings

From	To	Type	no_limit	Rate	Apply
Port 1 ▾	Port 1 ▾	Both ▾	Disabled ▾	64	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

Note: To perform precise bandwidth control, it is required to enable the flow control to mitigate the retransmission of TCP traffic.

Рисунок 8.2. Окно Bandwidth Settings and Port Bandwidth Table

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 <i>RX</i> (receive), <i>TX</i> (transmit) и <i>Both</i> . 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 <i>Enabled</i> .
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**».

802.1p Default Priority (Приоритет 802.1p по умолчанию)

Коммутатор позволяет назначить каждому порту приоритет 802.1p по умолчанию. Для просмотра окна, показанного ниже, следует открыть папку **CoS** и нажать на **802.1p Default Priority**.

Port Default Priority assignment

From	To	Priority	Apply
Port 1 ▾	Port 1 ▾	0 ▾	Apply

The Port Priority Table

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0

Рисунок 8.3. Окно 802.1p Default Priority

Данное окно позволяет задать приоритет 802.1p по умолчанию для любого порта Коммутатора. Приоритеты нумеруются от 0 – низший приоритет до 7 – наивысший приоритет. Для установки нового значения приоритета по умолчанию выберите диапазон портов в выпадающих меню **From** и **To**, а затем установите значение приоритета от 0 до 7 в поле **Priority**. Для принятия сделанных настроек следует кликнуть **Apply**.

Приоритет пользователя 802.1p

DES-30xx позволяет назначить класс обслуживания для каждого приоритета 802.1p. Для просмотра следующего окна необходимо нажать на **802.1p User Priority** в папке **CoS**.

User Priority Configuration	
Priority-0	Class-1
Priority-1	Class-0
Priority-2	Class-0
Priority-3	Class-1
Priority-4	Class-2
Priority-5	Class-2
Priority-6	Class-3
Priority-7	Class-3

Apply

Рисунок 8.4. Окно 802.1p User Priority

Назначив однажды приоритет группы портов Коммутатора, можно связать Class каждого из 4-х уровней с приоритетами 802.1p. Для принятия настроек нажмите **Apply**.

Работа по расписанию

Это выпадающее меню позволит Вам выбрать из Weight Fair (взвешенный циклический) и Strict (Строгий) механизмов опустошения приоритетов классов обслуживания. В папке CoS нажмите CoS Scheduling Mechanism, чтобы увидеть представленное ниже окно.

CoS Scheduling Mechanism	
Scheduling Mechanism	Strict

Apply

CoS Scheduling Mechanism Table	
Class ID	Mechanism
Class-0	Weight fair
Class-1	Weight fair
Class-2	Weight fair
Class-3	Strict

Рисунок 8.5. Окно CoS Scheduling Mechanism и CoS Scheduling Mechanism Table



Примечание: По умолчанию механизм CoS работает в строгом режиме для наивысшего класса (Class-3), что означает, что коммутатор будет рассматривать только самый высокий класс обслуживания для обеспечения строгого режима, в то время как в циклическом алгоритме опустошаются и другие очереди приоритетов.

Параметр	Описание
Strict	Самый высокий класс трафика обслуживается в первую очередь. Сначала будет передаваться трафик с наивысшим классом обслуживания, и только после этого будут обработаны другие очереди.
Weight Robin	Для распределения пакетов по приоритетам классов трафика используйте взвешенный циклический алгоритм (<i>WRR</i>).

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

QoS Output Scheduling (Механизм обработки очередей)

Изменение аппаратных очередей на Коммутаторе настраивается через CoS. При любых изменениях реализации CoS необходимо обратить внимание на то, как эти изменения повлияли на сетевой трафик в очередях с наименьшим приоритетом. Т.к. изменения могут привести к недопустимым уровням потерь пакетов или существенной 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 CoS. Для просмотра окна, представленного ниже, нажмите CoS **CoS Output Scheduling**.

Class ID	Weight
Class-0	1
Class-1	2
Class-2	4
Class-3	8

Рисунок 8.6 – Окно CoS Output Scheduling Configuration

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**.

Priority Setting (Настройка приоритета)

Priority Setting			
From	To	MainSelect	Apply
Port 1	Port 1	none	Apply
Priority Setting Table			
Port	Port Priority	Ethernet Priority	IP Priority
1	off	802.1p_priority	off
2	off	802.1p_priority	off
3	off	802.1p_priority	off
4	off	802.1p_priority	off
5	off	802.1p_priority	off
6	off	802.1p_priority	off
7	off	802.1p_priority	off
8	off	802.1p_priority	off
9	off	802.1p_priority	off
10	off	802.1p_priority	off

Рисунок 8. 7. Priority Setting

Установите следующие параметры настройки приоритета.

Параметр	Описание
From/To	Может быть установлена последовательная группа портов, начиная с выбранного порта.
Main Select	Выберите общую настройку приоритета для установленных портов: <ul style="list-style-type: none"> • port_priority – на базе портов • ethernet_priority – на базе MAC-адресов или 802.1p Priority • ip_priority – TOS-IP или DSCP-IP • none – нет установки приоритета
Type	В данном поле определяются настройки приоритета для ip_priority как mac base (на базе MAC-адресов) или 802.1p приоритет (802.1_priority)

Нажмите **Apply**, чтобы изменения вступили в силу.

TOS Priority Setting (Настройка приоритета TOS)

Используйте меню **TOS Priority Setting** для установки приоритета ToS для класса обслуживания на коммутаторе.

TOS Priority Setting		
TOS	Class ID	Apply
0 ▾	0 ▾	Apply

The Port Priority Table	
TOS	Class
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

Рисунок 8.8. TOS Priority Setting

Выберите значение **TOS** в выпадающем меню и **Class ID** выбранного уровня приоритета и нажмите кнопку **Apply**. Изменения отобразятся в окне **Port Priority Table**, представленном ниже.

DSCP Priority Setting (Настройка приоритета DSCP)

Используйте меню **DSCP Priority Setting** для установки приоритета DSCP для класса обслуживания коммутатора.

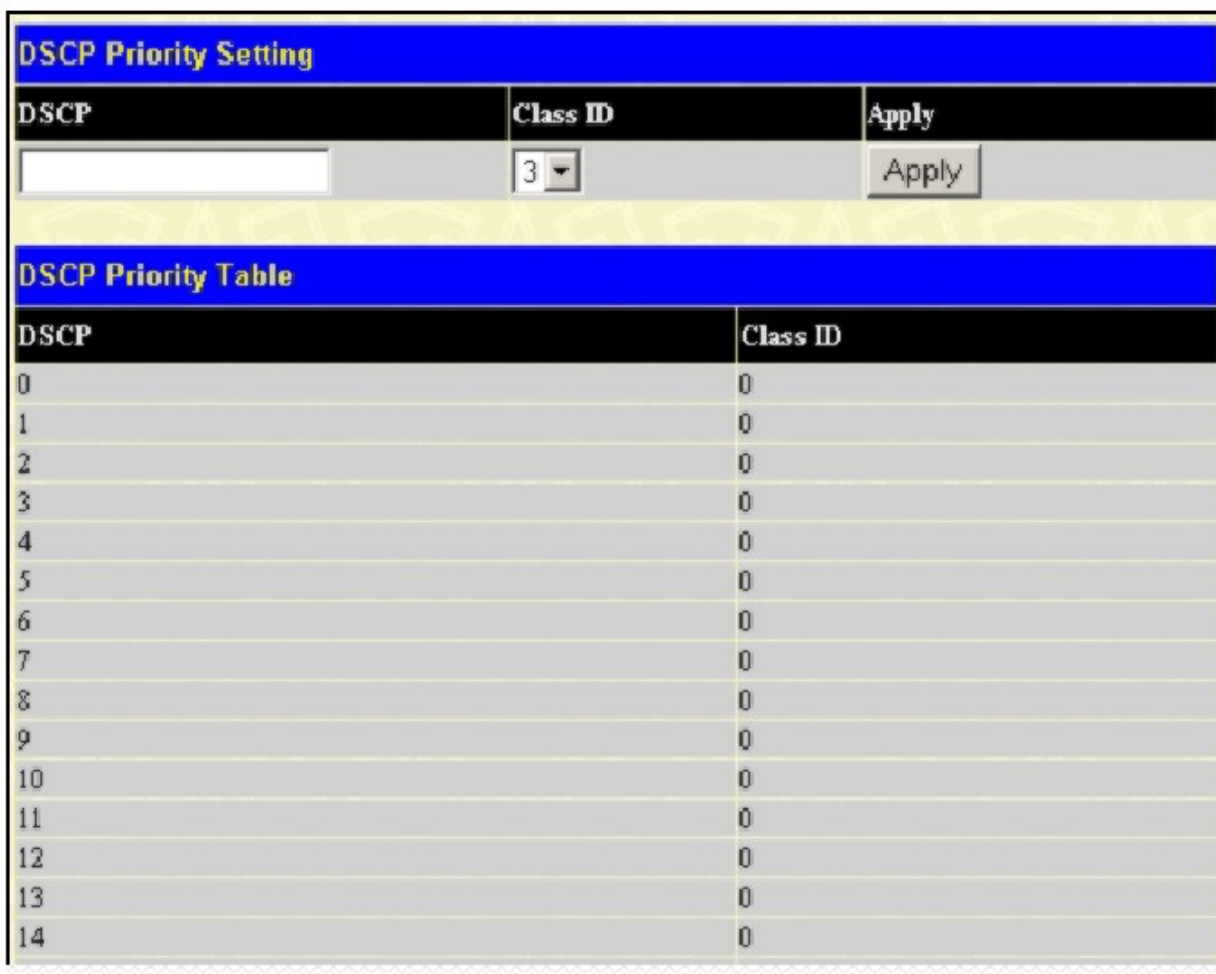


Рисунок 8. 9. DSCP Priority Setting

Определите уровень бит **DSCP** и приоритет **Class ID** с помощью выпадающего меню и нажмите кнопку **Apply**. Новые настройки отобразятся в окне **DSCP Priority Table**, показанном ниже.

Port Mapping Priority CoS (Перенаправление трафика с порта в определенную очередь приоритетов)

Port Mapping Priority CoS может быть использовано только в том случае, если оно было предварительно установлено для выбранных портов в меню **Priority Setting**. Доступно два уровня класса обслуживания.

From	To	Class	Apply
Port 1	Port 1	0	Apply

The Port Mapping Priority Table	
Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0

Рисунок 8.10. Port Mapping Priority CoS

Используйте меню **From/To** для выбора портов для конфигурации, выбранные порты сначала должны быть установлены для приоритетов на база порта в меню **Priority Setting**. Выберите уровень класса **Class** для портов, существует два уровня: 3 –для высокого приоритета и 0 – для низкого приоритета.

MAC Priority Setting (Настройка MAC-приоритета)

Используйте меню **MAC Setting**, чтобы назначить уровень класса обслуживания отдельно назначенным MAC-адресам.

MAC Address	Class ID	Apply
00:00:00:00:00:00	3	Apply

MAC Priority Table	
MAC Address	Class ID

Рисунок 8.11. MAC Priority Setting

Впечатайте **MAC Address**, выберите уровень приоритета **Class ID** и нажмите кнопку **Apply**.

Раздел 9

CPU Interface Filtering

Вследствие потребностей в дополнительной безопасности коммутатора, в коммутаторы DES-3018 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. 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. Похожей опцией является функция профиля доступа, упоминаемая ранее, функция. В качестве добавочного свойства CPU Filtering, в коммутаторе DES-3018 механизм фильтрации CPU можно включать и отключать глобально, 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.

Настройки CPU Interface Filtering

В следующем окне, пользователь может глобально подключить или отключить механизм CPU Interface Filtering, используя выпадающее меню для изменения состояния. Для доступа к этому окну, нажмите **CPU Interface Filtering > CPU Interface Filtering State**. Выберите **Enabled** для подключения тщательной проверки CPU пакетов коммутатором, и **Disabled** для отключения этой проверки.



Рисунок 9.1. Окно CPU Interface Filtering State Settings

Таблица профилей CPU Interface Filtering

В таблице **CPU Interface Filtering Table** отображаются созданные записи таблицы **CPU Access Profile Table**. Для просмотра настроек нажмите на гиперссылку номера **Profile ID**.

Profile ID	Type	Access Rule	Delete
1	Ethernet	Modify	X
2	IP	Modify	X
3	Packet Content	Modify	X

Рисунок 9.2 – Окно «CPU Interface»

Для добавления записи в таблицу **CPU Interface Filtering Table** нажмите кнопку **Add**, после чего откроется представленное ниже окно **CPU Interface Filtering 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 9.3 – Окно «CPU Interface Filtering Profile Configuration - Ethernet»

Параметры	Описание
Profile ID (1 - 3)	Идентификатор установленного профиля. Можно ввести значение от 1 до 3.
Type	<p>Выберите, какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адрес или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей.</p> <ul style="list-style-type: none"> <input type="checkbox"/> При выборе <i>Ethernet</i> коммутатор будет проверять заголовок каждого пакета на 2 уровне. <input type="checkbox"/> При выборе <i>IP</i> коммутатор будет проверять IP-адрес в

	<p>заголовке каждого пакета.</p> <p><input type="checkbox"/> Для скрывания данных заголовка пакета установите маску содержимого пакета <i>Packet Content Mask</i>.</p>
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, 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 IP Access Profile Configuration для профиля IP.

CPU Interface Filtering Configuration

Profile ID(1-3)	<input type="text" value="1"/>		
Type	IP <input type="button" value="v"/>		
Vlan	<input type="checkbox"/>		
Source IP Mask	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	
Destination IP Mask	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	
Dscp	<input type="checkbox"/>		
Protocol	<input type="checkbox"/>	<input checked="" type="radio"/> ICMP	<input type="checkbox"/> type <input type="checkbox"/> code
		<input type="radio"/> IGMP	<input type="checkbox"/> type
		<input type="radio"/> TCP	<input type="checkbox"/> src port mask <input type="text" value="0000"/> <input type="checkbox"/> dest port mask <input type="text" value="0000"/> <input type="checkbox"/> flag mask bit <input type="checkbox"/> urg <input type="checkbox"/> ack <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> fin
		<input type="radio"/> UDP	<input type="checkbox"/> src port mask <input type="text" value="0000"/> <input type="checkbox"/> dest port mask <input type="text" value="0000"/>
		<input type="radio"/> protocol id	<input type="checkbox"/> user mask <input type="text" value="00000000"/>

[Show All CPU Interface Filtering Table Entries](#)

Рисунок 9.4 – Окно «CPU Interface Filtering Configuration - IP»

Параметр	Описание
Profile ID	Введите идентификатор профиля из диапазона 1 – 3.

Type	<p>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.</p> <ul style="list-style-type: none"> <input type="checkbox"/> При выборе <i>Ethernet</i> коммутатор будет проверять заголовок каждого пакета на 2 уровне. <input type="checkbox"/> При выборе <i>IP</i> коммутатор будет проверять IP-адрес в заголовке каждого пакета. <input type="checkbox"/> Для скрытия данных заголовка пакета установите маску содержимого пакета <i>Packet Content Mask</i>.
VLAN	<p>При выборе данной опции коммутатор будет проверять идентификатор VLAN в заголовке каждого пакета и использовать его в качестве полного или частичного условия для принятия решения о передаче пакета.</p>
Source IP Mask	<p>Введите маску IP-адреса источника.</p>
Destination IP Mask	<p>Введите маску IP-адреса назначения.</p>
DSCP	<p>При выборе данной опции 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.</p>
Protocol	<p>Выбрав данную опцию, коммутатор будет проверять значение типа протокола в заголовке каждого пакета. Вам необходимо выбрать протокол (ы) в соответствии со следующими рекомендациями:</p> <p>Выберите ICMP для того, чтобы коммутатор проверял поле протокола управляющих сообщений в Интернете (Internet Control Message Protocol) в заголовке каждого пакета.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Выберите по значению типа Type или кода Code протокола ICMP будет применяться профиль доступа. <p>Выберите IGMP для того, чтобы коммутатор проверял поле межсетевого протокола управления группами (Internet Group Management Protocol) в заголовке каждого пакета.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Выберите тип Type IGMP, по которому будет формироваться профиль доступа <p>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).</p> <ul style="list-style-type: none"> <input type="checkbox"/> src port mask – задайте маску TCP порта источника в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. <input type="checkbox"/> dest port mask – задайте маску TCP порта назначения в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. <p>При выборе протокола UDP в качестве условия указывается номер UDP порта. Можно использовать или маску порта источника, или/и маску порта назначения.</p> <ul style="list-style-type: none"> <input type="checkbox"/> src port mask – задайте маску TCP порта источника в шестнадцатеричной системе счисления (hex 0x0-0xffff), по которой хотите производить фильтрацию. <input type="checkbox"/> dest port mask – задайте маску TCP порта назначения в шестнадцатеричной системе счисления (hex 0x0-0xffff), по

	<p>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.</p>
--	---

Для сохранения настроек нажмите **Apply**.

Окно **CPU Interface Filtering Configuration** , приведенное ниже – окно для **Packet Content Mask** .

Рисунок 9.5 – 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.

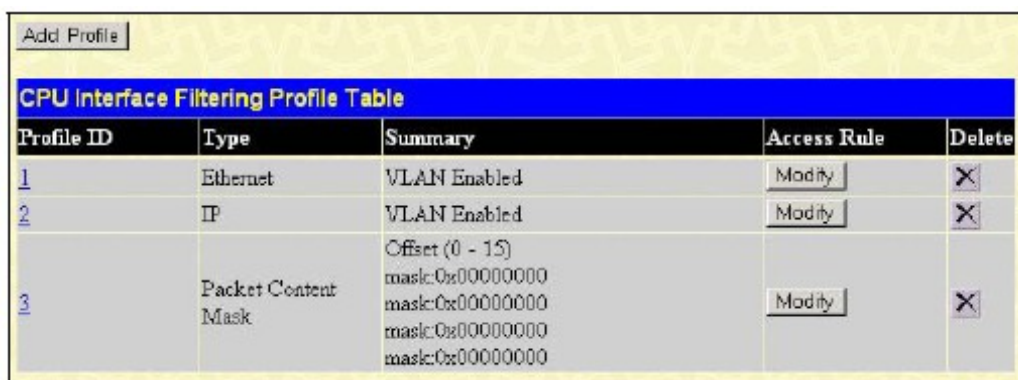
Параметр	Описание
Profile ID	Введите идентификатор профиля из диапазона 1 – 3.
Type	<p>Выберите, какой профиль доступа будет использоваться: на основе Ethernet (MAC-адрес), IP-адреса или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей.</p> <ul style="list-style-type: none"> <input type="checkbox"/> При выборе <i>Ethernet</i> коммутатор будет проверять заголовок каждого пакета на 2 уровне. <input type="checkbox"/> При выборе <i>IP</i> коммутатор будет проверять IP-адрес в заголовке каждого пакета. <input type="checkbox"/> Для скрытия данных заголовка пакета установите маску содержимого пакета <i>Packet Content Mask</i>.
Offset	Это поле указывает, что необходимо сравнить начало заголовка пакета с указанным значением:

	<ul style="list-style-type: none"> <input type="checkbox"/> value (0-15) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить первые 15 байт пакета. <input type="checkbox"/> value (16-31) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 16 по 31 байт пакета. <input type="checkbox"/> value (32-47) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 32 по 47 байт пакета. <input type="checkbox"/> value (48-63) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 48 по 63 байт пакета. <input type="checkbox"/> 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, нажмите кнопку **Apply**.

Для формирования правила ранее созданного CPU Access Profile:

Для открытия **CPU Interface Filtering Table** нажмите **CPU Interface** **CPU Interface Filtering State**.



CPU Interface Filtering Profile Table				
Profile ID	Type	Summary	Access Rule	Delete
1	Ethernet	VLAN Enabled	Modify	X
2	IP	VLAN Enabled	Modify	X
3	Packet Content Mask	Offset (0 - 15) mask:0x00000000 mask:0x00000000 mask:0x00000000 mask:0x00000000	Modify	X

Рисунок 9.6 – 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**. При каждой новой записи будет открываться новое окно, как показано ниже:

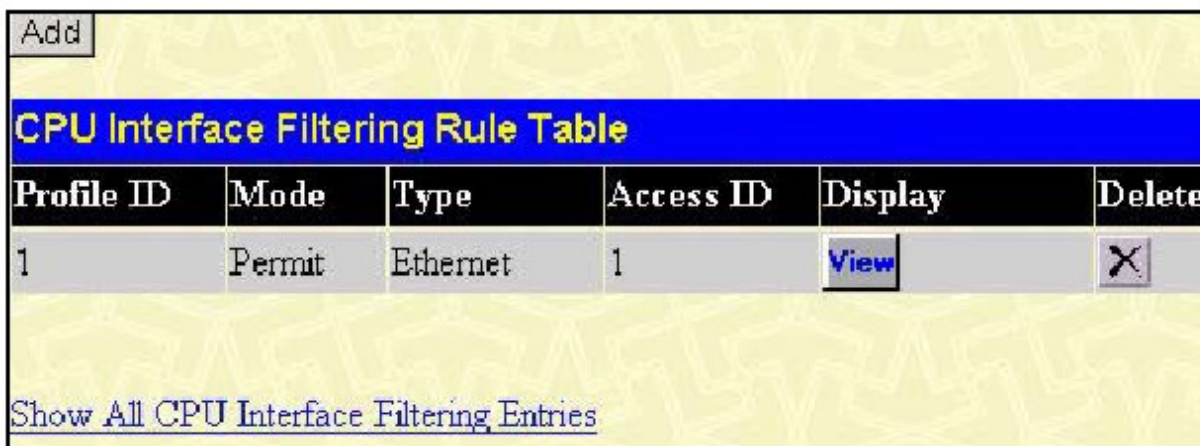


Рисунок 9.7 – Окно «CPU Interface Filtering Table - Ethernet»

Для создания нового правила для профиля доступа нажмите кнопку **Add**. Отобразится новое окно. Для удаления предварительно созданного правила нажмите соответствующую кнопку «X». Следующее окно применяется для создания правил для Ethernet-профиля.

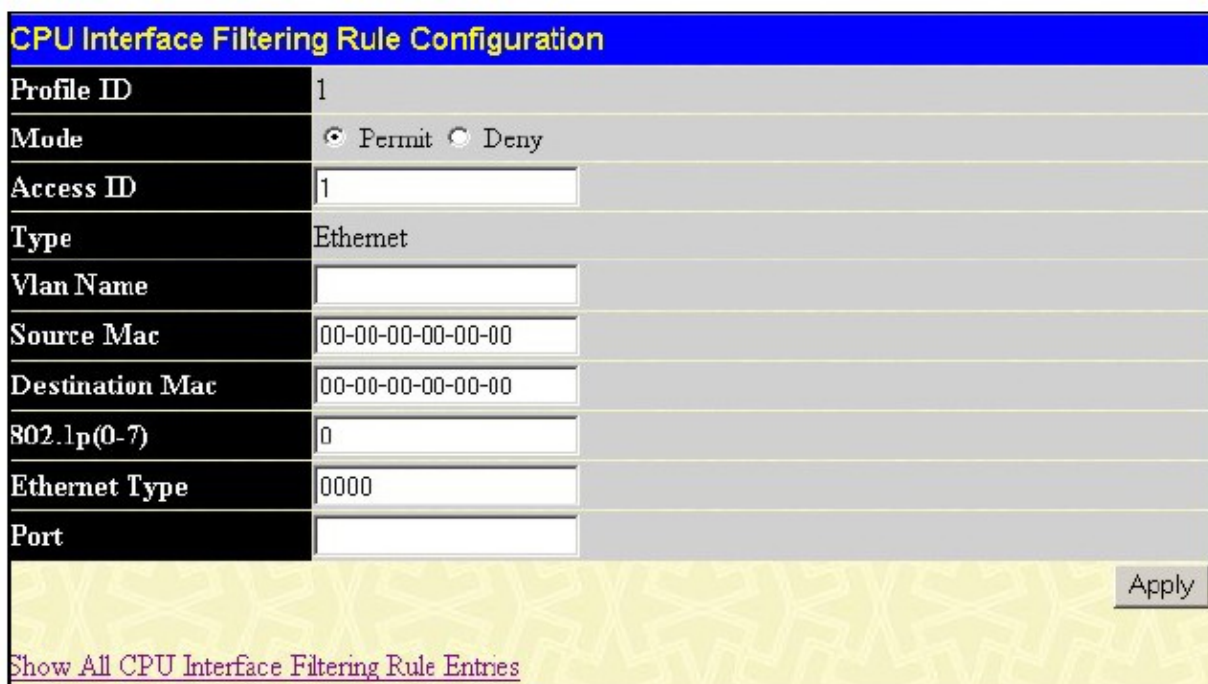



Рисунок 9.8. CPU Interface Filtering Rule Configuration – Ethernet

Для установки правила доступа CPU для профиля Ethernet настройте следующие параметры и нажмите **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 5.

Type	<p>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.</p> <ul style="list-style-type: none"> <input type="checkbox"/> При выборе <i>Ethernet</i> коммутатор будет проверять заголовок каждого пакета на 2 уровне. <input type="checkbox"/> При выборе <i>IP</i> коммутатор будет проверять IP-адрес в заголовке каждого пакета. <input type="checkbox"/> Для скрытия данных заголовка пакета установите маску содержимого пакета <i>Packet Content Mask</i>.
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  в Access Rule Table:

CPU Interface Filtering Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	Ethernet
Vlan Name	default
Source Mac	-----
Destination Mac	-----
802.1p	-----
Ethernet Type	-----
Activate State	Enabled
Port	8
Show All CPU Interface Filtering Rule Entries	

Рисунок 9.9 – Окно «CPU Interface Filtering Rule Display - Ethernet»

Следующее окно CPU Interface Filtering Rule Table отображает IP-профиль.

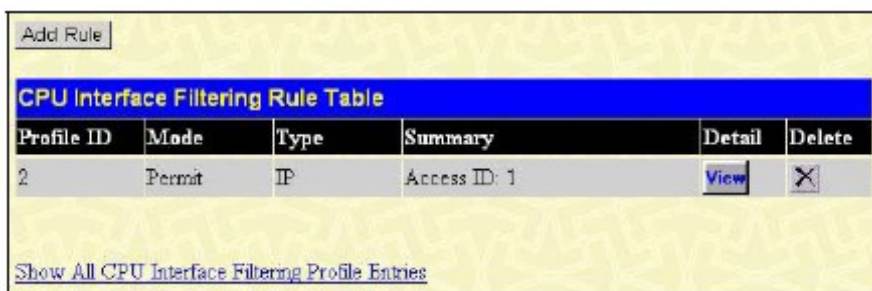


Рисунок 9.10 – Окно «CPU Interface Filtering Table - IP»

Для создания нового правила профиля доступа нажмите кнопку **Add**. Для удаления ранее созданного правила нажмите кнопку **X**. Следующее окно используется для настройки IP-правила CPU.




Рисунок 9.11 – Окно «CPU Interface Filtering Rule Configuration - IP»

Установите следующие настройки Access Rule Configuration для 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 5.
Type	Выберите, какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адрес или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. <input type="checkbox"/> При выборе <i>Ethernet</i> коммутатор будет проверять заголовок каждого пакета на 2 уровне.

	<input type="checkbox"/> При выборе <i>IP</i> коммутатор будет проверять IP-адрес в заголовке каждого пакета. <input type="checkbox"/> Для скрытия данных заголовка пакета установите маску содержимого пакета <i>Packet Content Mask</i> .
VLAN Name	Имя ранее настроенной VLAN.
Source IP	Введите маску IP-адреса источника.
Destination IP	Введите маску IP-адреса назначения.
Dscp	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  в таблице **Access Rule Table**.

CPU Interface Filtering Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	IP
Vlan Name	default
Source IP	-----
Destination IP	-----
Dscp	-----
Protocol	-----
Activate State	Enabled
Port	
Show All CPU Interface Filtering Rule Entries	

Рисунок 9.12. CPU Interface Filtering Rule Display - IP

Следующее окно **CPU Interface Filtering Rule Table** представляет собой таблицу правил CPU Interface для содержимого пакетов.

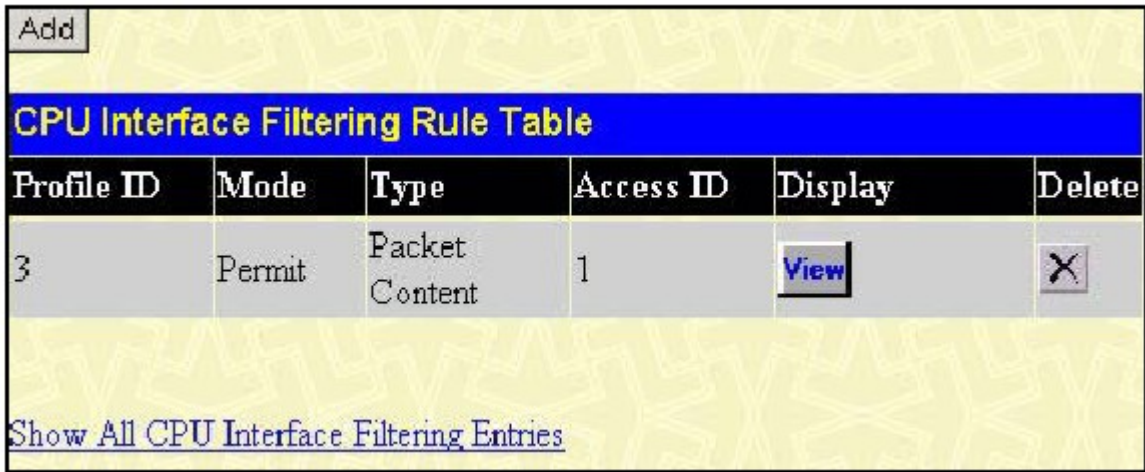


Рисунок 9.13 – Окно «CPU Interface Filtering Rule Table – Packet Content»

Для удаления ранее созданного правила выберите его и нажмите клавишу [X](#). Для добавления нового правила доступа CPU нажмите кнопку **Add**.

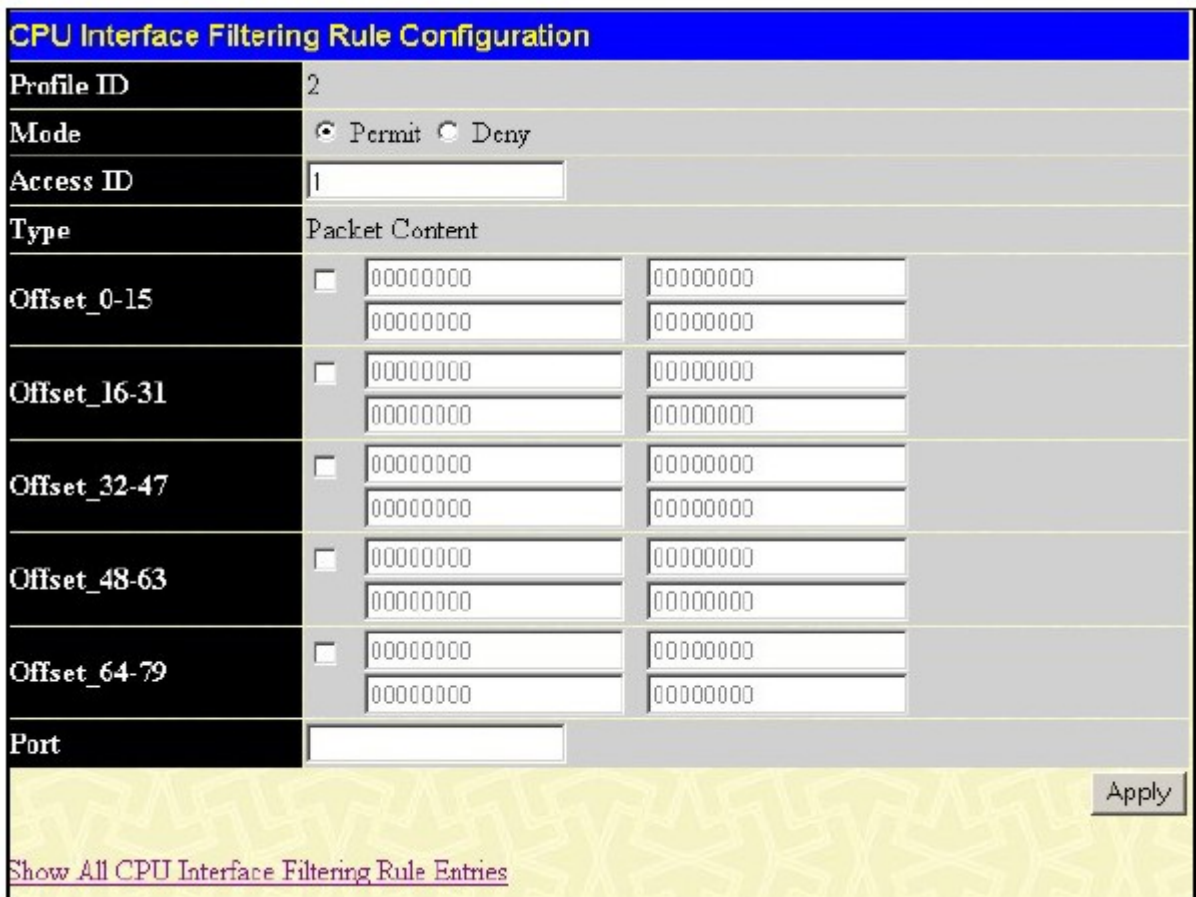



Рисунок 9.14 – Окно «CPU Interface Filtering Rule Configuration - Packet Content»

Чтобы установить правило доступа для содержимого пакетов, введите 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 5.
Type	Выберите, какой профиль доступа будете использовать: на основе Ethernet (MAC-адрес), IP-адрес или маску содержимого пакета. В этом поле осуществляется переключение между окнами соответствующих профилей. <input type="checkbox"/> При выборе <i>Ethernet</i> коммутатор будет проверять заголовок каждого пакета на 2 уровне. <input type="checkbox"/> При выборе <i>IP</i> коммутатор будет проверять IP-адрес в заголовке каждого пакета. <input type="checkbox"/> Для скрытия данных заголовка пакета установите маску содержимого пакета <i>Packet Content Mask</i> .
Offset	Это поле указывает, что необходимо сравнить начало заголовка пакета с указанным значением: <input type="checkbox"/> value (0-15) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить первые 15 байт пакета. <input type="checkbox"/> value (16-31) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 16 по 31 байт пакета. <input type="checkbox"/> value (32-47) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 32 по 47 байт пакета. <input type="checkbox"/> value (48-63) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 48 по 63 байт пакета. <input type="checkbox"/> value (64-79) - Введите значение в шестнадцатеричной системе счисления, с которым нужно сравнить с 64 по 79 байт пакета.
Port	Правило доступа может быть установлено на базе портов путем введения номера порта коммутатора в этом поле. Введение значения all назначит данное правило для всех портов коммутатора.

Для просмотра ранее настроенного правила нажмите  в таблице Access Rule Table.

CPU Interface Filtering Rule Display	
Profile ID	2
Access ID	3
Mode	Permit
Type	Packet Content
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	-----
Offset 32-47	-----
Offset 48-63	-----
Offset 64-79	-----
Activate State	Enabled
Port	8
Show All CPU Interface Filtering Rule Entries	

Рисунок 9.15 – Окно «CPU Interface Filtering Rule Display – Packet Content»

Раздел 10 - Безопасность

Traffic Control (Управление трафиком)

Port Security

Port Lock Entries

802.1X

Trusted Host (Доверенный хост)

Traffic Segmentation (сегментация трафика)

Следующий раздел будет полезен пользователю при установке функций безопасности на коммутаторе. На коммутаторе предусмотрены различные функции безопасности, включая управление трафиком, Port Security, 802.1x, доверенный хост и сегментация трафика. Все они подробно будут рассмотрены ниже.

Управление трафиком

Используйте меню Traffic Control для подключения, отключения функции управления широкоэвещательным штормом, а также для настройки пороговых значений для

широковещательных и многоадресных штормов, таких как **DLF (Destination Look Up Failure)**. Настройки управления трафиком применимы к отдельным модулям коммутатора. Для просмотра следующего окна нажмите **Security** **Traffic Control**:

Traffic Control Settings						
From	To	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold	Apply
Port 1	Port 1	Disabled	Disabled	Disabled	128	Apply

Traffic Control Table				
Port	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold (Kbit/sec)
1	Disabled	Disabled	Disabled	64
2	Disabled	Disabled	Disabled	64
3	Disabled	Disabled	Disabled	64
4	Disabled	Disabled	Disabled	64
5	Disabled	Disabled	Disabled	64
6	Disabled	Disabled	Disabled	64
7	Disabled	Disabled	Disabled	64
8	Disabled	Disabled	Disabled	64
9	Disabled	Disabled	Disabled	64
10	Disabled	Disabled	Disabled	64
11	Disabled	Disabled	Disabled	64
12	Disabled	Disabled	Disabled	64
13	Disabled	Disabled	Disabled	64
14	Disabled	Disabled	Disabled	64
15	Disabled	Disabled	Disabled	64
16	Disabled	Disabled	Disabled	64
17	Disabled	Disabled	Disabled	64
18	Disabled	Disabled	Disabled	64

Рисунок 10.1– Окно « Traffic Control Settings and Traffic Control Table»

Для настройки **Traffic Control**, выберите сначала группу портов, используя выпадающее меню **Group**. Далее включите или выключите **Broadcast Storm**, **Multicast Storm** и **Destination Unknown**, используя соответствующие выпадающие меню.

Цель этой функции исключить слишком большое количество широковещательных, многоадресных пакетов, а также пакетов от неизвестных источников, которые переполняют сеть. Каждый порт имеет счетчик, который отсчитывает количество пакетов широковещательного трафика, получаемого в секунду. Каждую секунду этот счетчик обнуляется. При подключенной функции управления широковещательным, многоадресным штормом, а также сообщениями от неизвестных пользователей, порт будет отбрасывать указанные пакеты, когда значения счетчика будет эквивалентно или превысит указанный порог.

Значение **Threshold** (порог) – верхнее пороговое значение, при котором подключается функция управления трафиком. Иными словами, это то количество широковещательного, многоадресного и DLF-трафика, в кбит/с, при получении которого будет подключаться функция управления штормом-

трафиком. Значение **Threshold** может принимать значения от 64 до 1024000кбит в секунду, значение по умолчанию равно 64. Настройки для каждого порта могут быть просмотрены в том же окне в таблице **Traffic Control Table**. Нажмите **Apply** для принятия сделанных изменений.

Port Security

Динамическое изучение MAC-адресов для заданных портов (или диапазона портов) может быть заблокировано таким образом, 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* и нажать на **Apply**, тем самым закрыв порт.

Port Security – функция безопасности, которая предотвращает подключение к заблокированным портам коммутатора неавторизованных хостов (с MAC-адресами источников, не заданными как разрешенные для этого порта) и получения ими доступа к сети.

Для просмотра следующего окна, откройте папку **Security** и нажмите **Port Security**.

Port Security Settings					
From	To	Admin State	Max.Addr(0-10)	Lock Address Mode	Apply
Port 1	Port 1	Disabled	0	Permanent	Apply

Port Security Table			
Port	Admin State	Max.Learning Addr	Lock Address Mode
1	Disabled	1	Delete OnReset
2	Disabled	1	Delete OnReset
3	Disabled	1	Delete OnReset
4	Disabled	1	Delete OnReset
5	Disabled	1	Delete OnReset
6	Disabled	1	Delete OnReset
7	Disabled	1	Delete OnReset
8	Disabled	1	Delete OnReset
9	Disabled	1	Delete OnReset
10	Disabled	1	Delete OnReset
11	Disabled	1	Delete OnReset
12	Disabled	1	Delete OnReset
13	Disabled	1	Delete OnReset
14	Disabled	1	Delete OnReset
15	Disabled	1	Delete OnReset
16	Disabled	1	Delete OnReset

Рисунок 10- 2. Port Security Settings окно

Следующие параметры могут быть установлены:

Port Security Settings					
From	To	Admin State	Max.Addr (0-16)	Mode	Apply
Port1	Port1	Disabled	0	Delete OnReset	Apply

Port Security Table			
Port	Admin State	Max.Learning Addr	Lock Address Mode
1	Disabled	1	Delete OnReset
2	Disabled	1	Delete OnReset
3	Disabled	1	Delete OnReset
4	Disabled	1	Delete OnReset
5	Disabled	1	Delete OnReset
6	Disabled	1	Delete OnReset
7	Disabled	1	Delete OnReset
8	Disabled	1	Delete OnReset
9	Disabled	1	Delete OnReset
10	Disabled	1	Delete OnReset
11	Disabled	1	Delete OnReset
12	Disabled	1	Delete OnReset
13	Disabled	1	Delete OnReset
14	Disabled	1	Delete OnReset
15	Disabled	1	Delete OnReset
16	Disabled	1	Delete OnReset
17	Disabled	1	Delete OnReset
18	Disabled	1	Delete OnReset
19	Disabled	1	Delete OnReset
20	Disabled	1	Delete OnReset
21	Disabled	1	Delete OnReset
22	Disabled	1	Delete OnReset
23	Disabled	1	Delete OnReset
24	Disabled	1	Delete OnReset
25	Disabled	1	Delete OnReset
26	Disabled	1	Delete OnReset
27	Disabled	1	Delete OnReset
28	Disabled	1	Delete OnReset

From/To	Последовательная группа портов, которая начинается с отмеченного порта.
Admin State	Данное выпадающее меню позволяет включить/выключить функцию Port Security (закрывает таблицу MAC-адресов для выбранного 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: <i>Permanent</i> – закрытые адреса не будут устаревать после истечения таймера. <i>DeleteOnTimeout</i> – закрытые адреса будут устаревать после истечения таймера. <i>DeleteOnReset</i> – закрытые адреса не будут устаревать до тех пор, пока Коммутатор не будет перегружен.

Для принятия настроек нажмите **Apply**.



Примечание: Порты uplink-модулей (порты 9,10 для DES-3010F/FL/G, порты 17,18 для DES-3018, порты 25,26 для DES-3026) не поддерживают функцию port security.

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**:

Port Lock Entries Table					
VID	VLAN Name	MAC Address	Port	Type	Delete
1	default	00-08-02-0b-85-d2	2	Permanent	<input type="checkbox"/>
1	default	00-08-02-54-10-0a	2	Permanent	<input type="checkbox"/>
1	default	00-0c-6e-12-e1-1a	2	Permanent	<input type="checkbox"/>
1	default	00-50-8d-36-94-98	2	Permanent	<input type="checkbox"/>
1	default	00-50-ba-00-06-03	2	Permanent	<input type="checkbox"/>
1	default	00-50-ba-da-00-22	2	Permanent	<input type="checkbox"/>
1	default	00-e0-18-72-0d-e6	2	Permanent	<input type="checkbox"/>

Рисунок 10.3. Port Lock Entries Table

Эта функция применима только в том случае, если поле **Mode** в окне **Port Security** 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 VLAN записи 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 <i>Secured Permanent</i> , могут быть удалены.
Delete	Нажмите значок «x» в этом поле, чтобы удалить соответствующий MAC-адрес, который был постоянно изучен коммутатором

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 клиент-сервер. Такая модель работает на основе сервера RADIUS, 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.

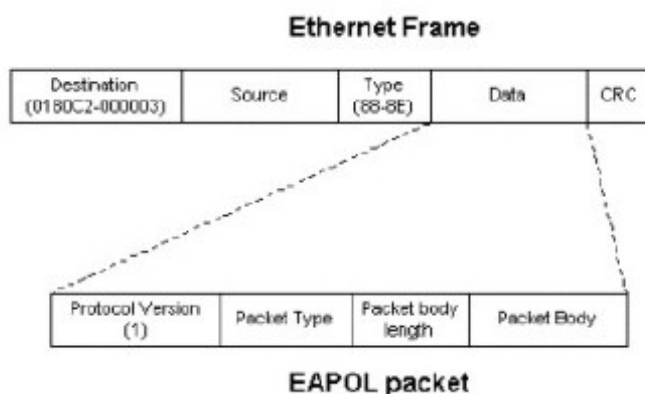


Рисунок 10.4 – Структура пакета EAPOL

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 компонента, каждая из которых крайне важна для создания и использования устойчивого безопасного метода доступа к локальной сети.

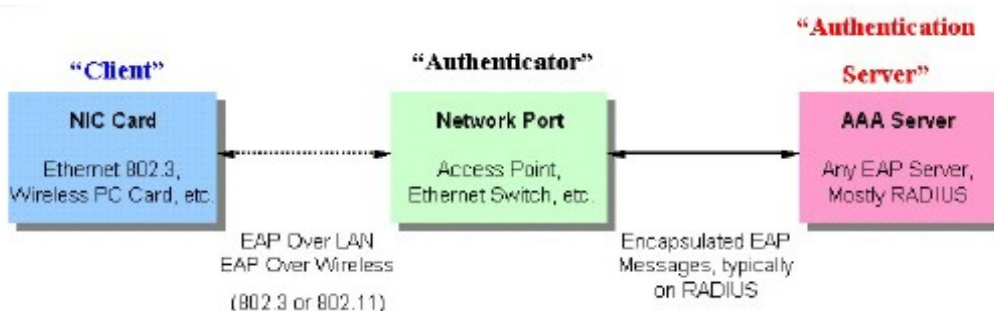


Рисунок 10.5– Три функции протокола 802.1x

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), обслуживаемые сервером RADIUS 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 сервером RADIUS и клиентом с помощью пакетов EAPOL, и информировать коммутатор, предоставлять или нет доступ к локальной сети и/или сервисам коммутатора.

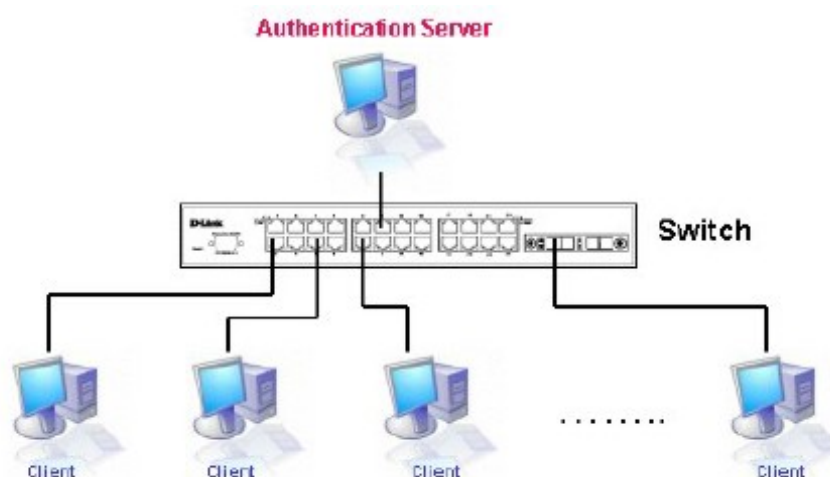


Рисунок 10.6 – Сервер аутентификации

Аутентификатор (Authenticator)

Коммутатор, который является аутентификатором, играет 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-3000 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**).

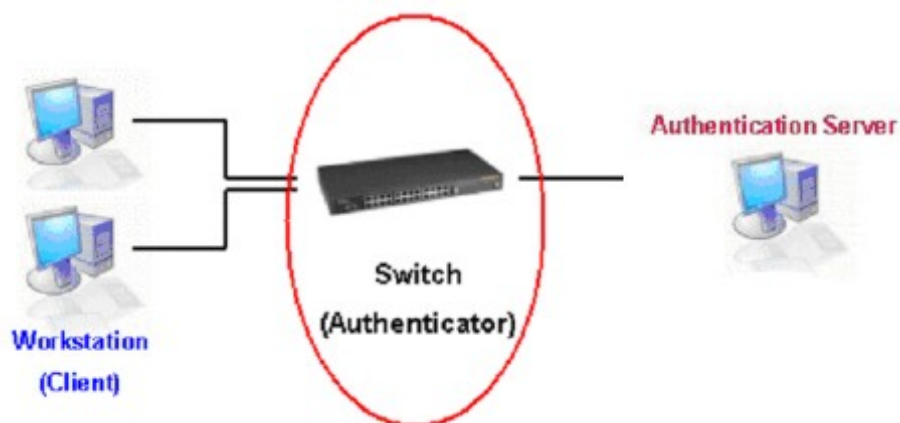


Рисунок 10.7 – Аутентификатор

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 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.

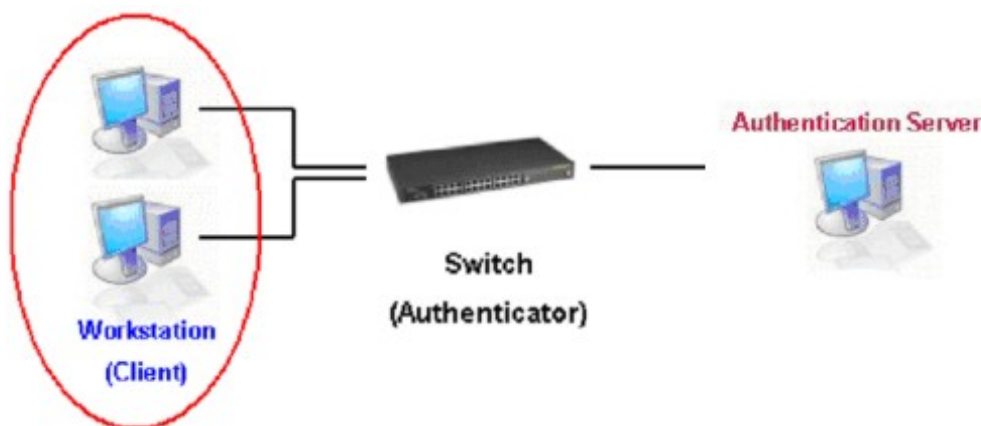


Рисунок 10.8 - Клиент

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.

802.1X Authentication process

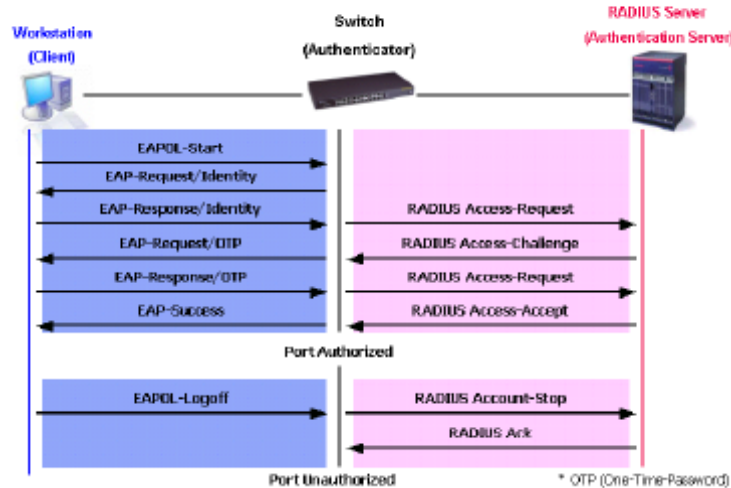


Рисунок 10.9 – Процесс аутентификации 802.1x

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

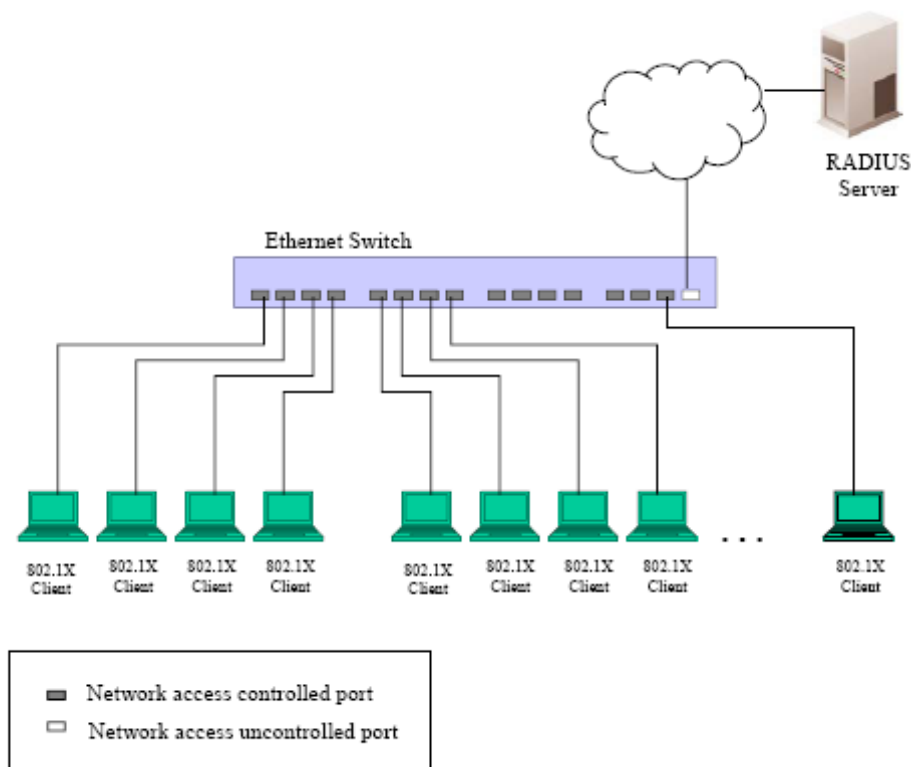


Рисунок 10.10 – Пример конфигурации сети на основе портов

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, повлияющее на смену 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 в данном случае обеспечиваемая безопасность минимальна, и подключение открыто для атак.

Аутентификация на основе MAC-адресов

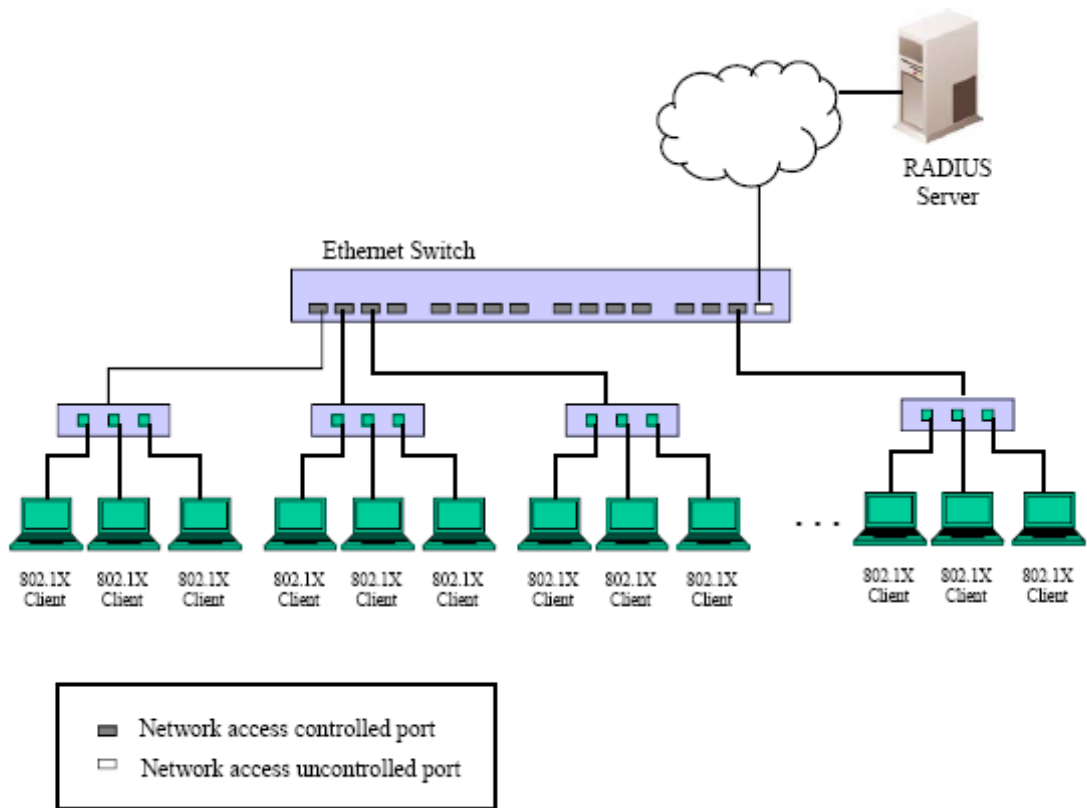


Рисунок 10.11 - Пример конфигурации сети на основе MAC-адресов

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 каждого логического порта 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.**

802.1X Authenticator Settings									
Port	AdmDir	Ctrl Stat	TxPeriod	Quiet Period	Supp- Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	auto	30	60	30	30	2	3600	no
2	both	auto	30	60	30	30	2	3600	no
3	both	auto	30	60	30	30	2	3600	no
4	both	auto	30	60	30	30	2	3600	no
5	both	auto	30	60	30	30	2	3600	no
6	both	auto	30	60	30	30	2	3600	no
7	both	auto	30	60	30	30	2	3600	no
8	both	auto	30	60	30	30	2	3600	no
9	both	auto	30	60	30	30	2	3600	no
10	both	auto	30	60	30	30	2	3600	no
11	both	auto	30	60	30	30	2	3600	no
12	both	auto	30	60	30	30	2	3600	no
13	both	auto	30	60	30	30	2	3600	no
14	both	auto	30	60	30	30	2	3600	no
15	both	auto	30	60	30	30	2	3600	no
16	both	auto	30	60	30	30	2	3600	no
17	both	auto	30	60	30	30	2	3600	no
18	both	auto	30	60	30	30	2	3600	no

Рисунок 10.12 – Окно «802.1X Authenticator Settings»

Для выполнения настроек на порту, нажмите гиперссылку номера необходимого порта под заголовком «Port», после чего отобразится следующая таблица:

802.1X Authenticator Settings	
From	Port 1 ▾
To	Port 1 ▾
AdmDir	both ▾
PortControl	auto ▾
TxPeriod	30
QuietPeriod	60
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled ▾
Show Authenticators Setting Apply	

Рисунок 10.13 – Окно «802.1X Authenticator Settings - Modify»

Данное окно позволит вам произвести следующие настройки:

Параметр	Описание
From [] To []	Введите один порт или диапазон портов.
AdmCtrlDir	В данном поле Вы можете выбрать вид трафика, подлежащего контролю. Если выбрано <i>in</i> , то будет производиться контроль входящего трафика через выбранные Вами в первом поле порты. Если выбрано <i>both</i> , то будет производиться контроль как входящего, так и исходящего трафика, через выбранные вами в первом поле порты.
Port Control	Данная настройка позволит контролировать состояние авторизации порта. <i>forceAuthorized</i> – 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. <i>forceUnauthorized</i> – порт будет находиться в неавторизованном состоянии, игнорируя все попытки клиента аутентифицироваться. Коммутатор не сможет произвести аутентификацию клиента через данный интерфейс. <i>Auto</i> – 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 <i>Auto</i> .
TxPeriod	Данное значение определяет период времени, который отводится для передачи пакетов запроса/идентификации (EAP Request/Identity) клиенту. По умолчанию данный параметр равен 30 секундам.

QuietPeriod	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 секундам.
SuppTimeout	Время обмена информацией между аутентификатором и клиентом. По умолчанию данный параметр равен 30 секундам.
ServerTimeout	Время обмена информацией между аутентификатором и сервером аутентификации. По умолчанию данный параметр равен 30 секундам.
MaxReq	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	Время ожидания (в секундах) перед повторной аутентификацией клиента. По умолчанию данный параметр равен 3600 секундам.
ReAuth	В данном поле определяется возможность повторной аутентификации с заданным периодом времени на данном порту. По умолчанию данная настройка отключена <i>Disabled</i> .

Для того чтобы настройки вступили в силу, нажмите **Apply**. Для просмотра конфигураций для **802.1X Authentication Settings** на базе порта, обращайтесь к таблице **802.1X Authentication Settings**.

Локальные пользователи

Для настройки локальных пользователей для 802.1X нажмите Security > 802.1X > Local Users. Это окно позволяет настроить локальных пользователей 802.1X на коммутаторе.

The screenshot shows the '802.1x Local User Table Configuration' window. At the top, there is a blue header with the title. Below it, there are three input fields for 'User Name', 'Password', and 'Confirm Password'. To the right of these fields is an 'Apply' button. Below the input fields, it says 'Total Entries: 2'. Underneath is another blue header for '802.1x Local User Table'. Below this header is a table with three columns: 'Index', 'User Name', and 'Delete'. The table contains two rows: the first row has '1' in the Index column, 'Darren' in the User Name column, and a delete icon (an 'X' in a box) in the Delete column; the second row has '2' in the Index column, 'Trinity' in the User Name column, and a delete icon in the Delete column.

802.1x Local User Table Configuration		
User Name	Password	Confirm Password
<input type="text"/>	<input type="text"/>	<input type="text"/>
		Apply
Total Entries: 2		
802.1x Local User Table		
Index	User Name	Delete
1	Darren	<input type="checkbox"/>
2	Trinity	<input type="checkbox"/>

Рисунок 10.14. Окно 802.1x Local User Table Configuration and 802.1x Local User Table

Введите имя пользователя User Name, пароль Password и подтверждение этого пароля. Установленные должным образом локальные пользователи будут отображены в том же окне в таблице **802.1x Local User Table**.

Port Capability

Нажмите Security > 802.1X > 802.1X Capability Settings, чтобы открыть следующее окно:

802.1X Capability Settings			
From	To	Capability	Apply
Port 1	Port 1	None	Apply

802.1X Capability Table	
Port	Capability
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None
14	None
15	None
16	None
17	None
18	None

Рисунок 10.15. 802.1x Capability Settings and Table окно

Для установки на коммутаторе 802.1x аутентификации на базе портов, выберите соответствующие порты в полях **From** и **To**. Далее подключите эти порты, выбрав *Authenticator* в выпадающем меню поля **Capability**. Нажмите **Apply**, чтобы изменения вступили в силу.

Установите следующие настройки 802.1x:

Параметр	Описание
From и To	Порты, настраиваемые для 802.1x
Capability	Возможны следующие варианты: <i>Authenticator</i> – Пользователь должен пройти процесс аутентификации для получения доступа к сети <i>None</i> – порт не будет находиться под контролем функций 802.1x

Инициализация портов для 802.1x на базе портов

Существующие настройки порта 802.1x и MAC отображаются и могут быть настроены при помощи показанного ниже окна.

Нажмите **Security > 802.1X > Initialize Ports**, чтобы увидеть следующее окно:

Initialize Port				
From	To	Apply		
Port 1 ▾	Port 1 ▾	Apply		
Initialize Port Table				
Port	Auth PAE State	Backend_State	Oper Dir	PortStatus
1	ForceAuth	Success	both	Authorized
2	ForceAuth	Success	both	Authorized
3	ForceAuth	Success	both	Authorized
4	ForceAuth	Success	both	Authorized
5	ForceAuth	Success	both	Authorized
6	ForceAuth	Success	both	Authorized
7	ForceAuth	Success	both	Authorized
8	ForceAuth	Success	both	Authorized
9	ForceAuth	Success	both	Authorized
10	ForceAuth	Success	both	Authorized

Рисунок 10.16. Initialize Port окно

Это окно позволит инициализировать порт или группу портов. Таблица **Initialize Port Table** в верхней половине окна отображает текущий статус порта (-ов).

Это окно отображает следующую информацию:

Параметр	Описание
From and To	Выберите порты для инициализации.
Port	Поле доступно только для чтения и отображает порт на коммутаторе.
MAC Address	MAC-адрес коммутатора, подключенного к соответствующему порту, если это имеет место.
Auth PAE State	Authenticator PAE State будет отображать одно из следующих значений: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth</i> или <i>ForceUnauth</i> .
Backend State	Это поле может принимать одно из следующих значений: <i>Request, Response, Success, Fail, Timeout, Idle</i> или <i>Initialize</i>.
Open Dir	Возможны следующие значения этого поля: <i>both</i> и <i>in</i>.
Port Status	Состояние порта может быть <i>Authorized</i> или <i>Unauthorized</i>.

Инициализация портов для 802.1x на базе MAC-адресов

Для инициализации портов для 802.1x на базе MAC-адресов, пользователю необходимо изначально подключить 802.1x на базе MAC-адреса в окне **Advanced Settings**. Нажмите **Security > 802.1X > 802.1X Initialize Ports**, чтобы увидеть следующее окно:

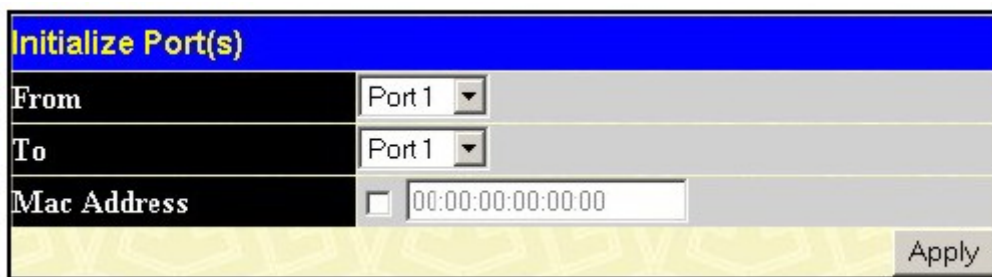


Рисунок 10.17. Initialize Ports (802.1x на основе MAC-адресов)

Для инициализации портов сначала выберите диапазон портов в поле **From** и **To**. Затем пользователю необходимо определить MAC-адрес для инициализации, введя его в поле **MAC Address** и отметив соответствующее окошко. Для инициализации, нажмите **Apply**.



Примечание: Пользователю необходимо глобально подключить 802.1X в окне **DES-3018 Web Management Tool** перед повторной аутентификацией портов. Информация в таблице **Initialize Ports Table** может быть просмотрена только после подключения 802.1X.



Примечание: Порты uplink-модулей (DES-3010F/FL/G порты 9-10, DES-3018 порты 17-18, DES-3026 порты 25-26) не поддерживают функции 802.1X.

Повторная аутентификация порта(-ов) для 802.1x на базе портов

Это окно позволяет повторно аутентифицировать порт или группу портов, выбор которых осуществляется с помощью выпадающих меню **From** и **To** и нажатия **Apply**. Таблица **Reauthenticate Port Table** отображает текущее состояние повторно аутентифицированного порта(-ов), после того, как была нажата кнопка **Apply**.

Нажмите **Security > 802.1X > Reauthenticate Port(s)**, чтобы увидеть следующее окно:

Reauthenticate Port				
From	To	Apply		
Port 1	Port 1	Apply		
Reauthenticate Port Table				
Port	Auth State	BackendState	OperDir	PortStatus
1	ForceAuth	Success	both	Authorized
2	ForceAuth	Success	both	Authorized
3	ForceAuth	Success	both	Authorized
4	ForceAuth	Success	both	Authorized
5	ForceAuth	Success	both	Authorized
6	ForceAuth	Success	both	Authorized
7	ForceAuth	Success	both	Authorized
8	ForceAuth	Success	both	Authorized
9	ForceAuth	Success	both	Authorized
10	ForceAuth	Success	both	Authorized

Рисунок 10.18. Reauthenticate Port and Reauthenticate Port Table окно

Это окно содержит следующую информацию:

Параметр	Описание
Port	Отображает номер повторно аутентифицируемого порта на коммутаторе.
MAC Address	Отображает физический адрес порта коммутатора .
Auth PAE State	Authenticator PAE State будет отображать одно из следующих значений: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth</i> или <i>ForceUnauth</i> .
Backend State	Это поле может принимать одно из следующих значений: <i>Request, Response, Success, Fail, Timeout, Idle</i> или <i>Initialize</i> .
Open Dir	Возможны следующие значения этого поля <i>both</i> и <i>in</i> .
Port Status	Состояние порта может быть <i>Authorized</i> или <i>Unauthorized</i> .



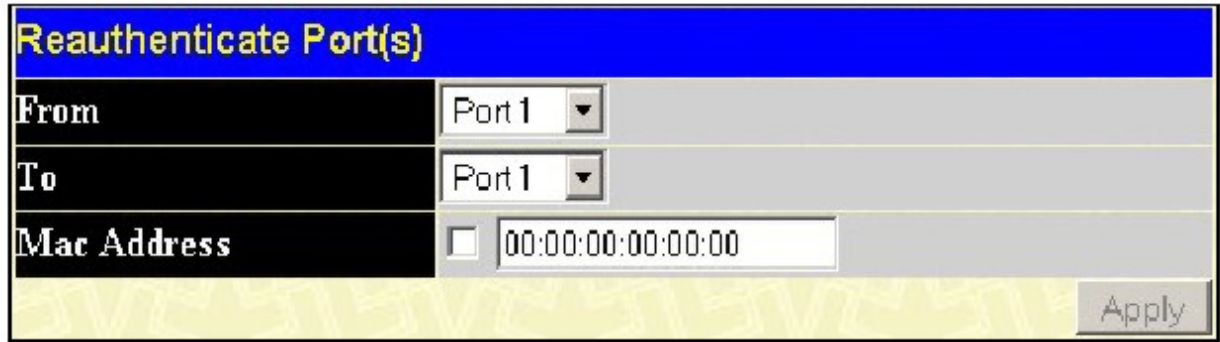
Примечание: Пользователь должен глобально подключить 802.1X в окне **DES-3018 Web Management Tool** перед повторной аутентификацией портов. Информация в таблице **Reauthenticate Ports Table** не может быть просмотрена до подключения 802.1X.



Примечание: uplink-порты модулей (DES-3010F/FL/G порты 9-10, DES-3018 порты 17-18, DES-3026 порты 25-26) не поддерживают функции 802.1X.

Повторная аутентификация порта (-ов) 802.1x на базе портов

Для повторной аутентификации портов 802.1x на базе MAC-адресов, необходимо изначально подключить 802.1x на базе MAC-адресов в окне **Advanced Settings**. Нажмите **Security > 802.1X > Reauthenticate Port(s)**, чтобы увидеть следующее окно:



Reauthenticate Port(s)	
From	Port 1
To	Port 1
Mac Address	<input type="checkbox"/> 00:00:00:00:00:00
<input type="button" value="Apply"/>	

Рисунок 10.19. Reauthenticate Ports –аутентификация 802.1x на основе MAC-адресов

Для повторной аутентификации портов, сначала выберите диапазон портов в поле **From** and **To**. Затем пользователю необходимо определить MAC-адрес для повторной аутентификации, введя его в поле **MAC Address** и отметив соответствующее окошко. Для повторной аутентификации, нажмите **Apply**.

Сервер RADIUS

Функция RADIUS на коммутаторе позволяет облегчить централизованное пользовательское администрирование, предоставляя при этом защиту от несанкционированного прослушивания сети. Для произведения настроек предусмотрено три окна. Для открытия окна «**Authentic RADIUS Server**» нажмите **Security** **802.1x** **Authentic Radius Server**.

Authentic Radius Server Setting					
Succession	First <input type="button" value="v"/>				
Radius Server	0.0.0.0				
Authentic Port	1812				
Accounting Port	1813				
Key	<input type="text"/>				
Confirm Key	<input type="text"/>				
Status	Valid <input type="button" value="v"/>				
<input type="button" value="Apply"/>					
Current Radius Server(s) Settings Table					
Succession	Radius Server	Auth UDP Port	Acct UDP Port	Key	Status
First					
Second					
Third					

Рисунок 10.20 – Окно « Authentic RADIUS Server and Current RADIUS Server Settings Table »

В окне отображается следующая информация:

Параметр	Описание
Succession	Выберите необходимый для настройки сервер RADIUS: <i>First</i> , <i>Second</i> или <i>Third</i> (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 сервера (ов) RADIUS, содержащего информацию об учетных записях пользователей. По умолчанию – это порт 1813.
Key	Введите ключ, идентичный тому, который вы вводили на сервере RADIUS.
Confirm Key	Подтвердите ввод ключа, идентичный тому, который вы вводили на RADIUS сервере.
Status	Данное поле позволяет включать (<i>Valid</i>) и отключать (<i>Invalid</i>) сервер RADIUS.

Trusted Host (Доверенный хост)

Для открытия приведенного ниже окна нажмите Security Trusted Host.

Security IP Management		
IP1 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP2 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP3 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP4 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP5 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP6 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP7 Access to Switch	<input type="text" value="0.0.0.0"/>	
IP8 Access to Switch	<input type="text" value="0.0.0.0"/>	

Note: Create a list of IP Addresses that can access the switch. Your local host IP Address must be one of the IP Addresses to avoid disconnection.

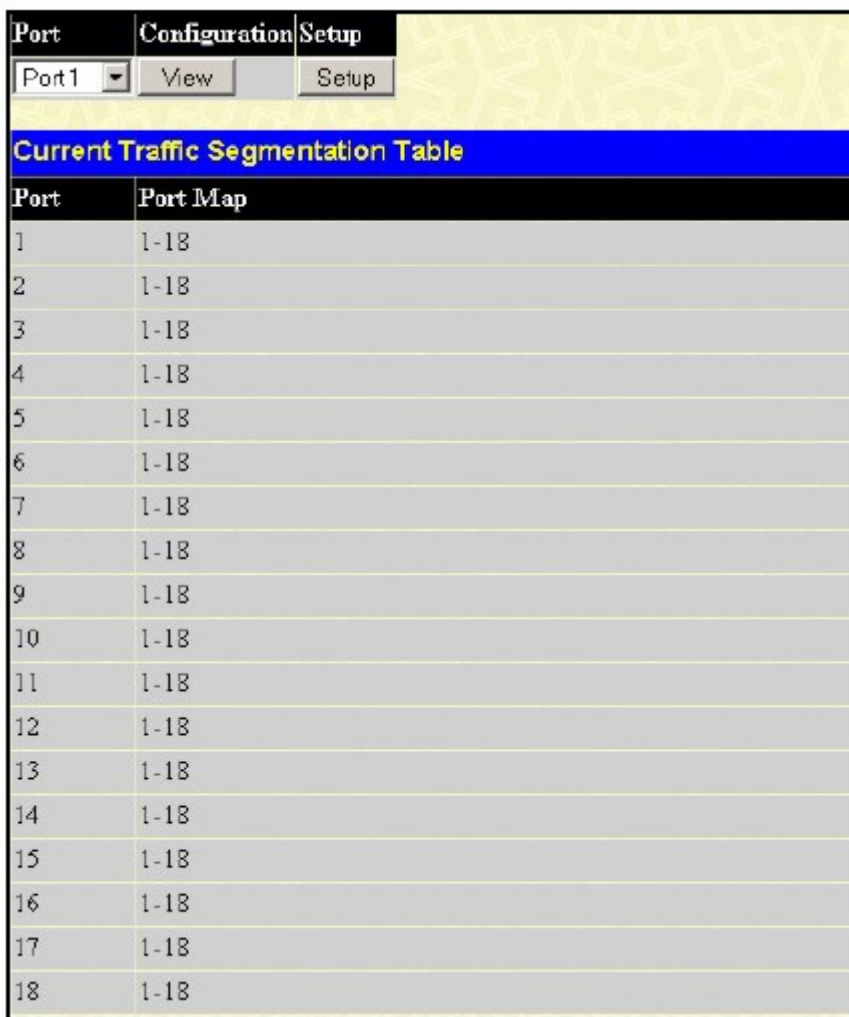
Рисунок 10.21 – Окно « Security IP Management»

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**.

Сегментация трафика

Сегментация трафика используется для ограничения трафика от единичного порта к группе портов одного коммутатора (в отдельно взятом случае) или к группе портов на другом коммутаторе в стеке (Single IP).

Этот метод сегментации трафика подходит для ограничения трафика в VLANs, но используется с некоторыми ограничениями. Этот метод заключается в направлении трафика, который не превышает порог Master switch CPU. Для просмотра окна, представленного ниже, нажмите Security Traffic Segmentation:



Port	Configuration	Setup
Port1	View	Setup
Current Traffic Segmentation Table		
Port	Port Map	
1	1-18	
2	1-18	
3	1-18	
4	1-18	
5	1-18	
6	1-18	
7	1-18	
8	1-18	
9	1-18	
10	1-18	
11	1-18	
12	1-18	
13	1-18	
14	1-18	
15	1-18	
16	1-18	
17	1-18	
18	1-18	

Рисунок 10.22 – Окно «Current Traffic Segmentation Table»

Нажмите кнопку **Setup**, чтобы открыть страницу Setup Forwarding ports, как показано ниже.



Рисунок 10.23 – Окно «Setup Forwarding Ports»

Эта страница позволяет определить, какому порту данного коммутатора в стеке будет разрешено пересылать пакеты на другие порты данного коммутатора.

Установка функции сегментации трафика на коммутаторе состоит из двух частей. Во-первых, Вы определяете порт на этом коммутаторе, используя выпадающее меню **Port**. Затем определяете другие порты, которые будут способны получать пакеты от порта, указанного в первой части.

После нажатия кнопки **Apply** будет установлено соответствие передающего порта и портов, которым разрешено принимать информацию с этого порта, в таблице **Traffic Segmentation**.

Выпадающее меню **Port** позволяет выбрать порт этого коммутатора. Это порт, который будет передавать пакеты.

Forward Port позволяет выбрать, какие из портов данного коммутатора будет иметь возможность пересылать пакеты. Эти порты смогут получать пакеты от порта, определенного выше.

Нажмите **Apply** для введения настроек в таблицу **Traffic Segmentation**.

После нажатия на кнопку **Apply**, комбинация передающего и принимающих портов будет занесена в таблицу **Current Traffic Segmentation Table (Текущую таблицу сегментации трафика)**.

Раздел 12 – Мониторинг

Использование CPU

Использование порта

Пакеты

Ошибки при передаче пакетов

Размер пакетов

MAC-адрес

Журнал коммутатора

Настройки журнала

Группа IGMP Snooping

Поиск порта маршрутизатора

Поиск таблицы ARP

Session Table

Контроль доступа по портам

Использование CPU

Окно «CPU Utilization» отображает процентное соотношение использования центрального процессора, выраженное в виде целого числа и вычисляемое как среднее значение временных интервалов. Для просмотра данного окна нажмите: **Monitoring** **CPU Utilization**.

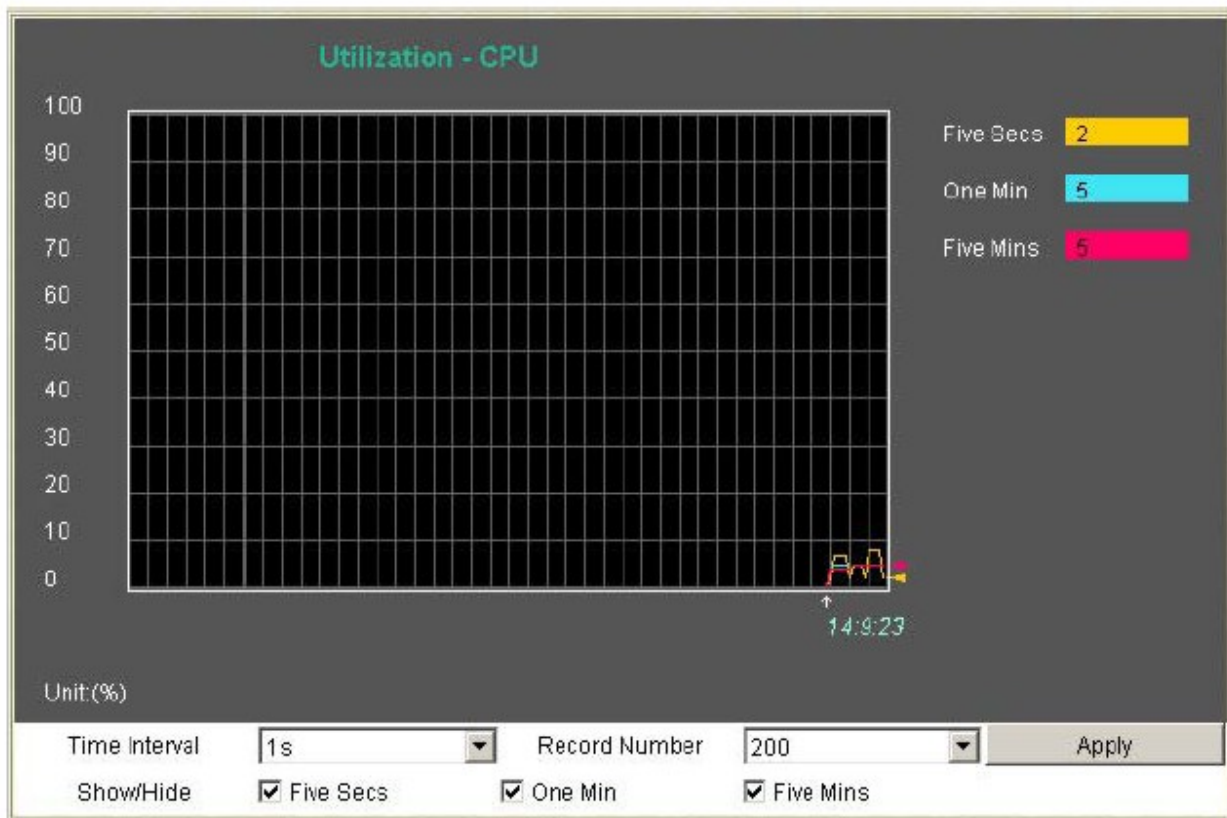


Рисунок 11.1 – Окно CPU Utilization

Для просмотра использования CPU на порт, используйте график в реальном масштабе времени в верхней части Web-страницы путем простого нажатия на этот порт. Нажмите **Apply** для того, чтобы настройки вступили в силу. Окно автоматически обновит статистику по параметрам, описанным ниже:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1сек.
Record Number	Выберите количество раз опроса коммутатора от 20 до 200. Данное значение по умолчанию равно 200.
Utilization	Отметьте, нужно ли отображать процентное использование процессора или нет.

Использование порта

Окно «Port Utilization» отображает процентное соотношение общей доступной полосы пропускания к полосе, приходящейся на порт. Для просмотра процентного соотношения использования портов, откройте: **Monitoring** □ **Port Utilization**.

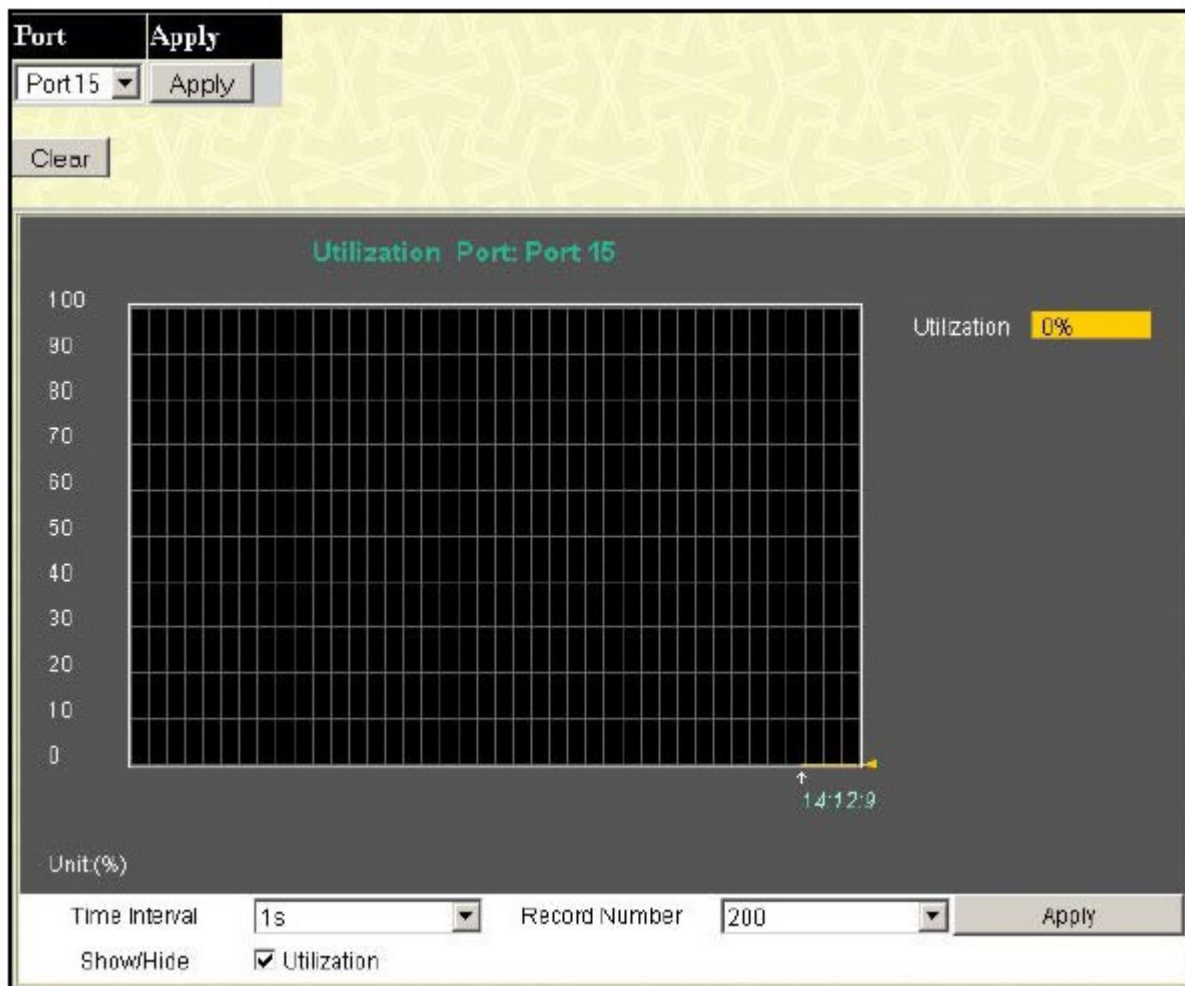


Рисунок 11.2 – Окно «Utilization Port»

Выберите единицу измерения и номер порта в выпадающем меню и нажмите **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 1сек.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 200.

Нажмите **Clear** для очистки поля. Нажмите **Apply** для того, чтобы изменения вступили в силу.

Пакеты

Web-менеджер позволяет просматривать различные статистики по пакетам, как в графическом виде, так и в виде таблицы. Вашему вниманию предлагается шесть окон.

Received (RX) (Полученные пакеты))

Для просмотра следующего графика по пакетам, полученным коммутатором, нажмите: **Monitoring** \square **Packets** \square **Received (RX)**. Из выпадающего меню выберите номер порта и нажмите **Apply** для отображения статистики по полученным пакетам на выбранном порту. Пользователь может также применять график в реальном масштабе времени, отображаемый в верху Web-страницы путем простого нажатия на порт.

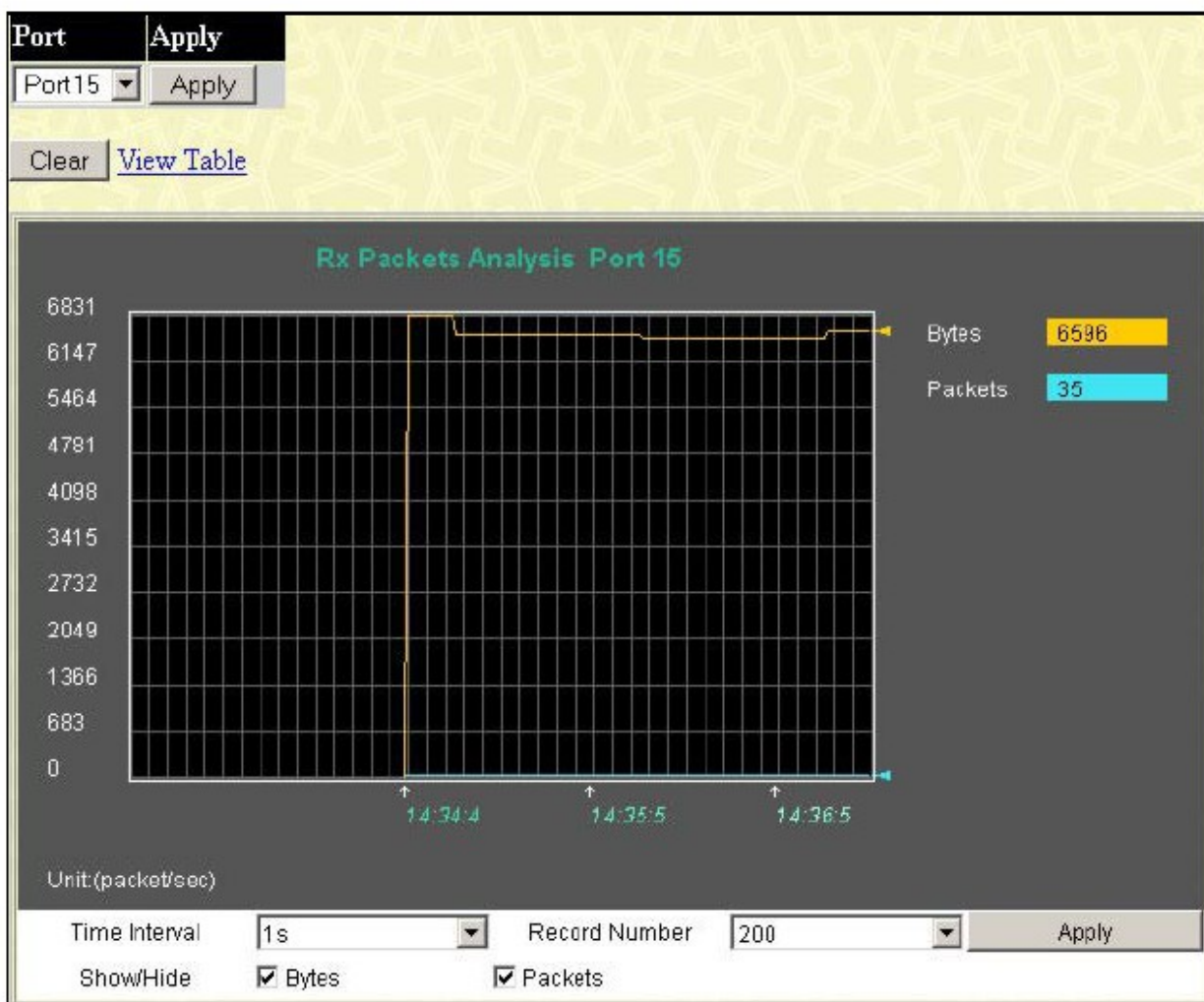


Рисунок 11.3 – Окно «Rx Packets Analysis» (график зависимости количества байт от количества переданных пакетов)

Для просмотра таблицы **Received Packets Table**, нажмите [View Table](#):

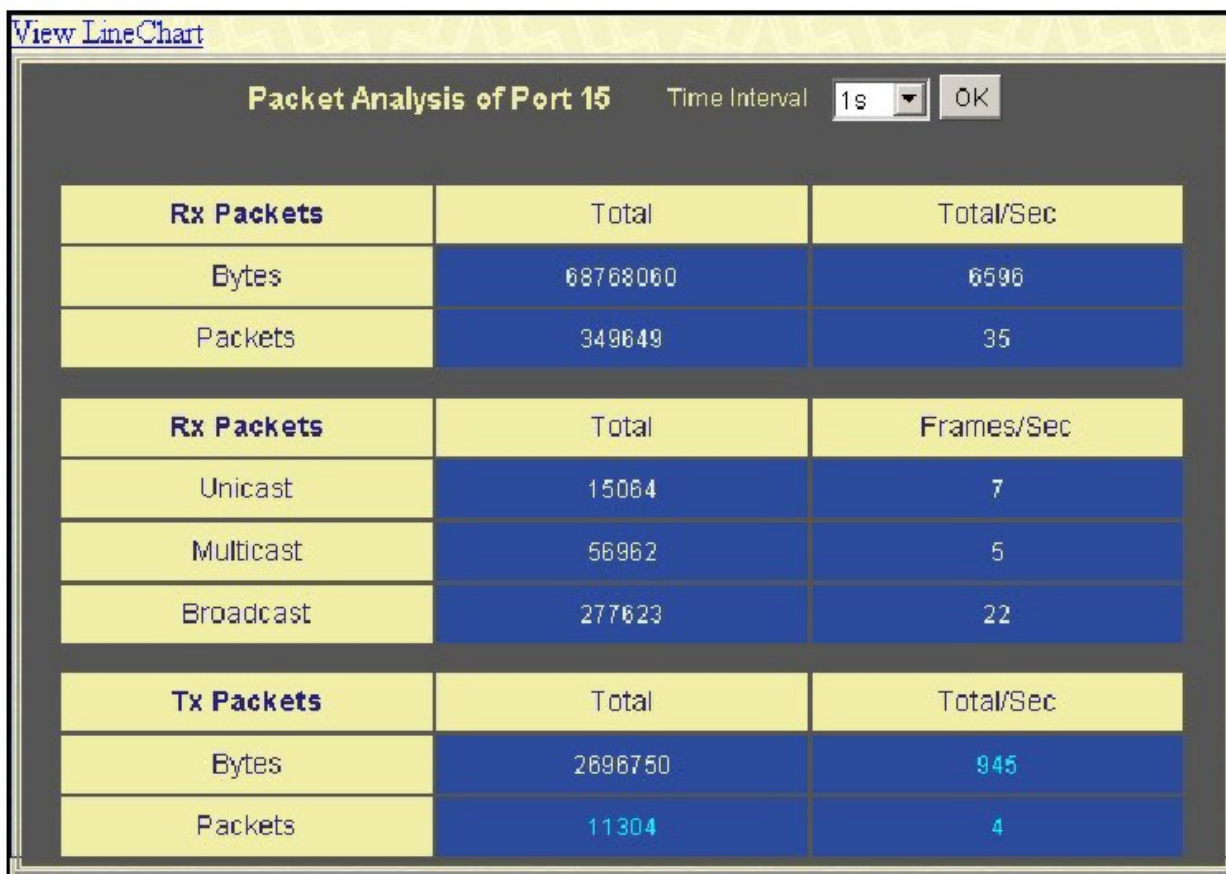


Рисунок 11.4 – Окно «Rx Packets Analysis» (таблица зависимости количества байт от количества переданных пакетов)

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 1сек.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 200.
Bytes	Показывает число байт, полученных на порту.
Packets	Показывает число пакетов, полученных на порту.
Unicast	Показывает число неискаженных одноадресных пакетов.
Multicast	Показывает число неискаженных многоадресных пакетов.
Broadcast	Показывает число неискаженных широковещательных пакетов.
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)**. Пользователь может также применять график в реальном масштабе времени, отображаемый в верху Web-страницы путем простого нажатия на порт.

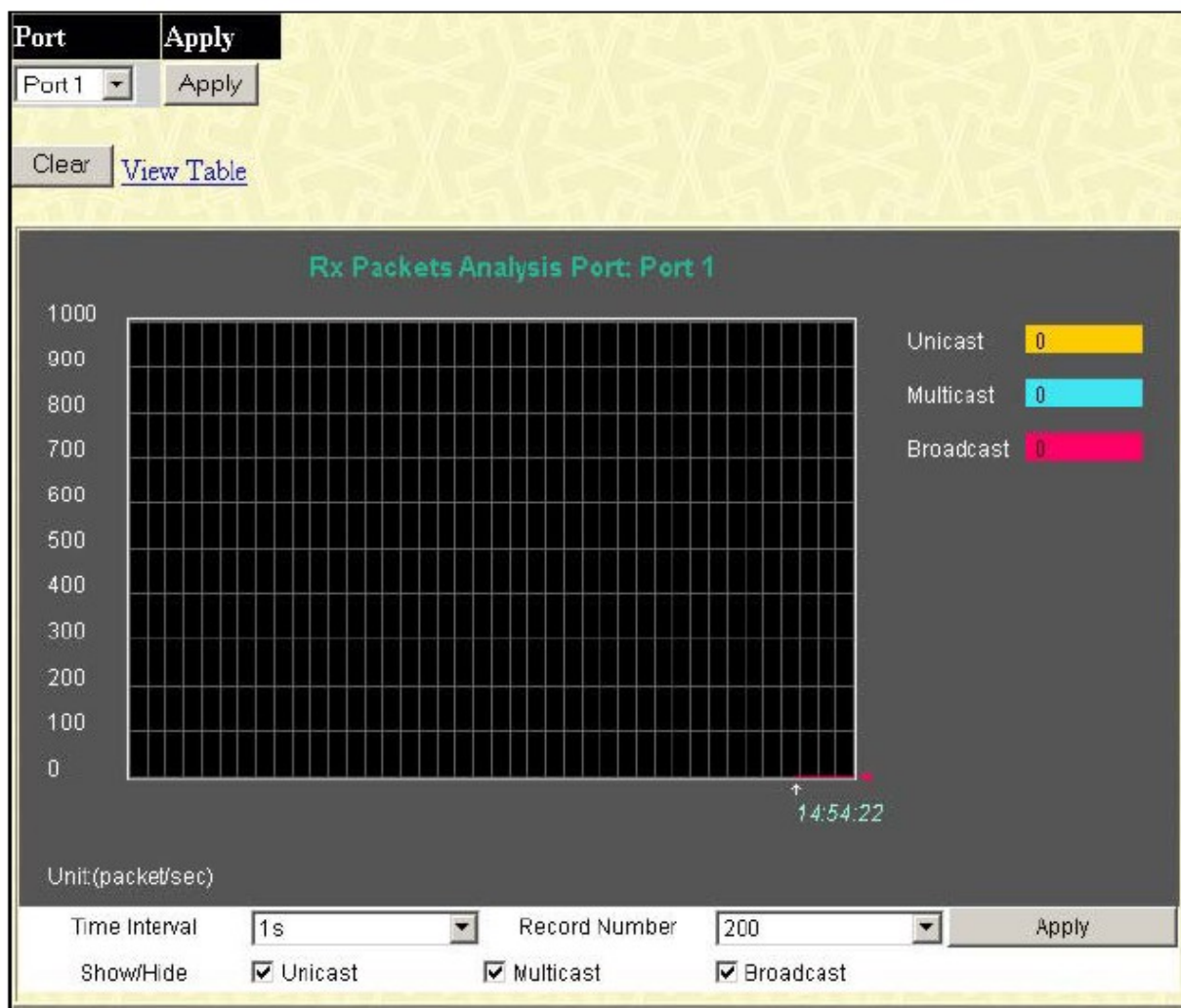


Рисунок 11.5 – Окно «Rx Packets Analysis» (график зависимости Unicast, Multicast и Broadcast пакетов)

Для просмотра таблицы UMB Cast Table, нажмите ссылку [View Table](#):

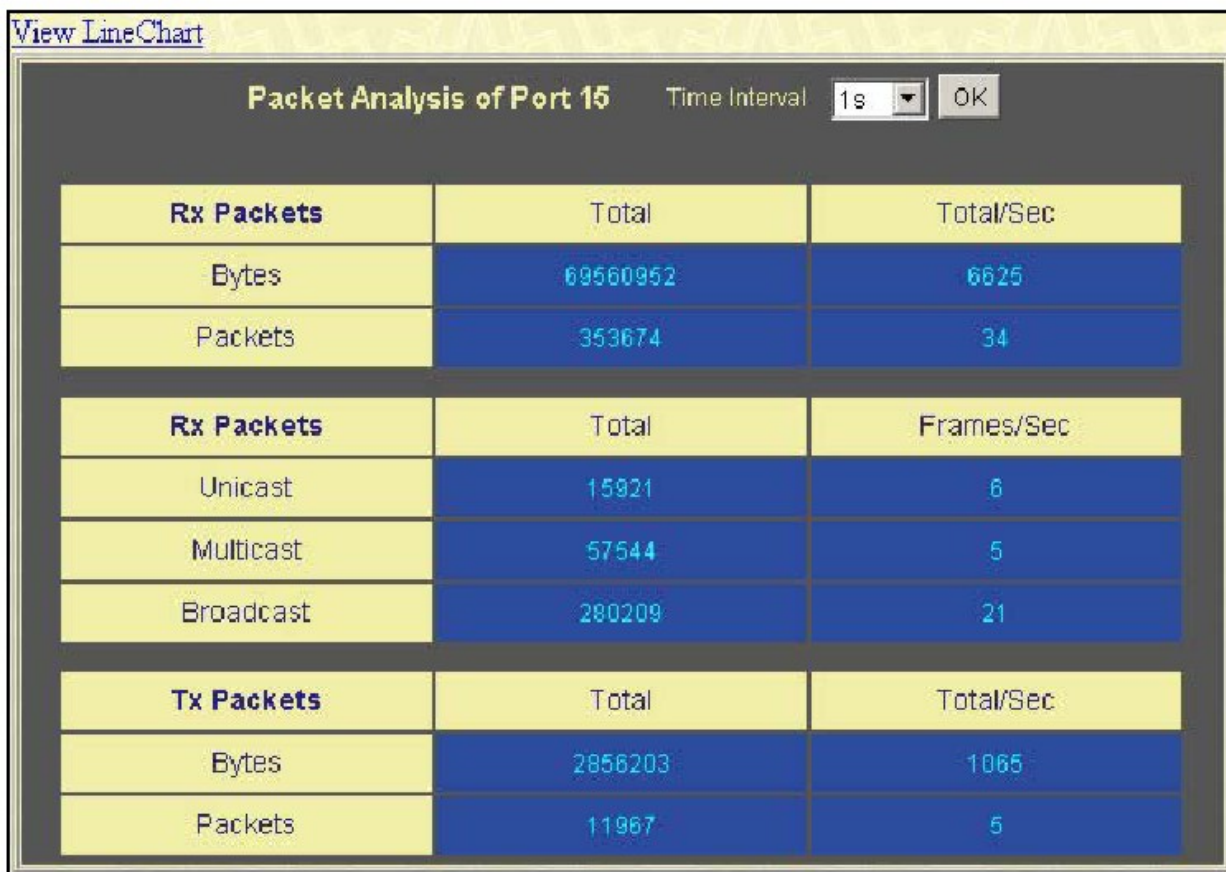


Рисунок 11.6 – Окно «Rx Packets Analysis» (таблица зависимости Unicast, Multicast и Broadcast пакетов)

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.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 20.
Unicast	Показывает число неискаженных одноадресных пакетов.
Multicast	Показывает число неискаженных многоадресных пакетов.
Broadcast	Показывает число неискаженных широковещательных пакетов.
Show/Hide	Отметьте, нужно ли отображать Multicast, Broadcast и Unicast 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.

Transmitted (TX) (Переданные пакеты)

Для просмотра графика пакетов, отправленных коммутатором, нажмите: **Monitoring** **Packets** **Transmitted (TX)**. Пользователь может также применять график в реальном масштабе времени, отображаемый вверху Web-страницы путем простого нажатия на порт.

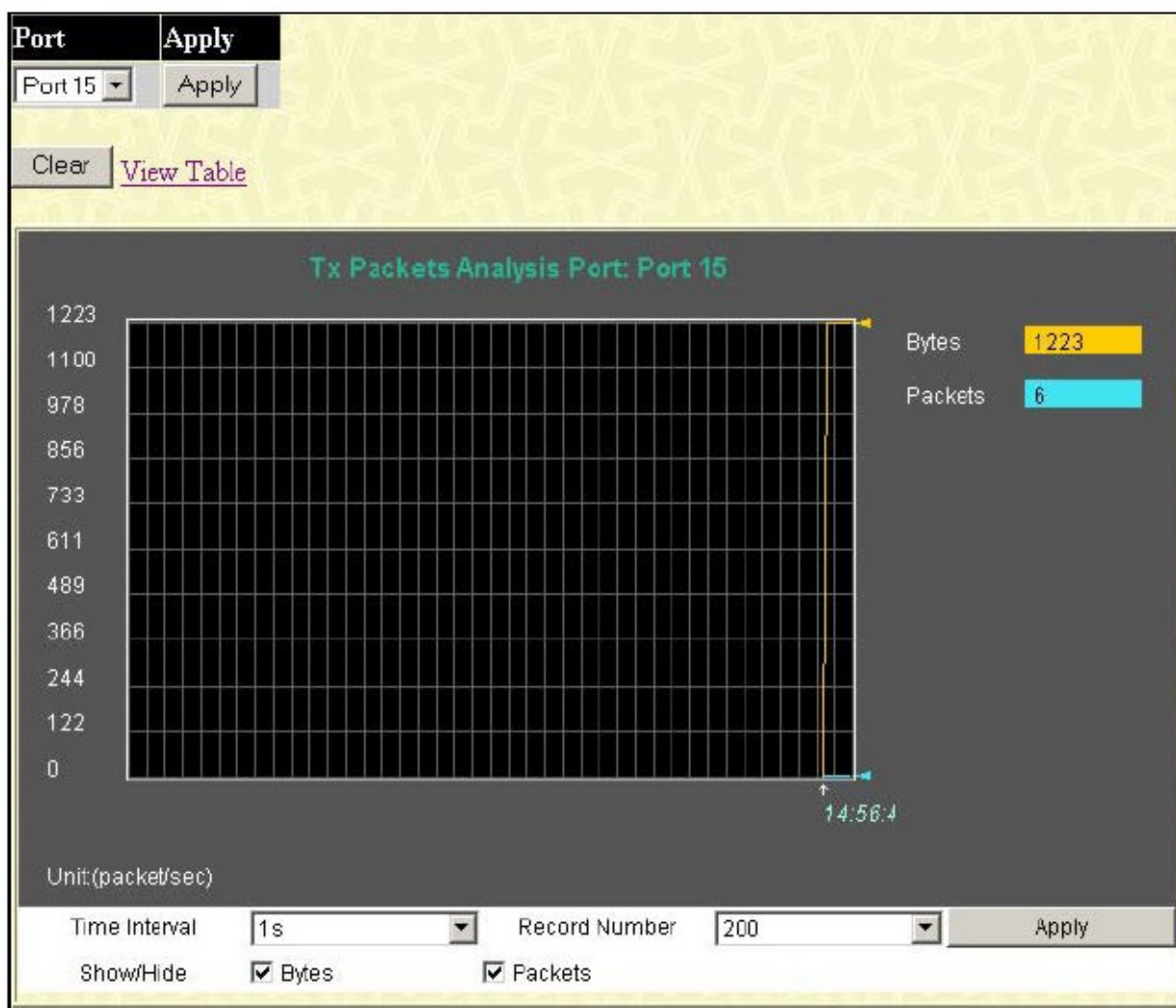


Рисунок 11.7 – Окно «Tx Packets Analysis» (график зависимости количества байт от количества переданных пакетов)

Для просмотра таблицы переданных коммутатором пакетов TX, нажмите [View Table](#):

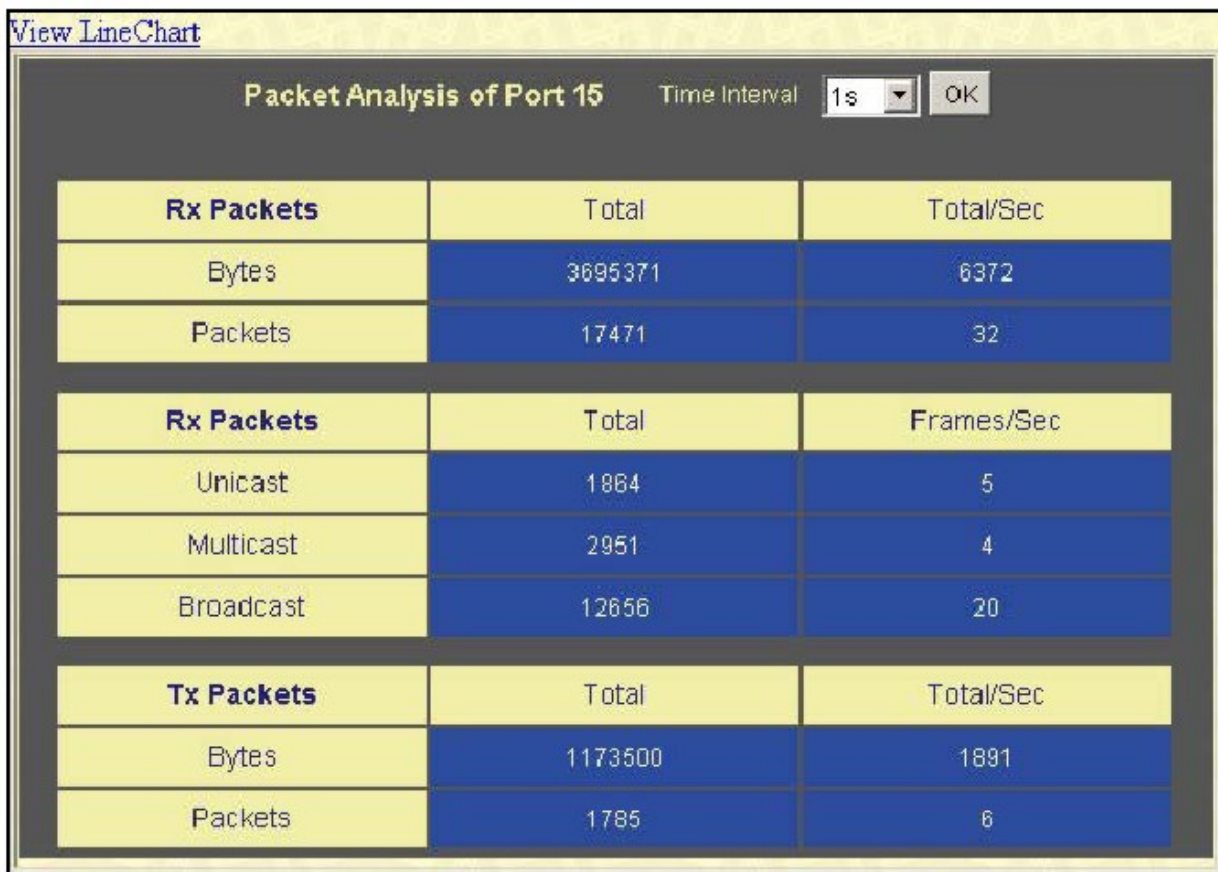


Рисунок 11.8 – Окно «Tx Packets Analysis» (таблица зависимости количества байт от количества переданных пакетов)

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 1сек.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 20.
Bytes	Показывает число байт, отправленных с данного порта.
Packets	Показывает число пакетов, отправленных с данного порта.
Unicast	Показывает число неискаженных одноадресных пакетов.
Multicast	Показывает число неискаженных многоадресных пакетов.
Broadcast	Показывает число неискаженных широковещательных пакетов.
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 при передаче пакетов

Web-менеджер позволяет просматривать статистику ошибок по порту, собранную агентом управления коммутатора, как в графическом виде, так и в виде таблицы. Вашему вниманию предлагается четыре окна.

Received (RX)

Для просмотра следующего графика ошибок по пакетам, полученным коммутатором, нажмите: **Monitoring** **Error** **Received (RX)**. Соответствующий порт выбирается в выпадающем меню **Port**. Пользователь может также применять график в реальном масштабе времени, отображаемый в верху Web-страницы путем простого нажатия на порт.

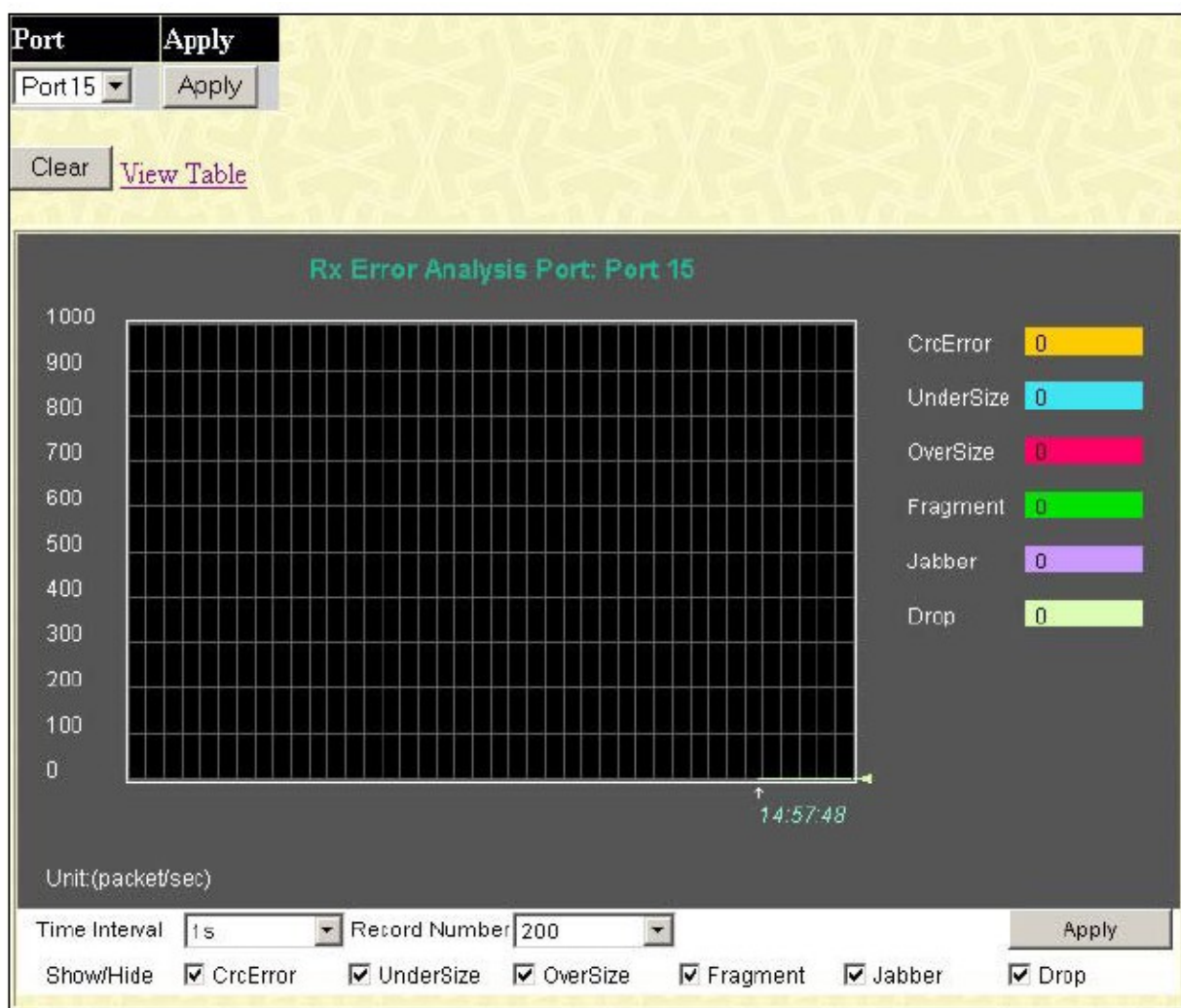


Рисунок 11.9 – Окно «Rx Error Analysis» (график зависимости)

Для просмотра следующей таблицы ошибок по пакетам, полученным коммутатором, нажмите [View Table](#):

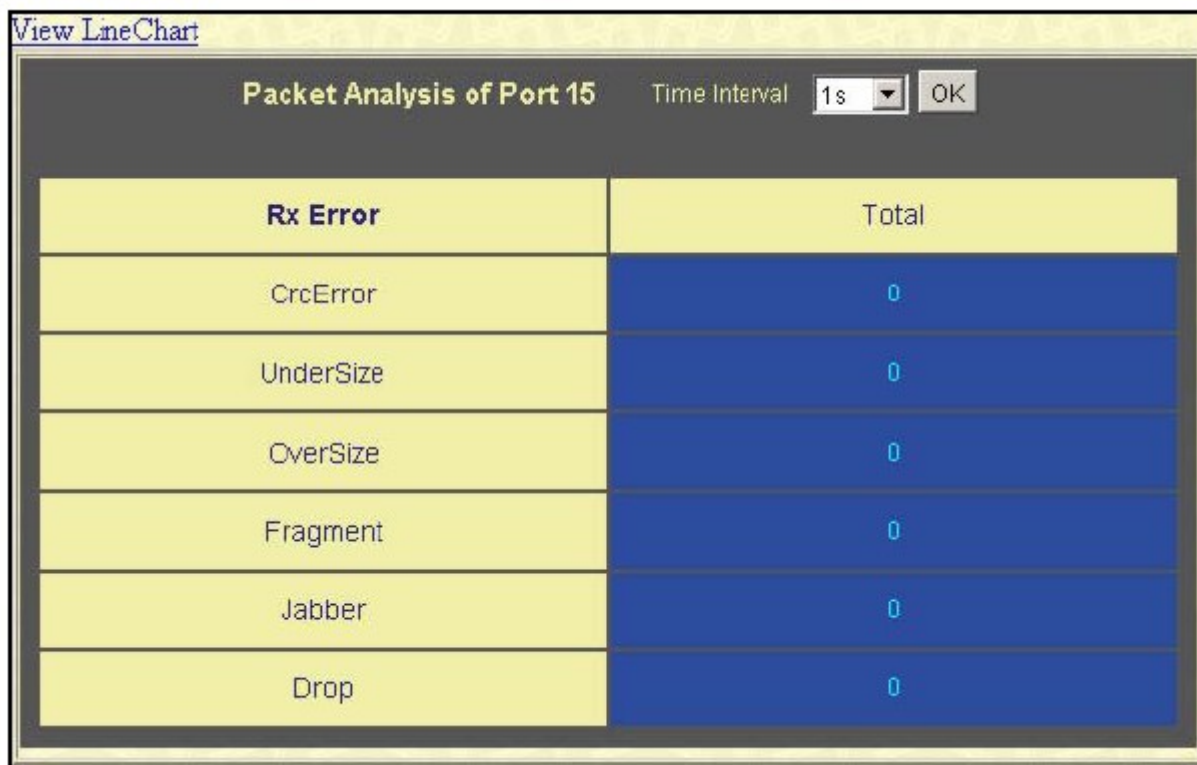


Рисунок 11.10 – Окно «Rx Error Analysis» (таблица)

Можно настроить 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.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 200.
Crc Error	Считает пакеты, которые не имеют целого количества байтов/октетов.
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 кадра 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 Crc Error, Under Size, Over Size, Fragment, Jabber и Drop errors.
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.

Transmitted (TX)

Для просмотра следующего графика ошибок по пакетам, отправленных коммутатором, нажмите: **Monitoring** **Error** **Transmitted (TX)**. Соответствующий порт выбирается в выпадающем меню **Port**. Пользователь может также применять график в реальном масштабе времени, отображаемый вверху Web-страницы путем простого нажатия на порт.

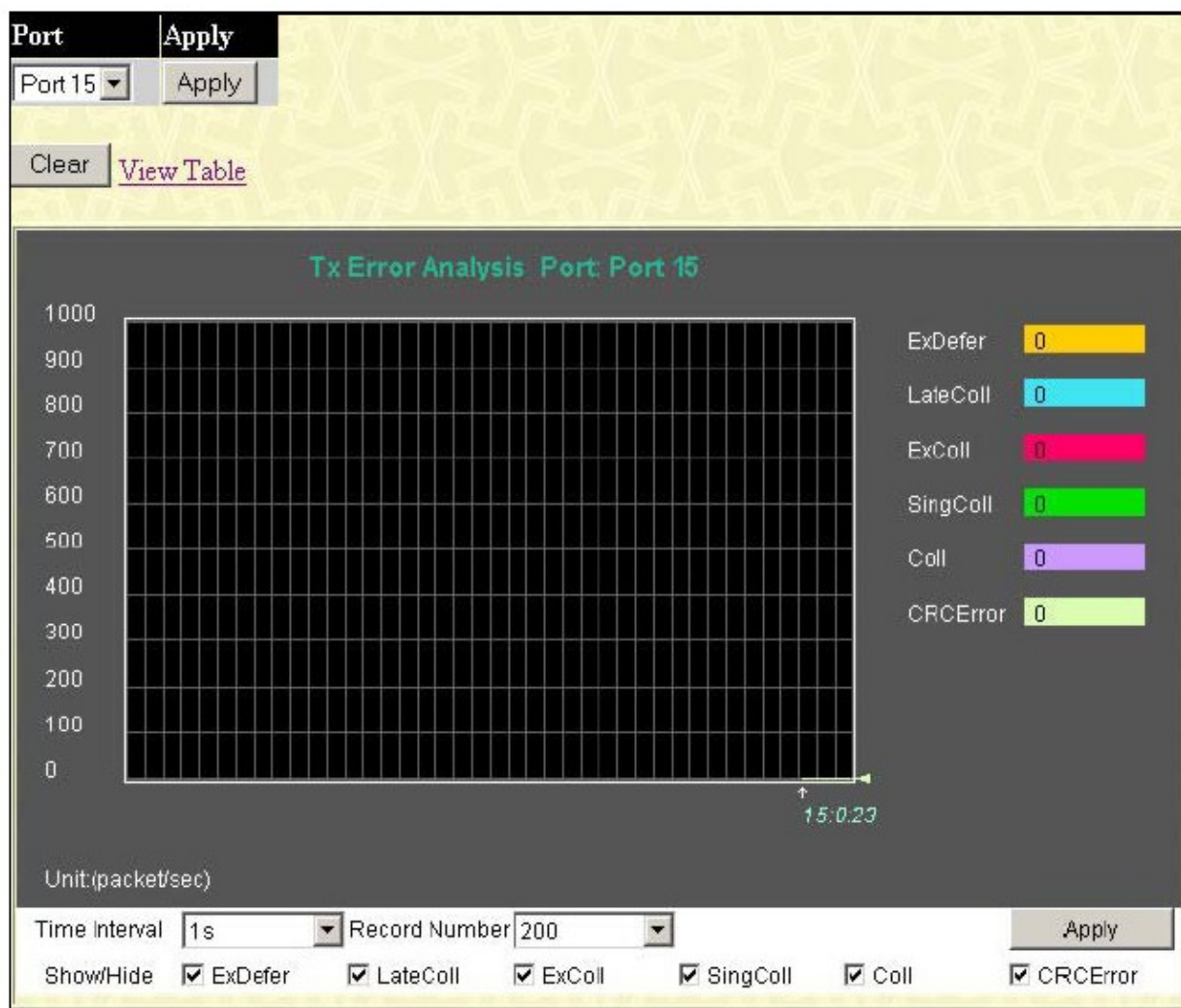


Рисунок 11.11 – Окно «Tx Error Analysis» (график зависимости)

Для просмотра следующей таблицы ошибок по пакетам, отправленным коммутатором, нажмите [View Table](#):

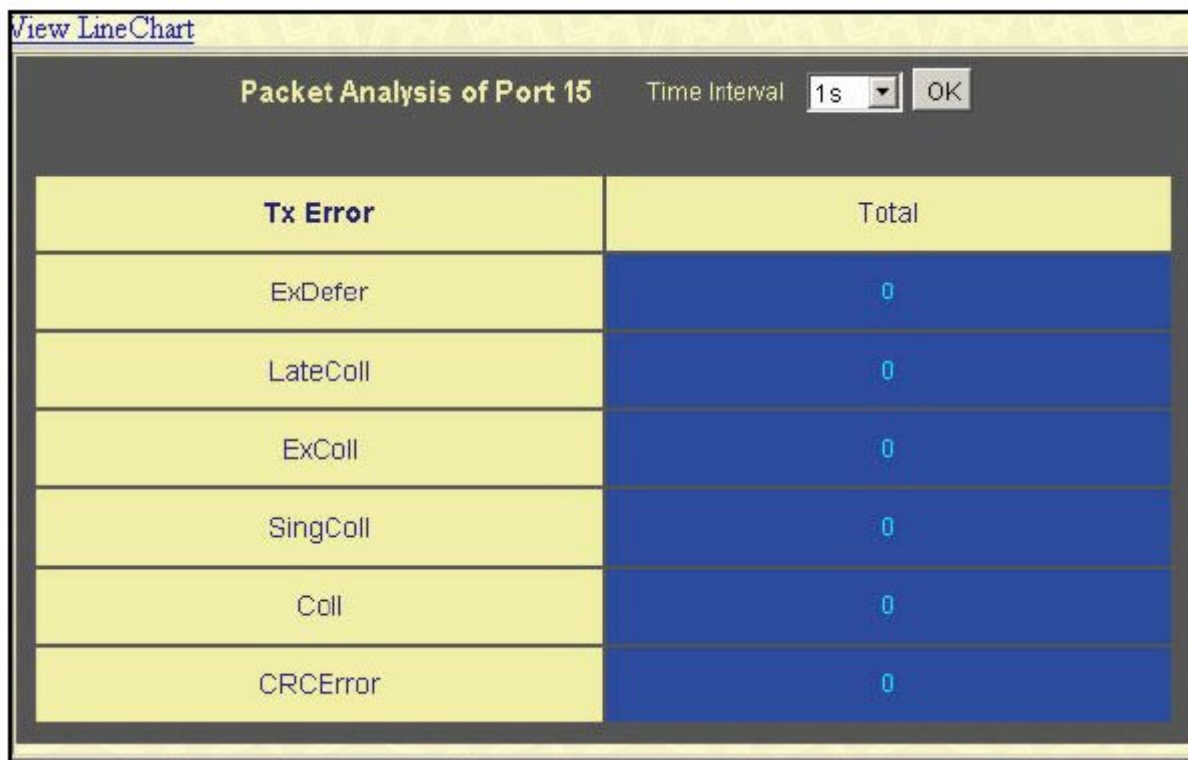


Рисунок 11.12 – Окно «Tx Error Analysis (таблица)»

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 1сек.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 20.
ExDefer	Показывает количество пакетов, которые были задержаны во время первой попытки передачи по определенному интерфейсу из-за того, что среда была занята.
LateColl	Показывает 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 более, чем одна коллизия.
Coll	Оценка общего числа коллизий в данном сегменте сети.
Show/Hide	Отметьте, нужно ли отображать или нет ExDefer, LateColl, ExColl, SingColl и Coll errors.
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-менеджер позволяет просматривать как в графическом виде, так и в виде таблицы, статистику по полученным коммутатором пакетам, разделенным на шесть групп, классифицированным по размеру.

Вашему вниманию предлагается два окна. Соответствующий порт выбирается в выпадающем меню **Port**. Пользователь может также применять график в реальном масштабе времени, отображаемый в верху Web-страницы путем простого нажатия на порт.



Рисунок 11.13 – Окно «Rx Size Analysis»(график зависимости)

Для просмотра следующей таблицы анализа пакетов по размеру, нажмите **View Table**:



Рисунок 11.14 – 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 1сек.
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 кадрюющие биты, но включая байты FCS).
65-127	Общее число полученных пакетов (включая «битые» пакеты), длиной от 65 до 127 байт (исключая кадрюющие биты, но включая байты FCS).
128-255	Общее число полученных пакетов (включая «битые» пакеты), длиной от 128 до 255 байт (исключая кадрюющие биты, но включая байты FCS).
256-511	Общее число полученных пакетов (включая «битые» пакеты), длиной от 256 до 511 байт (исключая кадрюющие биты, но включая байты FCS).
512-1023	Общее число полученных пакетов (включая «битые» пакеты), длиной от 512 до 1023 байт (исключая кадрюющие биты, но включая байты FCS).
1024-1518	Общее число полученных пакетов (включая «битые» пакеты), длиной от 1024 до 1518 байт (исключая кадрюющие биты, но включая байты FCS).
Show/Hide	Отметьте, нужно ли отображать или нет пакеты длиной 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.

MAC-адрес

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 продвижении пакетов через коммутатор.

Для просмотра таблицы с MAC-адресами нажмите: **Monitoring** **MAC Address Table**.

VID	Vlan Name	MAC Address	Port	Type
1	default	00-00-00-48-49-88	15	Dynamic
1	default	00-00-01-02-03-a2	15	Dynamic
1	default	00-00-11-22-33-45	15	Dynamic
1	default	00-00-50-77-16-00	15	Dynamic
1	default	00-00-5e-00-01-5f	15	Dynamic
1	default	00-00-e2-2f-44-ec	15	Dynamic
1	default	00-00-e2-64-e3-3e	15	Dynamic
1	default	00-00-e2-93-66-06	15	Dynamic
1	default	00-00-e2-98-fd-cd	15	Dynamic
1	default	00-01-02-03-92-27	15	Dynamic
1	default	00-01-06-30-10-63	15	Dynamic
1	default	00-01-30-12-13-02	15	Dynamic
1	default	00-01-6c-b7-cc-17	15	Dynamic
1	default	00-02-06-12-34-56	15	Dynamic
1	default	00-02-3f-72-c4-cb	15	Dynamic
1	default	00-02-a5-fd-66-97	15	Dynamic
1	default	00-02-b3-a5-a9-19	15	Dynamic
1	default	00-03-09-18-10-01	15	Dynamic
1	default	00-03-44-ae-bc-12	15	Dynamic
1	default	00-03-47-91-4a-1c	15	Dynamic

Total Entries: 311

Рисунок 11.15 – 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.
View All Entry	При нажатии на эту кнопку пользователь может просмотреть все записи таблицы адресов.

Журнал коммутатора

Web-менеджер позволяет просмотреть журнал, созданный агентом управления коммутатора. Для просмотра архива журнала, откройте папку **Monitoring** и нажмите на ссылку **Switch Log**.

Switch History		
Sequence	Time	Log Text
21	0000/00/00 00:11:45	Console session timed out (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
20	0000/00/00 00:02:08	Successful login through Web (Username: Anonymous, IP:10.53.13.94, MAC:00-50-8D-36-94-98)
19	0000/00/00 00:01:41	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
18	0000/00/00 00:00:06	Port 2 link up, 100Mbps FULL duplex
17	0000/00/00 00:00:05	System started up
16	0000/00/00 00:01:51	Firmware upgraded successfully (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
15	0000/00/00 00:01:37	Firmware upgrade was unsuccessful (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
14	0000/00/00 00:00:28	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
13	0000/00/00 00:00:06	Port 2 link up, 100Mbps FULL duplex
12	0000/00/00 00:00:05	System started up
11	0000/00/00 00:13:14	Firmware upgraded successfully (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
10	0000/00/00 00:12:54	Firmware upgrade was unsuccessful (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
9	0000/00/00 00:11:40	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
8	0000/00/00 00:00:10	Port 2 link up, 100Mbps FULL duplex
7	0000/00/00 00:00:05	System started up
6	0000/00/00 00:10:27	Configuration saved to flash (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
5	0000/00/00 00:08:00	Configuration saved to flash (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
4	0000/00/00 00:00:47	Successful login through Console (Username: Anonymous, IP:0.0.0.0, MAC:00-00-00-00-00-00)
3	0000/00/00 00:00:06	Port 1 link up, 100Mbps FULL duplex
2	0000/00/00 00:00:05	System started up

Clear Next

Рисунок 11.16. Окно Switch History

Коммутатор может записывать информацию о событиях в своем собственном журнале на настроенной принимающей станции SNMP traps 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.

Настройки журнала коммутатора

Используйте меню **Log Settings**, чтобы определить расписание или сроки, используемые для сохранения журнала коммутатора.

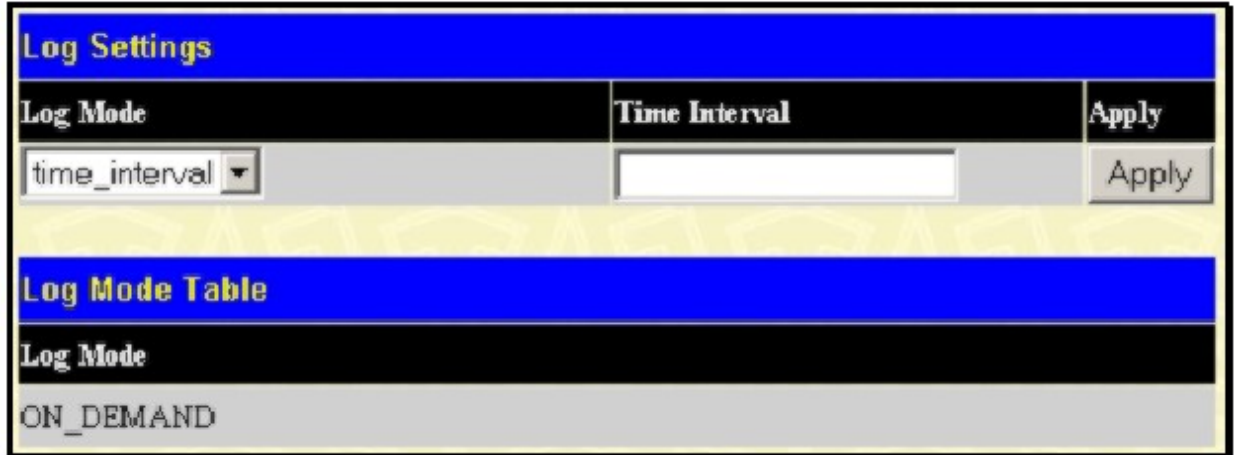


Рисунок 11.17. Log Settings меню

Выберите наиболее подходящий режим **Log Mode** и нажмите кнопку **Apply** для получения результата.

Параметр	Описание
time_interval , 1-65535	Определяет минимальный интервал между сохранением журнала в минутах
on demand	Определяет сохранение по запросу хоста, на котором хранится журнал.
log_trigger	Сохранение журнала происходит, когда переключаются предварительно установленные переключатели. Используйте команду config syslog host, чтобы определить используемые переключатели.

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**.

VLAN Name :	<input type="text"/>	<input type="button" value="Search"/>												
Total Entries : 0														
IGMP Snooping Group Table														
VLAN Name	Multicast Group	MAC Address	Reports											
	0.0.0.0	00.00.00.00:00.00	0											
Unit	Port Member													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Рисунок 11.18 – 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**.

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.



Примечание: Для установки IGMP snooping на коммутаторе, откройте папку **L2 Features** и выберите **IGMP Snooping**. Настройки и другая информация, относящаяся к IGMP snooping, может быть найдена в разделе 7 этого руководства под заголовком **IGMP Snooping**.

Browse Router Port

Окно «Browse Router Port» отображает порты коммутатора, которые на данный момент времени подключены к маршрутизатору. Подобный порт, настроенный пользователем (используя консоль или Web-интерфейс управления), отображается в качестве статического порта и обозначается буквой S. Буквой D обозначается порт, динамически настроенный коммутатором.

Total Entries:2																	
Browse Router Port																	
VLAN ID									VLAN Name								
1									default								
Ports																	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
																	Next

Рисунок 11.19 – Окно «Browse Router Port»

Browse ARP Table

Окно «Browse ARP Table» можно найти в меню **Monitoring**, в нем показаны текущие ARP-записи коммутатора. Для очистки таблицы ARP, нажмите **Clear All**.

Clear All			
Browse ARP Table			
Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	ff-ff-ff-ff-ff-ff	Local/Broadcast
System	10.17.11.11	00-80-c8-92-2d-58	Dynamic
System	10.53.13.33	00-40-05-00-30-01	Local
System	10.53.13.94	00-50-8d-36-94-98	Dynamic
System	10.255.255.255	ff-ff-ff-ff-ff-ff	Local/Broadcast

Рисунок 11.20 – Окно «Browse ARP Table»

Таблица сессий

Таблица сессий Session Table позволяет пользователю просмотреть детальную информацию по текущим настройкам сессии на коммутаторе. Отображается такая информация, как идентификатор сессии **Session ID** пользователя, начальное время **Login Time**, **Live Time**, configuration connection **From the Switch**, **Level** и **Name** пользователя. Нажмите **Reload** для обновления этого экрана.

Reload					
Total Entries :1					
Current Session Table					
ID	Login Time	Live Time	From	Level	Name
8	00000 days 00:00:04	00:31:49.890	Serial Port	1	Anonymous

Рисунок 11.21. Текущая таблица сессий

Контроль доступа по портам

Окна «Port Access Control» используются для контроля статистики по протоколу 802.1x аутентификации на основе портов, для их просмотра откройте: **Monitoring** **Port Access Control**. Вашему вниманию предлагается шесть окон.



Примечание: Состояние аутентификатора **Authenticator State** не будет отображаться на коммутаторе до тех пор, пока не будет включена аутентификация 802.1x на основе портов или на основе MAC-адресов. Для подключения 802.1x, обратитесь к записи **Switch 802.1x** в **DES-3018 Web Management Tool**.

Аутентификация RADIUS

Таблица «RADIUS Authentication» содержит информацию по аутентификации клиента на клиентской стороне. В данной таблице каждой строке соответствует сервер аутентификации RADIUS, содержащий секретную информацию клиента.

Для просмотра соответствующей таблицы: **Monitoring** **Port Access Control** **RADIUS Authentication**.

Server	UDP Port	Timeouts	Requests	Challenges	Access	Rejects	RoundTripTime	AccessRetrains	PendingRequests	AccessResponses	BadAuthenticators	UnknownTypes	PacketsDropped
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Рисунок 11.22 – 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 1сек. Для обнуления статистики нажмите кнопку *Clear* в верхнем левом углу.

Следующие параметры могут быть просмотрены:

Параметр	Описание
Server	Идентификационный номер, назначенный каждому серверу аутентификации RADIUS, которому пользователи сообщают свою секретную информацию.
UDP Port	UDP-порт, используемый клиентом для отправки запросов на этот сервер.
InvalidServerAddr	Количество пакетов доступ-ответ RADIUS, полученных от неизвестных адресов.
Identifier	NAS-идентификатор RADIUS клиента. (Необязательно такой же как sysname в MIB II)
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.
AccessRejects	Количество (действительных и недействительных) RADIUS пакетов отклонения доступа, полученных от данного сервера.

RoundTripTime	Временной интервал (в сотнях секунд) между последними «доступ-ответ»/ «Доступ-вызов», в течение которого необходимо отметить на этом сервере аутентификации RADIUS.
AccessRetrans	Количество повторных передач пакетов запроса доступа RADIUS, отправленных на этот сервер.
PendingRequests	Количество пакетов запроса доступа, предназначенных для этого сервера, которые не получают ответа
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.
UnknownTypes	Количество RADIUS пакетов неизвестного типа, полученных с данного сервера на аутентификационный порт.
PacketsDropped	Количество RADIUS пакетов, полученных с этого сервера на аутентификационный порт и удаленных по некоторым другим причинам.

Учетные записи RADIUS

Это окно показывает управляемые объекты, используемые для управления учетными записями клиентов RADIUS и отображения текущей статистики, соответствующей им. Каждая строка в данном окне соответствует серверу аутентификации RADIUS, содержащему секретную информацию пользователя. Для просмотра **RADIUS Accounting**, нажмите **Monitoring > Port Access Control > RADIUS Accounting**.

Server IP Addr	UDP Port	Timeouts	Requests	Responses	RoundTripTime	AccessRetrans	PendingRequests	MalformedResponses	BadAuthenticators	UnknownTypes	PacketCropped
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Рисунок 11.23 – 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
Server IP Addr	Идентификационный номер, назначенный каждому серверу аутентификации RADIUS (необязательно такой, как SysName в MIB II).
UDP Port	UDP-порт, используемый клиентом для отправки запросов на этот сервер.
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 так же, как и таймаут.
Requests	Количество пакетов RADIUS запроса учетной записи. В это поле не включается количество повторных передач.
Responses	Количество пакетов RADIUS, полученных на порт учетных записей сервера.
RoundTripTime	Временной интервал между самым последним запросом учетной записи и ответом на данный запрос, данный временной интервал отсчитывается на данном сервере учетных записей пользователя.
Access Retrans	Количество пакетов запроса доступа RADIUS, повторно переданных на данный аутентификационный сервер RADIUS.
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.
MalformedResponses	Количество искаженных пакетов RADIUS запроса учетной записи, 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.

Unknown Types	Количество пакетов RADIUS неизвестного типа, полученных с данного сервера на порт учетной записи пользователя.
PacketsDropped	Количество пакетов RADIUS, полученных с этого сервера на порт учетной записи пользователя, и удаленные по некоторым другим причинам.

Диагностика аутентификатора

Эта таблица содержит диагностическую информацию, относящуюся к действиям аутентификатора относительно каждого порта. Каждая запись в этой таблице соответствует определенному порту, поддерживающему функцию аутентификатора. Для просмотра **Authenticator Diagnostics**, нажмите **Monitoring > Port Access Control > Authenticator Diagnostics**.

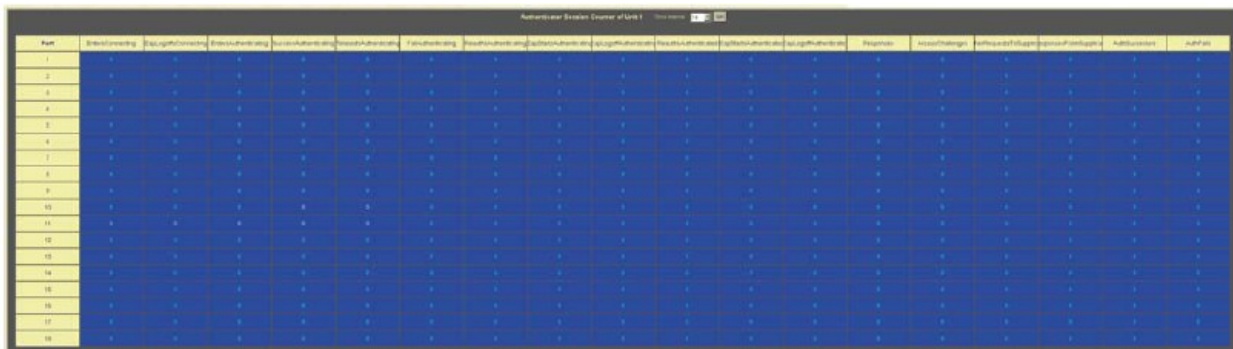


Рисунок 11.24. Authenticator Diagnostics окно

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.

Следующие поля могут быть просмотрены:

Параметр	Описание
Port	Идентификационный номер, назначенный порту системой, к которой относится порт.
EntersConnecting	Считает число переходов в состояние CONNECTING из любого другого состояния.
EapLogOffsConnecting	Считает число переходов из состояния CONNECTING в состояние DISCONNECTED как результат получения сообщения EAPOL-Logoff.
EntersAuthenticating	Считает число переходов из состояния CONNECTING в состояние AUTHENTICATING как результат получения сообщения EAP-Response/Identify.
SuccessAuthenticating	Считает число переходов из состояния AUTHENTICATING в состояние AUTHENTICATED как результат состояния выходного буфера аутентификации (Backend Authentication), показывающее успешную аутентификацию (authSuccess= TRUE) .
TimeoutsAuthenticating	Считает число переходов из состояния AUTHENTICATING в состояние ABORTING как результат состояния выходного буфера аутентификации (Backend Authentication), показывающее таймаут аутентификации (authTimeout= TRUE).
FailAuthenticating	Считает число переходов из состояния AUTHENTICATING в состояние HELD как результат состояния выходного буфера аутентификации (Backend Authentication), показывающее сбой аутентификации (authFail = TRUE).
ReauthsAuthenticating	Считает число переходов из состояния AUTHENTICATING в состояние ABORTING как результат запроса повторной аутентификации (reAuthenticate = TRUE).
EapStartsAuthenticating	Считает число переходов из состояния AUTHENTICATING в

	состояние ABORTING как результат получения EAPOL-Start сообщения.
EapLogOffAuthenticating	Считает число переходов из состояния AUTHENTICATING в состояние ABORTING как результат получения EAPOL-Logoff сообщения.
ReauthsAuthenticated	Считает число переходов из состояния AUTHENTICATED в состояние CONNECTING как результат запроса повторной аутентификации (reAuthenticate = TRUE).
EapStartsAuthenticated	Считает число переходов из состояния AUTHENTICATED в состояние CONNECTING как результат EAPOL-Start сообщения.
EapLogOffAuthenticated	Считает число переходов из состояния AUTHENTICATED в состояние DISCONNECTED как результат получения EAPOL-Logoff сообщения.
Responses	Считает число пакетов начального запроса доступа, отправленных от сервера аутентификации (например, выполнение sendRespToServer по записи из состояния Response).
AccessChallenges	Считает количество полученных пакетов вызов-доступ (Access Challenge) от сервера аутентификации.
OtherReqToSupp	Считает количество отправленных пакетов EAP-запросов (кроме сообщений Identity, Notification, Failure, Success), т.е. выполняется txReq на записи REQUEST. Показывает, что аутентификатор выбрал EAP-метод.
ResponsesFromSupplicant	Считает количество полученных ответов на начальные EAP-запросы (initial EAP-Request), кроме ответов EAP-NAK (т.е. rxResp принимает значение TRUE, являясь причиной перехода из состояния REQUEST в состояние RESPONSE, причем RESPONSE не типа EAP-NAK).
AuthSuccesses	Считает количество полученных отправленных сообщений о принятии аутентификации с сервера аутентификации (т.е. aSuccess принимает значение TRUE, являясь причиной перехода из состояния RESPONSE в состояние SUCCESS). Показывает успешную аутентификацию на сервере аутентификации.
AuthFails	Считает количество полученных от сервера аутентификации сообщений об отказе в аутентификации (т.е. aFail принимает значение TRUE, являясь причиной перехода из состояния RESPONSE в состояние FAIL). Показывает отказ в аутентификации сервера аутентификации.

Authenticator Session Statistics (Статистики сессий аутентификатора)

Эта таблица содержит объекты статистики сессий для аутентификатора PAE для каждого порта. Запись появится в этой таблице для каждого порта, поддерживающего функции аутентификатора. Для просмотра **Authenticator Session Statistics**, нажмите **Monitoring > Port Access Control > Authenticator Session Statistics**.

Port	Frames Rx	Frames Tx	Username	Time	Terminate Cause	Octets Rx	Octets Tx	ID	Authentic Method
1	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
2	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
3	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
4	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
5	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
6	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
7	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
8	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
9	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
10	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
11	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
12	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
13	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
14	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
15	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
16	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
17	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server
18	0	0		0	Supplicant Logoff	0	0		Remote Authentication Server

Рисунок 11.25. Окно Authenticator Session Counter

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.

Могут быть просмотрены следующие поля:

Параметр	Описание
Port	Идентификационный номер, назначенный порту системой, к которой относится порт.
Frames Rx	Количество кадров пользовательских данных, полученных данным портом в период сессии.
Frames Tx	Количество кадров пользовательских данных, переданных этим портом в период сессии.
UserName	Имя пользователя, представляющее идентичность Supplicant PAE.
Time	Продолжительность сессии в секундах.
Terminate Cause	Причина завершения сессии. Выделяют восемь возможных причин завершения сессии: <ol style="list-style-type: none"> 1) Supplicant Logoff (выход из системы) 2) Port Failure (ошибка порта) 3) Supplicant Restart (перезагрузка) 4) Reauthentication failure (сбой повторной аутентификации) 5) AuthControlledPortControl установлен в состояние ForceUnauthorized 6) Port reinitialization (переназначение порта) 7) Port Administratively Disabled (порт административно отключен) 8) Not Terminated Yet (еще не закончилась)
Octets Rx	Количество октетов пользовательских данных, полученных через этот порт, в период данной сессии.
Octets Tx	Количество октетов пользовательских данных, переданных через этот порт, в период данной сессии.
ID	Уникальный идентификатор сессии в виде печатной ASCII строки, содержащей как минимум три знака.
Authentic Method	Метод аутентификации, применяемый для установки сессии. Существуют следующие методы аутентификации: <ol style="list-style-type: none"> (1) <i>Remote Authentic Server</i> (Удаленный сервер аутентификации) – сервер аутентификации находится вовне системы аутентификатора. (2) <i>Local Authentic Server</i> (Локальный сервер аутентификации) – сервер аутентификации находится внутри системы аутентификатора.

Authenticator Statistics (Статистики аутентификатора)

Эта таблица содержит объекты статистики аутентификатора RAE для каждого порта. Запись появится в этой таблице для каждого порта, поддерживающего функции аутентификатора. Для просмотра статистик аутентификатора Authenticator Statistics, нажмите **Monitoring > Port Access Control > Authenticator Statistics**.

Port	Frames Rx	Frames Tx	Rx Start	Tx ReqId	Rx LogOff	Tx Req	Rx RespId	Rx Resp	Rx Invalid	Rx Error	Last Version	Last Source
1	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
2	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
3	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
4	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
5	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
6	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
7	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
8	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
9	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
10	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
11	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
12	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
13	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
14	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
15	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
16	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
17	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
18	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
19	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
20	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
21	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
22	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
23	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00
24	0	0	0	0	0	0	0	0	0	0	0	00-00-00-00-00

Рисунок 11.26. Окно Authenticator Statistics

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.

Могут быть просмотрены следующие поля:

Параметр	Описание
Port	Идентификационный номер, назначенный порту системой, к которой относится порт.
Frames Rx	Количество корректных кадров EAPOL, полученных аутентификатором.
Frames Tx	Количество корректных кадров EAPOL, переданных аутентификатором.
Rx Start	Число кадров EAPOL Start, полученных аутентификатором.
TxReqId	Число кадров EAPOL Req/Id, переданных аутентификатором.
RxLogOff	Число кадров EAPOL Logoff, полученных аутентификатором.
Tx Req	Число кадров EAP Request (кроме кадров Rq/Id), полученных аутентификатором.
Rx RespId	Число кадров EAP Resp/Id, полученных аутентификатором.
Rx Resp	Число действительных кадров EAP Response (кроме кадров Resp/Id), полученных аутентификатором.
Rx Invalid	Число EAPOL-кадров с заданным типом, полученных данным аутентификатором.
Rx Error	Число EAPOL-кадров, полученных данным аутентификатором, у которых поле Packet Body Length (Длина тела пакета) было некорректно.
Last Version	Номер версии протокола последнего полученного EAPOL-кадра.

Last Source	MAC-адрес источника последнего полученного EAPOL-кадра.
--------------------	---

Authenticator State

В данном пункте описывается состояние коммутатора согласно протоколу 802.1x. Для просмотра таблицы «Authenticator State»: **Monitoring** **Port Access Control** **Authenticator State**.

The screenshot shows a window titled "Authenticator State" with a "Time Interval" dropdown set to "1s" and an "OK" button. Below the title is a table with four columns: "Port", "Auth_PAE_State", "Backend_State", and "PortStatus". The table contains 18 rows, each representing a port from 1 to 18. All ports show a "ForceAuth" state, a "Success" backend state, and an "Authorized" port status.

Port	Auth_PAE_State	Backend_State	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized
13	ForceAuth	Success	Authorized
14	ForceAuth	Success	Authorized
15	ForceAuth	Success	Authorized
16	ForceAuth	Success	Authorized
17	ForceAuth	Success	Authorized
18	ForceAuth	Success	Authorized

Рисунок 11.27. Окно Authenticator State–802.1x на базе портов

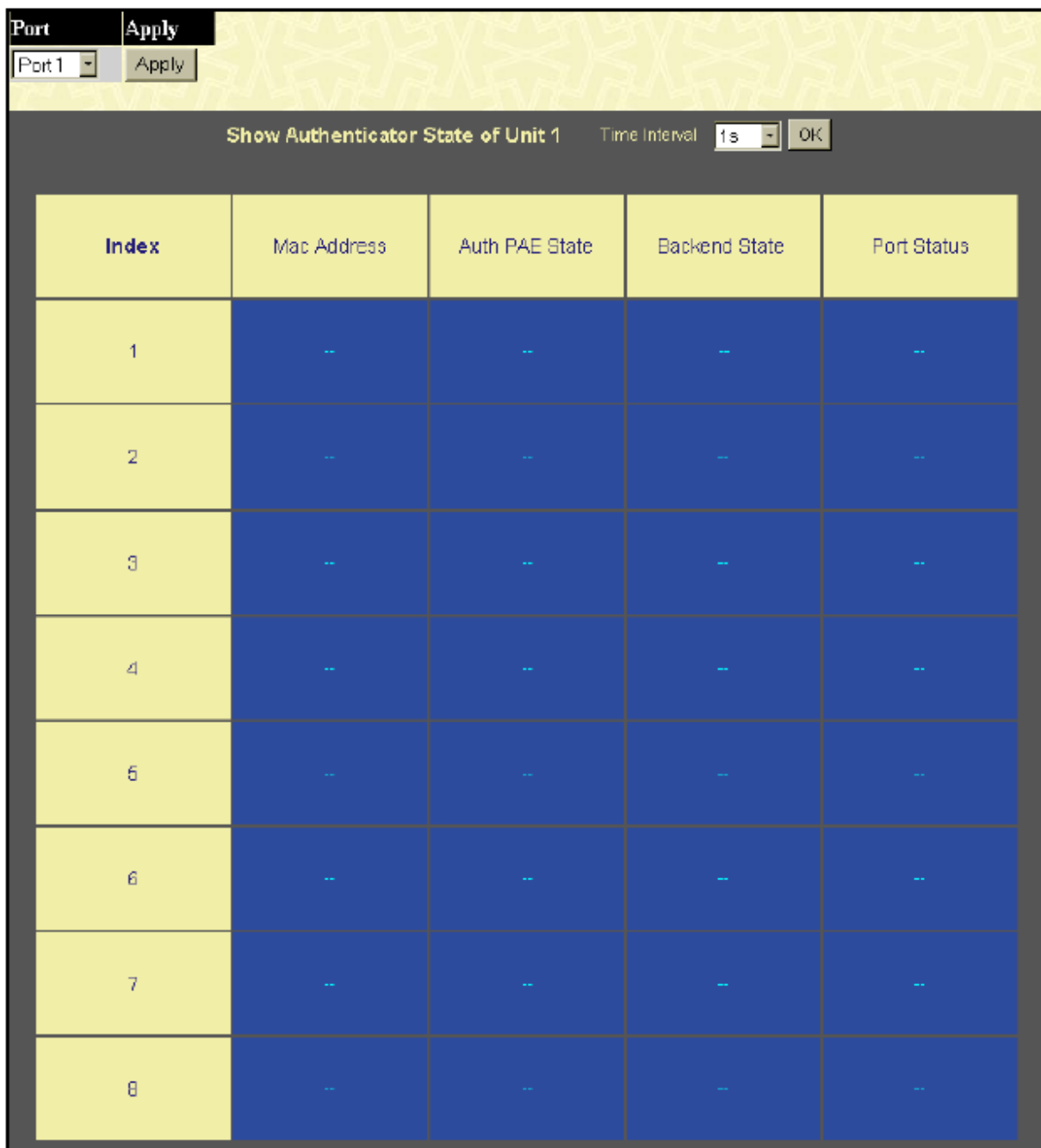


Рисунок 11.28. Authenticator State окно – 802.1x на базе MAC-адресов

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 **ОК**.

Информация, представленная в данном окне, описывается в таблице:

Параметр	Описание
MAC Address	Отображает MAC-адрес аутентификатора
Auth PAE State	Значение коммутатора (аутентификатора) Authenticator PAE State может быть <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth</i> или <i>N/A</i> . <i>N/A</i> (Not available – не доступен) свидетельствует о том, что возможность аутентификации портов отключена.
Backend State	Состояние выходного буфера аутентификации может быть <i>Request, Response, Success, Fail, Timeout, Idle, Initialize</i> или <i>N/A</i> . <i>N/A</i> (Not available – не доступен)

	свидетельствует о том, что возможность аутентификации портов отключена.
Port Status	Состояние порта может быть авторизованное <i>Authorized</i> , неавторизованное <i>Unauthorized</i> или не доступно <i>N/A</i> .

Сброс настроек коммутатора

Опция Reset имеет несколько функций во время сброса настроек коммутатора. Некоторые текущие параметры настроек можно сохранить, в то время как все другие конфигурационные настройки сбросятся к заводским по умолчанию.



Примечание: Только функция Reset System позволит сбросить коммутатор к заводским настройкам по умолчанию, после чего следует перезагрузка устройства. Все другие функции вносят заводские параметры по умолчанию в текущую конфигурацию, но не сохраняют ее. Reset System вернет конфигурацию коммутатора к состоянию, которое у него было после выпуска с завода.

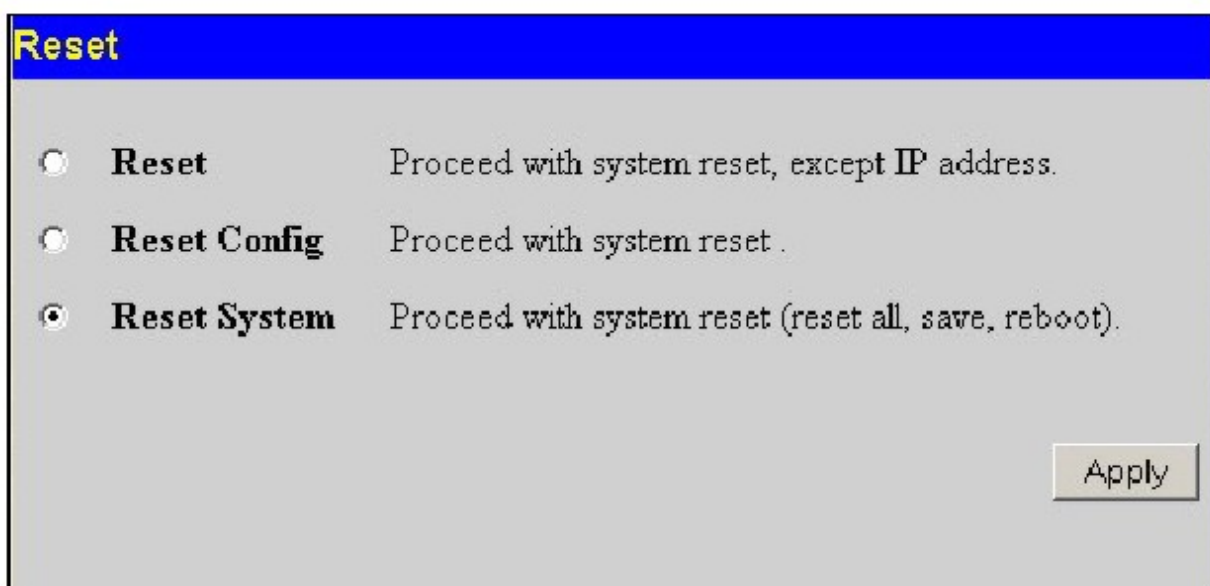


Рисунок 11.29. Окно Factory Reset to Default Value

Перезапуск коммутатора

Следующее окно используется для перезапуска коммутатора.

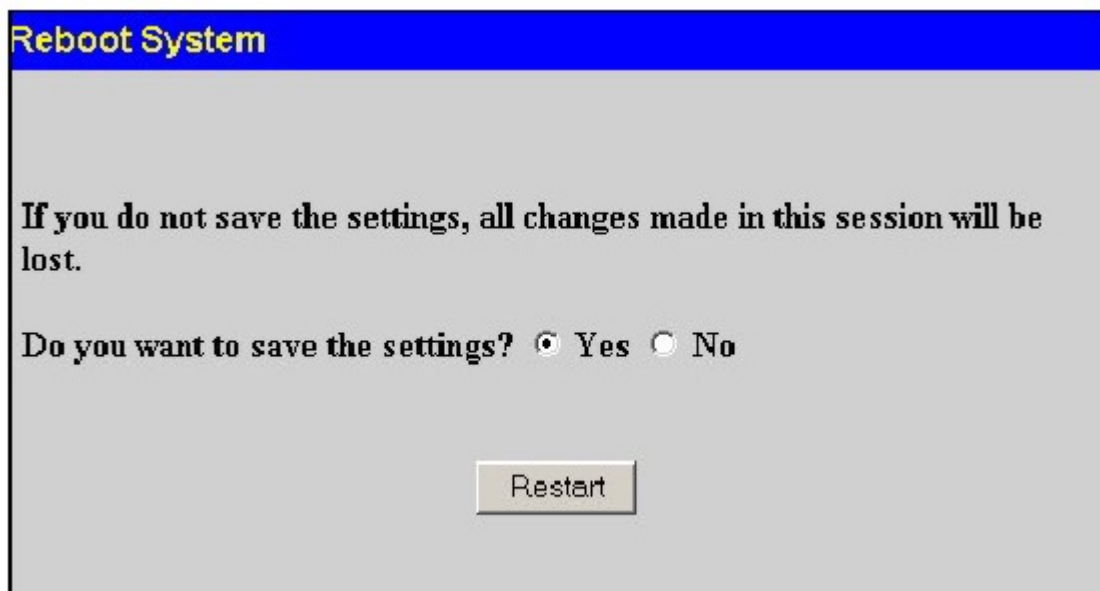


Рисунок 11.30 – Окно «Reboot System»

При выборе **Yes** коммутатор получит инструкцию сохранить текущую конфигурацию в NV-RAM перед перезапуском коммутатора.

При выборе **No** коммутатор получит инструкцию не сохранять текущую конфигурацию в NV-RAM перед перезапуском коммутатора.

Нажмите кнопку **Restart** для перезапуска коммутатора.

Сохранение изменений

Коммутатор обладает двумя видами памяти, оперативная RAM и энергонезависимая NV-RAM. Некоторые настройки будут работать только после перезапуска коммутатора. Во время перезапуска коммутатора стираются все настройки в памяти RAM и загружаются сохраненные настройки из NV-RAM. Таким образом, необходимо сохранить все настройки в долговременной памяти NV-RAM перед перезагрузкой коммутатора.

Выделяют три опции сохранения изменений:

- **Save Config** – сохраняет текущую конфигурацию в NV-RAM. Эта конфигурация будет загружаться при перезагрузке.
- **Save Log** – Сохраняет архив журнала коммутатора.
- **Save All** – Сохраняет и конфигурацию, и журнал.

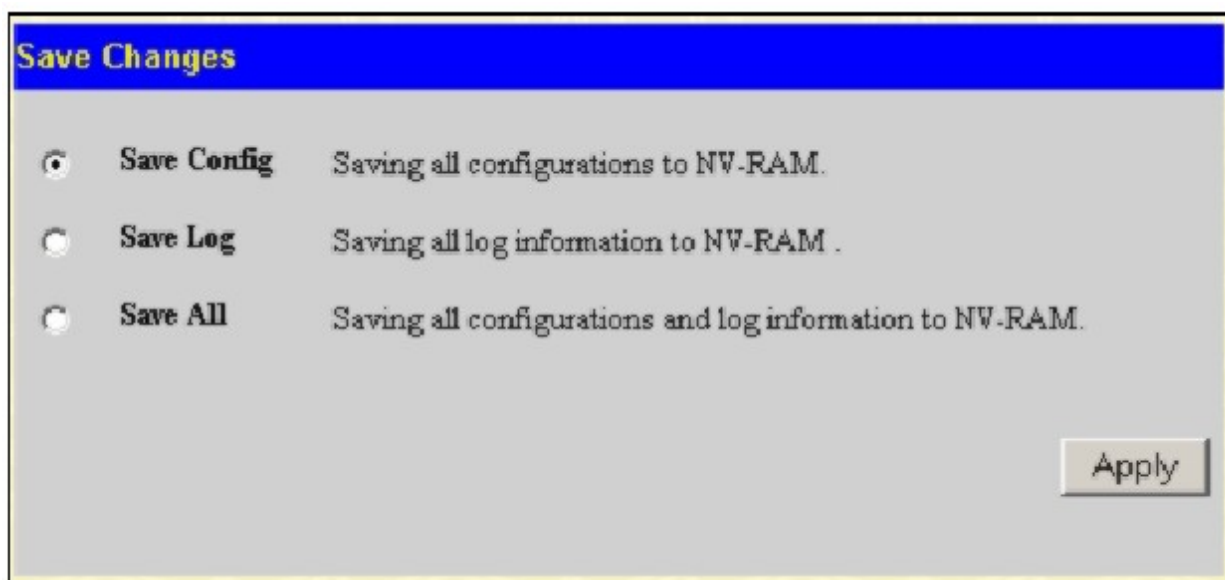


Рисунок 11.31. Окно Save Changes

Приложение А

Техническая спецификация

Физические параметры и условия эксплуатации	
Входное переменное напряжение. Внешнее устройство питания	Входное напряжение переменного тока: 100-120, 200-240, с частотой 50/60 Гц (внутренний универсальный источник питания)
Потребляемая мощность	DES-3010F – 10,7 Ватт DES-3010G – 9,9 Ватт DES-3018 - 10,5 Ватт DES-3026 - 11,6 Ватт
Рабочая температура	От 0 до 40С
Температура хранения	От -40 до 70С
Влажность	Рабочая: От 5% до 95% без конденсата Хранения: От 0% до 95% без конденсата
Размеры	для DES-3010F/FL/G: 280 мм x 180 мм x 44 мм (1U), для монтажа в 11” стойку для DES-3018/3026: 441 мм x 207 мм x 44 мм (1U), для монтажа в 19” стойку
Масса	DES-3010F/FL/G: 1.5 кг DES-3018/3026: 2.1 кг
Электромагнитное излучение (EMI)	FCC Class A, CE class A, C-Tick
Безопасность	CSA International

Основные									
Стандарты	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-T Gigabit Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1d/w Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.3x управление потоком для полнодуплексного режима IEEE 802.3 поддержка автосогласования Nway								
Протоколы	CSMA/CD								
Канал связи Ethernet Fast Ethernet Gigabit Ethernet	<table border="0"> <tr> <td>Полудуплекс</td> <td>Дуплекс</td> </tr> <tr> <td>10 Мбит/с</td> <td>20 Мбит/с</td> </tr> <tr> <td>100 Мбит/с</td> <td>200 Мбит/с</td> </tr> <tr> <td>n/a</td> <td>2000 Мбит/с</td> </tr> </table>	Полудуплекс	Дуплекс	10 Мбит/с	20 Мбит/с	100 Мбит/с	200 Мбит/с	n/a	2000 Мбит/с
Полудуплекс	Дуплекс								
10 Мбит/с	20 Мбит/с								
100 Мбит/с	200 Мбит/с								
n/a	2000 Мбит/с								
Сетевые кабели: 10BASE-T	2-хпарный кабель UTP категории 3,4,5 (100м) EIA/TIA-568 100 Ом STP (100 м)								
100BASE-TX	2-хпарный кабель UTP категории 5 (100м) EIA/TIA-568 100 Ом STP (100 м)								
Количество портов	DES-3010F – 8 портов 10/100 Мбит/с с автоопределением скорости Nway, 1 гигабитный порт 1000BASE-T, 1 оптический порт 100-BASE-FX. DES-3010F – 8 портов 10/100 Мбит/с с автоопределением скорости Nway, 1								

	<p>гигабитный порт 1000BASE-T, 1 оптический порт SFP. DES-3018 – 16 портов 10/100 Мбит/с с автоопределением скорости Nway, 2 слота дополнительных модулей. DES-3026 – 24 порта 10/100 Мбит/с с автоопределением скорости Nway, 2 слота дополнительных модулей DES-301T (дополнительный модуль) – 1 гигабитный порт 1000 BASE-T DES-201F (дополнительный модуль) – 1 100 BASE-FX порт DES-301G (дополнительный модуль) – 1 гигабитный порт SFP</p>
--	---

Производительность	
Метод коммутации	Store-and-forward
Буферизация пакетов	32 МВ на устройство
Фильтрация адресной таблицы	Поддержка 8К MAC-адресов на устройство.
Скорость фильтрации/передачи пакетов	14,880 pps на порт (для 10Мбит/с) 148,809 pps на порт (для 100Мбит/с) 1,488,100 pps на порт (для 1 Гбит/с)
Изучение MAC-адресов	Автоматическое обновление.

Приложение В

Кабели и коннекторы

При подключении коммутатора к другому коммутатору, мосту или концентратору необходим обычный кабель. Пожалуйста, проверьте, подходят ли pin-контакты устройств. Приведённые ниже рисунок и таблица демонстрируют стандартный разъём RJ-45 с распределением его pin-контактов.

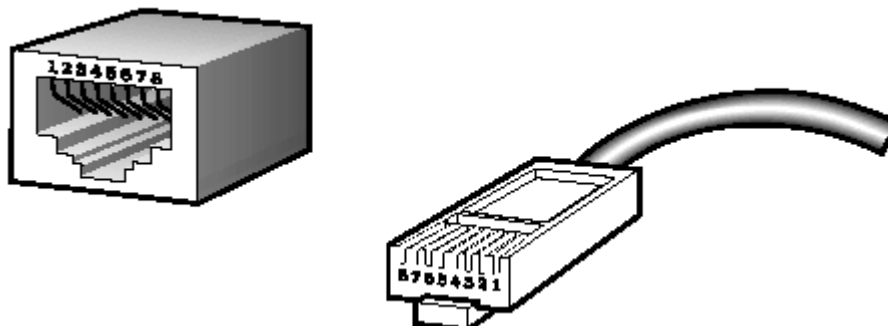


Рисунок В-1. Стандартный RJ-45 разъём с вилкой

Контакты разъёма RJ-45		
Контакты	MDI-X Port	MDI-II Port
1	BI-DB+	BI-DA+
2	BI-DB-	BI-DA-
3	BI-DA+	BI-DB+
4	BI-DD+	BI-DC+
5	BI-DD-	BI-DC-
6	BI-DA-	BI-DB-
7	BI-DC+	BI-DD+
8	BI-DC-	BI-DD-

Таблица В-1. Стандартный разъём RJ-45

Приложение С

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	10 км
	1000BASE-SX, модуль с поддержкой многомодового оптического кабеля	550 м
	1000BASE-LHX, модуль с поддержкой одномодового оптического кабеля	40 км
	1000BASE-ZX, модуль с поддержкой многомодового оптического кабеля	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
10BASE-T	UTP кабель 3 категории (10 Мбит/с)	100 м

Глоссарий

1000BASE-SX: оптоволоконный кабель, рассчитанный на длину до 10 км.

1000BASE-LX: оптоволоконный кабель, рассчитанный на длину до 550м.

100BASE-FX: Часть спецификации IEEE 802.3u Ethernet для скорости 100 Мбит/с с использованием оптических кабелей и стандарта FDDI TP-PMD для PMD (физическая среда).

100BASE-TX: Часть спецификации IEEE 802.3u Ethernet для скорости 100 Мбит/с с использованием 2-пар неэкранированного медного кабеля 5 категории.

10BASE-T: Спецификация IEEE 802.3i для сетей Ethernet с использованием неэкранированного кабеля на основе витой пары.

ATM: Asynchronous Transfer Mode (асинхронный режим передачи). Соединение, ориентированное на протокол передачи, основанный на использовании пакетов фиксированной длины. ATM рассчитан на передачу различных типов данных, включая голос, данные и видео.

ageing: автоматическое удаление из базы данных коммутатора устаревших динамических записей.

auto-negotiation: функция порта, которая позволяет ему объявлять свои параметры для скорости, дуплексного режима и контроля потока. Когда производится соединение со станцией, также поддерживающей auto-negotiation, соединение может самоопределить его оптимальные установки.

backbone port: магистральный порт, который не может распознавать адреса устройств и получает все фреймы с неопознанными адресами. Этот порт используется для соединения коммутатора с магистралью вашей сети. Обратите внимание, что магистральные порты также известны как выделенные нисходящие порты.

backbone: Магистраль, часть сети, по которой передается основной трафик и которая является чаще всего источником и приемником других сетей.

bandwidth: Полоса пропускания, диапазон между самой высокой и самой низкой частотой, доступной для передачи сетевых сигналов. Диапазон частот измеряется в герцах (Гц).

baud rate: скорость переключения в линии. Также известная, как скорость линии между сегментами сети.

BOOTP: Bootstrap Protocol. Протокол BOOTP позволяет автоматически составлять карту IP-адресов, собирая MAC-адреса устройств при каждом старте устройств. К тому же, протокол может связывать маску подсети и шлюз к устройству, установленному по умолчанию.

bridge: Мост. Устройство, соединяющее две или несколько физических сетей и передающее пакеты из одной сети в другую. Мосты работают на канальном уровне OSI модели.

broadcast: Широковещание. Система доставки пакетов, при которой копия каждого пакета передается всем узлам, подключенным к сети. Примером широковещательной сети является Ethernet.

broadcast storm: широковещательный шторм. Многократные одновременные передачи сообщений, которые обычно поглощают доступную полосу пропускания сети и могут вызвать отказ сети.

console port: консольный порт. 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 только тогда, когда канал передачи данных не занят в течение некоторого периода времени. Когда два устройства передают одновременно, возникает коллизия, и конфликтные устройства своей повторной передачей создают задержку на неопределённое время.

data center switching: точка агрегации в корпоративной сети, где коммутатор предоставляет высокопроизводительный доступ к серверной ферме, высокоскоростное соединение и контроль точки с целью управления и обеспечения безопасности.

Ethernet: Стандарт организации локальных сетей (LAN) совместно разработанный Xerox, Intel и Digital Equipment Corporation. Ethernet обеспечивает скорость 10Мбит/с, используя CSMA/CD.

Fast Ethernet: 100 мбитная технология, основанная на методе Ethernet/CD.

Flow Control: (IEEE 802.3z) Управление потоком. Методы, используемые для контроля за передачей данных между двумя точками сети и позволяющие избежать потери данных в результате переполнения приемных буферов.

forwarding: Процесс продвижения пакета к месту его назначения посредством сетевого устройства.

full duplex: Дуплексный режим. Одновременная передача данных между станцией-отправителем и станцией-получателем.

half duplex: Полудуплексный режим. Способность канала в каждый момент времени только передавать или принимать информацию. Прием и передача, таким образом, должны выполняться поочередно.

IP address: Internet Protocol address. Уникальный протокол для устройств, подсоединенных к сети с использованием TCP/IP. Адрес записывается как 4-х байтовое значение с разделением точками, состоит из номера сети, номера подсети, номера хоста.

IPX: Internetwork Packet Exchange. Протокол, позволяющий соединения в NetWare

LAN - Local Area Network: Локальная сеть. Сеть, соединяющая такие устройства как компьютеры, принтеры, сервера, покрывающая относительно небольшую площадь.

latency: Временная задержка между моментом, когда устройство получило пакет и моментом, когда пакет был отправлен на порт назначения.

line speed: смотрите baud rate.

main port: Порт отказоустойчивой линии, который переносит трафик данных в нормальных эксплуатационных режимах.

MDI - Medium Dependent Interface: Порт Ethernet, где передатчик одного устройства соединён с приёмником другого.

MDI-X - Medium Dependent Interface Cross-over: Порт Ethernet, где линии передатчика и приёмника пересекаются.

MIB - Management Information Base: База управляющей информации. База данных, где хранится информация для управления сетью, которая используется и поддерживается протоколом сетевого управления SNMP. Значение MIB-объекта может быть изменено или извлечено с помощью команд SNMP и сетевой системы управления (например, D-Link D - View) с GUI-интерфейсом. MIB-объекты образуют древовидную структуру с открытыми (стандартными) и закрытыми (частными) ветвями.

multicast: Многоадресная рассылка. Режим копирования одиночных пакетов и их передачи заданному подмножеству сетевых адресов. Эти адреса задаются в поле адреса приемника (Destination address field).

protocol: набор правил соединения между устройством и сетью. Правила диктуют формат, временные интервалы, последовательность и контроль ошибок.

resilient link: пара портов, которые могут быть сконфигурированы таким образом, что при захвате передачи данных одним портом, другой вынужден простаивать. Смотрите также main port и standby port.

RJ-45: стандартный 8-пиновый разъём для IEEE 802.3 10BASE-T

RMON: Remote Monitoring. Модуль SNMP MIB II, который позволяет мониторить и управлять устройством, обрабатывая до 10 различных потоков информации.

RMON Redundant Power System: устройство обеспечивающей резервный источник питания для коммутатора.

server farm: Кластер серверов, занимающий центральную позицию и обслуживающий большое количество пользователей.

SLIP - Serial Line Internet Protocol: протокол, позволяющий реализовать IP при соединении двух систем последовательными линиями.

SNMP - Simple Network Management Protocol: Простой протокол сетевого управления. Первоначально протокол предполагалось использоваться в управлении TCP/IP. Сейчас SNMP широко используется в компьютерах и сетевом оборудовании и может использоваться для управления многими аспектами сети и конечными станциями.

Spanning Tree Protocol (STP): Система на основе моста для того, чтобы обеспечивать нечувствительность к ошибкам в сетях. STP работает, позволяя создавать параллельные пути для трафика, и гарантирует, что избыточные пути будут дезактивированы, если основные пути исправны и активированы.

stack: Группа сетевых устройств, которые интегрированы в группу, образующую одно логическое устройство.

standby port: порт на безотказной линии, который возьмёт на себя передачу данных. Если главный порт будет неисправен.

switch: устройство, которое фильтрует, пересылает и заливаает пакеты, основываясь на адресе доставки пакета. Коммутатор изучает адреса, связанные с каждым портом другого коммутатора и строит таблицы, основанные на этой информации, которая используется для осуществления связи.

TCP/IP: стек протоколов связи, обеспечивающий эмуляцию терминала Telnet, передачу по FTP и другие сервисы для связи в компьютерной сети.

telnet: TCP/IP протокол, который предоставляет терминальный виртуальный сервис, позволяя пользователю авторизоваться на другом компьютере и разрешая доступ к хосту так, как если бы пользователь был напрямую соединён с ним.

TFTP - Trivial File Transfer Protocol: позволяет перемещать файлы (такие как обновление программного обеспечения) с удалённого устройства, используя возможности управления коммутатора (передача без аутентификации).

UDP - User Datagram Protocol: стандартный протокол Интернета, позволяющий приложению на одном устройстве посылать пакет приложению другого устройства.

VLAN - Virtual LAN: группа устройств, объединённых логически (независимо от топологии сети).

VLT - Virtual LAN Trunk: соединение Коммутатор-коммутатор, которое передаёт трафик всех VLAN-ов на каждый коммутатор.

VT100: тип терминала, который использует ASCII символы. VT100-терминалы представляют информацию в текстовом виде.