D-Link ™ DES-3028/DES-3028P/DES-3052/DES-3052P

Управляемые коммутаторы 10/100Мбит/с Fast Ethernet

ВЕРСИЯ I

Руководство пользователя

СОДЕРЖАНИЕ

Предисловие

Руководство пользователя для коммутаторов DES-3028/DES-3028P/DES-3052/DES-3052P 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/Fast Ethernet.

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

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

Раздел 6, Администрирование – Детально обсуждаются настройки основных функций коммутатора, включая информацию об устройстве, IP-адрес, настройка порта, DHCP/BOOTP Relay, учетные записи пользователей, зеркалирование портов, настройки системного журнала и его записей, настройки SNTP, MAC-уведомление, сервисы TFTP, настройка нескольких копий программного обеспечения, Ping-тест, Safeguard Engine, менеджер SNMP, система PoE, управление через единый IP-адрес, Forwarding & Filtering, а также сервис SMTP.

Раздел 7, Функции 2 уровня – Обсуждается функционал 2 уровня коммутатора, включая VLAN, агрегирование каналов, IGMP Snooping и Spanning Tree.

Раздел 8, Класс обслуживания (CoS). – Содержит информацию, относящуюся к классу обслуживания (CoS), включая полосу пропускания порта, приоритет по умолчанию 802.1P, приоритет пользователя 802.1P, работу CoS по расписанию, очереди CoS на выходе, настройки приоритета, приоритет на основе TOS, DSCP, портов и MAC-адресов.

Раздел 9, Списки управления доступом (ACL) – Обсуждаются списки управления доступом (ACL), доступные на коммутаторе, включая временной диапазон, таблицу профилей доступа и CPU Interface Filtering.

Раздел 10, Безопасность – Обсуждаются доступные на Коммутаторе функции безопасности, включая управление трафиком, безопасность на уровне портов (Port Security), записи блокировки портов, SSL, SSH, 802.1X, доверенный хост (Trusted Host), управление аутентификацией доступа и сегментацию трафика.

Раздел 11, Мониторинг – Содержит описание функций мониторинга, включая использование CPU, использование порта, информацию о количестве пакетов, пакетов с ошибками, размер пакетов, MAC-адресе, журнале коммутатора, группе IGMP Snooping, поиске порта маршрутизатора, статических настройках ARP, таблицу сессий и управление доступом к порту.

Приложение A, Техническая спецификация – Техническая спецификация для коммутаторов DES-3028/DES-3028P/DES-3052/DES-3052P.

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

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

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

Предполагаемые читатели

Руководство пользователя для коммутаторов DES-3028/DES-3028P/DES-3052/DES-3052P содержит необходимую информацию для их настройки и управления. В дальнейшем термин «Коммутатор» будет означать любой из четырех коммутаторов серии. Это руководство предназначено преимущественно для администраторов сети, знающих принципы сетевого управления и терминологию.

Условные обозначения

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

Замечания, предупреждения и предостережения

ЗАМЕЧАНИЕ содержит важные указания, помогающие наиболее эффективно использовать устройство.

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

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

Инструкция по безопасности

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

 Предостережения безопасности

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

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

• Убедитесь, что характеристики питания подключаемых устройств соответствуют нормам, действующим в данной местности.

• Используйте только подходящие силовые кабели. Если нужный кабель не входил в комплект поставки, то приобретите силовой кабель, который одобрен для использования в вашей стране. Силовой кабель

должен соответствовать характеристикам напряжения и тока, необходимым для данного устройства. Характеристики напряжения и тока кабеля должны быть больше, чем мощность, указанная на устройстве.

• Чтобы избежать удара электрическим током, при работе с устройством пользуйтесь заземленными должным образом электрическими розетками и кабелями.

• Соблюдайте характеристики кабеля-удлинителя и шины питания. Удостоверьтесь, что общий номинальный ток всех устройств, подключенных к кабелю-удлинителю или шине питания, не превышает лимит 80% номинального тока кабеля-удлинителя или шины питания.

• Для обеспечения защиты системы от внезапных кратковременных скачков электропитания используйте ограничитель напряжения, формирователь линии или источник бесперебойного питания (UPS).

• Кабели, используемые для подключения устройства, необходимо размещать таким образом, чтобы на них не наступали и не спотыкались об них. Убедитесь также, что на кабелях ничего не лежит.

• Не заменяйте используемые кабели питания или штепсели, не проконсультировавшись у квалифицированного электрика или в энергетической компании. Всегда следуйте существующим в стране нормам по прокладке кабелей.

• При подключении или отключении от сети в «горячем» режиме источника питания, рекомендуемого для использования с данным устройством, соблюдайте следующие указания:

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

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

Общие меры безопасности для устройств, устанавливаемых в стойку

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

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

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

• Перед началом работы убедитесь, что стабилизаторы прикреплены к стойке и что стойка устойчиво упирается в пол. Установите передний и боковой стабилизаторы на стойку или только передний стабилизатор для соединения нескольких стоек.

• Всегда загружайте оборудование в стойку снизу вверх, начиная с самого тяжелого.

• Перед добавлением компонента в стойку, убедитесь, что стойка устойчива.

• Соблюдайте осторожность, передвигая компоненты стойки по удерживающим рельсам, - рельсы могут защемить пальцы

• После того, как компонент вставлен в стойку, аккуратно удлините рельс в положение захвата, и тогда поместите компонент в стойку

• Не перегружайте ветвь питания переменного тока распределительной сети, обеспечивающей электропитание стойки. Стойка при полной загрузке не должна потреблять более 80% мощности, доступной для данной ветви распределительной сети.

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

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

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

ПРЕДОСТЕРЕЖЕНИЕ: При необходимости заменить заземляющий провод или работающее оборудование нужно обеспечить наличие другого заземляющего провода. Свяжитесь с соответствующей инспекцией или электриком, если сомневаетесь, что подходящее заземляющее устройство имеется в наличии.

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

Защита от электростатического разряда

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

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

Раздел 1

Введение

Описание коммутаторов DES-3028/28P/52/52P
Технические характеристики
Порты
Компоненты передней панели
Описание боковой панели
Описание задней панели
Комбо-порты Gigabit Ethernet

Описание коммутаторов DES-3028/28P/52/52P

Коммутаторы DES-3028, DES-3028P, DES-3052 и DES-3052P объединены в единую серию в продуктовой линейке D-Link. Эти устройства обеспечивают высокую производительность, отказоустойчивость, масштабируемость и гибкость построения сети. Помимо этого, эти коммутаторы оснащены функционалом безопасности и обеспечивают взаимодействие устройств на основе признанных стандартов.

Данное руководство описывает установку, эксплуатацию и настройку коммутаторов DES-3028, DES-3028P, DES-3052 и DES-3052P. Эти коммутаторы идентичны в настройках и по основным аппаратным средствам, соответственно большая часть информации в данном руководстве будет универсальной для всех коммутаторов этой серии. Соответствующие изображения на экране, возникающие при настройке через Web-интерфейс, будут представлены для одного из коммутаторов серии, однако пользователь без труда сможет выполнить аналогичные настройки и для других коммутаторов.

Технические характеристики

- Агрегирование портов (LACP) согласно IEEE 802.3ad
- Управление доступом IEEE 802.1x на основе портов и MAC-адресов
- IEEE 802.1Q VLAN
- Поддержка протоколов покрывающего дерева: IEEE 802.1D Spanning Tree, IEEE 802.1W Rapid Spanning Tree и IEEE 802.1s Multiple Spanning
- Поддержка списков управления доступом (ACL)
- Поддержка технологии Single IP Management (управление через единый IP-адрес)
- Управление аутентификацией доступа с помощью протоколов TACACS, XTACACS и TACACS+
- Внутренний Flash-диск для сохранения настроек и программного обеспечения
- Поддержка протокола SNTP (Simple Network Time Protocol)
- Поддержка MAC-уведомления
- Отображение статистики по использованию системы и портов
- Поддержка системного журнала
- Настройки на основе портов
- Таблица MAC-адресов: до 8K адресов на устройство
- Буфер пакетов до 512Кбайт
- Группы VLAN на основе портов
- Агрегирование портов с гибким распределением нагрузки и функцией fail-over
- Поддержка IGMP Snooping
- SNMP
- Поддержка Secure Sockets Layer (SSL) и Secure Shell (SSH)
- Зеркалирование портов

- Поддержка MIB для:
- RFC1213 MIB II
- RFC1493 Bridge
- RFC2819 RMON
- RFC2665 Ether-like MIB
- RFC2863 Interface MIB
- Private MIB
- RFC2674 для 802.1p
- IEEE 802.1x MIB
- Управление потоком IEEE 802.3x в полнодуплексном режиме
- Очереди приоритетов IEEE 802.1p
- IEEE 802.3u 100BASE-TX
- Консольный порт RS-232 DCE для управления коммутатором
- Отслеживание с помощью светодиодных индикаторов состояния порта (индикаторы link/act, speed и т.д.)
- IEEE 802.3 10BASE-T
- Высокопроизводительная коммутация, позволяющая осуществлять продвижение и фильтрацию пакетов со скоростью, соответствующей среде передачи: максимум 14 881 пакетов/с для каждого порта Ethernet 10Мбит/с, максимум 148 810 пакетов/с для каждого порта 100Мбит/с Fast Ethernet.
- Поддержка режимов полного и полудуплекса для соединений 10 и 100Мбит/с. В режиме полного дуплекса порт коммутатора может одновременно передавать и принимать данные. Этот режим используется для соединения с конечными станциями и коммутаторами, поддерживающими данный режим. Соединение с концентраторами должны осуществляться в режиме полудуплекса.
- Поддержка управления широковещательным/многоадресным штормом
- Неблокирующая схема коммутации store and forward с автоматическим выбором скорости и протокола.
- Поддержка управления входящей / исходящей скоростью на основе портов.
- Эффективный механизм распознавания и создания таблицы адресов.

Порты

В представленной ниже таблице содержится информация о количестве портов на коммутаторах:

DES-3028 и DES-3028P	DES-3052 и DES-3052P
Двадцать четыре порта 10/100BASE-T Два комбо-порта 1000BASE-T/SFP Два порта 1000Base-T Один консольный порт DCE RS-232 DB-9 с разъемом типа «мама»	Сорок восемь портов 10/100BASE-T Два комбо-порта 1000BASE-T/SFP Два порта 1000Base-T Один консольный порт DCE RS-232 DB-9 с разъемом типа «мама»

Следующая таблица описывает свойства каждого типа портов, доступных на коммутаторе:

Порты 10/100/1000BASE-T	Комбо-порты 1000BASE-T /SFP	Порты 1000Base-T

IEEE 802.3 IEEE 802.3u Управление потоком IEEE 802.3x в режиме полного дуплекса Поддержка автоматического определения полярности MDI-X/MDI-II	Поддержка следующих SFP-трансиверов: DEM-310GT (1000BASE-LX) DEM-311GT (1000BASE-SX) DEM-314GT (1000BASE-LH) DEM-315GT (1000BASE-ZX) DEM-210 (одномодовое волокно, 100BASE-FX) DEM-211 (многомодовое волокно, 100BASE-FX) Поддержка следующих трансиверов WDM: DEM-330T (TX-1550/RX-1310нм), до 10км, одномодовое волокно DEM-330R (TX-1310/RX-1550нм), до10км, одномодовое волокно DEM-331T (TX-1550/RX-1310нм), до 40км, одномодовое волокно DEM-331R (TX-1310/RX-1550нм), до 40км, одномодовое волокно Поддержка IEEE 802.3z и IEEE 802.3u	Поддержка IEEE 802.3 Поддержка IEEE 802.3u Поддержка IEEE 802.3ab Поддержка IEEE 802.3z Управление потоком IEEE 802.3x в режиме полного дуплекса

ПРИМЕЧАНИЕ: Комбо-порты SFP Коммутатора не могут использоваться одновременно с соответствующими портами 1000BASE-T. Если в одно и то же время используются оба порта из пары (например, порт 25 SFP и порт 25 1000BASE-T), то порт SFP имеет больший приоритет, и соответствующий порт 1000BASE-T не будет использоваться.

Компоненты передней панели

DES-3028P

- Двадцать четыре порта 10/100Base-TX (10/100Мбит/с)
- 2 комбо-порта 1000BASE-T/SFP (располагаются справа)
- Два порта 1000BASE-T (располагаются справа)
- Один консольный порт DCE RS -232 DB-9 с разъемом типа «мама»
- Светодиодные индикаторы Power (Питание), Console (Консоль), Link/Act/Speed для каждого порта.

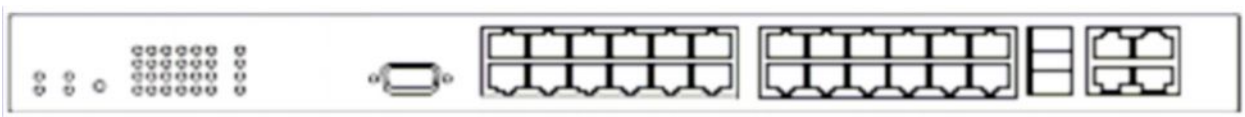


Рисунок 1.1 – Вид передней панели коммутатора DES-3028P

DES-3052P

- Сорок восемь портов 10/100Base-TX (10/100Мбит/с)
- 2 комбо-порта 1000BASE-T/SFP (располагаются справа)

- Два порта 1000BASE-T (располагаются справа)
- Один консольный порт DCE RS -232 DB-9 с разъемом типа «мама»
- Светодиодные индикаторы Power (Питание), Console (Консоль), Link/Act/Speed для каждого порта.

Рисунок 1.2 – Вид передней панели коммутатора DES-3052P

Светодиодные индикаторы

Следующая таблица содержит список индикаторов, расположенных на коммутаторе серии DES-30xx, а также их описание:

	Индикатор	Цвет	Статус	Описание
На устройство	**Power**	Зеленый	Горит	Питание включено
			Не горит	Питание выключено
	Console	Зеленый	Горит	Используется консоль
			Не горит	Консоль не используется
Кнопка выбора режима	**Link/Act/Speed**	Зеленый	Горит	Режим Link/Act/Speed
	PoE	Зеленый	Горит	Режим PoE.
На порт 10/100 Мбит/с	**Link/Act/Speed**	Зеленый/ Желтый	Горит (зеленый)	Указывает на активное соединение на скорости 100Мбит/с
			Мигает (зеленый)	Указывает на прием или передачу данных (активность) на порту со скоростью 100Мбит/с
			Горит (желтый)	Указывает на активное соединение на скорости 10Мбит/с
			Мигает (желтый)	Указывает на прием или передачу данных (активность) на порту со скоростью 10Мбит/с
			Не горит	Канал отсутствует.
	PoE	Зеленый	Горит	Питаемое PoE устройство подключено.
			Мигает	На порту обнаружена ошибка.
			Не горит	Устройство получает питание от источника переменного тока или устройство PoE не обнаружено.
На порт GE	**Link/Act/Speed для портов 1000Base-T**	Зеленый/ Желтый	Горит (зеленый)	Указывает на активное соединение на скорости 1000Мбит/с

			Мигает (зеленый)	Указывает на прием или передачу данных (активность) на порту со скоростью 1000Мбит/с
			Горит (желтый)	Указывает на активное соединение на скорости 100Мбит/с
			Мигает (желтый)	Указывает на прием или передачу данных (активность) на порту со скоростью 100Мбит/с
			Не горит	Канал отсутствует.
	Link/Act/Speed для портов SFP	Зеленый/ Желтый	Горит (зеленый)	Указывает на активное соединение на скорости 1000Мбит/с
			Мигает (зеленый)	Указывает на прием или передачу данных (активность) на порту со скоростью 1000Мбит/с
			Горит (желтый)	Указывает на активное соединение на скорости 100Мбит/с
			Мигает (желтый)	Указывает на прием или передачу данных (активность) на порту со скоростью 100Мбит/с
			Не горит	Канал отсутствует.

Установка трансиверов SFP

Коммутаторы DES-3028/28P/52/52P оснащены портами SFP (Small Form Factor Portable), которые предназначены для использования с оптическим трансиверами в целях организации uplink-канала к различным сетевым устройствам на дальние расстояния. SFP-порты поддерживают переачу данных в режиме полного дуплекса, автосогласование скорости и могут использоваться с оптическим трансиверами DEM-310GT (1000BASE-LX), DEM-311GT (1000BASE-SX), DEM-210 (100BASE-FX, одномодовое волокно), DEM-211 (100BASE-FX, многомодовое волокно), DEM-314GT (1000BASE-LH), DEM-315GT (1000BASE-ZX), DEM-330T/R (WDM) и DEM-331T/R (WDM). Рисунок ниже показывает, как установить трансиверы SFP на Коммутатор.

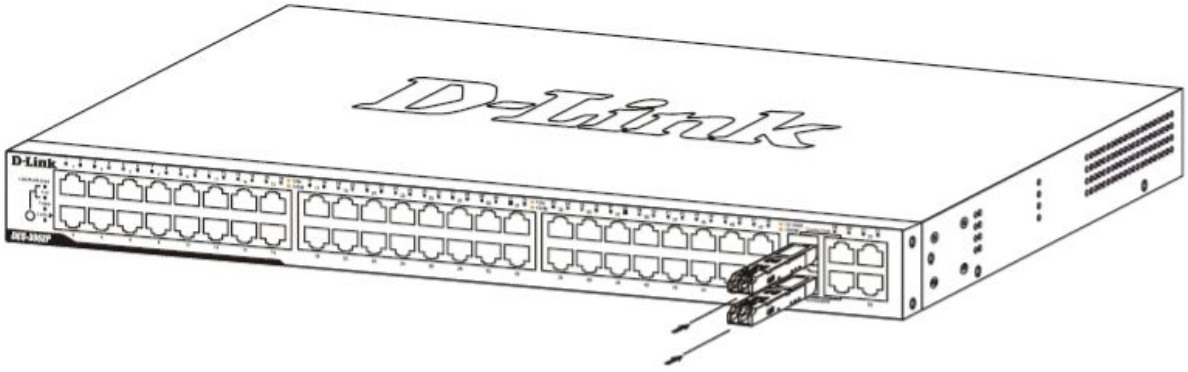


Рисунок 1.3 – Установка оптических трансиверов на коммутатор DES-3028/28P/52/52P

Раздел 2

Установка

Комплект поставки
Перед началом работы
Настольное размещение коммутатора
Монтаж коммутатора в стойку
Включение электропитания

Комплект поставки

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

- Один коммутатор серии DES-30xx
- Один шнур питания переменного тока (AC)
- CD-диск с руководством пользователя
- Набор для крепления в стойку (петли и винты)
- Четыре резиновые «ножки» с одной клейкой стороной
- RS-232 консольный шнур

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

Перед началом работы

Местоположение коммутатора может значительно влиять на его характеристики. Пожалуйста, следуйте данным рекомендациям для установки коммутатора.

- Установите коммутатор на прочную горизонтальную поверхность, которая может выдержать, по крайней мере, 4,24 кг. Не помещайте тяжелые предметы на коммутатор.
- Электрическая розетка должна быть не далее 1,82 м от коммутатора.
- Осмотрите шнур питания и проверьте, чтобы он был плотно закреплен в разъеме питания переменного тока.
- Убедитесь, что существует надлежащий теплоотвод и соответствующая вентиляция вокруг коммутатора. Оставьте по 10 см свободного пространства перед передней и задней панелью коммутатора.
- Установите коммутатор в довольно прохладном и сухом месте с допустимым рабочим диапазоном температур и влажности.
- Установите коммутатор таким образом, чтобы отсутствовали источники сильного электромагнитного поля, вибрация, пыль и воздействия прямых солнечных лучей.
- Когда будете устанавливать коммутатор на горизонтальную поверхность, прикрепите резиновые ножки на основание устройства. Резиновые «ножки» коммутатора предохранят корпус от царапин.

Настольное размещение коммутатора

Прежде чем установить коммутатор на стол или полку, прикрепите сначала прилагающиеся к коммутатору резиновые «ножки». Прикрепите эти амортизационные «ножки» в углы основания устройства. Обеспечьте достаточное вентиляционное пространство между коммутатором и другими предметами поблизости.

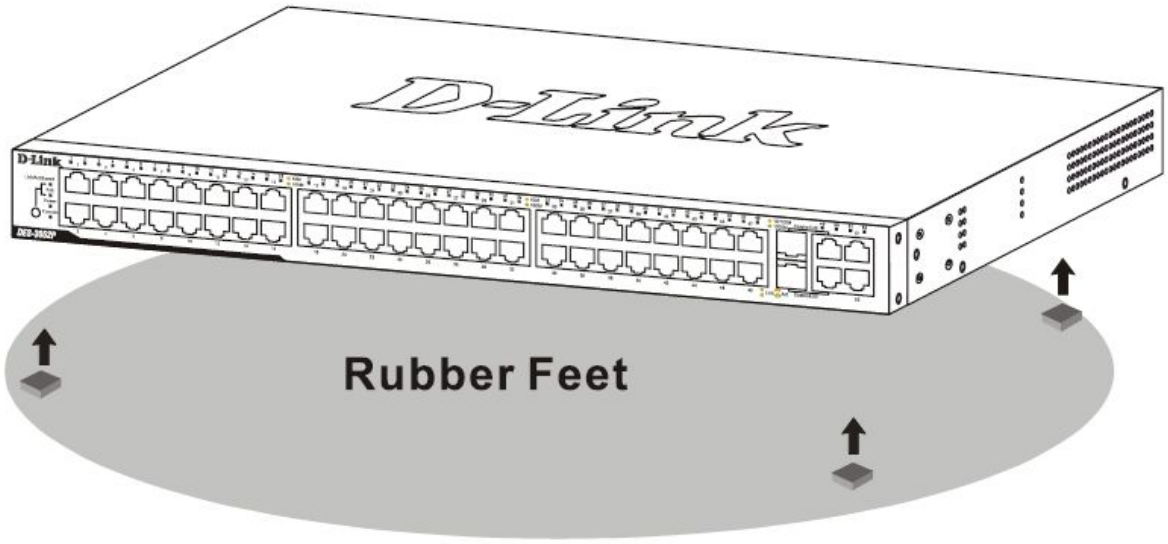


Рисунок 2.1 – Подготовка коммутатора к установке на стол или полку

Монтаж коммутатора в стойку

Коммутатор может быть установлен в стандартную 19'' стойку. Используйте следующие рисунки в качестве руководства.

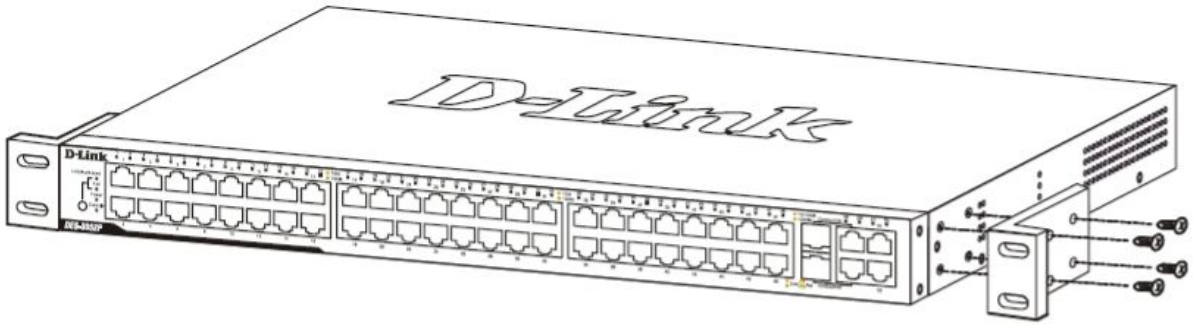


Рисунок 2.2 – Прикрепление петлей к коммутатору

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

Монтаж коммутатора в стандартную 19'' стойку

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

вынимайте из стойки более одного устройства, поскольку это может привести к опрокидыванию стойки и нанесению повреждений.

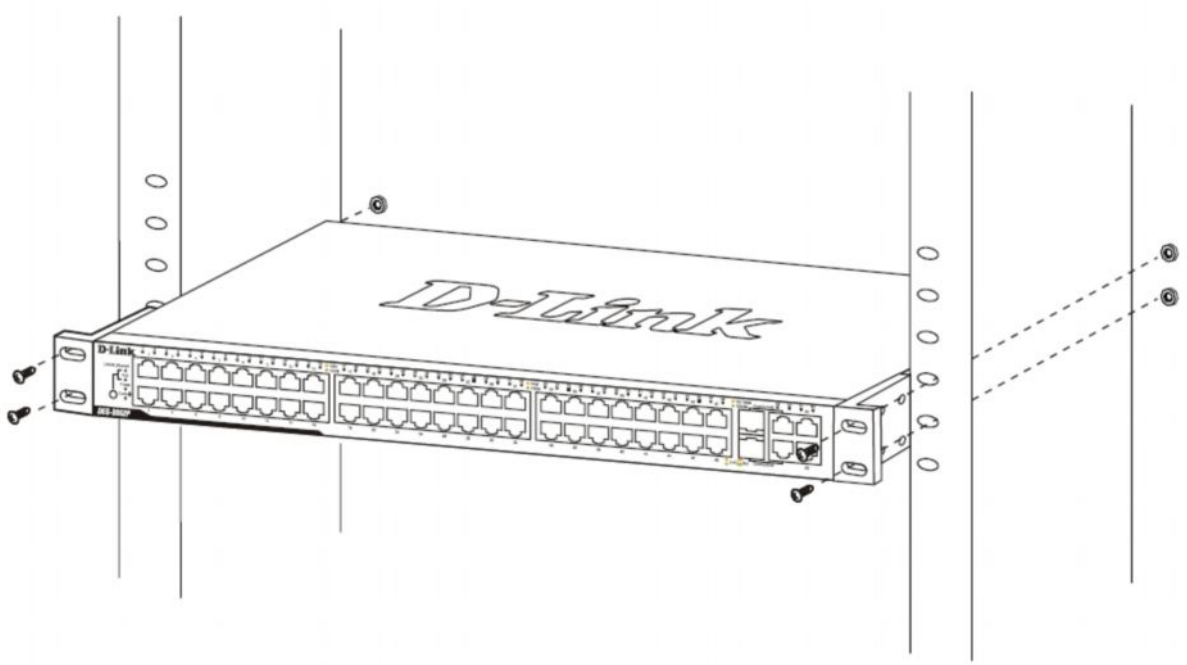


Рисунок 2.3 – Монтаж коммутатора в стойку

Включение электропитания переменным током

Один конец шнура питания вставьте в разъем питания коммутатора, а другой конец в гнездо ближайшей розетки. После того, как включите коммутатор, сразу же замигают светодиодные индикаторы. Подобное мигание означает установку системы в исходное состояние.

Отключение электричества

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

Раздел 3

Подключение коммутатора

Подключение коммутатора к конечному узлу

Подключение коммутатора к концентратору или коммутатору

Подключение коммутатора к магистрали сети или серверу

Примечание: Все порты 10/100/1000Мбит/с NWay Ethernet 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 или 1000 Мбит/с с разъемом RJ-45, а также большинство маршрутизаторов. Конечный узел может быть подключен к любому порту коммутатора по витой паре категории 3, 4 или 5 UTP/STP-кабеля. Конечный узел может быть подключен к любому порту Коммутатора.

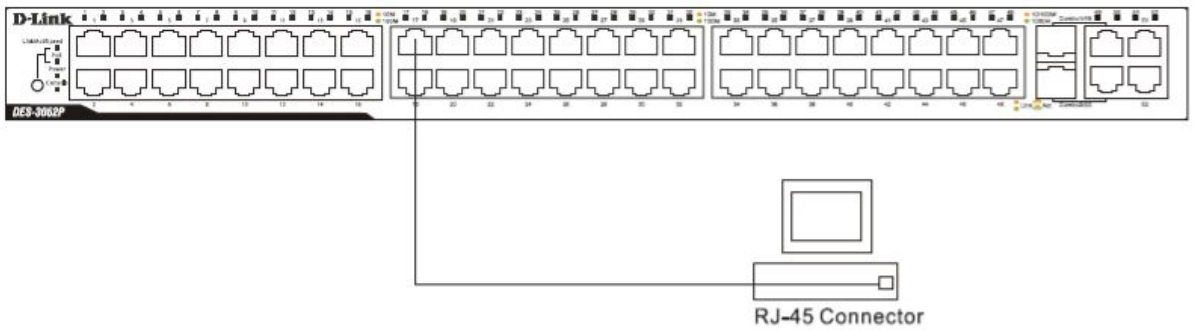


Рисунок 3.1 – Подключение коммутатора к конечному узлу

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

Подключение коммутатора к концентратору или коммутатору

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

- Концентратор или коммутатор 10 Base-T может быть подключен к коммутатору по витой паре категории 3, 4 или 5 неэкранированного/экранированного (UTP/STP) кабеля.
- Концентратор или коммутатор 100Base-TX может быть подключен к коммутатору по витой паре 5 категории неэкранированного/экранированного (UTP/STP) кабеля.

- Концентратор или коммутатор 1000Base-T может быть подключен к коммутатору по витой паре 5e категории неэкранированного/экранированного (UTP/STP) кабеля.
- Коммутатор, поддерживающий оптические порты uplink, может быть подключен к SFP-портам с помощью оптических кабелей.

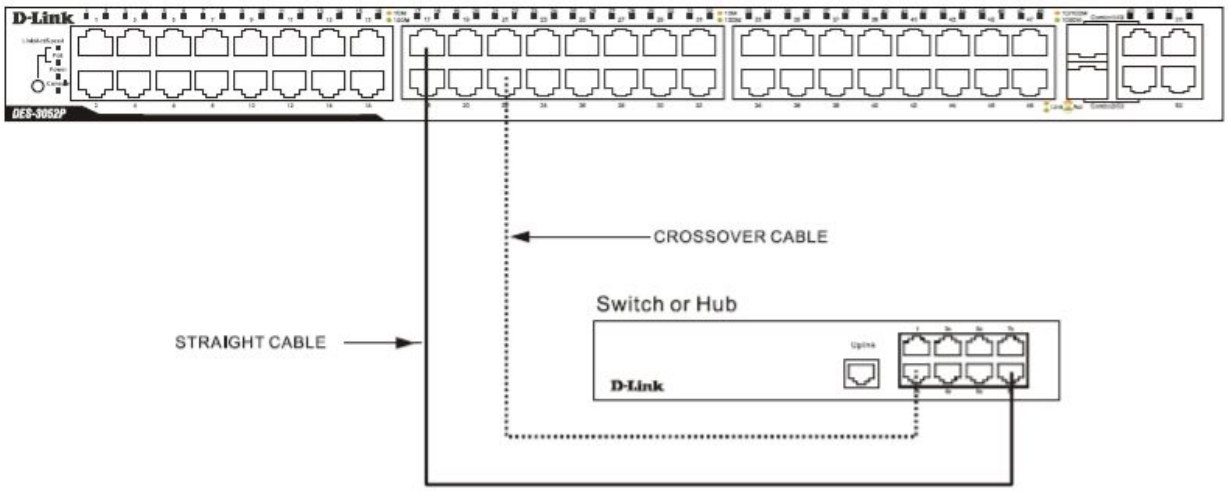


Рисунок 3.2 – Коммутатор, подключенный к обыкновенному (не Uplink) порту концентратора или коммутатора с помощью прямого или кроссового кабеля

ПРИМЕЧАНИЕ: При использовании SFP-порта соответствующий порт 10/100/1000BASE-T из пары будет отключен.

Раздел 4

Введение в управление коммутатором

Функции управления

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

Web-интерфейс управления

После успешной установки коммутатора, можно настраивать его, проверять состояние устройства по светодиодам на передней панели и графически отображать статистику, используя Web-браузер, например, Netscape Navigator (версии 6.2.3 и выше) или Microsoft Internet Explorer (версия 6.0).

Управление через SNMP- протокол

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

Подключение к консольному порту коммутатора (RS-232 DCE)

Коммутатор снабжен консольным портом RS-232, с помощью которого можно осуществить подключение к компьютеру или терминалу для управления и настройки коммутатора. Данный порт – это коннектор DB-9 типа «мама», выполненный для подключения терминального оборудования (DTE – Data Terminal Equipment).
Для использования консольного порта вам понадобится следующее оборудование:

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

Для подключения терминала к консольному порту:

1. Подключите кабель RS-232 с коннектором типа «мама» к консольному порту коммутатора и плотно закрутите винты.

2. Подключите другой конец кабеля к терминалу или последовательному порту компьютера. Установите программное обеспечение эмулятора терминала следующим образом:
3. Выберите подходящий последовательный порт (COM порт 1 или COM порт 2).
4. Установите скорость передачи данных 9600 бод.
5. Установите формат данных: 8 бит данных; 1 стоповый бит и отсутствие контроля по четности.
6. Установите отсутствие управление потоком.
7. В **Properties** следует выбрать режим *VT 100* для запуска режима эмуляции.
8. Необходимо выбрать терминальные клавиши для функций, стрелок и Crtl. Убедитесь, что выбранные клавиши, не совпадают с «горячими клавишами» Windows.

Примечание: Когда используется 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

9. После того, как терминал установлен правильно, следует вставить шнур питания в гнездо питания на задней панели коммутатора. На терминале отобразится процесс загрузки.
10. После того, как завершится процесс загрузки, появится окно **console login**.
11. Если регистрация в программе интерфейса командной строки (CLI) еще не произведена, следует нажать клавишу **Enter,** не вводя информацию в полях **Имя пользователя** (User name) и **Пароль** (Password), т.к. они не заданы по умолчанию. Администратор, прежде всего, должен создать имя пользователя и пароль. Если учетные записи пользователей были установлены ранее, следует зарегистрироваться, введя соответствующие имя пользователя и пароль, и продолжить настройку коммутатора.
12. Введите команды для выполнения требуемых задач. Многие команды требуют привилегии доступа уровня администратора. Прочитайте следующий раздел для получения информации по настройке учетных записей пользователей. В документации на CD-диске просмотрите ***Справочное руководство по интерфейсу командной строки для коммутаторов серии DES-3028/28P/52/52P,*** где приведен список всех команд и дополнительная информация по использованию CLI.
13. После того, как задачи выполнены, нужно 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 нет имени пользователя и пароля: таким образом, для доступа к интерфейсу командной строки необходимо будет дважды нажать Enter.

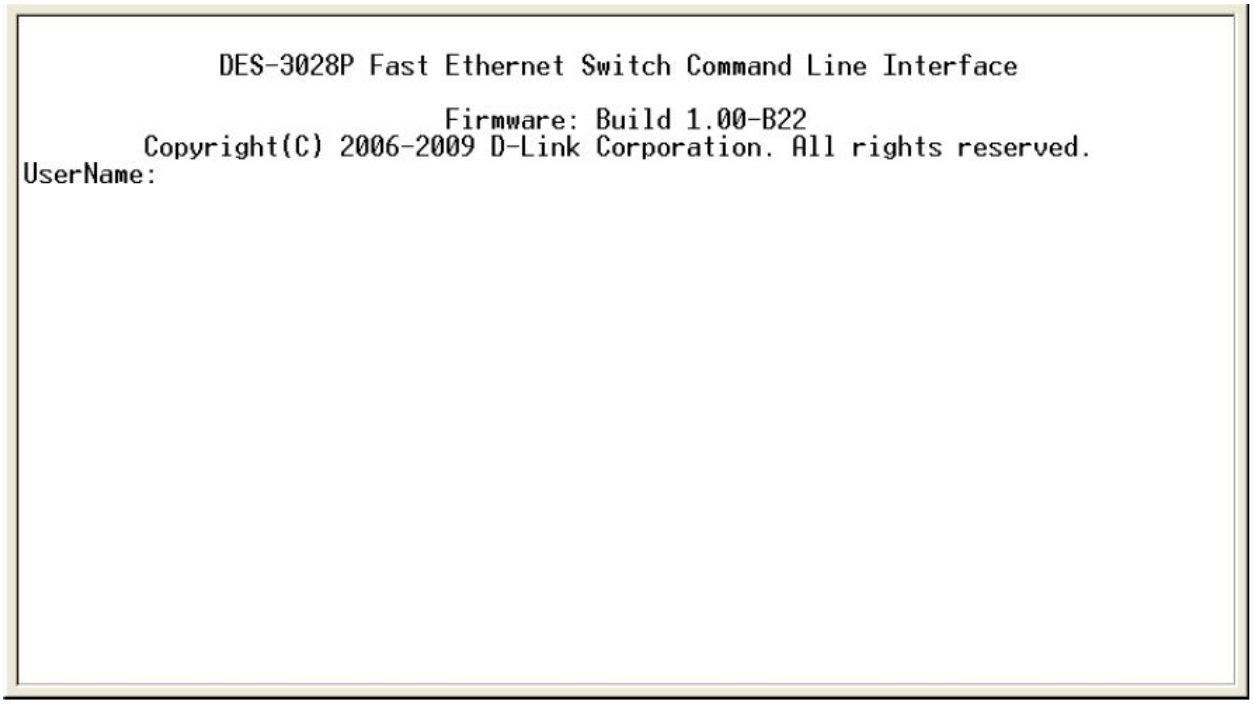


Рисунок 4.1 – Исходный экран при первом подключении

Первое подключение к коммутатору

Коммутатор поддерживает 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 является идентичным «s».

Во время первого подключения к коммутатору появится регистрационное окно.

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

Нажмите Enter в обоих полях Username (Имя пользователя) и Password (Пароль). После чего будет предоставлен доступ к командной строке **DES-3028P:4#,** как это показано ниже.

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

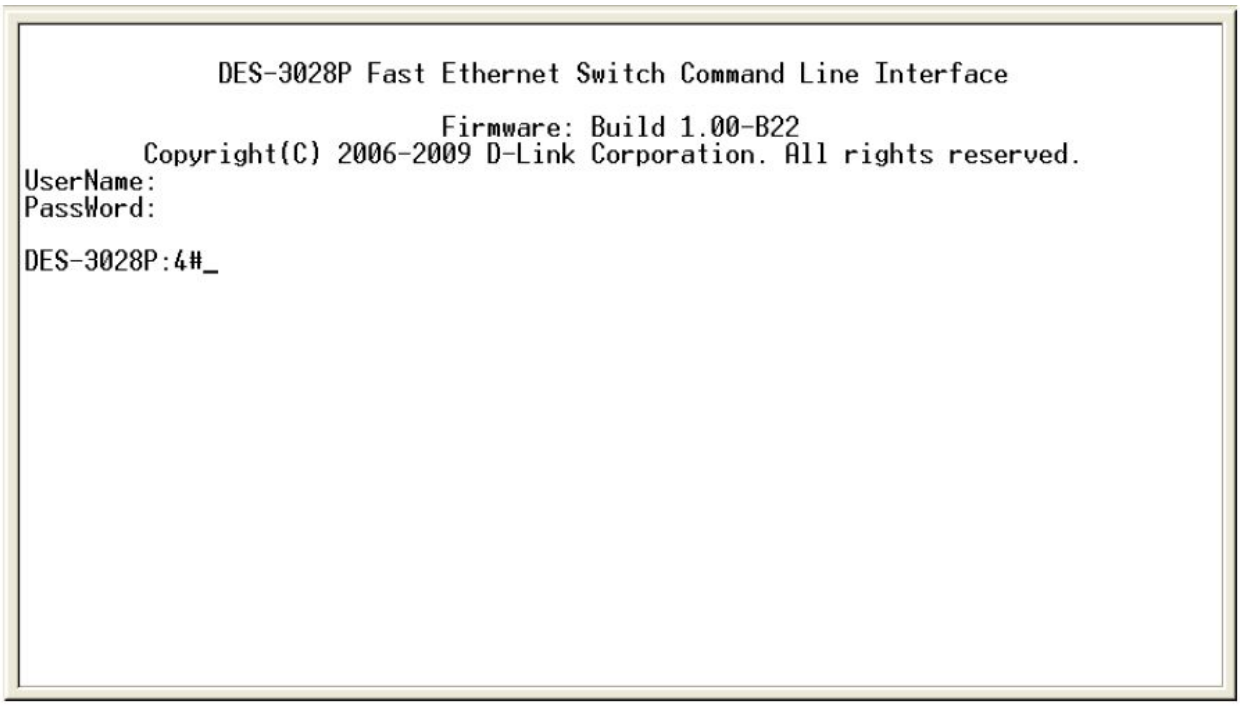


Рисунок 4.2 – Командная строка

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

Защита паролем

В коммутаторах серии DES-30xx по умолчанию нет имени пользователя и пароля. 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 коммутатора.
После первоначальной регистрации, создайте новые пароли для каждого имени пользователя для предотвращения доступа к коммутатору неавторизованных пользователей и запишите пароли.

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

- В командной строке CLI введите созданную учетную запись администратора, следующую за *<user name>,* и нажмите клавишу Enter.
- Вас попросят ввести пароль. Введите пароль *<password>* , использованный для созданной учетной записи администратора и нажмите клавишу Enter.
- Для подтверждения пароля вас попросят ввести его еще раз. Введите тот же пароль и нажмите клавишу Enter.
- Удачное создание новой учетной записи администратора будет подтверждено сообщением.

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

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

```
DES-3028:4# create account admin newmanager
Command: create account admin newmanager

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

Success.

DES-3028:4#
```

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

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.

Коммутатор серии DES-30xx поддерживает протокол SNMP версий: 1, 2c и 3. Можно указать, какую версию SNMP использовать для контроля и управления коммутатором. Три версии SNMP протокола различаются в уровне обеспечиваемой безопасности между управляющей станцией и сетевым оборудованием.

В SNMP версиях v.1 и v.2 аутентификация пользователей осуществляется при помощи так называемой «строки сообщества» («community string»), данная функция похожа на пароли. Удаленный пользователь 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, можно 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 или ограничено выполнение определенных функций управления SNMP. Функции «разрешено» или «запрещено» определяются идентификатором объекта (OID – Object Identifier), связанного со специальной базой MIB. В SNMP v.3 доступен дополнительный уровень безопасности: в данной версии SNMP сообщения могут быть зашифрованы. Для получения большей информации по настройке SNMP v.3 в коммутаторе, прочитайте раздел под названием Управление.

Traps

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

Базы управляющей информации MIB

Коммутатор хранит в базе управляющей информации MIB управляющую информацию и значения счетчика. Коммутатор использует стандартный модуль MIB-II. В результате, значения объектов MIB могут быть извлечены из любого сетевого управляющего программного обеспечения, основанного на проколе SNMP. Помимо стандартной базы MIB-II, коммутатор также поддерживает свою собственную базу MIB, в качестве расширенной базы данных управляющей информации. 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). По умолчанию, IP-адрес коммутатора - 10.90.90.90. Можно изменить этот адрес, для того чтобы получить схему распределения 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:

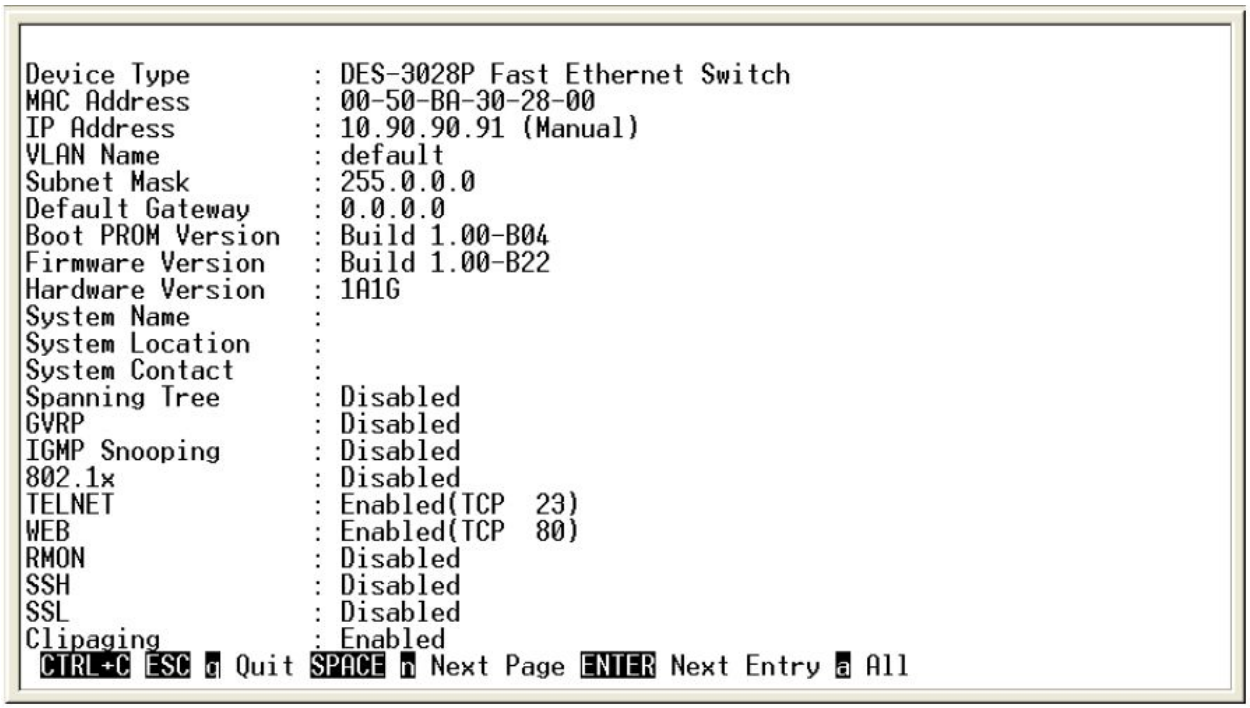


Рисунок 4.3 – Команда «show switch»

MAC-адрес коммутатора можно также найти через управляющую Web-программу в окне **Switch Information (Basic Settings)** в меню **Configuration.**
IP-адрес коммутатора должен быть установлен до начала управления коммутатором с помощью Web-интерфейса управления. IP-адрес коммутатора может быть автоматически установлен, используя протоколы BOOTP или DHCP: в данном случае должен быть известен текущий адрес, назначенный коммутатору. Также IP-адрес может быть установлен с помощью интерфейса командной строки CLI 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.

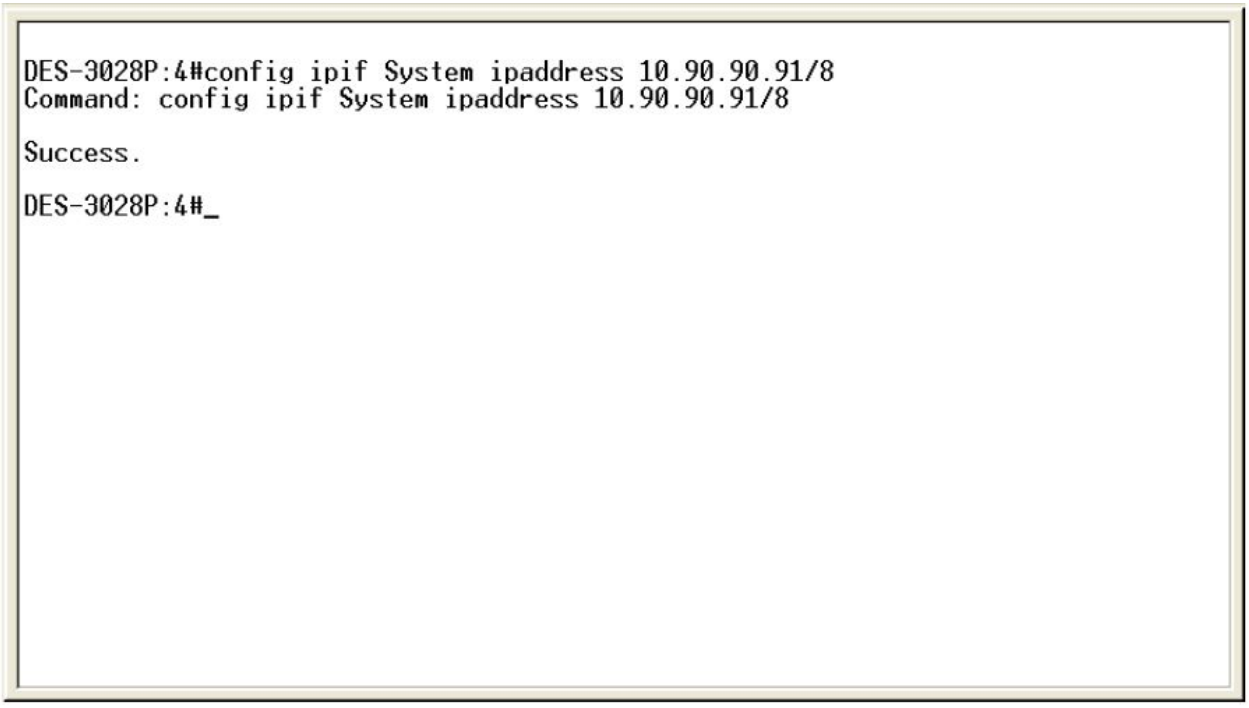


Рисунок 4.4 – Назначение IP-адреса коммутатору

В приведенном выше примере коммутатору назначен IP-адрес 10.90.90.91 с маской подсети 255.0.0.0 (в формате CIDR -10.90.90.91/8). Системное сообщение **Success** свидетельствует о том, что команда успешно выполнена. Теперь можно настраивать и управлять коммутатором через Telnet и CLI или через Web-интерфейс управления.

Раздел 5

Настройка коммутатора через Web-интерфейс

Введение

Все программные функции коммутатора серии DES-30xx могут управляться, настраиваться и контролироваться через встроенный Web-интерфейс управления (HTML). Коммутатором можно управлять с удаленных станций сети через стандартный браузер, такой как Opera, Netscape Navigator/Communicator или Microsoft Internet Explorer. Браузер работает как универсальное средство доступа и может соединяться с коммутатором напрямую через HTTP-протокол.
Модуль управления через Web-интерфейс и консольная программа (Telnet) – это различные способы для доступа к одному и тому же внутреннему коммутирующему программному обеспечению и его настройки. Таким образом, все настройки, встречающиеся в Web-интерфейсе идентичны тем, которые представлены в консольной программе.

Регистрация в Web-интерфейсе управления

Для того чтобы начать настройку коммутатора, просто запустите браузер, установленный на компьютере, и укажите IP-адрес, который определён для устройства. URL в адресной строке должен выглядеть следующим образом: http://123.123.123.123, где вместо чисел 123 необходимо вставить реальный IP-адрес коммутатора.

Примечание: Заводской IP-адрес коммутатора по умолчанию 10.90.90.90.

На открывшейся странице нажмите **Login.** Откроется окно аутентификации пользователя, как показано ниже:

Рисунок 5.1 – Окно Enter Network Password

Оставьте поля User Name (Имя пользователя) и Password (Пароль) незаполненными и нажмите **ОК**. Это позволит зарегистрироваться в пользовательском Web-интерфейсе. Возможности по управлению коммутатором, доступные с помощью Web-интерфейса управления, поясняются ниже.

Пользовательский Web-интерфейс

Web-интерфейс обеспечивает доступ к различным настройкам и опциям управления коммутатора, позволяет просмотреть статистические данные, в том числе и в виде графиков.

Поля Web-интерфейса пользователя

Рисунок, представленный ниже, демонстрирует окно пользовательского интерфейса управления: оно делится на три отдельные области, как это и описывается далее в таблице.

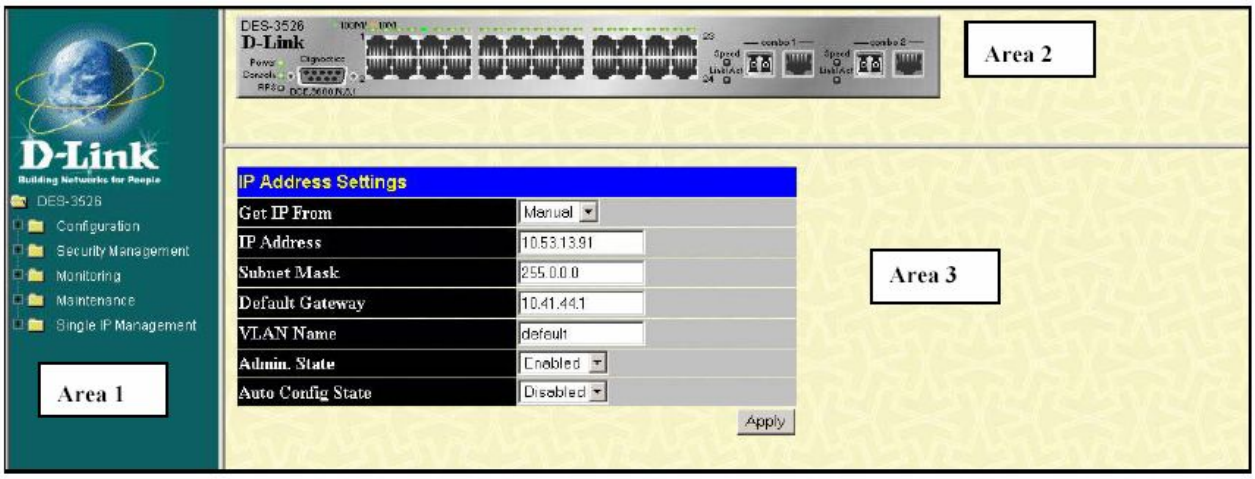


Рисунок 5.2 – Главная страница Web-менеджера

Область	Функция
Area 1	Выберите форму для отображения: меню или окно. Иконка папки должна быть открыта, для того чтобы отображались осуществленные гиперссылки, кнопки меню и подпапки, содержавшиеся в них. Щелкните по логотипу D-Link, чтобы

	перейти на сайт D-Link.
Area 2	Отображает графическое представление передней панели коммутатора почти в реальном режиме времени. Данная область отображает порты коммутатора, модули расширения, светодиодную индикацию, дуплексный режим, контроль потока, зависящие от выбранного режима. Можно выбирать различные области для представления различных функций управления, включая конфигурацию портов.
Area 3	Представленная здесь информация по коммутатору базируется на выборе пользователя и введённых конфигурационных данных.

Примечание: Любые изменения, произведенные в настройках коммутатора во время текущей сессии, должны быть сохранены в Web-меню (описанном ниже) Save Changes или с помощью команды Save (Сохранить) в интерфейсе командной строки CLI.

Опции, доступные через Web-интерфейс

При управлении коммутатором через Web-браузер сначала появляется окно регистрации, в котором необходимо ввести соответствующее имя пользователя и пароль. Ниже приведен список и описание основных папок, доступных через Web-интерфейс:

Administration (Управление) – содержит опции, позволяющие настроить основные функции Коммутатора, включая Device Information (Информацию об устройстве), IP Address (IP-адрес), Port Configuration (Настройка порта), DHCP/BOOTP Relay, User Accounts (Учетные записи пользователей), Port Mirroring (Зеркалирование портов), System Log Settings (Настройки журнала Коммутатора), Log Settings, SNTP Settings (Настройки SNTP), MAC Notification Settings (Настройки MAC-уведомления), TFTP Services (Сервисы TFTP), Multiple Image Services, Ping Test (Ping-тест), Safeguard Engine, SNMP Manager (SNMP-менеджер), PoE System (система PoE), Single IP Settings (Настройки управления через единый IP-адрес), Forwarding & Filtering (продвижение и фильтрация пакетов) и SMTP Service (сервис SMTP).

Layer 2 Features (Функции уровня 2) – содержит опции, позволяющие настроить функции уровня 2 Коммутатора, включая VLAN, агрегирование каналов, IGMP Snooping и Spanning Tree.

CoS (Класс обслуживания) – содержит опции, позволяющие настроить Port Bandwidth (полоса пропускания порта), 802.1P Default Priority (приоритет по умолчанию 802.1p), 802.1P User Priority (приоритет пользователя 802.1P), CoS Scheduling Mechanism (работа CoS по расписанию), CoS Output Scheduling, Priority Settings (настройки приоритета), TOS Priority Settings (настройки приоритета TOS), Port Mapping Priority Settings и MAC Priority (приоритет на основе MAC-адреса).

ACL (Списки управления доступом) – содержит опции, позволяющие настроить Time Range (временной диапазон), Access Profile Table (таблица профилей доступа) и CPU Interface Filtering.

Security (Безопасность) – содержит опции, позволяющие настроить Traffic Control (управление трафиком), Port Security (безопасность на уровне портов), Port Lock Entries, SSL, SSH, 802.1x, Trusted Host (доверенный хост), Access Authentication Control (управление аутентификацией доступа) и Traffic Segmentation (сегментация трафика).

Monitoring (Мониторинг)– содержит опции, позволяющие отслеживать CPU Utilization (использование CPU), Port Utilization (использование порта), Packets (количество пакетов), Packet Errors (ошибки в пакетах), Packet Size (размер пакетов), MAC Address(MAC-адрес), Switch Log (Журнал Коммутатора), IGMP Snooping Group (группа IGMP Snooping), Browse Router Port (Поиск порта маршрутизатора), Static ARP Settings (Статические настройки ARP), Session Table (Таблица сессий) и Port Access Control (Управление доступом на основе портов).

Switch Maintenance (Обслуживание Коммутатора)– содержит информацию, касающаяся Reset (сброс настроек), Reboot System (перезагрузка системы), Save Changes (сохранение изменений) и Logout (выход из системы).

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

Раздел 6

Управление

Информация о Коммутаторе

Окно **Device Information** содержит основные настройки большинства функций Коммутатора. При регистрации это окно появляется автоматически. Для возврата к окну **Device Information** кликните по папке **DES- 30xx Web Management Tool**. Окно Device Information отображает **MAC Address** (задается на заводе и не может быть изменен), **Boot PROM**, **Firmware Version** (версия программного обеспечения) и **Hardware Version** (версия аппаратного обеспечения). Это окно позволяет просмотреть версию PROM и программного обеспечения, а также MAC-адрес Коммутатора для записи в адресную таблицу других сетевых устройств, если это необходимо. Пользователь может также ввести **System Name** (Имя системы), **System Location** (Расположение устройства) и **System Contact** (Контакт системы)**,** что позволяет задать информацию о Коммутаторе в соответствии с предпочтениями пользователя. Кроме того, это окно отображает статус основных опций коммутатора, что позволяет получить быстрый доступ к их текущему статусу. Также в этом окне представлены гиперссылки на окна настроек соответствующих параметров.

Рисунок 6-1. Окно Device Information

Описание полей, доступных для настройки, приводится ниже:

Параметр	Описание

System Name	Введите системное имя Коммутатора, если это требуется. Это имя будет идентифицировать устройство в сети.
System Location	Введите расположение Коммутатора, если это необходимо.
System Contact	Введите контактное лицо для данного устройства, если это необходимо.
Serial Port Auto Logout Time	Введите время завершения сессии для консольного интерфейса. Это автоматически приведет к отключению пользователя после завершения заданного временного интервала. Выберите одну из следующих опций: *2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes* или *Never*. По умолчанию настроено *10 minutes*.
Serial Baud Rate	Это поле задает бодовую скорость на последовательном порту Коммутатора. На выбор доступны следующие опции: *9600*, *19200*, *38400* и *115200.* Для подключения к Коммутатору с помощью интерфейса командной строки CLI, необходимо выбрать опцию *115200*, которая утсановлена по умолчанию.
MAC Address Aging Time	В данном поле задаётся период опроса MAC-адресов (время хранения MAC-адреса в таблице MAC-адресов). Чтобы изменить данный параметр надо задать новый период в секундах. Значение этого поля может быть от 10 до 1 000 000 секунд. Значение по умолчанию 300 секунд.
IGMP Snooping	Чтобы включить глобально IGMP Snooping, выберите опцию *Enabled*. По умолчанию IGMP snooping выключена (*Disabled)*. Включение опции IGMP snooping позволяет задать использование только маршрутизатора многоадресной рассылки (см. ниже). Для настройки IGMP Snooping для отдельных VLAN воспользуйтесь опцией **IGMP Snooping**, находящейся в **L2 Features > IGMP Snooping**.
Multicast Router Only	Это поле задает, что Коммутатор будет продвигать весь многоадресный трафик на маршрутизатор с включенной опцией многоадресной рассылки. В противном случае Коммутатор будет осуществлять продвижение всего многоадресного трафика на любой IP-адрес маршрутизатора. По умолчанию опция выключена (*Disabled)*.
Telnet Status	По умолчанию возможность настройки Коммутатора через Telnet включена (*Enabled)*. Чтобы запретить возможность настройки через Telnet, выберите опцию *Disabled (выключено)*.
Telnet TCP Port Number (1-65535)	Номер TCP-порта. Порты TCP нумеруются от *1* до *65535*. TCP-порт, который, как правило, используется для протокола Telnet, - *23*.
Web Status	Возможность настройки Коммутатора через Web-интерфейс включена (*Enabled)* по умолчанию. При выборе опции *Disabled* (выключено) у пользователя не будет возможности настройки через Web-интерфейс.
Web TCP Port Number (1-65535)	Номер TCP-порта для Web-интерфейса (GUI). Порты TCP нумеруются от *1* до *65535*. TCP-порт, который, как правило, используется для протокола Web, - *80*.
RMON Status	Данное поле позволяет включить (*Enabled)* или выключить (*Disabled)* возможность удаленного мониторинга (RMON) за Коммутатором.
Link Aggregation Algorithm	В этом поле определяется алгоритм, который использует Коммутатор для балансировки нагрузки между портами, объединенными в группу агрегированных каналов. На выбор доступны такие опции, как *MAC Source*, *MAC Destination*, *MAC Src & Dest*, *IP Source, IP Destination* или *IP Src & Dest* (За более подробной информацией обратитесь к разделу Агрегирование каналов данного Руководства).
Switch 802.1X	Значение данного поля по умолчанию *Disabled* (выключено). Это поле необходимо включить для настройки определенных опций 802.1X. Более подробная информация, касающаяся 802.1X, будет рассмотрена далее в главе **Port Access Entity**. Аутентификация 802.1X на основе портов определяет, что порты,

	настроенные для 802.1X, инициализируются только на основе номера порта, а затем проводится аутентификация в соответствии с заданными параметрами. Авторизация на основе MAC-адресов определяет, что порты, настроенные для 802.1X, инициализируются на основе номера порта и MAC-адреса компьютера, а затем проводится авторизация в соответствии с заданными параметрами.
Auth Protocol	Протокол аутентификации 802.1X на Коммутаторе установлен как RADIUS Eap и не может быть изменен.
Syslog Status	Позволяет включить или выключить запись событий в журнал Коммутатора. По умолчанию значение *Disabled* (Выключено).
Port Security Trap Log	Данное поле позволяет включить или выключить функцию Port security trap log. По умолчанию значение Disabled (Выключено).
ARP Aging Time (0-65535)	Пользователь может задать максимальное время в минутах, в течение которого может храниться неиспользуемая запись в ARP-таблице Коммутатора. По истечении этого времени запись будет удалена из таблицы. Значение данного параметра может лежать в диапазоне от *0* до *65535* минут. Значение по умолчанию - *20* минут.
GVRP	Данное выпадающее меню позволяет пользователю глобально включить или выключить функцию GVRP на Коммутаторе.

Кликните по **Apply** для принятия выполненных изменений.

IP-адрес

Первоначально до подключения коммутатора к Ethernet его IP-адрес может быть установлен с помощью интерфейса командной строки. Если IP-адрес не изменялся ранее, следует обратиться к руководству по работе с командной строкой для DES-3028/28P/52/52P или вернуться к изучению раздела 4 данного руководства. Для изменения IP-адреса через Web-интерфейс, нужно зайти в меню **IP Address**, расположенное в папке **Administration**.

Чтобы настроить IP-адрес Коммутатора:
Откройте папку **Configuration** и кликните по ссылке **IP Address**. В окне **IP Address Settings** отобразятся текущие IP-настройки Коммутатора, как это показано ниже.

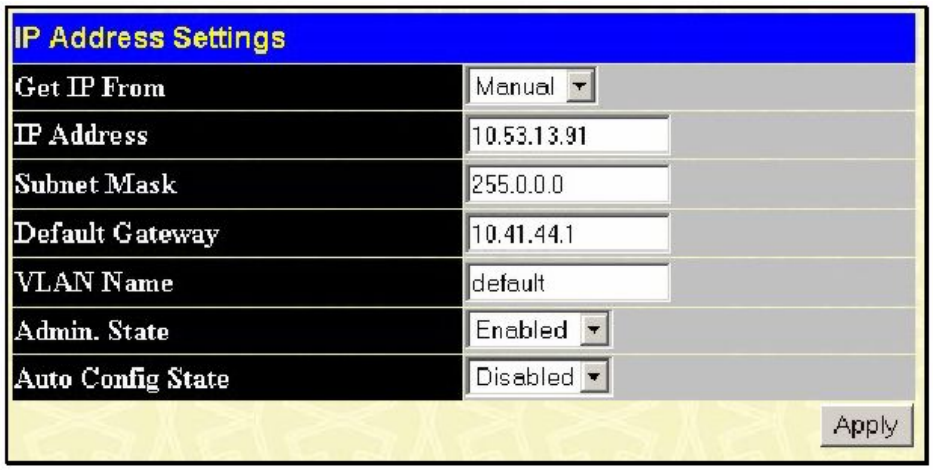


Рисунок 6-2. Окно IP Address Settings

Чтобы задать вручную IP-адрес Коммутатора, маску подсети и адрес шлюза по умолчанию:

1. В поле **Get IP From** из выпадающего меню следует выбрать *Manual*.
2. Ввести соответствующие IP-адрес и адрес маски подсети (Subnet Mask).

3. Если доступ к Коммутатору будет производиться через другую подсеть, следует ввести IP-адрес основного шлюза (Default Gateway). Если Коммутатор будет управляться через подсеть, в которой он находится, можно оставить адрес по умолчанию (0.0.0.0).
4. Если ни одна сеть VLAN пока не была сконфигурирована на Коммутаторе, можно использовать имя VLAN по умолчанию - *Default*. Если VLAN были предварительно установлены на Коммутаторе, необходимо установить VLAN ID (VID) той VLAN, которая содержит порт, соединённый с управляющей станцией. Причем с данной управляющей станции будет осуществляться доступ к Коммутатору. Доступ к управлению станцией будет осуществляться со станций, VID которых соответствует указанному здесь.

Примечание: По умолчанию установлен IP-адрес Коммутатора 10.90.90.90 с маской подсети 255.0.0.0 и основным шлюзом 0.0.0.0.

Чтобы задать настройки IP-адреса, маски подсети, адреса основного шлюза с помощью протоколов BOOTP или DHCP, в поле **Get IP From** следует выбрать соответственно *BOOTP* или *DHCP*. Таким образом указывается способ получения коммутатором IP-адреса при следующей перезагрузке.

Настройки IP-адреса:

Параметр	Описание
BOOTP	При включении Коммутатор будет посылать широковещательный BOOTP-запрос. При этом IP-адрес, маска подсети, основной шлюз коммутатора будут назначаться центральным BOOTP-сервером. Если данная опция установлена, то Коммутатор до использования настроек по умолчанию или предустановленных настроек сначала ищет BOOTP-сервер, чтобы получить от него указанные настройки.
DHCP	При включении Коммутатор посылает широковещательный DHCP-запрос. При этом IP-адрес, маска подсети, шлюз по умолчанию будут получены от центрального DHCP-сервера. Если данная опция установлена, то Коммутатор до использования настроек по умолчанию или предустановленных настроек сначала ищет DHCP-сервер, чтобы получить от него указанные настройки.
Manual	Выбор данной опции позволяет ввести вручную IP-адрес, маску подсети и основной шлюз Коммутатора. Значение данных параметров должно выглядеть следующим образом: xxx.xxx.xxx.xxx, где xxx – десятичное число от 0 до 255. Эти адреса должны быть уникальными в сети, поэтому рекомендуется задание этих настроек системным администратором.
Subnet Mask	Этот параметр определяет размер подсети, в которую включен коммутатор. Значение данного поля должно выглядеть следующим образом: xxx.xxx.xxx.xxx, где xxx – десятичное число от 0 до 255. Для класса сетей A маска подсети должна быть 255.0.0.0, для класса B – 255.255.0.0 и для класса C – 255.255.255.0. Но допускаются и другие маски подсети.
Default Gateway	IP-адрес, на который посылаются пакеты, имеющие адрес назначения вне данной подсети. Обычно это адрес маршрутизатора или IP-шлюза. Если данная сеть не является частью Интранет или необходимо сделать Коммутатор недоступным из внешней сети, не следует изменять значение данного поля.
VLAN Name	Данный параметр позволяет задать имя VLAN, с которой управляющая станция сможет осуществлять управление Коммутатором, используя TCP/IP (через Web-интерфейс или Telnet). Управляющие станции других VLAN не смогут управлять Коммутаторм, несмотря на то, что их IP-адреса указаны в меню Security IP Management. Если VLAN ещё не сконфигурированы на Коммутаторе, VLAN по умолчанию содержит все порты коммутатора. Т.к. в таблице Security IP Management по умолчанию нет информации, то любая управляющая станция, которая соединится с Коммутатором, может получить доступ к коммутатору, пока не будет определена управляющая VLAN или IP-адрес управляющей станции.
Admin State	Данный параметр позволяет пользователю выбирать/отменять Admin State для IP-интерфейса, используя выпадающее меню. Отключение данной функции

	запретит удалённое управление коммутатором, и единственный способ сконфигурировать Коммутатор будет использование интерфейса командной строки.
Auto Config State	Когда установлена эта опция, коммутатор получит конфигурационный файл через TFTP и автоматически станет DHCP- клиентом. Конфигурационный файл будет загружен после инсталяции. Для того, чтобы использовать Auto Config, DHCP-сервер должен быть настроен на передачу TFTP-серверу IP-адреса и имени конфигурационного файла в пакете ответа от DHCP. TFTP-сервер должен находиться в рабочем состоянии и хранить в своей основной директории запрашиваемый коммутатором конфигурационный файл. При необходимости обратитесь за дополнительной информацией к руководствам по программному обеспечению DHCP-сервера и/или TFTP-сервера. Если процесс автоконфигурации не может быть завершен, Коммутатор вернется к последней версии конфигурационного файла, сохраненной в энергонезависимой памяти коммутатора.

Для применения настроек кликните по **Apply**.

Настройка IP-адреса Коммутатора с помощью интерфейса командной строки

У каждого коммутатора может быть свой IP-адрес, который используется для связи с SNMP-менеджером или другими приложениями TCP/IP (например, BOOTP, TFTP). IP-адрес Коммутатора по умолчанию 10.90.90.90. Зная порядок распределения адресов в сети, можно изменить адрес коммутатора по умолчанию.

Только после задания IP-адреса коммутатора можно будет осуществлять управление устройством с помощью Web-интерфейса. IP-адрес Коммутатора может быть назначен автоматически с помощью протоколов BOOTP и DHCP, в этом случае должен быть известен текущий адрес Коммутатора. С помощью командной строки IP-адрес Коммутатора может быть установлен следующим образом:

- Запустив интерфейс командной строки, введите команду **config ipif System ipaddress xxx.xxx.xxx.xxx/ yyy.yyy.yyy.yyy**. Где x - IP-адрес, назначенный IP- интерфейсу (System), y – соответствующая маска подсети.
- Также можно ввести команду **config ipif System ipaddress xxx.xxx.xxx.xxx/z.** Где x – IP-адрес, назначенный IP-интерфейсу (System); z – соответствующий количество подсетей в CIDR-нотации.

IP- интерфейсу, называемому **System**, на Коммутаторе может быть назначен IP-адрес и маска подсети, которые могут быть использованы для подключения управляющей станции к Telnet или Web-интерфейсу управления комутатором. Затем обычно управляющая станция соединяется с Telnet или управляемым Web-агентом коммутатора.

Системное сообщение **Success** укажет на успешное выполнение команды. Теперь настройка и управление Коммутатором может осуществляться с помощью Telnet, CLI или Web-интерфейса управления. При этом необходимо использовать указанный выше IP-адрес для подключения к Коммутатору.

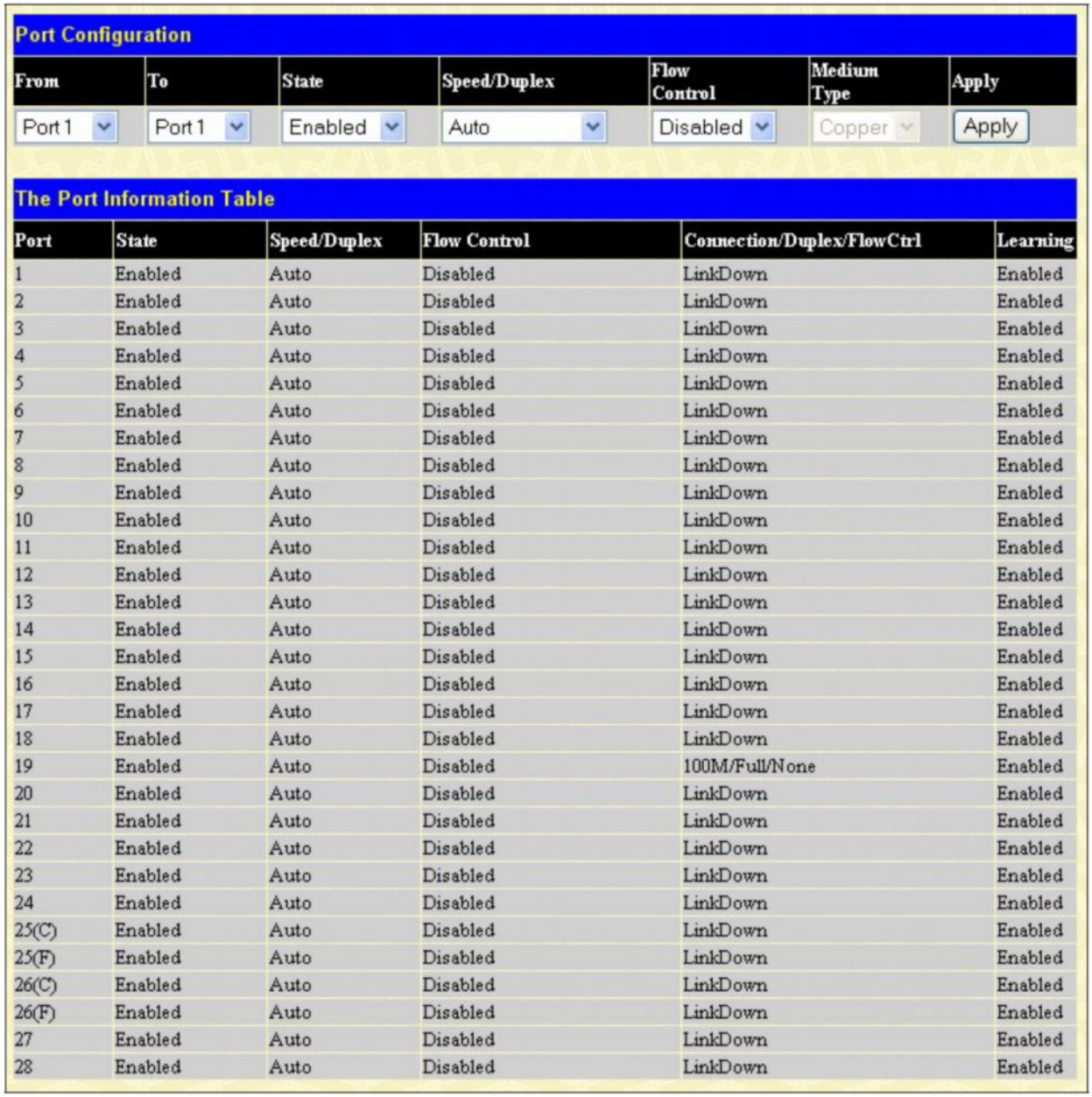
Предупреждение: При потере пароля обратитесь, пожалуйста, на официальный сайт D-Link, на котором описан порядок восстановления пароля.

Конфигурирование портов

Эта глава содержит информацию по индивидуальной настройке различных атрибутов и свойств для физических портов, включая скорость на порту и управление потоком.

Настройки портов

Кликните по меню **Administration** > **Port Configuration > Port Settings** , в результате появится следующее окно:



Port Configuration

From	To	State	Speed/Duplex	Flow Control	Medium Type	Apply
Port 1	Port 1	Enabled	Auto	Disabled	Copper	Apply

The Port Information Table

Port	State	Speed/Duplex	Flow Control	Connection/Duplex/FlowCtrl	Learning
1	Enabled	Auto	Disabled	LinkDown	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
19	Enabled	Auto	Disabled	100M/Full/None	Enabled
20	Enabled	Auto	Disabled	LinkDown	Enabled
21	Enabled	Auto	Disabled	LinkDown	Enabled
22	Enabled	Auto	Disabled	LinkDown	Enabled
23	Enabled	Auto	Disabled	LinkDown	Enabled
24	Enabled	Auto	Disabled	LinkDown	Enabled
25(C)	Enabled	Auto	Disabled	LinkDown	Enabled
25(F)	Enabled	Auto	Disabled	LinkDown	Enabled
26(C)	Enabled	Auto	Disabled	LinkDown	Enabled
26(F)	Enabled	Auto	Disabled	LinkDown	Enabled
27	Enabled	Auto	Disabled	LinkDown	Enabled
28	Enabled	Auto	Disabled	LinkDown	Enabled

Рисунок 6-3. Окно Port Configuration

Для настройки портов Коммутатора необходимо:

1. Выбрать порт или диапазон портов, используя выпадающие меню **From…To…**.
2. Другие выпадающие меню используются для конфигурирования следующих параметров:

Параметр	Описание
From…. To	С помощью выпадающих меню выберите порт или диапазон портов для настройки.
State	Поле используется для включения и выключения заданных портов.
Speed/Duplex	Поле **Speed/Duplex** позволяет установить скорость и режим работы (дуплекс/полудуплекс) для заданных портов. *Auto* означает автоматический выбор скорости при работе с устройствами 10 и 100 Мбит/с, в режимах полного и полудуплекса. Опция *Auto* позволяет портам автоматически определять

	максимально возможную скорость, при которой будет обеспечиваться совметимость устройств. Другие доступные опции *Auto*, *10M/Half*, *10M/Full, 100M/Half* и *100M/Full*, *1000M/Full_M* и *1000M/Full_S*. При выборе опций, отличных от Auto, никаких автоматических настроек порта не производится. Коммутатор позволяет пользователю настроить два вида гигабитных соединений; *1000M/Full_M* и *1000M/Full_S*. Гигабитные соединения работают только в режиме полного дуплекса и поддерживают определенные характеристики, отличающиеся от других режимов работы. Параметры *1000M/Full_M* (master) и *1000M/Full_S* (slave) относятся к соединениям, работающим на основе кабеля 1000BASE-T для соединения между портом Коммутатора и другим устройством, поддерживающим соединение Gigabit Ethernet. Настройка коммутатора master (*1000M/Full_M)* позволяет порту определять характеритстики, относящиеся к дуплексу, скорости и типу физического уровня. Настройка master будет также определять взаимоотношение коммутаторов master и slave между двумя соединенными физическим уровнями. Это взаимоотношение необходимо для установки контроля времени между двумя физическими уровнями. Контроль времени устанавливается на физическом уровне коммутатора master локальным источником. Настройки коммутатора slave (*1000M/Full_S)* используют циклический счетчик, при котором отчет времени начинается с получения данных от коммутатора master. Если на одном конце соединения установлено *1000M/Full_M*, на другом конце соединения необходимо настроить *1000M/Full_S*. Выбор других настроек может привести к статусу отсутствия канала на обоих концах соединения.
Flow Control	Данное поле отображает схему управления потоком, используемую для различных настроек порта. Порты, настроенные в режиме полного дуплекса, используют управление потоком 802.3x; при использовании полудуплекса используется управление потоком методом обратного давления. Настройка *Auto* определяет автоматический выбор схемы аутентификации из двух. По умолчанию настроено *Disabled*.
Medium Type	Эта опция используется только для комбо-портов. При настройке комбо-портов здесь задается тип используемой транспортной среды. SFP-порты необходимо установить как *Fiber*, а порты 1000BASE-T как *Copper*.
Learning	При включении данной опции (*Enabled)* MAC-адреса источника и назначения автоматически появляются в таблице продвижения. По умолчанию настроено *Enabled*. И это значение не доступно для изменения.

Для применения настроек кликните **Apply**.

Порты, отключенные из-за обнаружения ошибки (Port Error Disabled)

Следующее окно содержит информацию о портах, перешедших в состояние disabled (выключен) по таким причинам, как STP loopback detection (обнаружение петли) или отключения канала. Чтобы просмотреть это окно, кликните по **Port Configuration > Port Error Disabled**.

Рисунок 6- 4. Окно Port Error Disabled

Здесь отображаются следующие параметры:

Параметр	Описание
Port	Отображает номер порта, который был отключен в результате обнаружения ошибки.

Port State	Отображает текущий статус порта (*Enabled* или *Disabled)*.
Connection Status	В этом поле содержится uplink-статус отдельных портов.
Reason	Описывает причину состояния error-disabled, как, например, обнаружение петли STP loopback.
Description	В этом поле содержатся дальнейшие пояснения.

Описание портов

Коммутатор поддерживает функцию описания портов, позволяющую дать различные названия портам Коммутатора. Чтобы присвоить имена различным портам, кликните по **Administration** > **Port Configuration** > **Port Description.** В результате откроется следующее окно:

С помощью выпадающих меню **From** и **To** выберите порт или диапазон портов, а затем введите их описание. Кликните по **Apply**, чтобы добавить описания в **Port Description Table**.

Поле **Medium Type** доступно только для комбо-портов. Для комбо-портов это поле определяет тип используемой транспортной среды. При использовании SFP-портов из пары должно быть указано *Fiber,* в то время как при использовании портов 1000BASE-T из пары должно быть указано *Copper*. В таблице отобразится результат: **C** – означает использование медных портов и **F** – оптических портов.

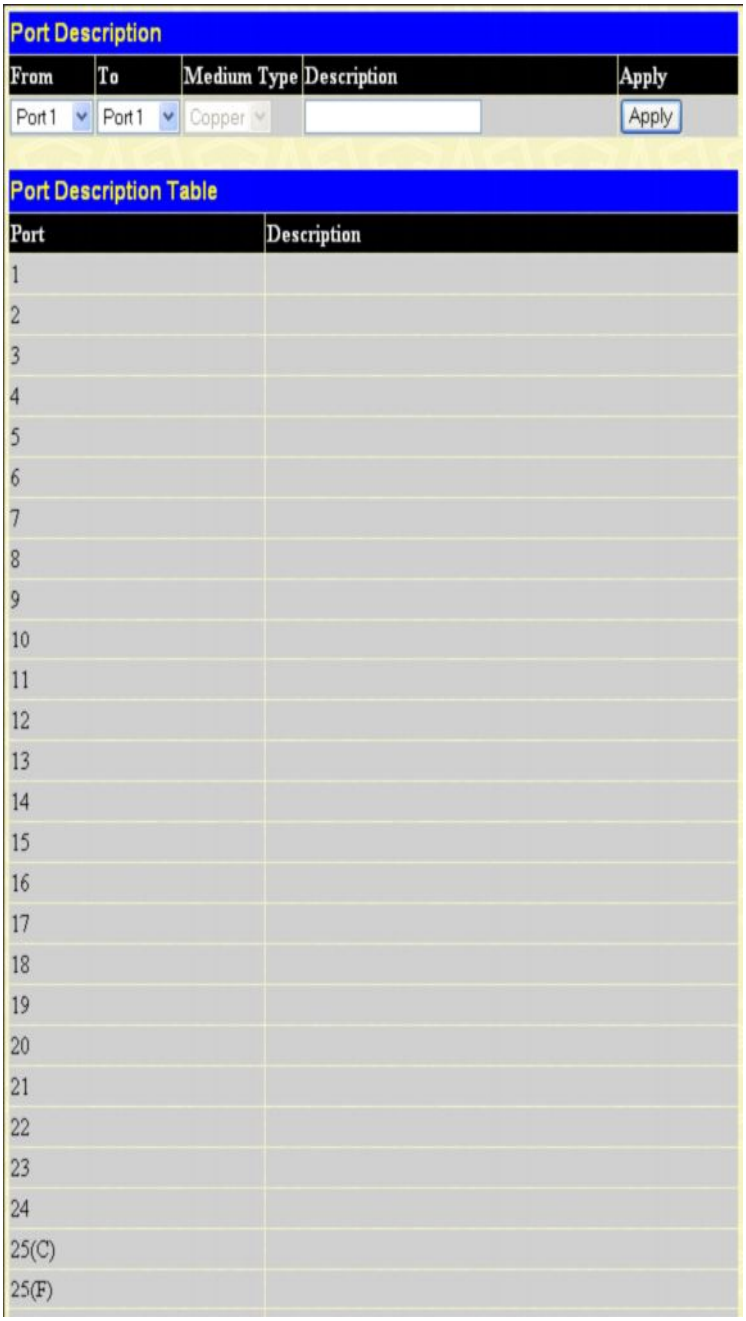


Рисунок 6- 5. Окно Port Description

DHCP/BOOTP Relay

Чтобы включить и настроить **DHCP/BOOTP Relay Global Settings** на Коммутаторе, кликните по **Administration > DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Global Settings**:

Глобальные настройки DHCP / BOOTP Relay

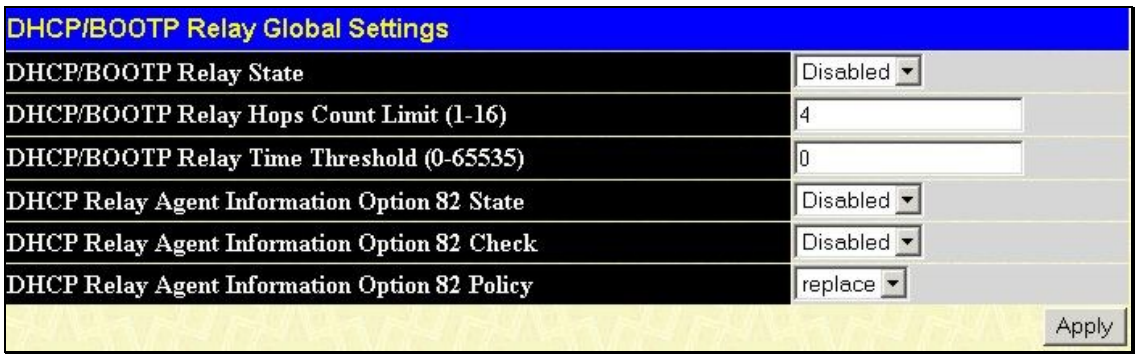


Рисунок 6-6. Окно DHCP/ BOOTP Relay Global Settings

Могут быть установлены следующие поля:

Параметр	Описание
Relay State	Значение данного поля может с использованием выпадающего меню переключаться между *Enabled* (включено) и *Disabled* (выключено).
Relay Hops Count Limit (1-16)	Введите в данном поле максимальное количество шагов (от 1 до 16) при отправке DHCP/BOOTP-пакетов. Значение по умолчанию равно *4*.
Relay Time Threshold (0-65535)	Позволяет задать значение от *0* до *65535* секунд и определяет максимальный лимит времени при маршрутизации DHCP/BOOTP-пакета. Если задано значение *0*, то Коммутатор не будет обрабатывать значение поля в секундах BOOTP- или DHCP-пакета. Если задано значение, отличное от 0, то Коммутатор будет использовать это значение наряду с предыдущим параметром при принятии решения о продвижении BOOTP- или DHCP-пакета.
DHCP Agent Information Option 82 State	Данное выпадающее меню позволяет включить (*Enabled)* или выключить (*Disabled)* Option 82 на Коммутаторе. По умолчанию установлено значение *Disabled.* • *Enabled* – при выборе данной опции Relay Agent (Агент перенаправления запросов) будет добавлять информацию option 82 в DHCP-запрос клиента. Затем пакет отправляется на DHCP-сервер. DHCP – сервер получает пакет. Если сервер поддерживает опцию option-82, он может использовать поля remote ID и/или circuit ID для назначения IP-адреса и применения политик, таких как ограничения количества IP-адресов, выдаваемых одному remote ID или circuit ID. Затем DHCP – сервер копирует поле опции option-82 в DHCP - ответе. – Если сервер не поддерживает option 82, он игнорирует поля этой опции и не отсылает их в ответе. • DHCP - сервер отвечает в режиме Unicast агенту перенаправления запросов. Агент проверяет, предназначен ли он его клиенту, путём анализа IP – адреса назначения пакета. • Агент удаляет поля опции option-82 и направляет пакет на порт, к которому подключён DHCP - клиент, пославший пакет DHCP – запроса. *Disabled*- выбор данной опции позволяет отключить option 82.
DHCP Agent Information Option 82 Check	Данное выпадающее меню содержит две опции (*Enabled* и *Disabled)* и используется для включения/выключения на Коммутаторе функции проверки значения поля option 82 пакета. *Enabled*– Когда выбрано значение *Enabled*, то агент перенаправления запросов будет проверять значение поля пакета option 82. Так, если коммутатор получит пакет, содержащий option 82, от DHCP-клиента, то пакет будет отброшен. *Disabled*- Когда значение поля выбрано *Disabled,* агент перенаправления запросов не будет проверять значение поля option 82 пакета.

DHCP Agent Information Option 82 Policy	Значение данного поля может переключаться с использованием выпадающего меню между *Replace, Drop* и *Keep*. Оно используется для установки на Коммутаторе политики обработки пакетов, когда значение **DHCP Agent Information Option 82 Check** установлено *Disabled* (выключено). Значение по умолчанию *Replace.* *Replace*- При выборе данной опции поле option 82 будет удаляться из пакетов, полученных от DHCP-клиента. *Drop*- При выборе данной опции если от DHCP-клиента пришел пакет с полем option 82, то он будет отброшен. *Keep*- При выборе данной опции поле option 82 будет оставаться неизменным в пакетах, полученных от DHCP-клиента.

Кликните по **Apply** для применения выполненных изменений.

ПРИМЕЧАНИЕ: Если коммутатор получает от DHCP-клиента пакет, содержащий поле option-82, и функция **DHCP Agent Information Option 82 Check** включена, то коммутатор отбросит пакет. Однако возможность настроить клиента с полем option 82 существует. В случае необходимо выключить функцию **DHCP Agent Information Option 82 Check**. Поле **DHCP Agent Information Option 82 Policy** позволяет настроить действие, которое коммутатор будет осуществлять при получении пакета, содержащего option-82.

Реализация Option 82 в коммутаторах серии DES-30xx

Команда **config dhcp_relay option_82** задает настройки option 82 агента DHCP relay, установленного на Коммутаторе. Форматы подопций circuit ID и remote ID следующие:

ПРИМЕЧАНИЕ: В подопции circuit ID для автономного коммутатора поле Module всегда равняется 0.

Формат подопции Circuit ID:

1.	2.	3.	4.	5.		6.	7.
1	6	0	4	VLAN	Module	Port	
1 байт	1 байт	1 байт	1 байт	2 байта		1 байт	1 байт

a. Тип подопции

b. Длина

c. Тип Circuit ID

d. Длина

e. VLAN: входящий VLAN ID пакета DHCP-клиента.

f. Модуль: Для автономного коммутатора в данном поле установлено значение 0, для стекируемого коммутатора здесь установлен Unit ID.

g. Порт: Номер входящего порта пакета DHCP-клиента, нумерация портов начинется с 1.

Формат подопции Remote ID:

1.	2.	3.	4.	5.
2	8	0	6	MAC address

1 байт	1 байт	1 байт	1 байт	6 байт

1. Тип подопции
2. Длина
3. Тип удаленного иидентификатора
4. Длина
5. MAC-адрес: системный MAC-адрес Коммутатора.

Рисунок 6-7. Формат подопций Circuit ID и Remote ID

Настройки интерфейса DHCP/BOOTP Relay

DHCP/ BOOTP Relay Interface Settings позволяет пользователю установить сервер по IP-адресу для передачи информации DHCP/ BOOTP на Коммутатор. Пользователь может ввести настроенный ранее IP-интерфейс, который будет подключен непосредственно к серверу DHCP/BOOTP. Заданные должным образом настройки отобразятся в окне **BOOTP Relay Table** в низу данного окна, когда пользователь кликните кнопку **Add** под заголовком **Apply**. Пользователь может добавить до 4 IP-адресов IP-интерфейса на Коммутаторе. Записи могут быть удалены путем нажатия на соответствующий значок ✕. Чтобы включить и настроить **DHCP/BOOTP Relay Global Settings** на Коммутаторе, кликните **Administration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings**:

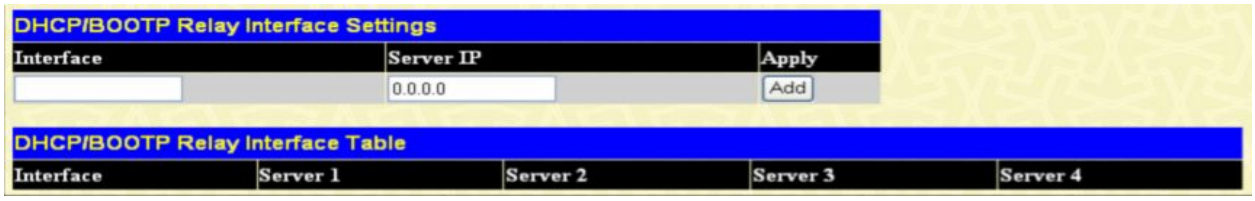


Рисунок 6-8. Окно DHCP/BOOTP Relay Interface Settings и DHCP/BOOTP Relay Interface Table

Для просмотра и изменения доступны следующие параметры.

Параметр	Описание
Interface	IP-интерфейс Коммутатора, непосредственно подключаемый к серверу.
Server IP	Ввеите IP-адрес DHCP/BOOTP-сервера. До четырех IP-адресов серверов может быть настроено для каждого IP-интерфейса.

Учетные записи пользователей

Окно **User Account Management** позволяет управлять привилегиями пользователей. Для просмотра существующих учетных записей пользователей откройте папку **Administration** и кликните по ссылке **User Accounts**. В результате откроется окно **User Account Management**, как показано ниже.

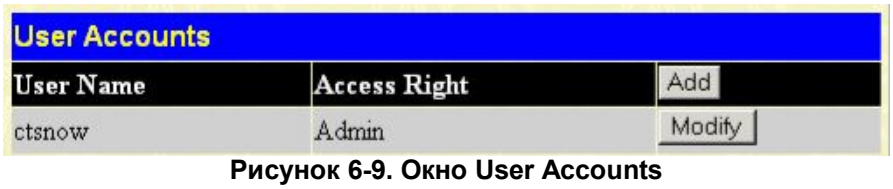


Рисунок 6-9. Окно User Accounts

Чтобы добавить нового пользователя, кликните по кнопке **Add**. Чтобы изменить или удалить существующего пользователя, кликните по соответствующей этому пользователю кнопке **Modify**.

Рисунок 6-10. Окно User Accounts Add Table

Добавьте нового пользователя, введя имя пользователя User Name и пароль New Password, а также подтверждение пароля в поле Confirm New Password. Выберите уровень привилегий (*Admin* или *User)* в выпадающем меню Access Right.

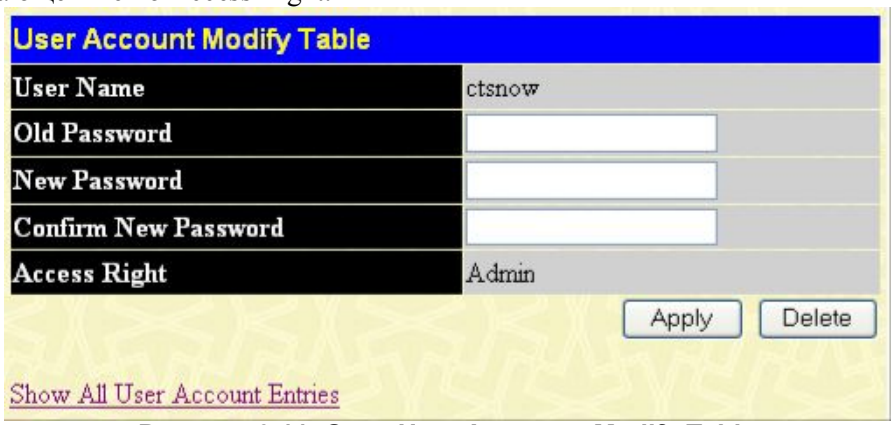


Рисунок 6-11. Окно User Accounts Modify Table

Существует возможность удалить или изменить созданные учетные записи пользователей в таблице **User Account Modify Table**. Для удаления учетной записи пользователя кликните по кнопке **Delete**. Чтобы изменить пароль, введите его сначала в поле *New Password,* а затем повторите ввод в поле *Confirm New Password.*. Уровень привилегии (*Admin* или *User*) доступен для просмотра в поле **Access Right**.

Зеркалирование портов

Коммутатор дает возможность копировать переданные и принятые блоки данных на порт и перенаправлять копии на другой порт, к которому может быть подключено устройство, позволяющее осуществлять мониторинг трафика, например, сниффер или RMON-устройство. Эта функция особенно полезна для поиска и устранения неисправностей.

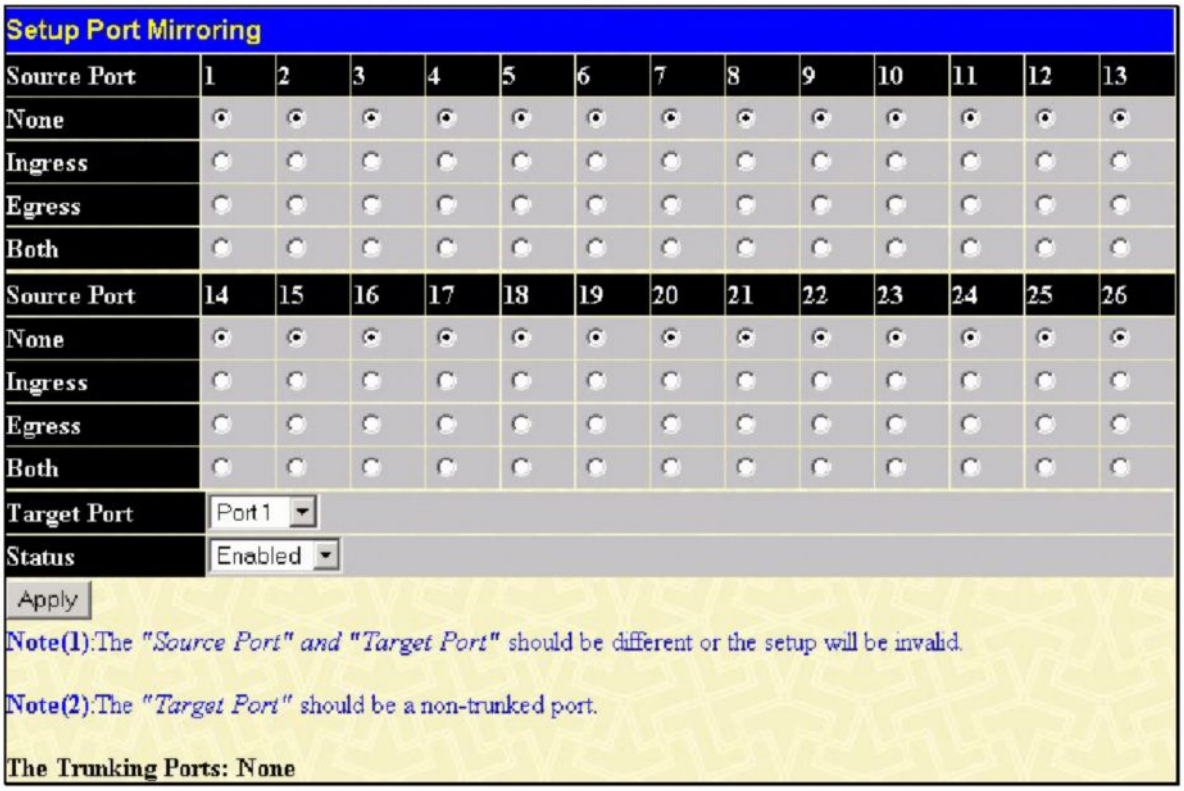


Рисунок 6-12. Окно Setup Port Mirroring

Для настройки зеркалирования портов необходимо:

- Выбрать Source Port (порт-источник), с котрого будут копироваться блоки данных, и Target Port (порт-приёмник), который будет получать скопированные данные.
- Выбрать направление: Ingress (вход), Egress (выход) или Both (оба); и изменить значение поля Status на *Enabled*.
- Для применения настроек кликните **Apply**.

Примечание: Нельзя сделать зеркалирование более быстрого порта на медленный. Например, если попытаться зеркалировать порт 100Мбит/с на порт 10Мбит/с, это приведёт к проблемам с пропускной способностью. Порт, с которого копируются данные, всегда должен поддерживать скорость такую же или ниже, чем порт, на который идёт пересылка скопированных данных. Также принимающий порт не может быть членом группы агрегированных каналов связи.

Настройки системного журнала

Коммутатор поддерживает отправку сообщений о нештатных событиях на серверы, количество которых не превышает четырех. В папке **Administration** кликните по **System Log Settings**, в результате появится следующее окно.

Рисунок 6-13. Окно System Log Host

Параметры, которые необходимо задать для добавления и редактирования **сервера системного журнала,** одинаковы. Ниже приводится таблица с описанием этих параметров.

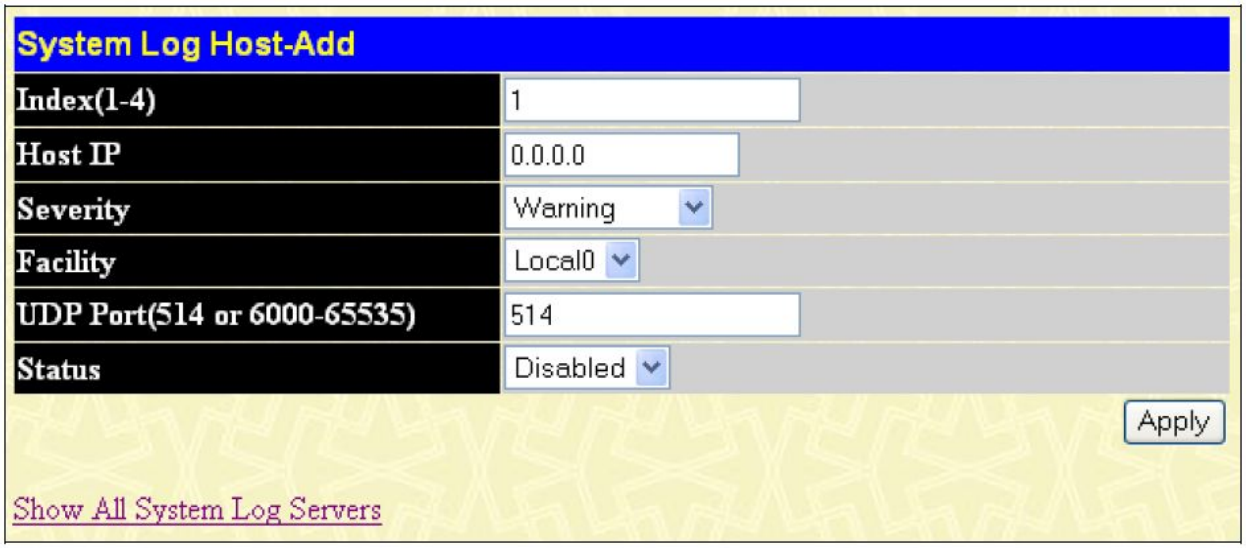


Рисунок 6-14. Окно Configure System Log Server – Add (добавить)

Для настройки доступны следующие параметры:

Параметр	Описание
Index	Индекс сервера системного журнала (1-4).
Server IP	IP-адрес сервера системного журнала.
Severity	Данное выпадающее меню позволяет выбрать уровень проблемы для отправки сообщений предупреждения. Значения могут быть следующими: *Warning, Informational* и *All*.
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: **Числовой Код** — **Facility**
	0 — сообщения ядра 1 — сообщения пользовательского уровня 2 — почтовафя система 3 — системные демоны 4 — сообщения безопасности/авторизации 5 — сообщения, генерируемые внутри системы подсистемой syslog line printer 6 — подсистема сетевых новостей

	7	подсистема UUCP
	8	демон часов
	9	сообщения безопасности/авторизации
	10	FTP-демон
	11	подсистема NTP
	12	Аудит журнала регистрации
	13	Предупреждение журнала регистрации
	14	демон часов
	15	**локальное использование 0(local0)**
	16	**локальное использование 1(local1)**
	17	**локальное использование 2(local2)**
	18	**локальное использование 3(local3)**
	19	**локальное использование 4(local4)**
	20	**локальное использование 5(local5)**
	21	**локальное использование 6(local6)**
	22	**локальное использование 7(local7)**
UDP Port (514 or 6000-65535)	Введите номер UDP-порта, используемого для отправки сообщений системного журнала. По умолчанию задано 514.	
Status	Данное поле используется для включения (*Enabled)* или выключения (*Disabled)* соответствующего сервера.	

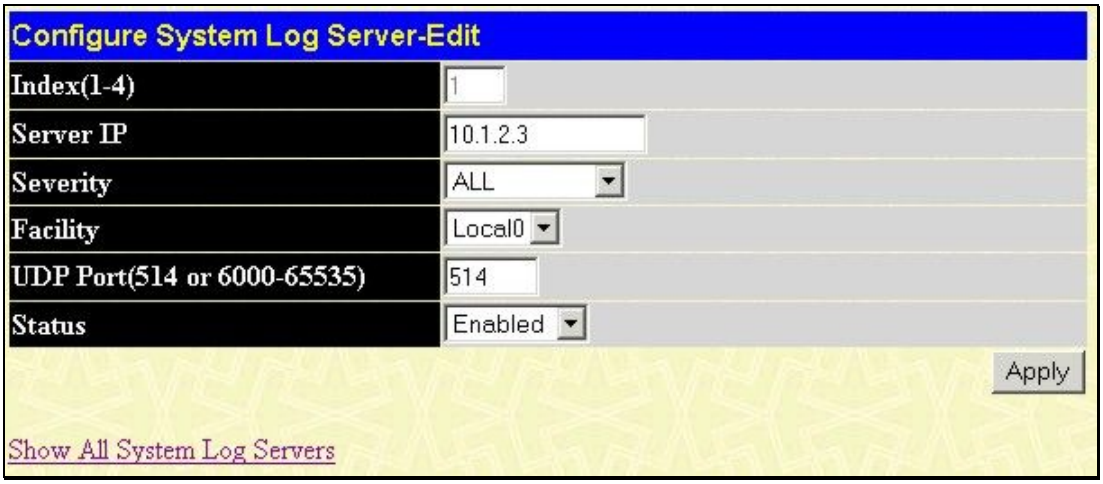


Рисунок 6-15. Окно Configure System Log Server– Edit (редактировать)

Для применения настроек системного журнала кликните **Apply**. Чтобы удалить запись в окне **System Log Host**, кликните по соответствующему значку ✕ под заголовком Delete. Для возврата к окну **System Log Host** кликните по Show All System Log Servers.

Выбор режима сохранения системного журнала Коммутатора

Окно **System Log Save Mode Settings** позволяет выбрать метод, каким будет производиться сохранение журнала Коммутатора в его flash-памяти. Чтобы просмотреть это окно, откройте папку **Administration** и кликните по **System Log > System Log Save Mode Settings.**

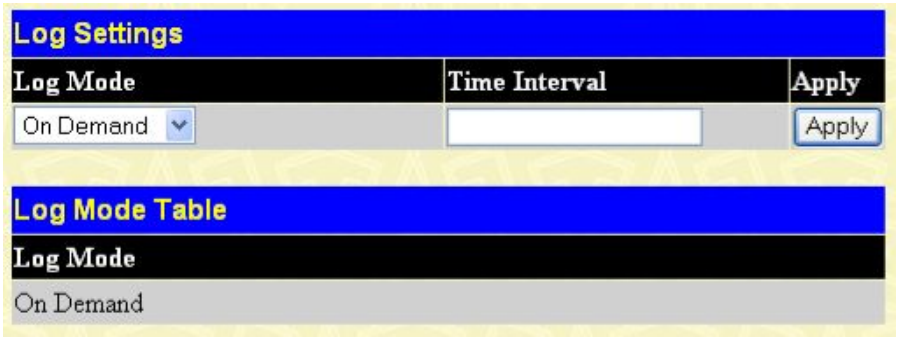


Рисунок 6-16. Окно Log Settings

Могут быть установлены следующие параметры:

Параметр	Описание
Log mode	Данное выпадающее меню позволяет выбрать режим записи информации в системный журнал. Доступны следующие опции: On Demand (по требованию), Log Trigger и Time Interval (временной интервал).
Time Interval	IP-адрес сервера системного журнала.

Настройки SNTP

Настройка времени

Для задания временных настроек коммутатора откройте папку **Admininistration**, а затем папку **SNTP** и кликните по ссылке **Time Setting.** Откроется окно, представленное ниже.

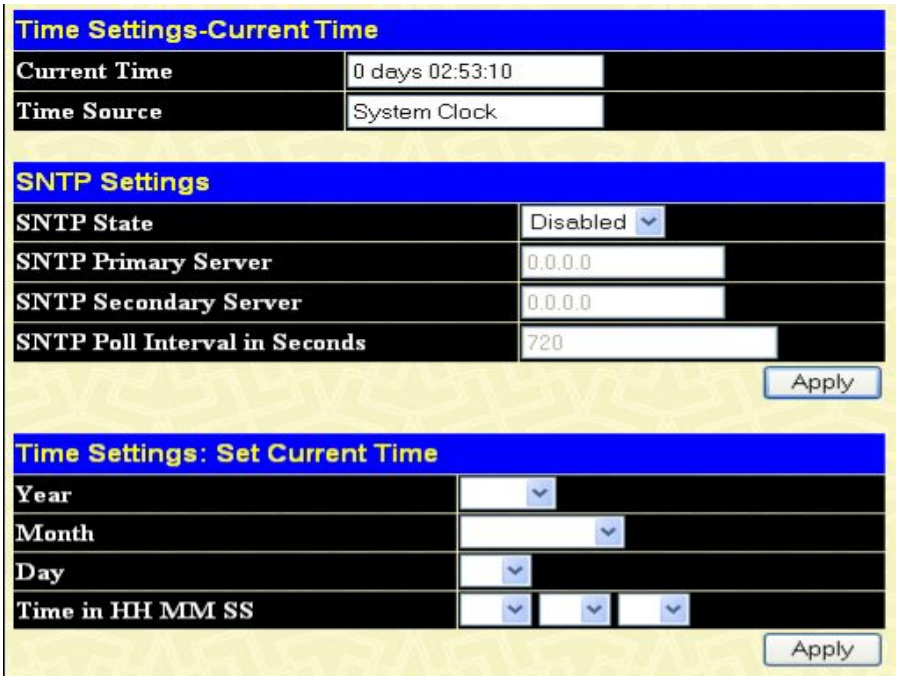


Рисунок 6- 17. Окно Current Time

В данном окне доступны следующие параметры, часть из которых может быть изменена, другая часть доступна только для просмотра:

Параметр	Current Time: Status Описание

Current Time	В этом поле отображаются локальные настройки системной даты и времени.
Time Source	В этом поле отображается источник, с которого получены настройки времени.
Current Time: SNTP Settings	
SNTP State	Данное выпадающее меню позволяет включить (*Enabled*) или отключить (*Disabled*) SNTP.
SNTP Primary Server	IP-адрес первичного сервера, с которого будет получена SNTP-информация.
SNTP Secondary Server	IP-адрес вторичного сервера, с которого будет получена SNTP-информация.
SNTP Poll Interval in Seconds	Интервал времени в секундах между запросами на обновление SNTP-информации.
Current Time: Set Current Time	
Year	Введите текущий год при желании обновить системное время.
Month	Введите текущий месяц при желании обновить системное время.
Day	Введите текущий день при желании обновить системное время.
Time in HH MM	Введите текущее время в часах, минутах и секундах при желании обновить системное время.

Для применения выполненных настроек кликните по **Apply**.

Часовые пояса и DST

Представленное ниже окно содержит опции для настройки часовых поясов и перевода времени на зимнее и летнее время, для его открытия нажмите **Administration ⇨ SNTP ⇨ Time Zone and DST**

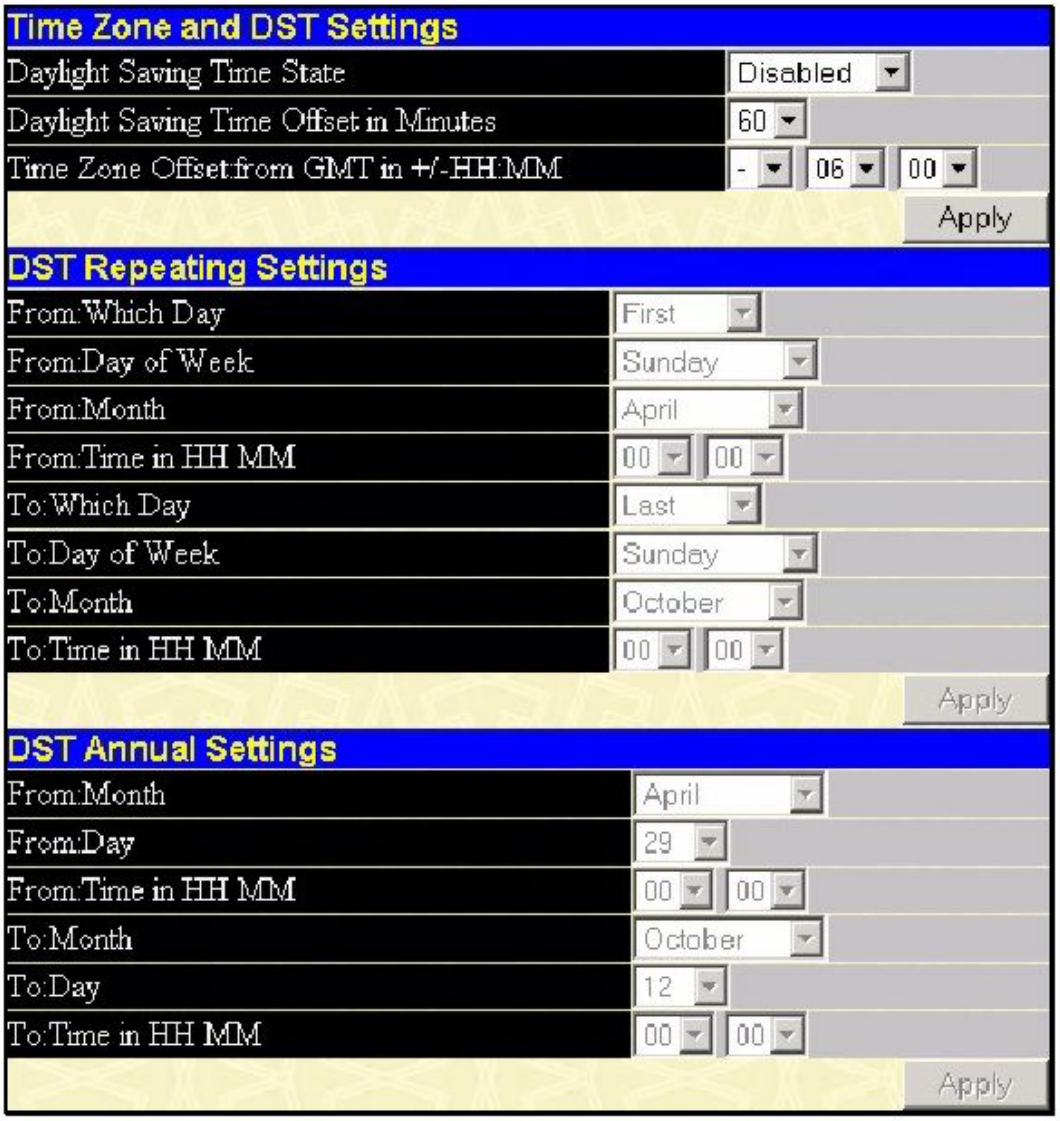


Рисунок 6- 18. Окно Time Zone and DST Settings

Могут быть установлены следующие параметры:

Параметр	Описание
Time Zone and DST Settings	
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 +/- HH: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,	

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

Для принятия настроек в окне **Time Zone and DST** кликните по **Apply**.

MAC-уведомление

MAC Notification (MAC-уведомление) используется для изучения MAC-адресов и занесения их в базу данных.

Глобальные настройки MAC-уведомления

Для глобальной настройки на Коммутаторе MAC-уведомления необходимо открыть следующее окно. Для этого нужно открыть папку **MAC Notification Settings** в папке **Administration.**

Рисунок 6- 19. Окно MAC Notification Global Settings

Существует возможность настроить следующие параметры:

Параметр	Описание
State	Позволяет включить/выключить MAC-уведомление на Коммутаторе.
Interval (sec)	Задает временной интервал в секундах между уведомлениями.
History size	Максимальный размер истории уведомлений. Может быть определено до 500 записей.

Настройки MAC-уведомления на порту

Для изменения настроек MAC-уведомления на порту или группе портов Коммутатора можно установить следующие параметры:

Параметр	Описание
From…To	Выбор порта или группы портов, для которых будет настроено MAC-уведомление.
State	Настройка MAC-уведомления для определенного порта.

Необходимо кликнуть по **Apply** для применения настроек.

Сервисы TFTP

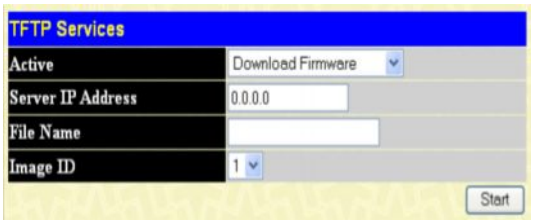


Рисунок 6-20. Окно TFTP Services

Простейший протокол передачи данных (Trivial File Transfer Protocol ,TFTP) позволяет обновлять программное обеспечение коммутатора путем заугрузки с TFTP-сервера на коммутатор. Конфигурационный файл также можно загрузить на коммутатор с TFTP-сервера. Там же можно сохранить настройки коммутатора и журнал событий. На TFTP-сервере должно быть запущено соответствующее программное обеспечение, позволяющее выполнить передачу файла.

Для Коммутаторов серии DES-30xx предусмотрена возможность передачи программного обеспечения и конфигурационных файлов с/на встроенный Flash-диск Коммутатора. С помощью опций, представленных в данном окне, пользователь может добавить файл с программным обеспечением или конфигурационным файл с TFTP-сервера на flash-память Коммутатора, а также выполнить обртную операцию – загрузить файлы из flash-памяти на TFTP-сервер. Более подробная информация о настройках Flash-диска приводится в следующем разделе **Flash File Services**.

Программное обеспечение TFTP-сервера входит во многие пакеты управления сетью, как, например, NetSight, или же может представлять отдельную программу. Чтобы обновить программное обеспечение Коммутатора или его конфигурационный файл, кликните по ссылке **TFTP Services**, расположенной в папке **Administration**. Для настройки доступны следующие параметры:

Параметр	Описание
Operation	В выпадающем меню выберите нужный сервис TFTP: *Download Firmware* - Введите IP-адрес TFTP-сервера и определите положение файла на TFTP-сервере. Кликните **Start** для записи IP-адреса TFTP-сервера и начала передачи файла. *Download Configuration* - Введите IP-адрес TFTP-сервера, путь и имя конфигурационного файла на TFTP-сервере. Кликните **Start** для записи IP-адреса TFTP-сервера и начала передачи файла. *Upload Configuration* - Введите IP-адрес TFTP-сервера, путь и имя файла с настройками на TFTP-сервере. Кликните **Start** для записи IP-адреса TFTP-сервера и начала передачи файла. *Upload Log* - Введите IP-адрес TFTP-сервера, путь и имя файла для архива журнала коммутатора на TFTP-сервере. Кликните **Start** для записи IP-адреса TFTP-сервера и начала передачи файла.

Server IP Address	Введите IP-адрес сервера, с которого будет загружаться программное обеспечение.
File Name	Введите путь и имя файла программного обеспечения или конфигурационного файла для загрузки с/на TFTP-сервер.
Image ID	Позволяет сохранить или загрузить файл с программным обеспечением на внутреннем Flash-диске.

Кликните **Start** для начала передачи файла.

Поддержка нескольких версий программного обеспечения

В настройке файлов, хранящихся во Flash-памяти, будут полезны опции, содержащиеся в следующих окнах.

Информация о программном обеспечении

Следующее окно содержит информацию о существующем программном обеспечении на коммутаторе.

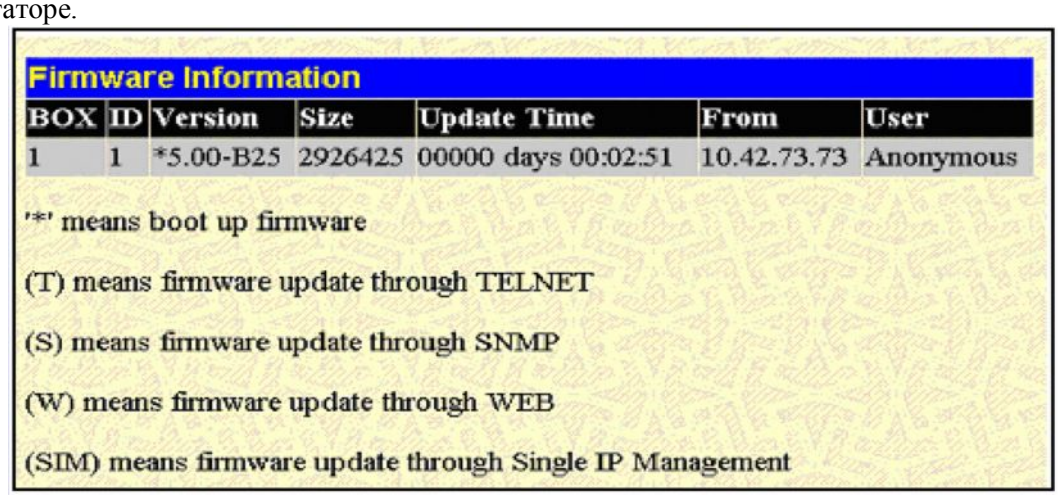


Рисунок 6.21 – Окно Firmware Information

Настройка образа программного обеспечения

Следующее окно позволяет определить, какой из двух образов программного обеспечения будет использоваться в качестве загрузочного файла по умолчанию. Также можно удалить один из двух образов программного обеспечения.

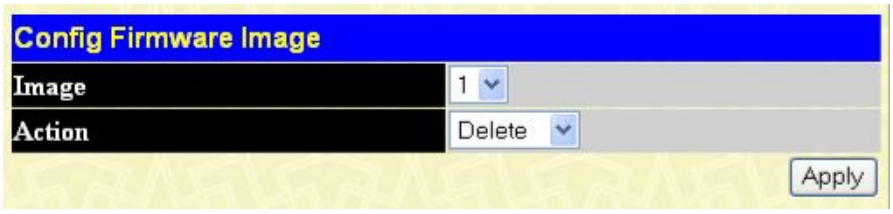


Рисунок 6- 22. Окно Config Firmware Image

Ping Test

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

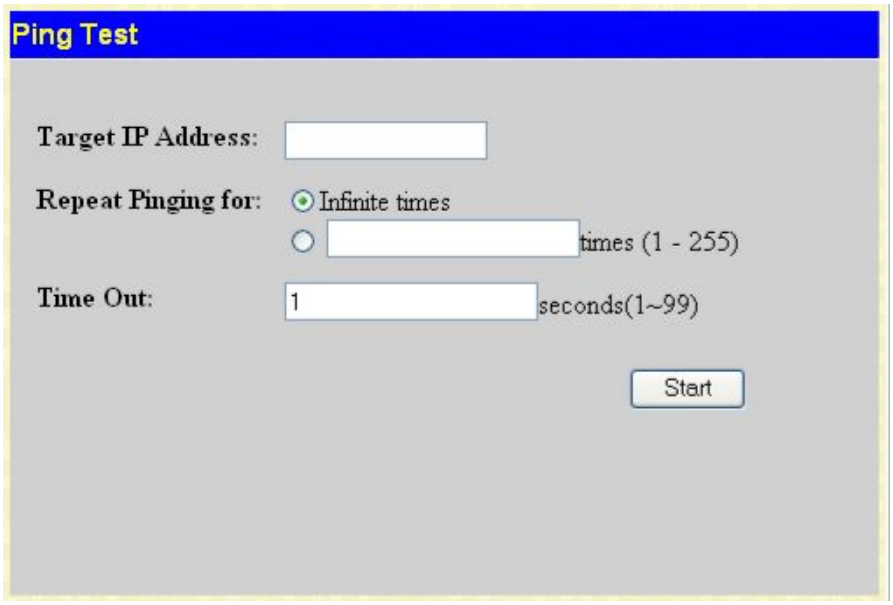


Рисунок 6.23 – Окно Ping Test

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 запуска программы ping.

Safeguard Engine

Периодически злоумышленные хосты на сети будут атаковать коммутатор, используя пакетный флудинг (от англ. flooding – наводнение, ARP-шторм) или другие способы. Без применения Safeguard Engine количество таких атак может значительно возрасти. Для уменьшения влияния этой проблемы в программное обеспечение коммутатора была добавлена функция Safeguard Engine.

Safeguard Engine позволяет сохранить коммутатор в работоспособном состоянии при атаке, минимизируя рабочую загрузку коммутатора и одновременно давая возможность пересылать важные пакеты по сети в ограниченной полосе пропускания. При использовании функции Sfeguard Engine когда коммутатор а) получает слишком много пакетов для обработки или б) использует слишком много памяти, он переходит в режим **Exhausted (**истощенный режим). В этом режиме коммутатор будет отбрасывать все ARP- пакеты и все широковещательные IP-пакеты в течение определенного временного интервала. Каждые пять секунд коммутатор будет проверять количество флудинг-пакетов. Если на коммутатор по-прежнему поступает слишком много широковещательных и ARP-пакетов, то Коммутатор продолжит отбрасывать все ARP-пакеты и широковещательные IP-пакеты на 5 секунд. По истечении 5 секунд коммутатор снова проверит входящий поток пакетов. Если флуд приостановлен, коммутатор снова начинает принимать все пакеты. Если проверка показывает по-прежнему слишком много флудинг-пакетов, поступающих

на коммутатор, то он перестает принимать все ARP- пакеты и все широковещательные IP-пакеты в течение удвоенного времени (10с). Удвоение времени происходит до достижения 320 секунд, и далее этот интервал уже не будет увеличиваться. Для лучшего понимания изучите следующий пример Safeguard Engine.

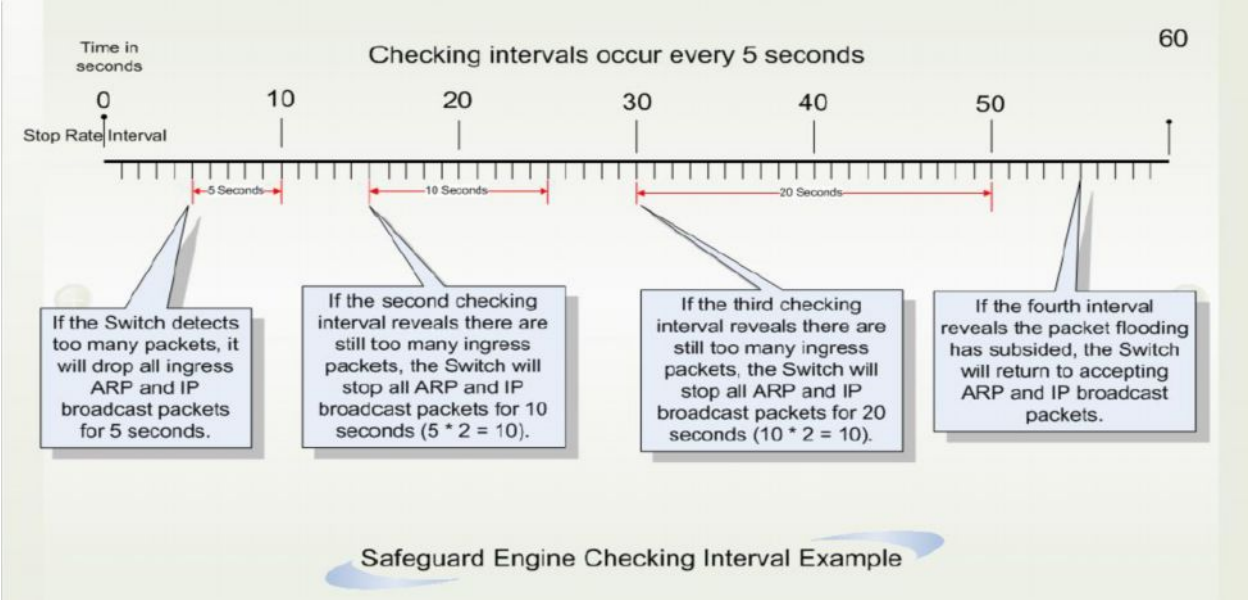


Рисунок 6- 24. Пример Safeguard Engine

Для каждого последующего интервала проверки, при которой обнаруживается флудинг-пакетов, коммутатор будет удваивать время, в течение которого он будет отбрасывать ARP- пакеты и широковещательные IP-пакеты. В показанном выше примере коммутатор удваивает время отбрасывания ARP- пакетов и широковещательных IP-пакетов, когда в течение интервала по 5 секунд были обнаружены флудинг-пакеты. (первая остановка = 5 секунд, вторая остановка = 10 секунд, третья остановка = 20 секунд). Если коммутатор больше не обнаруживает флудинг-пакеты, период отбрасывания ARP- пакетов и широковещательных IP-пакетов возвращается к 5 секундам, и при необходимости процесс может быть запущен вновь.

В истощенном режиме поток пакетов уменьшается наполовину по сравнению с уровнем, в котором находился коммутатор перед входом в истощенный режим. После того, как поток пакетов стабилизируется, то сначала произойдет увеличение скорости на 25%, и лишь затем коммутатор вернется в нормальный режим.

Примечание: При работе коммутатора в истощенном режиме можно подключаться к коммутатору только с IP-адресов доверенных хостов.

Для настройки Safeguard Engine на коммутаторе нажмите **Security> Safeguard Engine**, после чего откроется следующее окно:

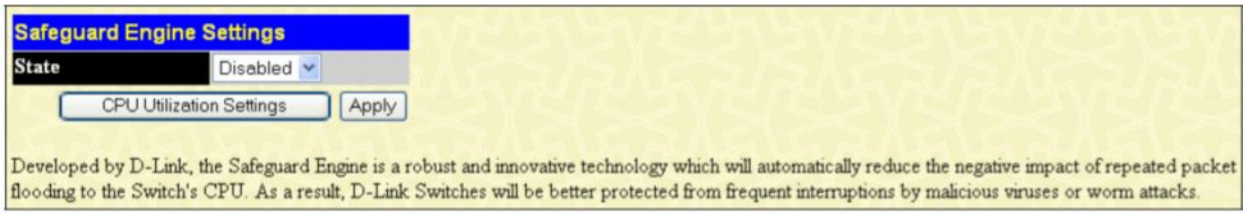


Рисунок 6-25. Окно Safeguard Engine

Чтобы включить Safeguard Engine, выберите опцию *Enabled* в выпадающем меню **State** и кликните по кнопке **Apply**.
Чтобы настроить определенные параметры Safeguard Engine, кликните по кнопке **CPU Utilization Settings**. В результате появится следующее окно.

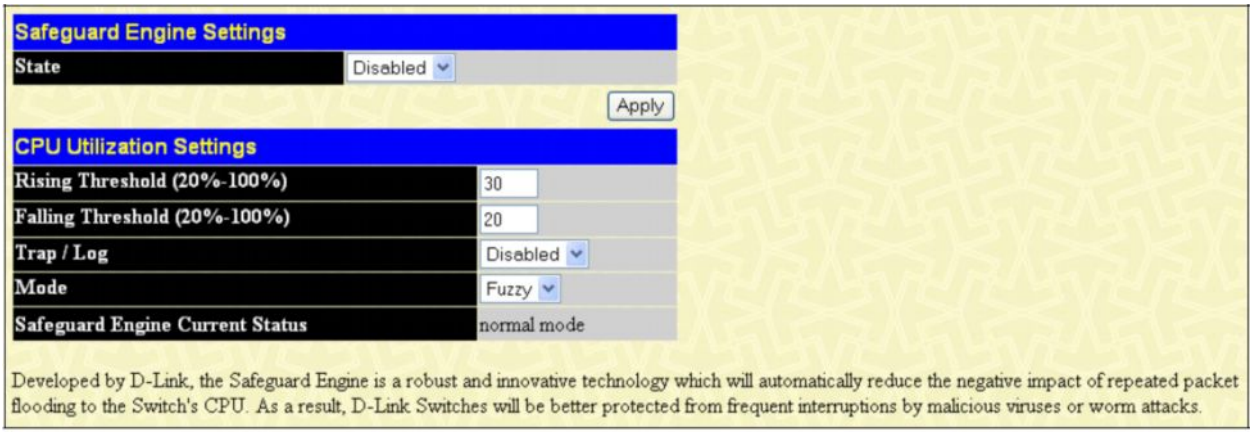


Рисунок 6- 26. Окно Safeguard Engine – CPU Utilization Settings

В появившемся окне заполните следующие поля:

Параметр	Описание
State	Данное выпадающее меню позволяет включить (Enabled) или выключить (Disabled) функцию Safeguard Engine.
Rising Threshold	Пользователь может установить значение в процентах <20-100> верхнего порога загрузки CPU, при котором включается механизм Safeguard Engine. Если загрузка CPU достигнет этого значения, механизм Safeguard Engine начнёт функционировать.
Falling Threshold	Пользователь может установить значение в процентах <20-100> нижнего порога загрузки CPU, при котором выключается механизм Safeguard Engine. Если загрузка CPU снизится до этого значения, механизм Safeguard Engine перестанет функционировать.
Trap/Log	Позволяет включить/выключить отправку сообщений об активации механизма Safeguard Engine в журнал коммутатора / SNMP.
Mode	На выбор доступны опции *Fuzzy* и *Strict*.

SNMP-менеджер
Настройки SNMP

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

Управляемые устройства поддерживают программное обеспечение SNMP (называемое агентом), работающее локально на оборудовании. Определенный набор управляемых объектов обслуживается SNMP и используется для управления устройством. Эти объекты определены в базе данных управляющей информации MIB (Management Information Base), которая обеспечивает стандартное представление информации, контролируемое встроенным SNMP-агентом. Протокол SNMP определяет оба формата спецификаций MIB и используется для доступа к информации по сети.
Коммутатор серии DES-30xx поддерживает протокол SNMP версий: 1, 2c и 3. Можно указать, какую версию SNMP использовать для контроля и управления коммутатором. Три версии SNMP протокола различаются в уровне обеспечиваемой безопасности между управляющей станцией и сетевым оборудованием.
В SNMP версиях v.1 и v.2 аутентификация пользователей осуществляется при помощи так называемой «строки сообщества» («community string»), данная функция похожа на пароли. Удаленный пользователь приложения SNMP и коммутатора должен использовать одну и ту же community string. Пакеты SNMP от станций, не прошедших аутентификацию будут игнорироваться (удаляться).
По умолчанию community strings для коммутатора, использующего версии v.1 и v.2 протокола SNMP, следующие:
public – позволяет авторизованным станциям управления извлекать объекты MIB.
private – позволяет авторизованным станциям управления извлекать и изменять объекты MIB.
SNMP версии v.3 использует более сложный процесс, который подразделяется на два этапа. Первая часть – это сохранение списка пользователей и их свойств, которые позволяют работать SNMP-менеджеру. Вторая часть описывает, что каждый пользователь из списка может делать в качестве SNMP-менеджера.
Коммутатор разрешает заносить в список и настраивать группы пользователей с определенным набором привилегий. Можно также устанавливать различные версии SNMP для занесенной в список группы SNMP-менеджеров. Таким образом, можно создать группу SNMP-менеджеров, которым разрешено просматривать информацию только в режиме чтения или получать запросы, используя SNMP v.1, в то время как другой группе можно назначить более высокий уровень безопасности и дать привилегию чтения/записи, используя SNMP v3.
Индивидуальным пользователям и группам SNMP-менеджеров, использующим SNMP v.3, может быть разрешено или ограничено выполнение определенных функций управления SNMP. Функции «разрешено» или «запрещено» определяются идентификатором объекта (OID – Object Identifier), связанного со специальной базой MIB. Дополнительный уровень безопасности доступен в SNMP v.3, в данной версии SNMP сообщения могут быть зашифрованы. Для получения дополнительной информации по настройке SNMP v.3 в коммутаторе, прочитайте раздел под названием Управление.

Traps

«Traps» - это аварийные сообщения, сообщающие о событиях, происходящих в коммутаторе. События могут быть такими серьезными, как перезапуск (кто-нибудь случайно выключил коммутатор), или менее 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 / многоадресном шторме (Broadcast\Multicast Storm).

Базы управляющей информации MIB

Коммутатор хранит в базе управляющей информации MIB управляющую информацию и значения счетчика. Коммутатор использует стандартный модуль MIB-II. В результате, значения объектов MIB могут быть извлечены из любого сетевого управляющего программного обеспечения,

основанного на протоколе SNMP. Помимо стандартной базы MIB-II, коммутатор также поддерживает свою собственную базу MIB, в качестве расширенной базы данных управляющей информации. Определяя идентификатор объекта MIB, можно также извлечь собственную базу данных MIB. Значения MIB можно либо только читать, либо читать-записывать.
Коммутаторы DES-3028/28P/52/52P обеспечивают гибкое SNMP-управление. Настройки SNMP могут быть изменены в зависимости от сети и предпочтений администратора. С помощью меню SNMP V3 существует возможность выбрать версию SNMP, используемую для определенных задач.
Коммутаторы DES-3028/28P/52/52P поддерживают Simple Network Management Protocol (SNMP) версий 1, 2c и 3. Администратор сети может указать версию SNMP, используемую для управления Коммутатором. Три версии SNMP протокола различаются в уровне обеспечиваемой безопасности между управляющей станцией и сетевым оборудованием.
Настройки SNMP доступны в папке SNMP V3 Web-менеджера. Назначение рабочих станций, для которых доступно SNMP-управление, доступно в меню Management Station IP Address.

Настройки SNMP Traps

Следующее окно применяется для настроек SNMP trap на Коммутаторе. Для работы с показанным ниже окном кликните **Administration > SNMP Manager > SNMP Trap Settings**:

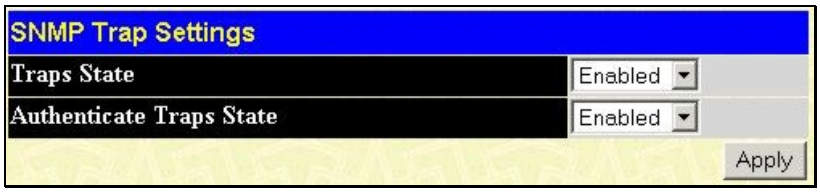


Рисунок 6- 27. Окно SNMP Trap Settings

Чтобы включить или выключить Traps State и/или Authenticate Traps State, задайте соответствующие значения в выпадающих меню и кликните по **Apply**.

Таблица пользователей SNMP

Таблица **SNMP User Table** отображает всех сконфигурированных на коммутаторе SNMP-пользователей.
Для открытия данной таблицы кликните **Administration > SNMP Manager > SNMP User Table**. В результате откроется окно **SNMP User Table,** как показано ниже.

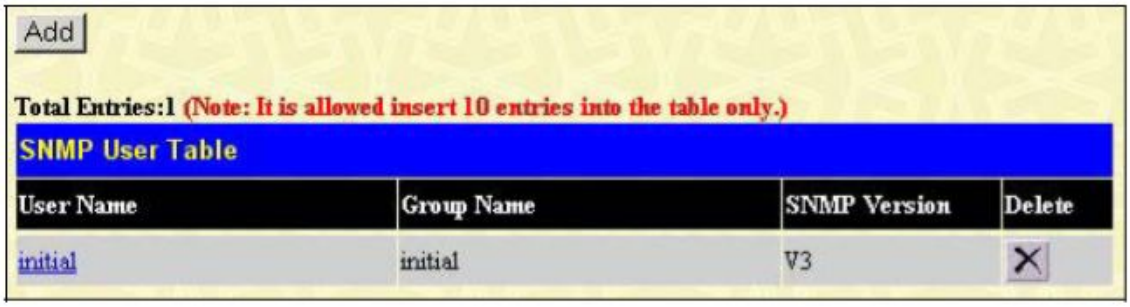


Рисунок 6- 28. Окно SNMP User Table

Чтобы удалить существующую запись в таблице **SNMP User Table**, кликните под заголовком **Delete** по соответствующему нужной записи знаку .
Чтобы отобразить более подробную информацию по определенному пользователю, кликните по кнопке **View** под заголовком **Display**. В результате откроется окно **SNMP User Table Display**, как показано ниже.

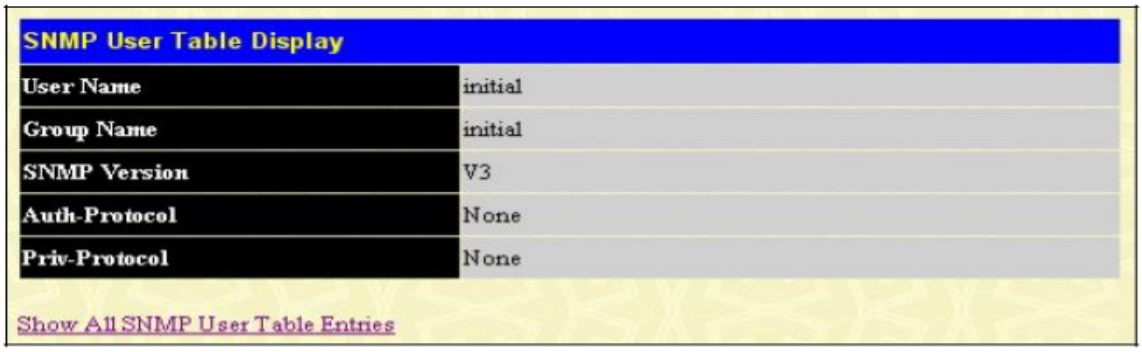


Рисунок 6- 29. Окно SNMP User Table Display

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 возврата к таблице SNMP-пользователей кликните по ссылке Show All SNMP User Table Entries. Чтобы добавить новую запись в окне **SNMP User Table Configuration**, кликните по кнопке **Add** в окне **SNMP User Table**. В результате откроется окно **SNMP User Table Configuration**, как показано ниже.

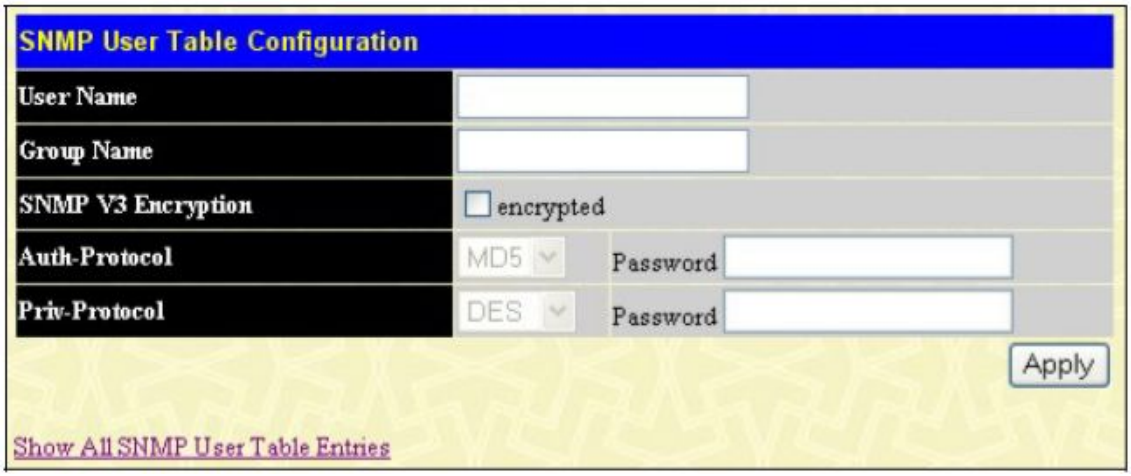


Рисунок 6- 30. Окно SNMP User Table Configuration

Здесь для настройки доступны 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 Version	*V1* – свидетельствует о том, что используется SNMP версии 1. *V2* – свидетельствует о том, что используется SNMP версии 2. *V3* – свидетельствует о том, что используется SNMP версии 3.
Auth-Protocol	*MD5* – свидетельствует о том, что будет использоваться уровень аутентификации HMAC-MD5-96. Данное поле доступно, когда в поле SNMP Version выбрана версия *V3* и подключено шифрование в поле Encryption, пользователя попросят ввести пароль. *SHA* – свидетельствует о том, что будет использоваться протокол HMAC-SHA. Данное поле доступно, когда в поле SNMP Version выбрана версия *V3* и подключено шифрование в поле Encryption, пользователя попросят ввести пароль.
Priv-Protocol	*None* – определяет, что протокол аутентификации не используется. *DES* – 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.
Encrypted	Поставьте галочку в соответствующем поле для использования протокола SNMP V3. Данное поле доступно только в режиме использования SNMP V3.

Чтобы принять выполненные изменения, кликните по **Apply**. Для возврата к таболице SNMP-пользователей кликните по ссылке Show All SNMP User Table Entries.

Таблица просмотра SNMP (SNMP View Table)

SNMP View Table используется для просмотра «community strings», которые определяют, к каким объектам MIB можно получить доступ через удаленный SNMP-менеджер. Для работы с данным окном кликните **Administration > SNMP Manager** > **SNMP View Table**. В результате появится следующее окно:

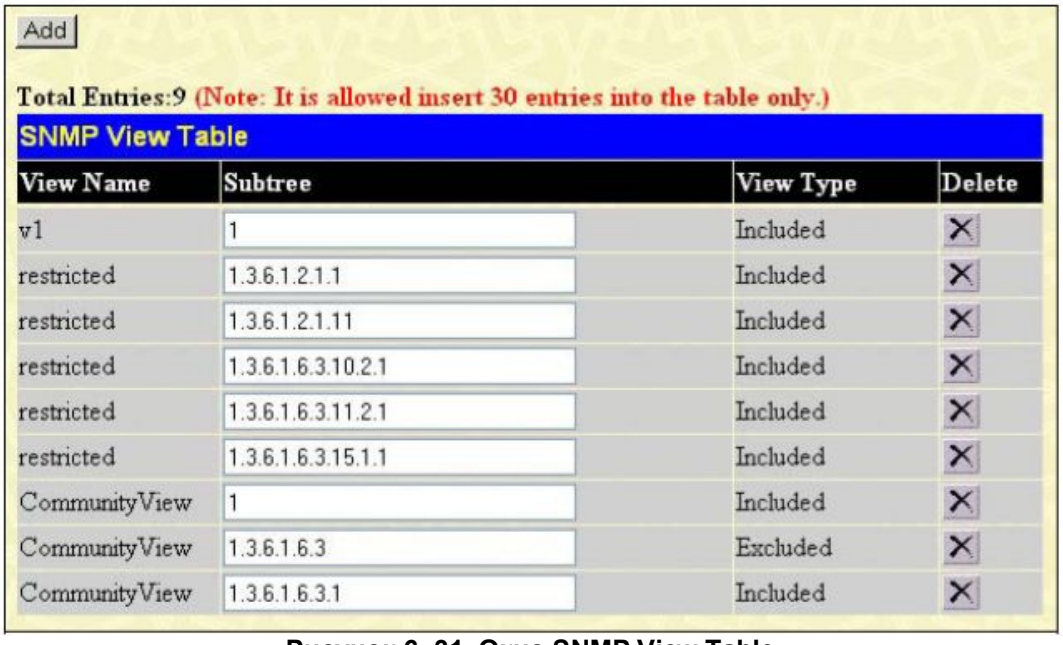


Рисунок 6- 31. Окно SNMP View Table

Чтобы удалить существующую запись в SNMP View Table, кликните в колонке Delete по соответствующему удаляемой записи знаку . Для создания новой записи кликните по кнопке **Add,** и появится следующее окно.

Рисунок 6-32. Окно SNMP View Table Configuration

Могут быть установлены следующие параметры:

Параметр	Описание
View Name	Введите цифробуквенную строку длиной до 32 символов. Используется для идентификации вновь созданных видов SNMP.
Subtree OID	Поддереров идентификатора объекта (OID) для данного вида. OID идентифицирует объектное дерево (дерево MIB), доступ к которому регулируется SNMP-менеджером.
View Type	Выбор опции Included позволяет включить данный объект в список объектов, к которым SNMP-менеджер сможет получить доступ. Выбор опции Excluded, чтобы исключить данный объект из списка объектов, к которым SNMP-менеджер сможет получить доступ.

Для применения новых настроек кликните по **Apply**. Для возврата к **SNMP View Table** кликните по ссылке Show All SNMP View Table Entries.

Таблица SNMP-групп

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 работы с окном **SNMP Group Table** откройте **Administration > SNMP Manager** и кликните по **SNMP Group Table**. Появится следующее окно:

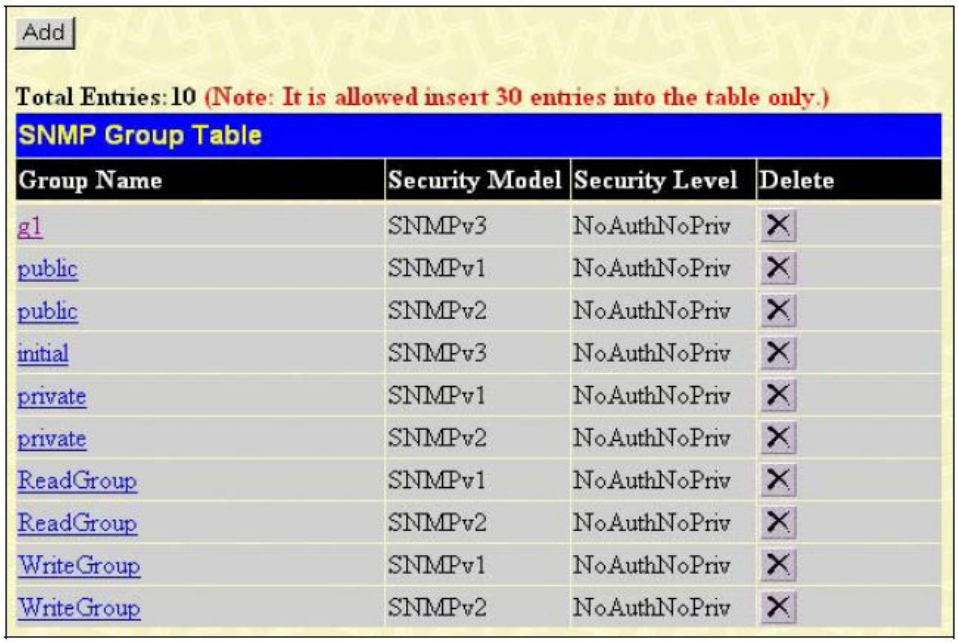


Рисунок 6- 331. Окно SNMP Group Table

Для удаления существующей записи в Таблице SNMP-групп кликните по соответствующему знаку ✕ под заголовком Delete.

Для отображения настроек текущей записи **SNMP Group Table** кликните по кнопке View, расположенной под заголовком Display. В результате отобразится следующее окно.

Рисунок 6-34. Окно SNMP Group Table Display

Чтобы добавить новую запись в Таблицу SNMP-группы Коммутатора, кликните по кнопке **Add** в верхнем левом углу окна **SNMP Group Table**. В результате откроетсфя окно **SNMP Group Table Configuration,** как показано ниже.

Рисунок 6-35. Окно SNMP Group Table Configuration

Для установки доступны 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	*SNMP v1* – свидетельствует о том, что будет использоваться SNMP версии 1. *SNMP v2* – свидетельствует о том, что будет использоваться SNMP версии 2. SNMP v.2 поддерживает централизованную и распределенную модели сетевого управления. В данной версии есть улучшения в структуре управляющей информации (Structure of Management Information, SMI), а также добавлены некоторые функции безопасности. *SNMP v3* – свидетельствует о том, что будет использоваться SNMP версии 3. SNMP v3 обеспечивает безопасный доступ к оборудованию, благодаря сочетанию аутентификации и шифрования пакетов, передаваемых по сети.
Security Level	Настройки уровня безопасности применимы только для SNMP v.3. *NoAuthNoPriv* – свидетельствует о том, что будет отсутствовать авторизация, а также шифрование пакетов, отправляемых между коммутатором и удаленным SNMP-менеджером. *AuthNoPriv* – свидетельствует о том, что будет затребована авторизация, но будет отсутствовать шифрование пакетов, отправляемых между коммутатором и удаленным SNMP-менеджером. *AuthPriv* – свидетельствует о том, что будет затребована авторизация и пакеты, пересылаемые между коммутатором и удаленным SNMP-менеджером, будут шифроваться.

Для принятия новых настроек кликните по **Apply**. Для возврата к Таблице SNMP-групп кликните по ссылке 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 папку **SNMP Manager** (находится в папке **Administration**) и кликните по **SNMP Community Table**, что откроет следующее окно:

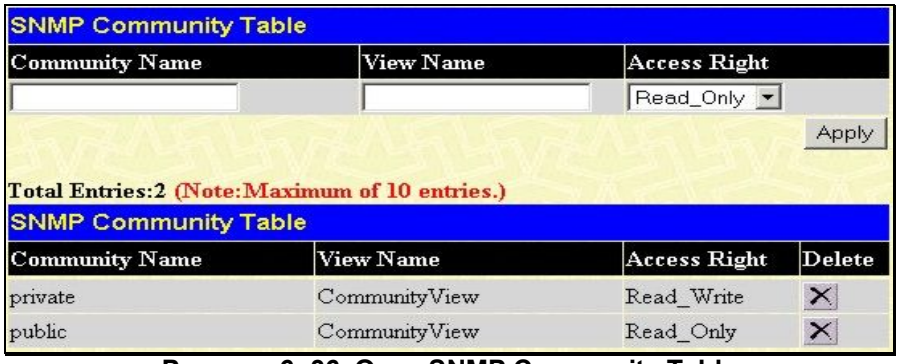


Рисунок 6- 36. Окно SNMP Community Table

Могут быть установлены следующие параметры:

Параметр	Описание
Community Name	Введите имя, которое может состоять из буквенно-цифровой последовательности длиной не более 32 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 информацию в содержимое баз MIB коммутатора.

Чтобы принять выполненные настройки, кликните **Apply**. Для удаления записи из таблицы **SNMP Community Table** кликните под заголовком **Delete** по соответствующей кнопке .

Таблица хоста SNMP

Окно **SNMP Host Table** позволяет настроить получателей SNMP trap. Откройте папку **SNMP Manager** (находится в папке **Administration**) и кликните по ссылке **SNMP Host Table**. В результате откроется окно **SNMP Host Table**, показанное ниже. Чтобы удалить запись в **SNMP Host Table**, кликните под заголовком **Delete** по соответствующей кнопке . Чтобы отобразить текущие настройки записи **SNMP Group Table**, кликните по соответствующей ссылке записи под заголовком Host IP Address.

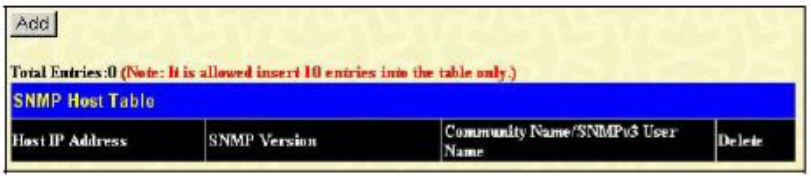


Рисунок 6-37. Окно SNMP Host Table

Чтобы добавить новую запись в Таблицу хоста SNMP, кликните по кнопке **Add** в верхнем левом углу окна. В результате откроется окно **SNMP Host Table Configuration**, как показано ниже.

Рисунок 6- 38. Окно SNMP Host Table Configuration

Могут быть установлены следующие параметры:

Параметр	Описание
Host IP Address	Наберите IP-адрес удаленной станции управления, которая будет служить SNMP-хостом коммутатора.
P Version	*V1* – свидетельствует о том, что будет использоваться SNMP версии 1. *V2* – свидетельствует о том, что будет использоваться SNMP версии 2. *V3-NoAuth-NoPriv*– свидетельствует о том, что будет использоваться SNMP версии 3 с уровнем безопасности NoAuth-NoPriv. *V3-Auth-NoPriv* – свидетельствует о том, что будет использоваться SNMP версии 3 с уровнем безопасности Auth-NoPriv. *V3-Auth-Priv* – свидетельствует, что будет использоваться SNMP версии 3 с

	уровнем безопасности Auth-Priv.
Community String / SNMP V3 User Name	Введите «community string» или имя пользователя SNMP V3.

Для принятия новых настроек кликните по **Apply.** Для возврата в таблицу **SNMP Host Table** кликните по 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 engine на Коммутаторе. Чтобы отобразить SNMP Engine ID Коммутатора, откройте папку **SNMP Manger** (расположена в папке **Administration**) и кликните по **SNMP Engine ID**. В результате откроется окно **SNMP Engine ID Configuration**.

Рисунок 6- 39 Окно SNMP Engine ID

Чтобы изменить Engine ID, введите новое значение Engine ID в соответствующем поле и кликните по кнопке **Apply.**

Питание PoE

Модели DES-3028P и DES-3052P поддерживают питание Power over Ethernet (PoE) в соответствии со спецификацией IEEE 802.3af. Порты 1-24/1-48 коммутаторов позволяют осуществлять питание устройств (Power Devices, PDs) от 48 В постоянного тока через UTP-кабель Ethernet категории 5 или Категории 3. И DES-3028P, и DES-3052P поддерживают стандарт PSE (Power Source over Ethernet) со схемой контактов Alternative A, когда питание подается через контакты 1, 2, 3 и 6. DES-3028P и DES-3052P совместимы со всеми устройствами 802.3af D-Link.

Коммутаторы DES-3028P и DES-3052P поддерживают следующие функции PoE:

- Автоматическое обнаружение подключения устройств с поддержкой PoE и начало их питания.
- Автоматическое отключение питания, если: 1) общая потребляемая мощность превышает допустимое значение; 2) потребляемая мощность на отдельном порту превышает допустимый лимит для этого порта.
- Автоматическое отключение порта в случае короткого замыкания. Другие порты при этом останутся активными.

Коммутаторы обеспечивают питание в соответствии со следующей классификацией:

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

Устойства получают питание в соответствии со следующей классификацией:

Класс	Максимальная мощность
0	0,44 – 12,95 Вт
1	0,44 – 3,84 Вт
2	3,84 – 6,49 Вт
3	6,49 – 12,95 Вт

Для настройки функций PoE на DES-3028P и DES-3052P кликните **Administration > PoE Configuration.** Окно PoE System позвляет назначить ограничение мощности, при превышение которого будет отключена система PoE. Для настойки ограничения мощности введите в поле Power Limit значение от 37Вт до 185Вт (для DES-3028P) или соответственно от 37Вт до 370Вт (для DES-3052P). По умолчанию установлено 185Вт (для DES-3028P) и 370Вт (для DES-3052P). Когда общая потребляемая мощность превышает данное значение, PoE-контроллер отключит подачу питания для предотвращения перегрузки источника питания.

Чтобы задать настройки PoE на Коммутаторе кликните **Administration > PoE Configuration**, после чего откроется окно для настройки пользователем.

Настройка системы PoE

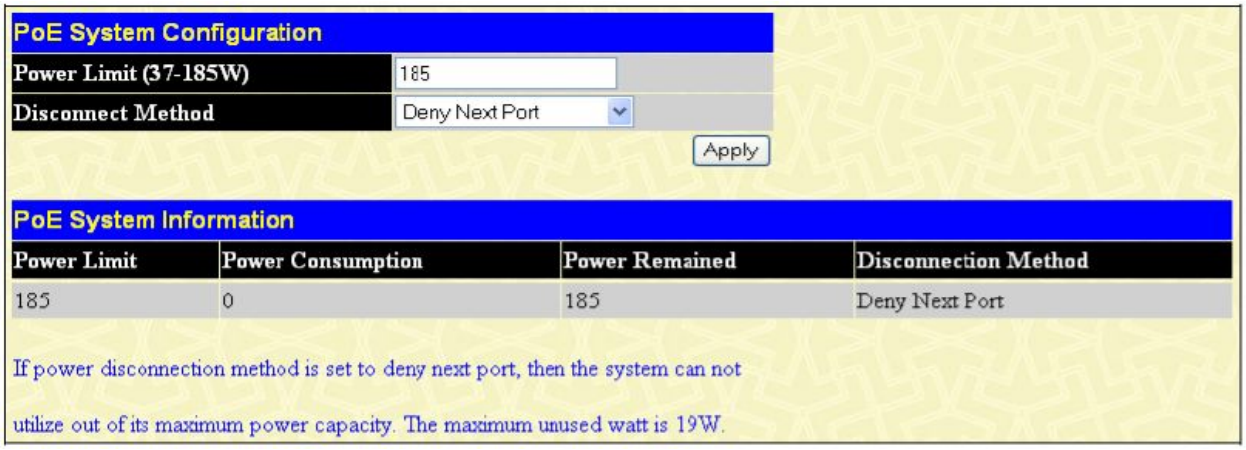


Рисунок 6- 40. Окно PoE System Configuration

Настройки PoE на основе портов

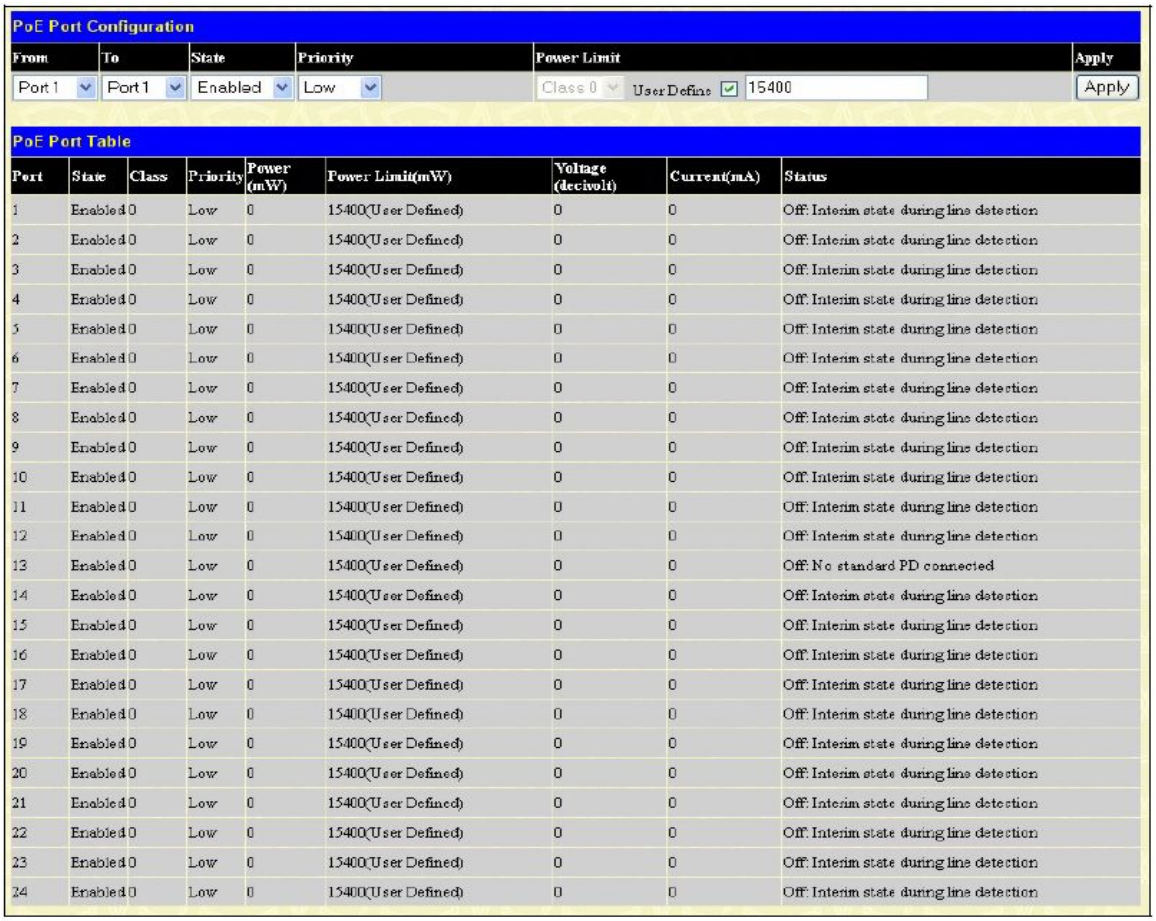


Рисунок 6- 41. Окно PoE Port Configuration

В показанном выше окне доступны следующие параметры:

Параметр	Описание
PoE System	
Power Limit	Устанавливает ограничение мощности, которую передает источник питания Коммутатора на порты PoE. Пользователь может установить Power Limit от 37 до 185Вт (для DES-3028P) или от 37 до 370 Вт (для DES-3052P). По умолчанию установлено 185Вт (для DES-3028P) и соответственно 370 Вт (для DES-3052P).
Power Disconnect Method	PoE-контроллер поддерживает один из алгоритмов **Deny next port** (запретить следующий порт) или **Deny low priority port** (запретить порт с наименьшим приоритетом), чтобы снизить потребляемую мощность до приемлемого уровня. Выбор между двумя методами осуществляется в выпадающем меню **Power Disconnect Method**. По умолчанию используется алгоритм **Deny next port**. Ниже приводится краткое описание обоих методов: **Deny next port** – После превышения лимита следующий порт, пытающийся получить питание, получит отказ независимо от его приоритета. **Deny low priority port -** После превышения лимита следующий порт, пытающийся получить питание, приведет к отключению порта с минимальным приоритетом в пользу портов с более высоким приоритетом.
PoE Configuration	
From… To…	Данный выпадающие меню позволяют задать диапазон портов, для которых будет включено или выключено питание PoE.
State	Данное выпадающее меню позволяет включить или выключить питание PoE для указанных ранее портов.

Priority	Данное выпадающее меню дает возможность задать приоритеты портов PoE.
Power Limit	Данное поле позволять задать ограничение для порта PoE. После превышения указанного порога PoE перейдет к указанному ранее методу Power Disconnect Method. Доступны значения от 1000 до 15400мВт.

Кликните **Apply** для принятия выполненных настроек PoE. Статус всех настроенных портов PoE отображается в таблице в нижней части экрана, как показано выше.

Настройки управления через единый IP-адрес (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.

Обновление технологии SIM до версии v1.6

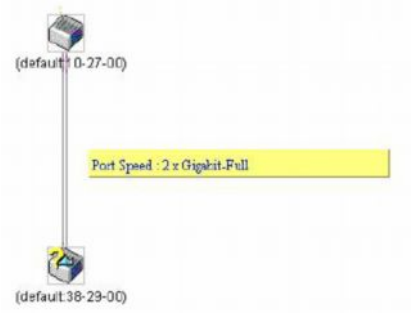
Коммутаторы DES-3028/28P/52/52P в данном релизе поддерживают управление согласно технологии SIM версии 1.6.

Это обеспечивает ряд преимуществ, а именно:

1. Теперь CS может автоматически повторно обнаруживать коммутаторы MS, которые оставили SIM-группу при перезагрузке или сбоя Web. Эта функция реализована с помощью пакетов Discover и Maintain, которые члены SIM-группы передают после перезагрузки. MAC-адрес и пароль коммутаторов MS сохранены в базе данных CS. Если происходит перезапуск MS, то CS удерживает информацию MS в своей базе данных и при повторном обнаружении MS автоматически добавляет MS в дерево SIM. При этом не требуется никаких настроек для повторного обнаружения коммутатора.

Однако существует нексколько случаев, когда сохраненные коммутаторы MS не могут быть восстановлены. Например, если питание коммутатора отключено, или он стал членом другой группы, или он стал коммутатором CS.

2. Теперь топология поддерживает некоторые функции для соединений, являющихся членами группы агрегированных каналов. Будут отображены скорость и количество Ethernet-соединений, входящих в эту группу агрегированных каналов, как показано на рисунке ниже.



3. В этой версии улучшены возможности загрузки на коммутатор и сохранения на TFTP-сервере:
Программное обеспечение – Теперь коммутатор поддерживает загрузку с TFTP-сервера нескольких версий программного обеспечения для MS.
Конфигурационные файлы – Коммутатор поддерживает загрузку нескольких конфигурационных файлов MS с/на TFTP-сервер.
Журнал – Коммутатор поддеживает загрузку нескольких файлов журнала на TFTP-сервер для MS.
4. Пользователь может управлять масштабом окна Топология, настраивая оптимальное отображение конфигурации.

Настройки 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 Settings,** после чего появится следующее окно.

Рисунок 6.42 – Окно «SIM Settings» (disabled – отключено)

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:

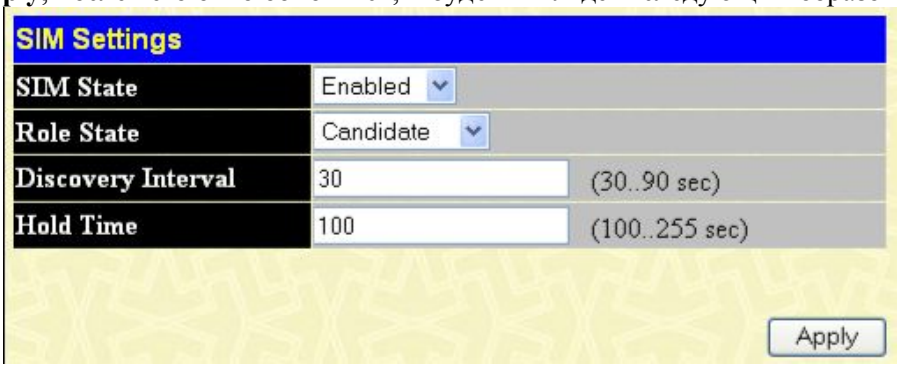


Рисунок 6.43 – Окно SIM Settings (enabled – включено)

Если требуется настроить Коммутатор как Commander Switch (CS), выберите значение Commander в поле **Role State** и кликните по **Apply**. Тогда окно будет выглядеть так:

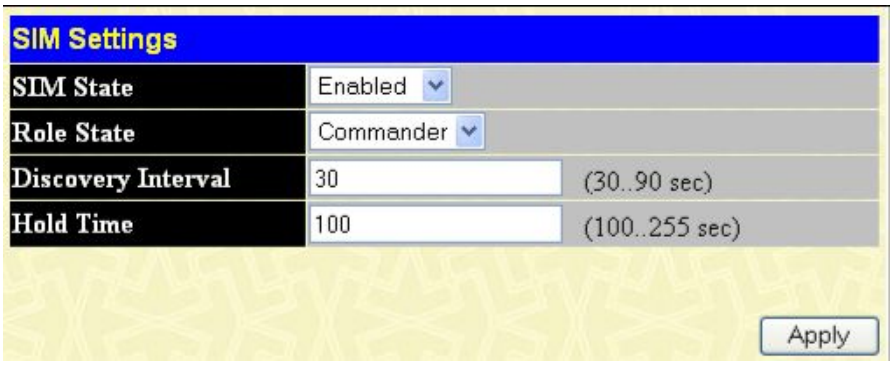


Рисунок 6.44 – Окно «SIM Settings» (значение Commander)

Можно настроить следующие параметры:

Параметр	Описание

SIM State	Используйте выпадающее меню для изменения SIM-состояния коммутатора. *Disabled* переведет все функции SIM коммутатора в нерабочее состояние.
Role State	Используйте выпадающее меню для изменения роли коммутатора в SIM-группе. Возможно два варианта: *Candidate* – Candidate Switch (CaS) не является членом SIM-группы, но подключен к управляющему коммутатору Commander Switch (CS). Данная роль коммутатора в SIM-группе является настройкой по умолчанию. *Commander* – Выберите данный вариант, чтобы коммутатор выполнял роль управляющего CS. Пользователь может подключить другие коммутаторы к управляющему поверх Ethernet, чтобы они стали членами этой SIM-группы. 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, кликните по **Apply**.
После включения коммутатора в качестве управляющего CS, в папке **Single IP Management** для помощи пользователю в настройке SIM через Web-интерфейс появятся ссылки: **Topology, Firmware Upgrade**, **Configuration Backup/Restore** и **Upload Log File.**

Топология сети

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

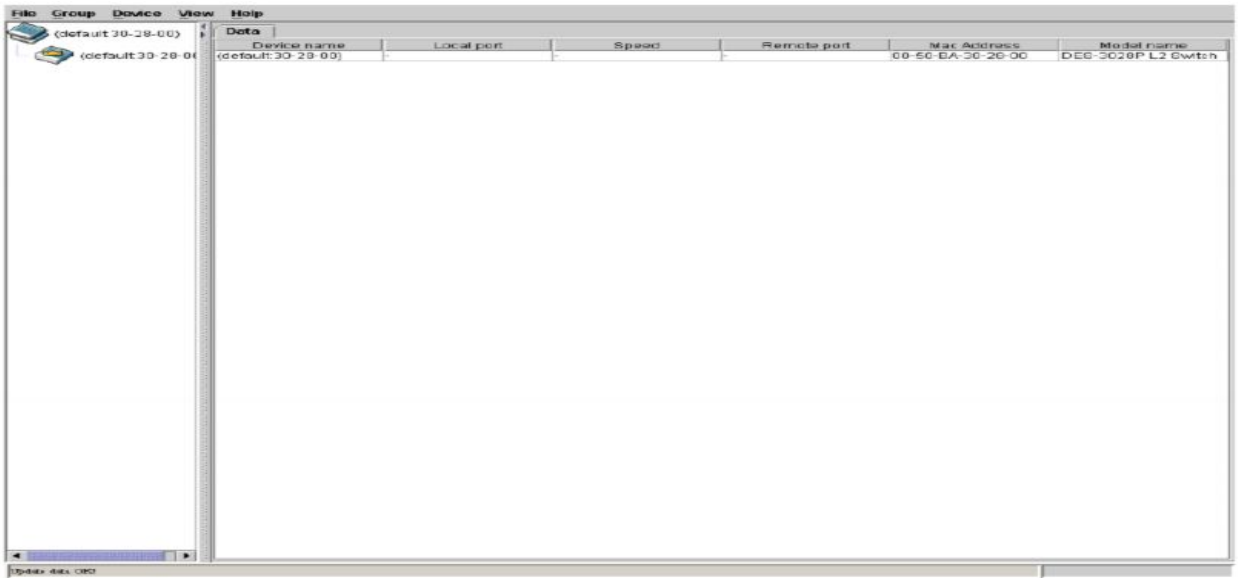


Рисунок 6.45 – Окно Single IP Management – Tree View

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).

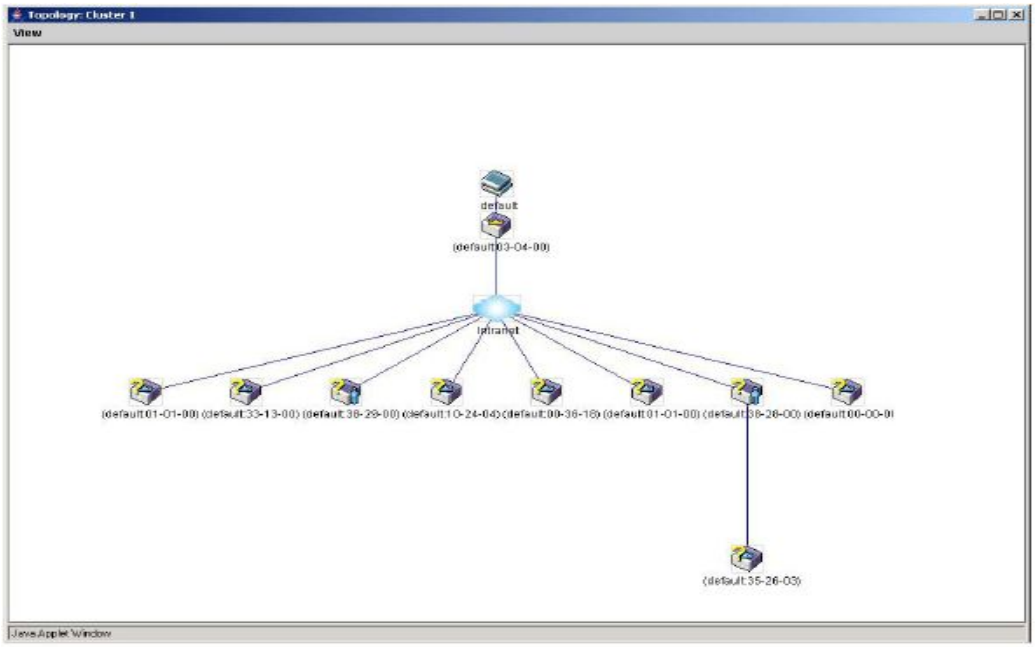


Рисунок 6.46 – Окно Topology View

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.

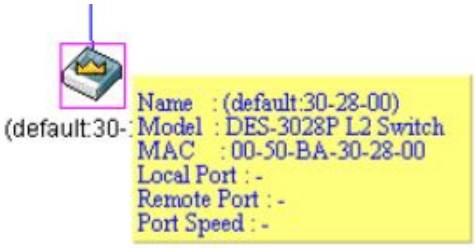


Рисунок 6.47 – Получение информации об устройстве, используя значки устройств

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

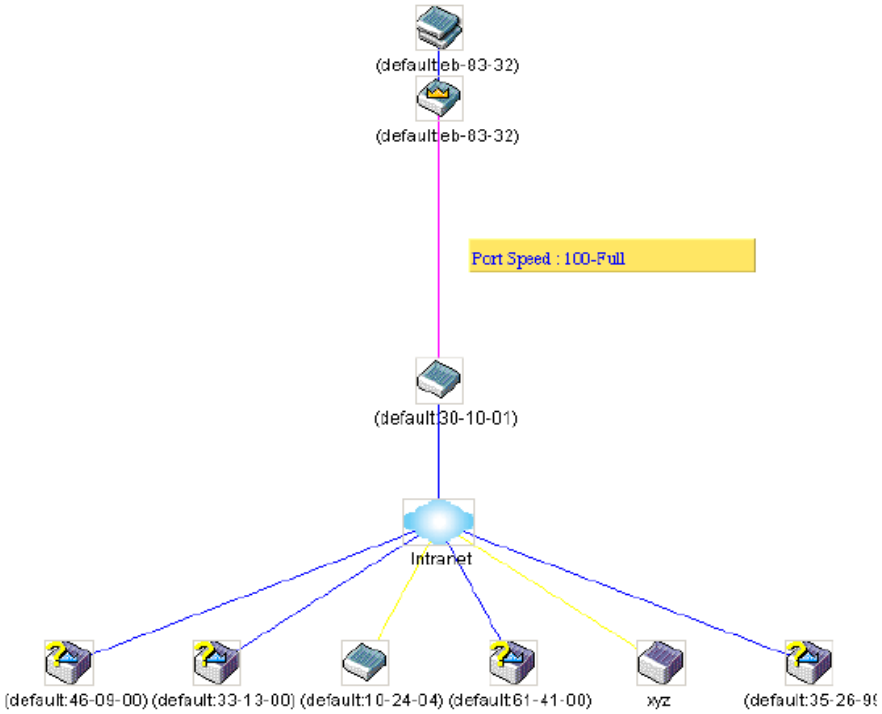


Рисунок 6.48 – Получение информации о скорости порта, используя значки устройства

Нажатие правой кнопки мышки

Нажатие правой кнопки мышки на устройстве позволит пользователю работать с различными опциями в зависимости от роли коммутатора в SIM-группе.

Группировка иконок

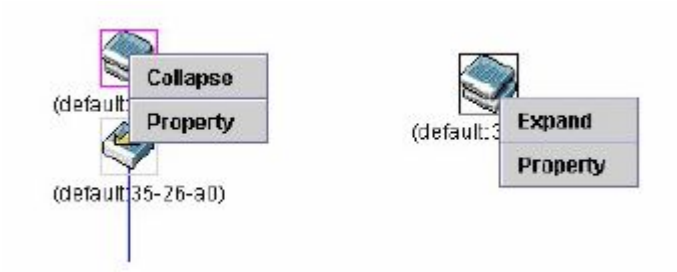


Рисунок 6.49 –Нажатие правой кнопкой мышки на значок группы

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.

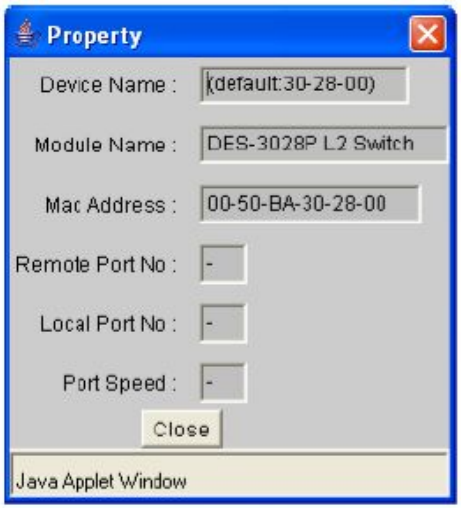


Рисунок 6.50 – Окно Property

Значок управляющего коммутатора

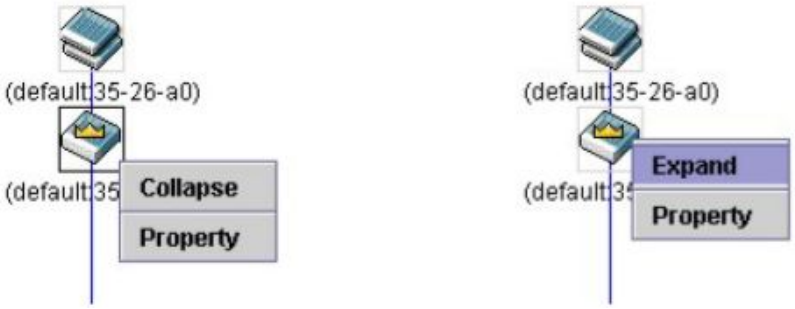


Рисунок 6.51 – Нажатие правой кнопкой мыши по значку управляющего коммутатора

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.

Значок члена группы

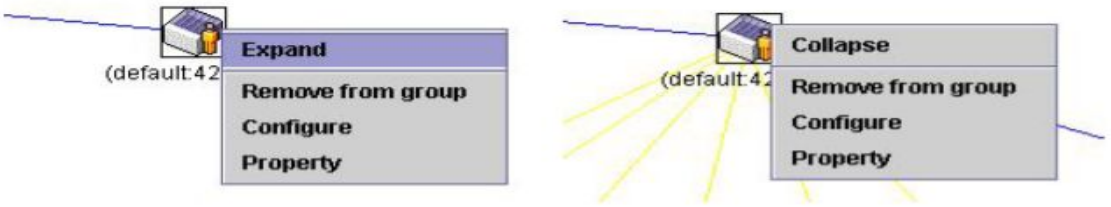


Рисунок 6.52 - Нажатие правой кнопки мышки по значку члена группы

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-интерфейс управления для настройки коммутатора.
- **Property** – показать на экране информацию о группе.

Значок коммутатора CaS

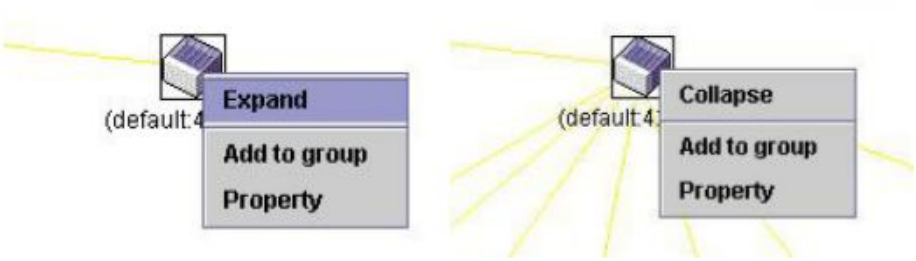


Рисунок 6.53 - Нажатие правой кнопки мыши по значку CaS

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** или **Cancel** для закрытия окна.

Рисунок 6.54 – Диалоговое окно Input password

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

Линейка меню

В окне **Single IP Management** для настройки устройств предусмотрена линейка меню, изображенная ниже

Рисунок 6.55 – 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 **ОК** для ввода пароля или **Cancel** для закрытия окна.

Рисунок 6.56 - Диалоговое окно Input password

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

Device

▪ **Configure** – открыть Web-интерфейс управления 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.

Рисунок 6.57 - Окно About

Обновление программного обеспечения для членов SIM-группы

Окно **Firmware Upgrade** используется для обновления программного обеспечения на коммутаторе, являющемся членом SIM-группы, с управляющего коммутатора CS. Для работы с окном кликните **Administration > Single IP Management Settings > Firmware Upgrade**. В данном окне представлена таблица, включающая коммутаторы MS, номер порта на управляющем коммутаторе, к которому подключен MS, MAC-адрес, название модели и версию. Чтобы установить программное обеспечение на выбранный коммутатор, необходимо отметить соответствующее поле под заголовком Port, ввести IP-адрес сервера, на котором находится программное обеспечение, и указать путь и имя файла программного обеспечения. Далее необходимо кликнуть по **Download**.

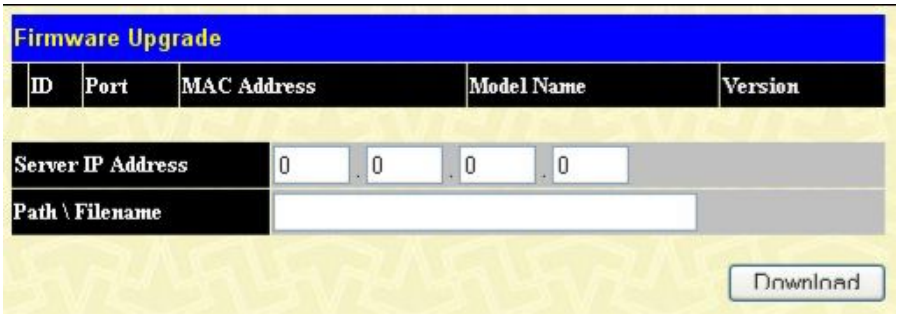


Рисунок 6.58 – Окно Firmware Upgrade

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. В данном окне представлена таблица, включающая коммутаторы MS, номер порта на управляющем коммутаторе, к которому подключен MS, MAC-адрес, название модели и версию. Чтобы установить конфигурационный файл на выбранный коммутатор, необходимо отметить соответствующее поле под заголовком Port, ввести IP-адрес сервера, на котором находится конфигурационный файл, и указать путь и имя конфигурационного файла. Далее необходимо кликнуть по **Download.** Аналогично существует возможность сохранить конфигурационный файл на Коммутаторе (для этого используется кнопка **Upload**). Для работы с данным окном кликните **Administration > Single IP Management Settings > Configuration Backup/Restore**.

Рисунок 6.59 – Окно Configuration File Backup/Restore

Загрузка файла журнала Коммутатора

Следующее окно используется для загрузки файлов журнала коммутаторов, являющихся членами SIM-группы на определенный компьютер. Для работы с этим окном кликните **Administration > Single IP Management > Upload Log File**. Для этого необходимо ввести IP-адрес коммутатора, члена SIM-группы, а затем указать путь для сохранения файла на компьютере. Далее необходимо кликнуть по кнопке **Upload**.

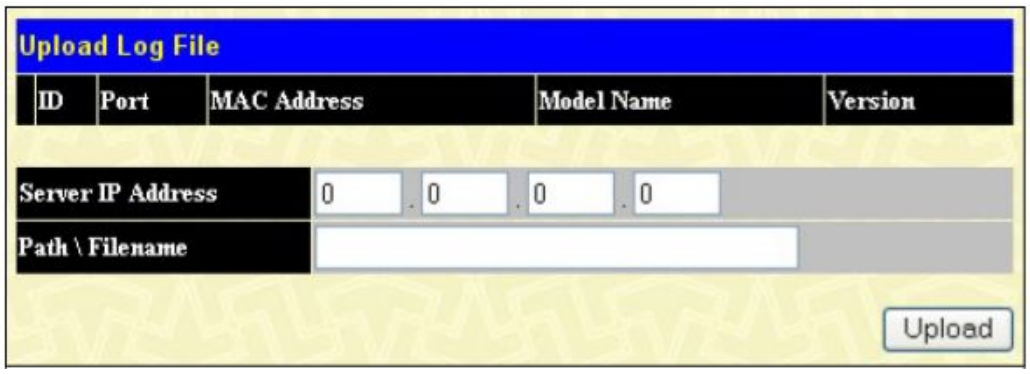


Рисунок 6-60. Окно Upload Log File

Продвижение и фильтрация пакетов (папка Forwarding Filtering)

Продвижение пакетов на заданный Unicast-адрес (Unicast Forwarding)

Папка **Forwarding Filtering** открывается из меню **Administration,** далее следует кликнуть по ссылке **Unicast Forwarding,** в результате откроется следующее окно.

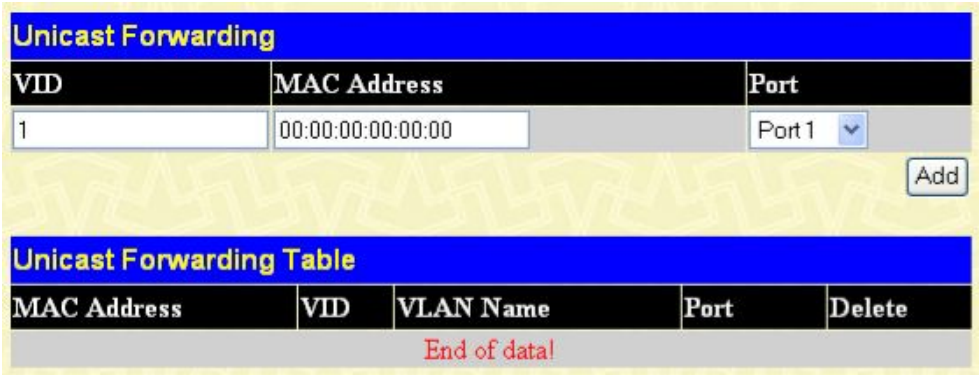


Рисунок 6- 61. Окно Unicast Forwarding

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

Параметр	Описание
VLAN ID (VID)	Идентификатор VLAN (VLAN ID), которой принадлежит MAC-адрес, указанный в соответствующем поле.
MAC Address	MAC-адрес, на который будут пересылаться все пакеты. Это должен быть одноадресный (unicast) MAC-адрес.
Allowed to Go Port	Позволяет задать номер порта, к которому относится вышеупомянутый MAC-адрес.

Для принятия настроек необходимо кликнуть **Apply**. Для удаления записи в таблице **Unicast Forwarding Table** следует кликнуть по соответствующему ***X*** под заголовком **Delete**.

Multicast Forwarding

Следующий рисунок и таблица демонстрируют, как создать **Multicast Forwarding** (многоадресная рассылка) на Коммутаторе. Необходимо открыть папку **Forwarding Filtering**, кликнуть по ссылке **Multicast Forwarding**, после чего откроется следующее окно:

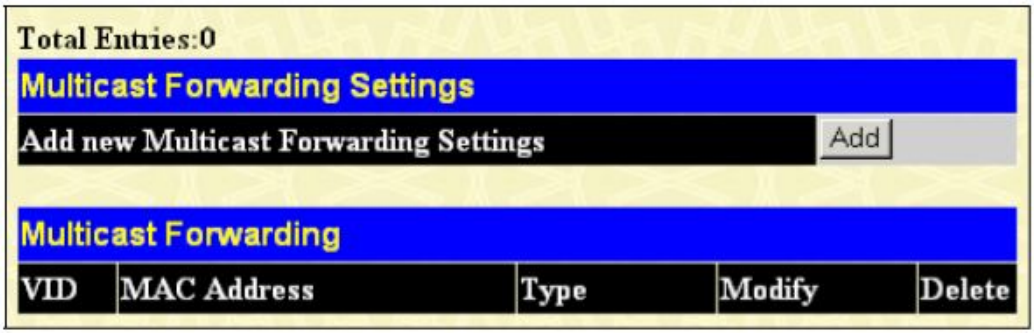


Рисунок 6- 62. Окно Multicast Forwarding Settings

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

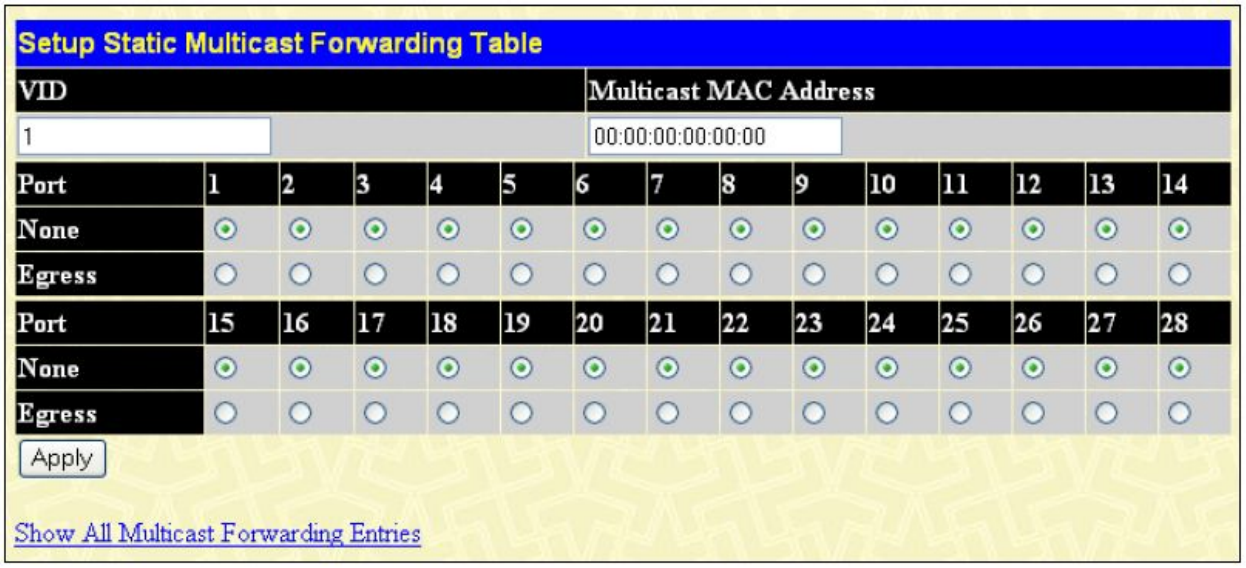


Рисунок 6- 63. Окно Setup Static Multicast Forwarding Table

Могут быть установлены следующие параметры:

Параметр	Описание
VID	Идентификатор VLAN (VLAN ID), которой принадлежит соответствующий MAC-адрес.

Multicast MAC Address	MAC-адрес статического источника многоадресных пакетов. Это должен быть многоадресный MAC-адрес.
Port Settings	Позволяет выбрать порты, которые будут членами статической многоадресной группы, и порты, которым будет запрещено присоединяться динамически к многоадресной группе. Помимо этого существует возможность указать порты, которые могут присоединиться к многоадресной группе, используя GMRP. Возможны следующие опции: *None* – динамическое присоединение к многоадресной группе не ограничено. Когда выбрано значение None, порт не может быть членом статической многоадресной группы. *Egress* – порт, являющийся постоянным членом многоадресной группы.

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

Режим фильтрации порта многоадресной рассылки

Следующий рисунок и таблица помогают пользователю создать многоадресную рассылку на Коммутаторе. Для этого следует открыть папку **Forwarding Filtering** и кликнуть по линку **Multicast Port Filtering Mode Setup**, откроется следующее окно:

Рисунок 6- 64. Окно Multicast Filtering Mode

Могут быть настроены следующие параметры:

Параметр	Описание
From/To	Эти два выпадающих меню позволяют задать диапазон портов, для которых будет настроена фильтрация.
Mode	Это выпадающее меню позволяет задать действие, которое предпримет Коммутатор при получении многоадресного пакета, предназначенного для передачи на какие-либо порты из заданного выше диапазона. • *Forward Unregistered Groups* – Выбор этой опции приведет к тому, что Коммутатор будет передавать многоадресный пакет, предназначенный для незарегистрированной многоадресной группы, по портам, определённым выше. • *Filter Unregistered Groups* - При выборе данной опции Коммутатор будет отфильтровывать многоадресный пакет, предназначенный для незарегистрированной многоадресной группы внутри диапазона портов, определённого выше.

Для принятия настроек необходимо кликнуть **Apply**.

Сервис SMTP

SMTP (Simple Mail Transfer Protocol) – это функция Коммутатора, которая позволяет рассылать информацию о событиях, происходящих на Коммутаторе, получаелям электронной почты, адреса которых задаются с помощью указанных в данном разделе опций. Коммутатор настраивается как клиент SMTP, а сервер как удаленное устройство, которое будет получать сообщения от коммутатора, помещать их в письмо e-mail и отправлять получателям, установленным на Коммутаторе. Эта функция особенно полезна сетевым администраторам, упрощая управление небольшими рабочими группами и увеличивая скорость обработки сообщений о нештатных ситуациях на Коммутаторе и обеспечивая безопасность.

При функционировании в качестве клиента SMTP Коммутатор играет четыре основные роли:

• Для корректной работы этой функции необходимо надлежащим образом настроить сервер и виртуальный порт сервера. Это достигается путем ввода корректных значений в поля **SMTP Server Address** и **SMTP Server Port** окна **SMTP Service Settings**.

• Далее необходимо настроить получателей сообщений электронной почты. Эта информация отправляется на сервер. Можно настроить до 8 получателей e-mail на Коммутаторе с помощью окна **SMTP Service Settings,** заполнив поле **Mail Receiver Address**.

• Администратор может настроить адрес e-mail источника, с которого будут доставляться сообщения настроенным получателям. Это предоставит администратору более полную информацию о функциях коммутатора и возникших проблемах. Адрес e-mail может быть настроен с помощью окна **SMTP Service Settings** и настройки поля Self Mail Address.

• Может быть настроена отправка тестовых сообщений для проверки, получат ли получатели e-mail сообщения от SMTP-сервера. Чтобы настроить отправку тестовых сообщений, необходимо включить сначала функцию SMTP, настроив поле SMTP State в окне **SMTP Service Settings,** а затем отправив email с помощью окна **SMTP Service**. Все получатели, настроенные SMTP, получат тестовое сообщение от SMTP-сервера, позволяющее проверить надежность данной функции.

Коммутатор будет отправлять сообщения e-mail, когда возникает хотя бы одно из приведенных событий:

• При холодном запуске коммутатора.

• При отключении порта (статус link down).

• При включении порта (статус link up).

• При неудачной аутентификации SNMP (запрещена Коммутатором).

• При сохранении конфигурационного файла коммутатора в энергонезависимой памяти NVRAM.

• При ошибке при агрузке программного обеспечения через TFTP. Это могут быть сообщения от TFTP-сервера вида: in-process (в процессе загрузки), invalid-file (некорректный файл), violation (нарушение), file-not-found (файл не найден), complete (завершение) и time-out (истечение времени).

• При сбросе настроек Коммутатора.

Информация в e-mail от SMTP-сервера, относящаяся к событиям на Коммутаторе, включает:

• Имя источника и IP-адрес.

• A timestamp denoting the identity of the SMTP server and the client that sent the message, as well as the time and date of the message received from the Switch. Messages that have been relayed will have timestamps for each relay.

• Событие на Коммутаторе, вызвавшее отправку сообщения e-mail.

• Если событие было инициировано пользователем (например, сохранение или обновление программного обеспечения), то IP-адрес, MAC-адрес и имя пользователя будет отправлено наряду с системным сообщением об ошибке.

• Если событие происходит не в первый раз, то второе и каждое последующее сообщение получит указание в теме сообщения о системной ошибке.

В процессе доставки могут возникать следующие события.

• Срочные сообщения обладают высоким приоритетом и отправляются получателям немедленно, тогда как обычная почта помещается в очередь для последующей передачи.

• Максимальное число непереданных сообщений, которое может быть размещено в очереди, не превышает 30. Любые новые сообщения будут отброшены, если очередь переполнена.

• Если отправленное сообщение не доставлено, оно помещается в очередь ожидания, а затем предпринимается следующая попытка доставить сообщение.

• Максимальное количество попыток доставить сообщение получаетлю равняется трем. Попытки отправки сообщения предпринима.тся каждые пять минут до достижения лимита попыток. Елс и после этого не удалось отправить сообщение, оно отбрасывается и не доставляется получателю.

Если коммутатор выключается или перезагружается, то сообщения в очереди будут утеряны.

Настройки SMTP-сервера

Следующее окно содержит опции по настройке SMTP-сервера Коммутаторе и установки адресов e-mail, на которые будут отсылаться уведомления при возникновении проблемы на Коммутаторе. Для работы со следующим окном откройте папку **Administration**, затем **SMTP Service** и кликните по ссылке **SMTP Server Settings**.

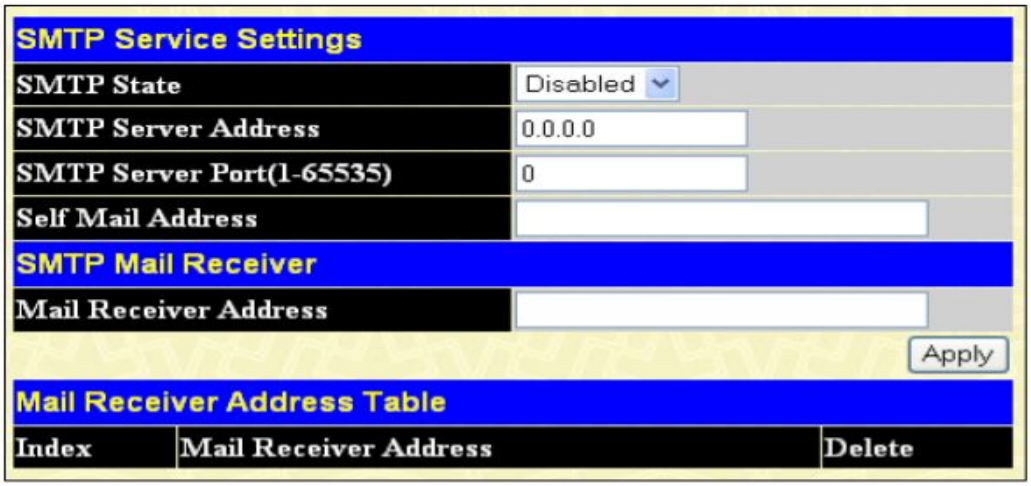


Рисунок 6- 65. Окно SMTP Service Settings и Mail Receiver Address Table

Следующие параметры могут быть установлены:

Параметр	Описание
SMTP State	Данное выпадающее меню позволяет включить или выключить сервис SMTP на Коммутаторе.
SMTP Server Address	Введите IP-адрес SMTP-сервера на удаленном устройстве. Это будет устройство, рассылающее сообщения e-mail.
SMTP Server Port	Введите номер виртуального порта, через который коммутатор будет подключаться к SMTP-серверу. Обычно номер порта для SMTP - 25, но можно установить также значение от 1 до 65535.
Self Mail Address	Введите адрес e-mail, с которого будут отправляться сообщения. Можнонастроить только один адрес. Эта строка не должна превышать 64 цифробуквенных символа.
Mail Receiver Address	Введите список адресов e-mail, на которые будут отправляться сообщения e-mail, относящиеся к событиям на Коммутаторе. До 8 адресов e-mail может быть настроено. Чтобы удалить эти адреса, отметьте соответствующие поля под загловком Delete в таблице Mail Receiver Address Table.

Кликните по **Apply** для принятия выполненных изменений.

Сервис SMTP

Следующее окно используется для отправки тестовых сообщений всем получателям, настроенным на Коммутаторе, тестируя установки и надежность SMTP-сервера. Для работы со следующим окном откройте папку **Administration**, затем папку **SMTP Service** и кликните по ссылке **SMTP Service**.

Рисунок 6- 66. Окно SMTP Service

Могут быть установлены следующие параметры.

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

Когда сообщение готово, кликните кнопку **Send** для отправки сообщения всем получателям SMTP, настроенным на Коммутаторе.

Раздел 7

Функции уровня 2

Виртуальные локальные сети (VLAN)
Агрегирование каналов
IGMP Snooping
Алгоритм покрывающего дерева (Spanning Tree)

Виртуальные локальные сети (VLAN)

Virtual Local Area Network (VLAN) – топология сети, сконфигурированная скорее на логическом уровне, нежели на физическом. VLAN могут использоваться для соединения нескольких сегментов LAN в автономную пользовательскую группу, которая ведет себя как единая сеть LAN. VLAN также позволяют логически сегментировать сеть на различные широковещательные домены, обеспечивая передачу пакетов преимущественно между портами одной VLAN. Как правило, VLAN соответствует отдельной подсети, хотя это необязательно.
VLAN позволяет увеличить производительность сети, не перегружая полосу пропускания сети, и в то же время улучшить безопасность сети, сокращая объемы передаваемого трафика между различными сегментами. Конечные узлы, часто взаимодействующие друг с другом, объединяются в одну VLAN независимо от их физического расположения в сети. VLAN можно также использовать для организации широковещательного домена, т.к. широковещательные пакеты будут отправляться только членам VLAN, в которой была инициирована широковещательная рассылка.

Замечания по реализации функции VLAN на коммутаторах серии DES-30xx

Независимо от того, каким образом определяются конечные узлы и задается их принадлежность к VLAN, для передачи пакетов между VLAN необходимо сетевое устройство, выполняющее функцию маршрутизатора между различными VLAN.
Коммутатор серии DES-30xx поддерживает два вида VLAN: VLAN IEEE 802.1Q и Port-Based VLAN (на основе портов). Для обеспечения совместимости с устройствами, не поддерживающими теги 802.1Q, существует возможность удаления тега 802.1Q из заголовков пакетов.
По умолчанию все порты Коммутатора принадлежат одной VLAN 802.1Q, называемой «default».
VID для "default" VLAN равен 1.
Если необходимо, возможно назначать одни и те же порты в различные Port-Based VLAN.

IEEE 802.1Q VLAN

Некоторые тематические термины:

- **Tagging (Тегирование) –** добавление тега (метки) 802.1Q VLAN в заголовок пакета.
- **Untagging (Удаление тега) –** удаление тега 802.1Q VLAN из заголовка пакета.
- **Ingress port** – порт коммутатора, принимающий пакеты и позволяющий принять решение о тегировании (при получении тегированного пакета информация не меняется, при получении нетегированного пакета тег с приоритетом по умолчанию и VID=PVID)
- **Egress port –** порт коммутатора, с которого отправляются пакеты на другой коммутатор или станцию. В случае если информация передается на тегированный порт, то добавляет тег к пакету. Если информация передается на нетегированный порт, то удаляет тег из заголовка пакета.

Любой порт может быть сконфигурирован как тегированный (tagged), так и нетегированный (untagged). Функция untagging (удаление тега) IEEE 802.1Q VLAN позволяет работать с коммутаторами, не поддерживающими распознавание тегов VLAN в заголовках пакетов. Функция тегирования (tagging) позволяет объединить в одну VLAN управляемые коммутаторы, поддерживающие 802.1Q, и включить функцию Spanning Tree на всех портах.
Основными характеристиками IEEE 802.1Q являются:

- Передача пакетов в VLAN через фильтр, позволяющий принять решение относительно тега.
- Единое глобальное покрывающее дерево (Spanning Tree).
- Использование простой схемы одноуровнего тегирования.
- Продвижение пакетов 802.1Q VLAN
- Решение о продвижении пакетов принимается на основе следующих правилах:
- Ingress rules – правила, управляющие тегированием входящих фреймов.
- Forwarding rules между портами – правила, управлющие продвижением или отфильтровкой пакетов.
- Egress rules – правила, управляющие тегированием исходящих пакетов.

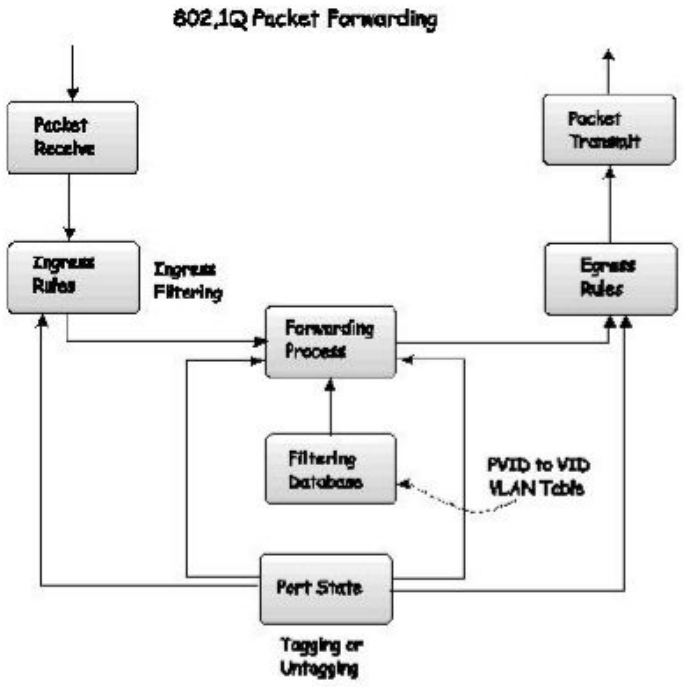


Рисунок 7-1. Продвижение пакетов согласно IEEE 802.1Q

Теги 802.1Q VLAN

На рисунке ниже отображен тег 802.1Q VLAN. Обратите внимание на четыре байта после MAC-адреса источника. Присутствует ли тег в данном пакете, можно судить по полю EtherType. Если значение этого поля равно 0x8100, то в следующих двух байтах пакета следует тег. Тег 802.1Q включает в себя 3 бита приоритета пользователя (802.1p), 1 бит Canonical Format Identifier (CFI – используется для инкапсуляции пакетов Token Ring с последующей передачи по магистралям сети Ethernet) и 12 бит VLAN ID (VID). VID – идентификатор VLAN, используется стандартом 802.1Q. Длина VID 12 бит позволяет только 4094 различных VLAN.

Добавление тега в заголовок пакета делает пакет длиннее на 4 байта. При этом оставшаяся часть пакета остается неизменной.

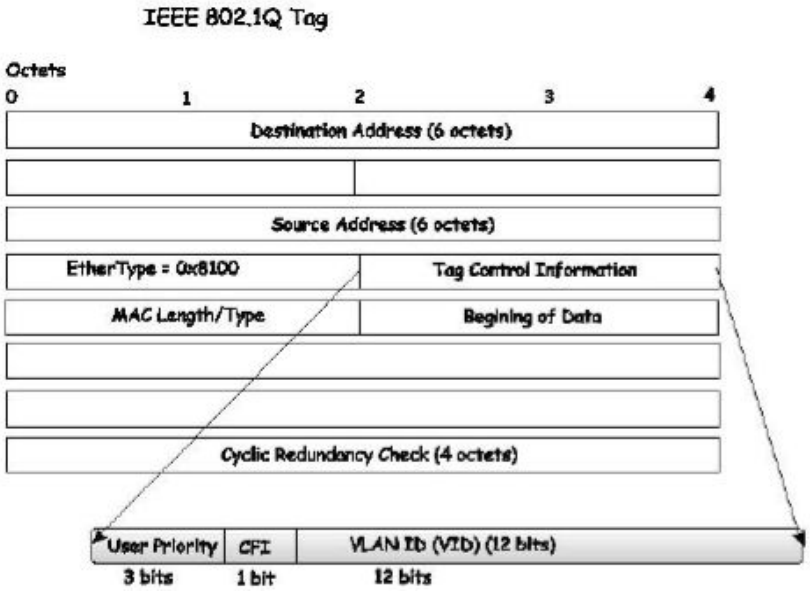


Рисунок 7- 2. Тег IEEE 802.1Q

EtherType и VLAN ID вставляются в пакет после поля MAC-адреса источника, но до исходного поля EtherType/Length или Logical Link Control. Поскольку пакет после добавления тега стал длиннее, чем первоначально, необходимо пересчитать контрольную сумму (Cyclic Redundancy Check, CRC).

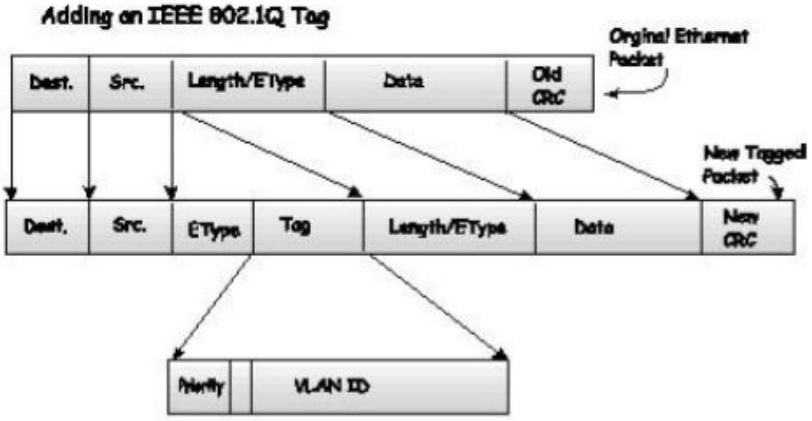


Рисунок 7- 3. Добавление IEEE 802.1Q тега

Тегирующие и нетегирующие порты

Каждый порт коммутатора с поддержкой 802.1Q может быть настроен как тегирующий или нетегирующий.

Тегирующие порты добавляют VID, приоритет и другую VLAN информацию в заголовки всех пакетов проходящих через эти порты. Если в пакет уже был добавлен тег, то порт сохраняет VLAN информацию в неизменном виде. Остальные устройства 802.1Q, принимая решение о продвижении пакетов, используют эту информацию VLAN.

Нетегирующий порт не позволяет считывать 802.1Q тег из проходящих через него пакетов. Таким образом, пакеты, полученные и переданные далее через нетегирующий порт, не содержат информации 802.1Q VLAN. (Следует помнить, что PVID используется только внутри Коммутатора). Удаление тега (Untagging) из заголовка пакета используется для продвижения пакетов с устройств, поддерживающих 802.1Q, на другие сетевые устройства без поддержки 802.1Q VLAN.

Фильтрация входящих пакетов (Ingress Filtering)

Порт Коммутатора, на который приходят пакеты и принимающий решения, касающиеся VLAN, называется Ingress Port. Если на порту задана настройка Ingress filtering, то Коммутатор на основе VLAN-информации в заголовке пакета (если таковая присутствует) будет принимать решение о дальнейшем продвижении пакета.

Если в пакете присутствует VLAN-информация, Ingress port сначала проверит, является ли он членом VLAN, указанной в теге. Если нет, то пакет будет отброшен. Если же порт назначения является членом 802.1Q VLAN, то пакет будет передан в сегмент сети, связанный с портом назначения.

Если пакет не содержит VLAN-информацию, Ingress Port присвоит ему собственный PVID в качестве VID (если это тегирующий порт). Затем Ingress Port определяет, является ли порт назначения членом той же самой VLAN (т.е. содержит такой же VID), что и он сам. 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 Ingress Filtering и позволяет избежать перегрузки полосы пропускания Коммутатора. В результате пакеты, принадлежащие другой VLAN, отбрасываются еще до того, как достигнут порта назначения, давая возможность избежать передачи избыточного трафика.

VLAN по умолчанию

Изначально все порты Коммутатора добавлены в одну VLAN с VID=1. При настройке новых Port-Based VLAN (на основе портов), порты, входящие в данные VLAN, автоматически удаляются из VLAN по умолчанию.

Помните, что пакеты одной VLAN могут попасть в другую VLAN только через внешний маршрутизатор.

Примечание: Если на Коммутаторе не настроена ни одна VLAN, то все пакеты пересылаются на любой порт назначения. Пакеты с неизвестным адресом источника будут передаваться на все порты. Широковещательные и многоадресные пакеты также будут направляться на все порты.

Ниже приведён пример:

Имя VLAN	VID	Порты Коммутатора
System (по умолчанию)	1	5, 6, 7, 8, 21, 22, 23, 24
Технический отдел	2	9, 10, 11, 12
Маркетинг	3	13, 14, 15, 16
Финансовый отдел	4	17, 18, 19, 20
Отдел продаж	5	1, 2, 3, 4

Таблица 7- 1. Пример VLAN – назначение портов различным отделам

Сегментация VLAN

Возьмём для примера пакет, переданный устройством на порт 1 (Port 1), который является членом VLAN 2. Если адрес назначения пакета – другой порт (найден в обычной таблице пересылки), тогда Коммутатор определяет, является ли другой порт (Port 10) членом VLAN 2 (значит, может принимать пакеты VLAN 2). Если Port 10 не относится к VLAN 2, тогда пакет будет отброшен Коммутатором и не достигнет своего адреса назначения. Если Port 10 относится к VLAN 2, то пакет будет передан далее. Такое вборочное продвижение пакетов с учетом принадлежности к VLAN и является сегментацией. Т.е.Port 1 может передавать данные только на порты, принадлежащие VLAN2.

Однако иногда есть необходимость организовать совместный доступ к таким сетевым устройствам, как принтеры и серверы, из различных VLAN. При этом имеетместо наложение нескольких VLAN, т.е. некоторые порты будут принадлежать более, чем одной VLAN-группе. Например, в VLAN 1 добавлены порты 1, 2, 3, и 4; а в VLAN 2 – порты 1, 5, 6, и 7. При этом, порт

1 принадлежит сразу двум группам VLAN. Порты 8, 9, и 10 не принадлежат ни одной VLAN-группе. Это означает, что порты 8, 9, и 10 находятся в одной VLAN-группе.

VLAN и группы агрегированных каналов

Члены группы агрегированных каналов обладают общими настройками VLAN. Любые VLAN-настройки, выполненные для одних членов группы агрегированных каналов, автоматически будут распространены на остальные порты.

Статическая запись VLAN

В папке **L2 Features** откройте папку **VLAN** и кликните по ссылке **Static VLAN Entry**, после чего откроется следующее окно:

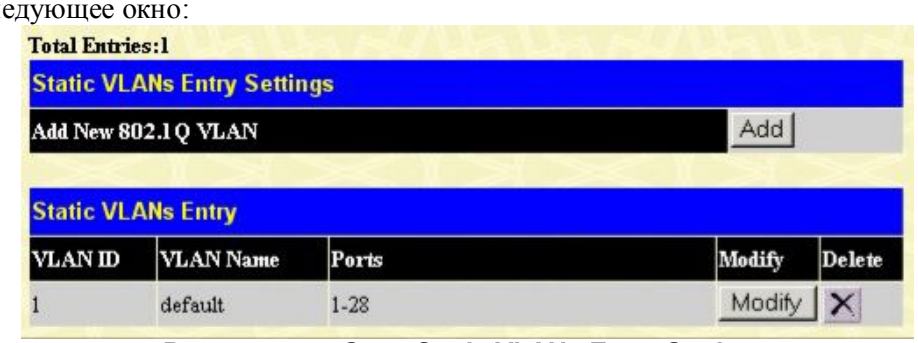


Рисунок 7- 4. Окно Static VLANs Entry Settings

Окно **802.1Q Static VLANs** показывает все сконфигурированные VLAN (имя и ID). Для удаления 802.1Q VLAN следует кликнуть по соответствующей кнопке *X* под надписью **Delete**.

Для создания новой 802.1Q VLAN необходимо в окне **802.1Q Static VLANs** кликнуть по кнопке **Add**. Появится новое окно, показанное ниже. Окно содержит опции, позволяющие задать настройки порта, а также присвоить уникальное имя и номер новой VLAN. Описание параметров представлено ниже в таблице:

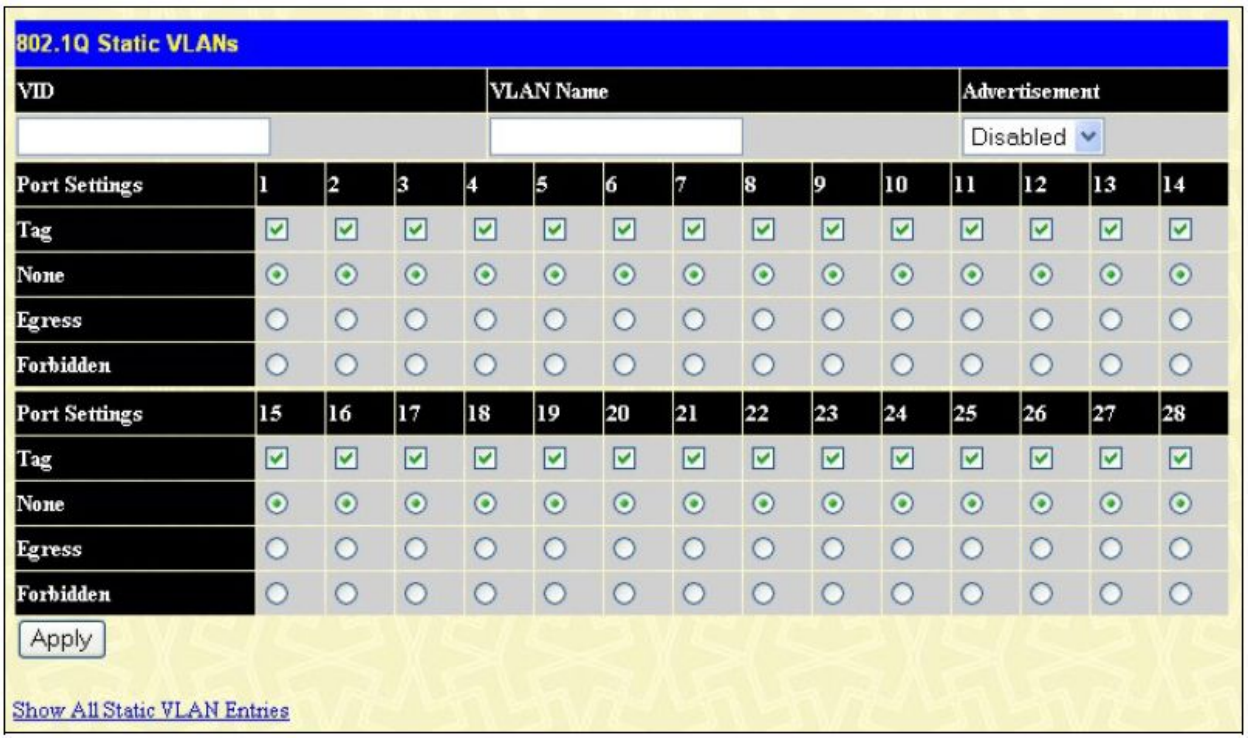


Рисунок 7- 5. Окно 802.1Q Static VLAN - добавить

Для возвращения в окно **Current 802.1Q Static VLAN Entry Settings** следует кликнуть по ссылке Show All Static VLAN Entries. Чтобы изменить уже существующую 802.1Q VLAN, необходимо кликнуть по соответствующей кнопке **Modify**. Появится новое меню для настроек порта и

назначения уникального имени и номера новой VLAN. Описание параметров представлено ниже в таблице.

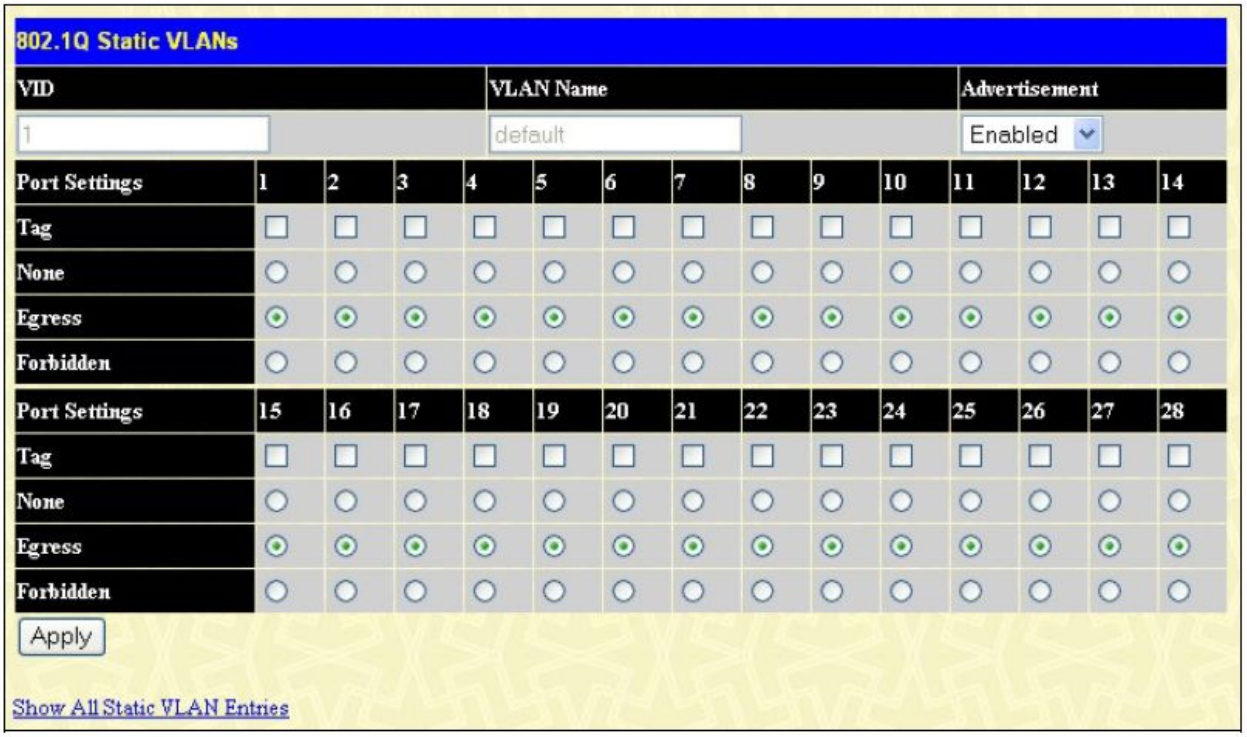


Рисунок 7- 6. Окно 802.1Q Static VLANs – изменить

Параметр	Описание
VID (VLAN ID)	Позволяет ввести VLAN ID в окне **Add** или отображает в окне **Modify** VLAN ID уже существующих VLAN. VLAN идентифицируются по имени или VID.
VLAN Name	Позволяет ввести имя новой VLAN в окне **Add** или редактировать имя VLAN в окне **Modify**.
Port Settings	Позволяет выбрать порты, которые будут являться членами VLAN.
Tag	Определяет порт как 802.1Q тегирующий или 802.1Q нетегирующий. Галочка в данном поле будет означать, что порт является тегирующим.
None	Позволяет задать порты, которые не являются членами VLAN
Egress	Используется для определения портов, являющихся статическими членами VLAN. Egress Port – это порты, которые передают трафик внутри VLAN. Эти порты могут быть как тегирующими, так и нетегирующими.

Для применения настроек следует кликнуть **Apply**. Кликните Show All Static VLAN Entries для возврата к окну **802.1Q Static VLANs**.

Настройки GVRP

В меню **L2 Features** откройте папку **VLAN** и кликните по **GVRP Settings**. Окно **GVRP Settings**, показанное ниже, позволяет определять, будет ли Коммутатор передавать другим коммутаторам с включенной функцией GARP VLAN Registration Protocol (GVRP) информацию по настройкам VLAN. Также может использоваться опция **Ingress Checking** для ограничения трафика путём фильтрации входящих пакетов, PVID которых не совпадает с PVID порта. Ниже приведено описание основных параметров, представленное в виде таблицы:

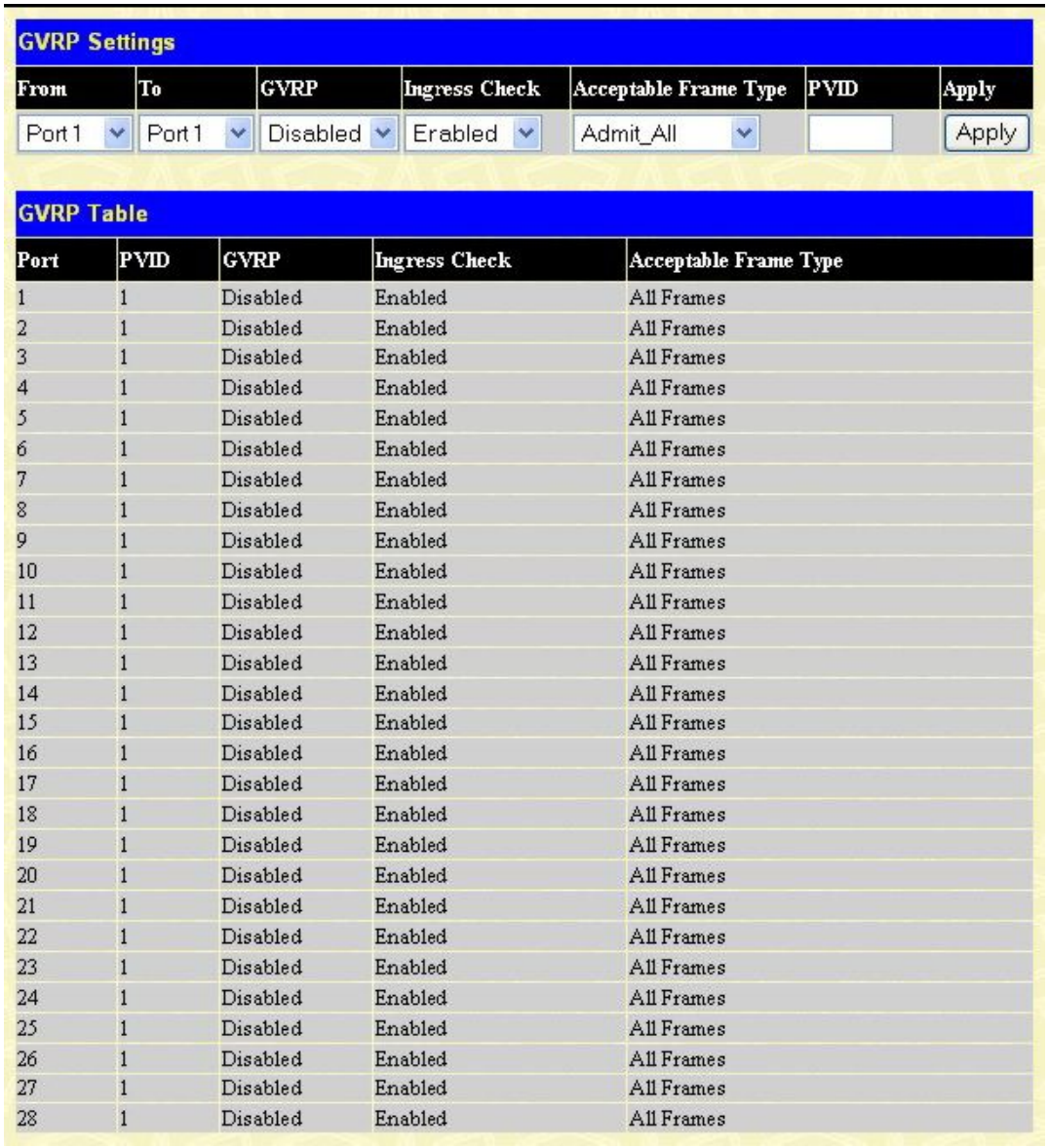


Рисунок 7- 7. Окно GVRP Settings

Можно настроить следующие параметры:

Параметр	Описание
From/To	Эти два поля позволяют указать диапазон портов, которые будут включены в VLAN на основе портов. Настройки VLAN задаются в окне **802.1Q Port Settings.**
GVRP	Включение опции Group VLAN Registration Protocol (GVRP) динамически позволяет порту динамически становиться членом VLAN. По умолчанию эта опция отключена.
Ingress Check	Данное поле может принимать значения Enabled (включено) и Disabled (выключено). При включении данной опции порт будет сравнивать VID пришедшего пакета с PVID порта. Если они различны, то порт отбросит пакет. Значение Disabled (выключено) позволяет выключить ingress-фильтр. По умолчанию, эта опция отключена.
PVID	Данное поле доступно только для чтения и отображает текущие настройки PVID для каждого порта, который вручную назначается VLAN при ее создании в таблице **802.1Q Port Settings**. По умолчанию все порты Коммутатора добавлены в VLAN по умолчанию с VID=1. PVID используется для тегирования исходящих пакетов, а также фильтрации входящих пакетов. Если порт настроен как тегирующий, то когда на него поступают нетегированные пакеты, порт добавит тег 802.1Q, используя PVID. Когда

	пакет достигает пункта его назначения, принимающее устройство будет использовать PVID для принятия решения о дальнейшем продвижении пакета. Если порт, на котором включена опция Ingress Filtering принимает пакет, то происходит сравнение VID пришедшего пакета с PVID порта. Если они не равны, то пакет будет отброшен. В противном случае пакет будет принят.
Acceptable Frame Type	Это поле означает типы фреймов, которые будут приниматься портом. Пользователь может выбрать либо *Tagged Only*, что означает, что будут приниматься только тегированные фреймы VLAN, либо *Admit_All*, что означает, что будут приниматься и тегированные, и нетегированные фреймы. По умолчанию выбрано значение *Admit_All.*

Для применения настроек следует кликнуть по **Apply**.

Агрегирование каналов
Понятие группы агрегированных каналов

Группа агрегированных каналов связи (Port trunk groups) используется для объединения портов в одну высокоскоростную магистраль. Коммутатор поддерживает до шести групп агрегированных каналов связи с количеством портов от 2 до 8 на группу. Таким образом, может быть достигнута потенциальная скорость передачи 800Мбит/с

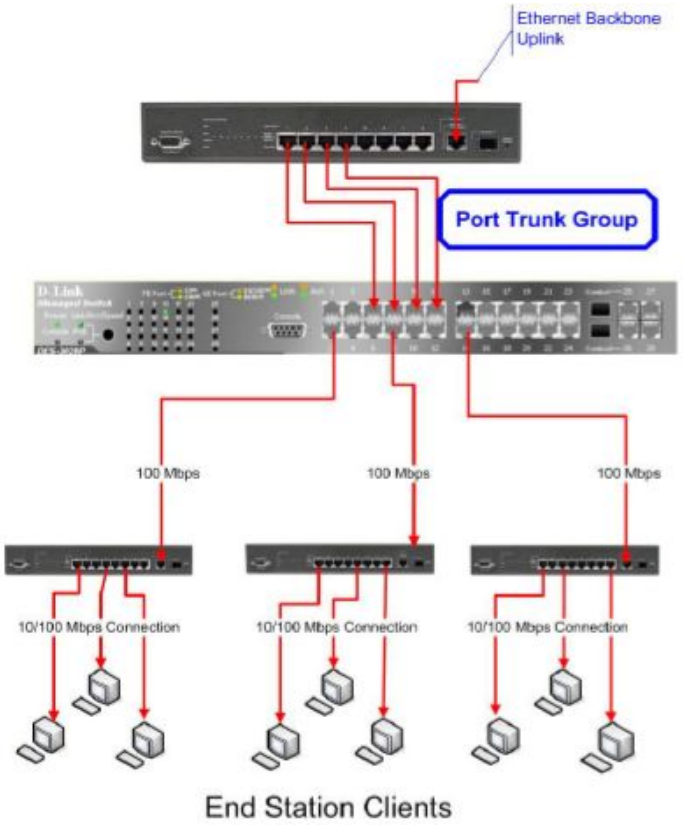


Рисунок 7-8. Пример группы агрегированных каналов связи

Коммутатор воспринимает все порты в группе агрегированных каналов связи как один порт. При этом данные, отправленные на конкретный хост (адрес назначения), отправляются на нужный порт в группе агрегированных каналов связи.

Примечание: Если какой-либо порт в группе агрегированных каналов связи будет выключен, данные, поступающие на этот порт, будут распределены по другим портам группы.

Объединение портов в группу позволяет использовать их как одну линию. При этом полоса пропускания группы агрегированных каналов равняется сумме полос пропускания отдельно взятых каналов. Это позволяет существенно увеличить полосу пропускания.
Такой прием агрегирования каналов обычно используется для подключения сетевых устройств, требующих высокой полосы пропускания, например сервера или магистрали сети.
Коммутатор позволяет создавать до шести групп агрегированных каналов, каждая из которых включает в себя количество портов от 2 до 8. Арегировать можно только те порты, номера которых образуют непрерывный диапазон. Два гигабитных порта коммутатора агрегировать нельзя: они могут использоваться только в качестве отдельного канала. Все порты группы должны быть членами одной и той же VLAN, их STP-статусы, статическая таблица многоадресной рассылки, статус управления трафика; сегментация трафика и параметры 802.1p должны быть одинаковы. Не допускается включение функций блокировки порта, зеркалирования порта и 802.1X для портов, входящих в группу агрегированных каналов. Помимо этого все порты, входящие в группу агрегированных каналов, должны поддерживать одинаковую скорость и работать в режиме полный дуплекс.

Master Port (главный порт) группы настраивается пользователем, и все параметры настройки, включая настройки VLAN, применяемые для Master Port, будут применяться для всех портов группы агрегированных каналов.
Между портами в группе агрегированных каналов автоматически производится распределение нагрузки, и выход из строя одного из портов группы приведет к перенаправлению трафика на оставшиеся порты группы.
На уровне коммутатора Spanning Tree Protocol (протокол покрывающего дерева) будет воспринимать группу агрегированных каналов как единый канал. На уровне портов STP будет использовать параметры главного порта при вычислении стоимости порта и определения состояния агрегированного канала связи. Во избежание образования петель, STP заблокирует как группу агрегированных каналов, так и единичный порт, который является избыточной связью.

Агрегирование каналов

Чтобы настроить группу агрегированных каналов, кликните по ссылке **Link Aggregation** в папке **Trunking** под заголовком **L2 Features.** В результате появится следующее окно для настройки:

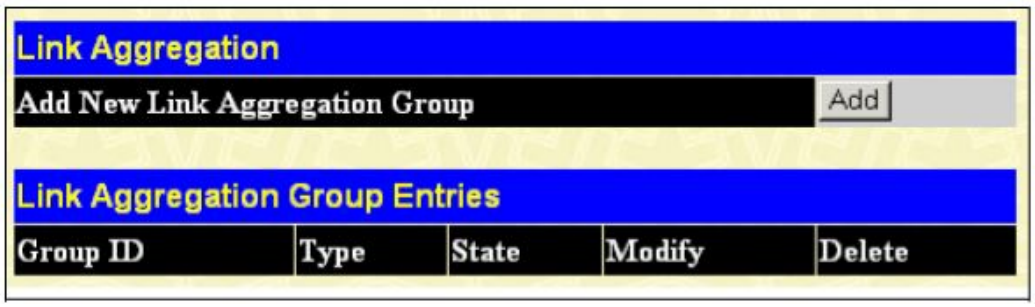


Рисунок 7-9. Окно Link Aggregation

Для настройки группы агрегированных каналов связи следует кликнуть по кнопке **Add**, чтобы добавить новую группу. Окно **Link Aggregation Settings** (показано ниже) используется для настройки групп. Чтобы изменить настройки группы, надо кликнуть по кнопке **Modify**, относящейся к соответствующей группе. Чтобы удалить группу, необходимо кликнуть по значку **X** под надписью **Delete**, относящейся к соответсвующей группе.

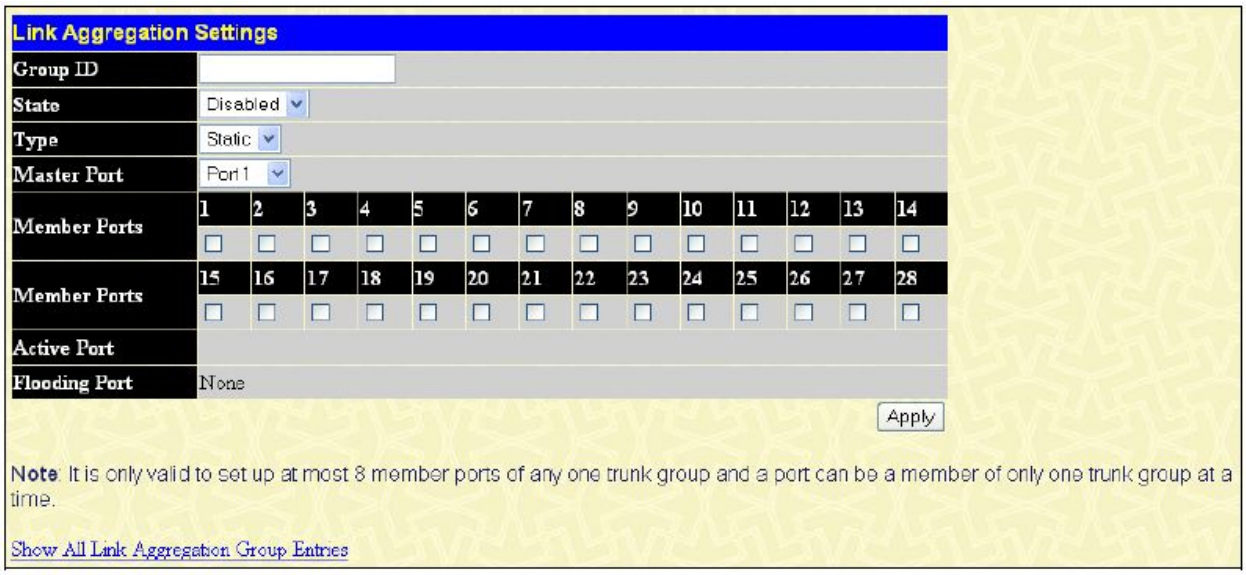


Рисунок 7-10. Окно Link Aggregation Settings - добавление

Настройки портов LACP

Для настройки агрегирования портов в соответствии с протоколом Link Aggregation Control Protocol(LACP) кликните **L2 Features > Trunking > LACP Port Settings,** после чего появится следующее окно:

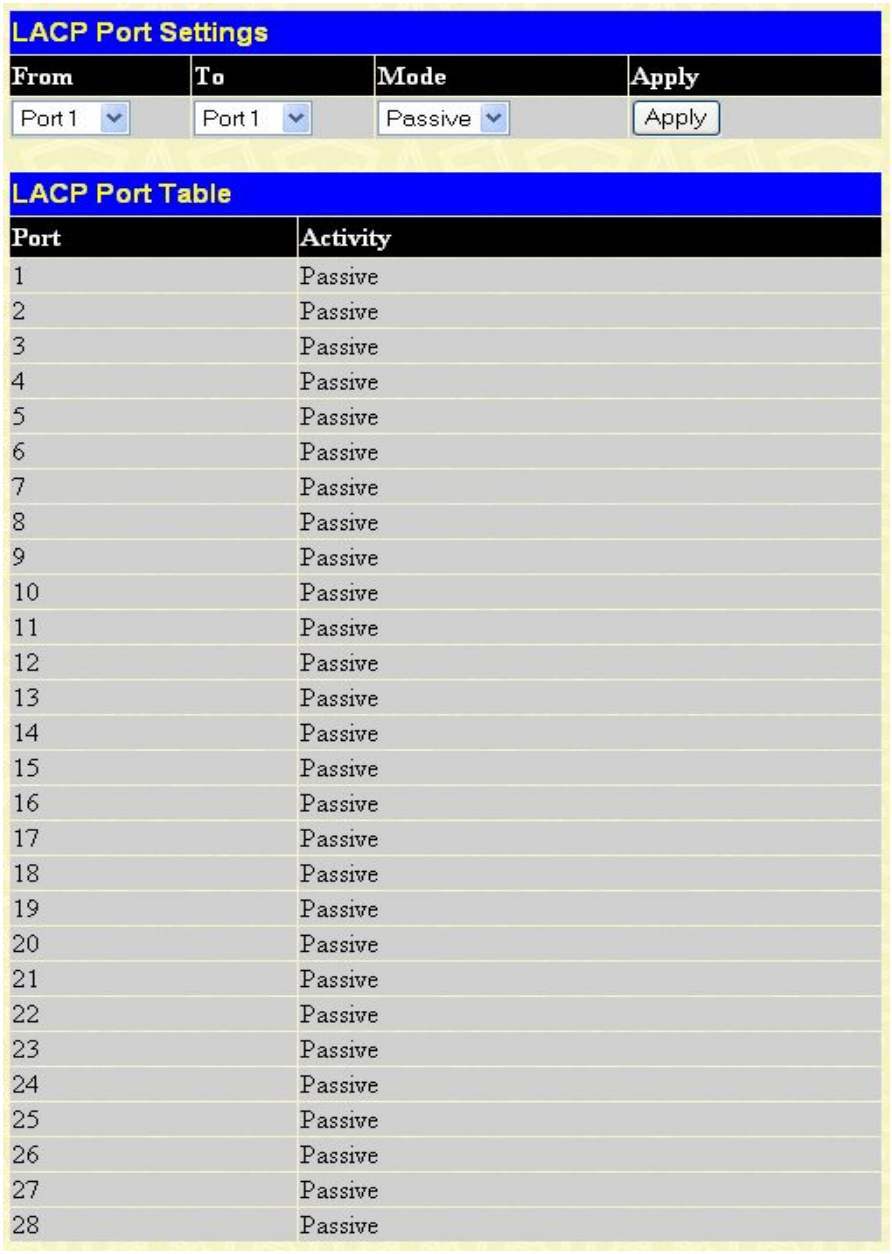


Рисунок 7- 11. Окно LACP Port Settings

Чтобы задать настройки группы агрегированных каналов LACP, выберите диапазон портов с помощью выпадающих меню **From** и **To**, укажите нужный режим в поле **Mode** (Passive или Active), а затем кликните по **Apply** для принятия изменений.

IGMP

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, к которому подключено определённое устройство, на основе сообщений IGMP, проходящих через Коммутатор.

Чтобы использовать IGMP Snooping, необходимо сначала определить это глобально в настройках Коммутатора (см. раздел **Расширенные настройки**). Затем можно сделать тонкую настройку для каждой VLAN, нажав на ссылку **IGMP Snooping** в папке **L2 Features**. Когда IGMP snopping включён, коммутатор может открыть или закрыть порт для определённого члена группы многоадресной 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** используется для просмотра настроек IGMP Snooping. Для изменения настроек надо кликнуть по кнопке **Modify,** соответствующей определенному VLAN ID.

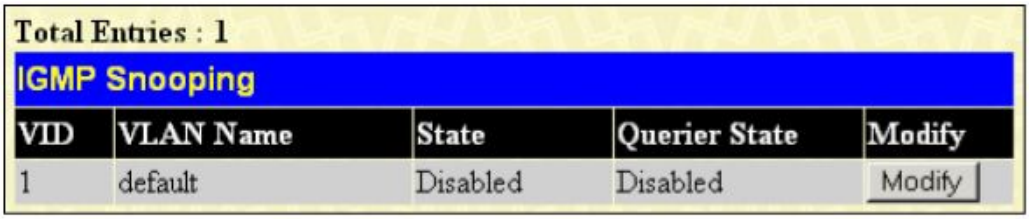


Рисунок 7- 12. Окно IGMP Snooping

После клика по кнопке **Modify** откроется окно **IGMP Snooping Settings**, представленное ниже:

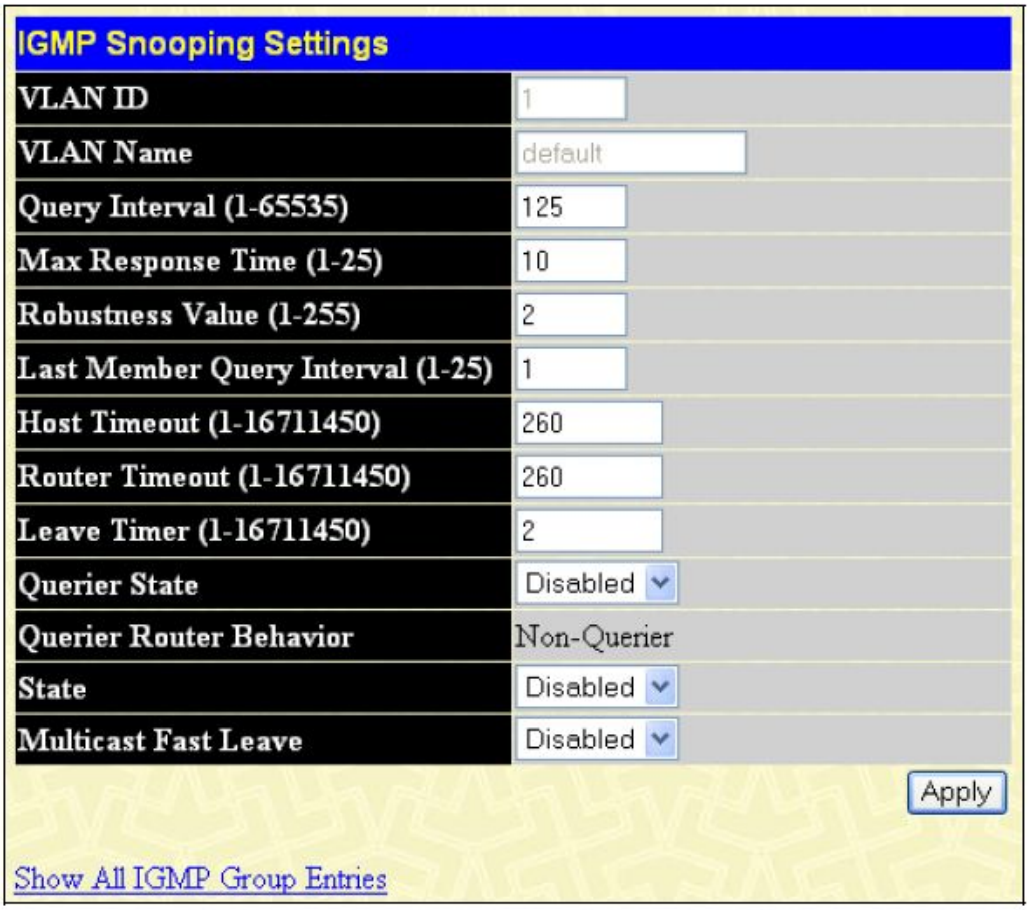


Рисунок 7- 13. Окно IGMP Snooping Settings

Следующие параметры доступны для просмотра и изменения.

Параметр	Описание
VLAN ID	Идентификатор VLAN, который наряду с именем VLAN, определяет ту VLAN, для которой пользователь желает изменить настройки IGMP snooping.
VLAN Name	Имя VLAN, которое наряду с ID VLAN, определяет VLAN, для которой пользователь желает изменить настройки IGMP snooping.
Query Interval	Данное поле используется для задания временного интервала (в секундах) между IGMP-запросами. Возможны значения от 1 до 65535. Значение по умолчанию 125.
Max Response Time	Задаёт максимальное время до посылки IGMP-ответа. Возможны значения от 1 до 25 (в секундах). Значение по умолчанию 10.

Robustness Variable	Эта переменная используется при предполагаемой потере пакетов. Если потеря пакетов на VLAN, как ожидается, будет высокой, значение Robustness Variable должно быть увеличено, чтобы покрыть увеличенную потерю пакетов. Возможны значения от 1 до 255. Значение по умолчанию 2.
Last Member Query Interval	Это поле указывает максимальный промежуток времени между отправкой групповых сообщений-запросов, включая те, которые были отправлены в ответ на запрос о выходе из группы. Значение по умолчанию =1
Host Timeout	Это максимальное количество времени в секундах, в течение которого сетевому узлу разрешается оставаться членом многоадресной группы без отправки коммутатору запроса о вступлении в группу. Значение по умолчанию = *260*.
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 по истечении этого времени не был получен ответ, хост будет исключен из группы многоадресной рассылки.
Querier State	Значение *Enabled* – для включения IGMP-запросов, *Disabled* – для отключения. Значение по умолчанию – *Disabled*.
Querier Router Behavior	Это поле, доступное только для чтения, описывает поведение маршрутизатора при отправке пакетов запроса. Выбор значения *Querier* означает, что маршрутизатор будет отправлять пакеты запроса IGMP. При этом выбр значения *Non-Querier* будет означать, что маршрутизатор не будет отправлять пакеты запроса IGMP. Это поле доступно только для чтения *(Querier)* в случае, когда поля **Querier State** и **State** установлены в значение Enabled.
State	Значение *Enabled* – для применения IGMP snopping. Значение по умолчанию – *Disabled.*
Fast Leave	Это поле позволяет пользователю включить функцию *Fast Leave*. При включении данной функции члены группы многоадресной рассылки смогут покинуть группу многоадресной рассылки незамедлительно (до истечения времени Last Member Query Timer) по получении Коммутатором пакета IGMP Leave Report Packet. По умолчанию установлено значение *Disabled*.

Необходимо кликнуть по **Apply** для применения настроек. Для возврата в окно **IGMP Snooping** кликните по ссылке Show All IGMP Group Entries.

Примечание: Функция Fast Leave адресована пользователям IGMPv2, желающим покинуть группу многоадресной рассылки. Наилучшим образом эта функция реализуется в VLAN, в которых к каждому порту подключен только один хост. Когда один хост в группе использует функцию Fast Leave, то это может привести к выборочному применению fast leave и на других хостах в группе.

Создание записи о статических портах маршрутизатора

Статический порт маршрутизатора – это порт, к которому прикреплён 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 коммутатора 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.

Откройте папку **IGMP Snooping** и кликните по ссылке **Static Router Ports Settings,** после чего откроется окно **Static Router Port Settings**, показанное ниже.

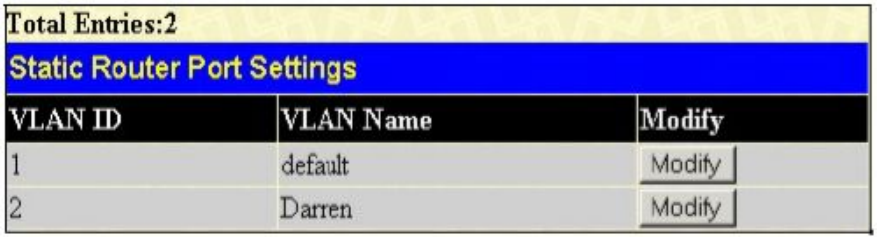


Рисунок 7- 14. Окно Current Static Router Port Entries

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

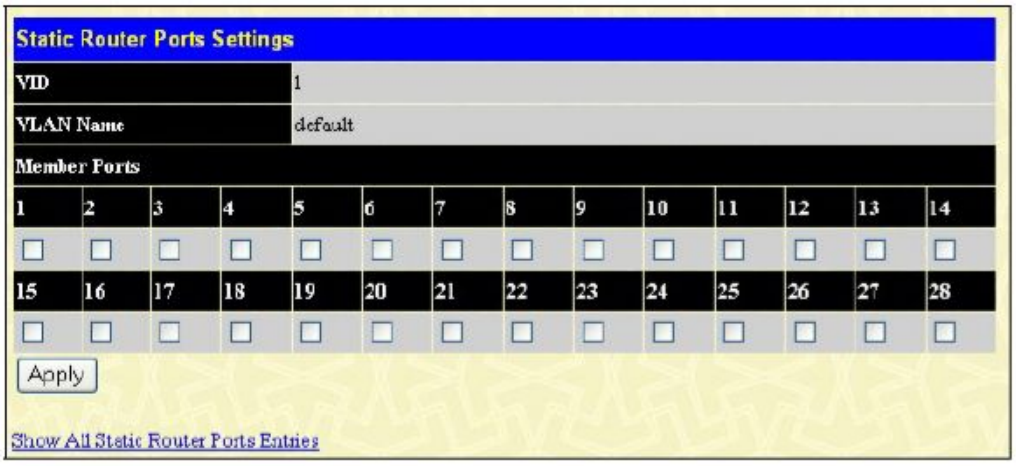


Рисунок 7- 15. Окно Static Router Ports Settings

Могут быть установлены следующие параметры:

Параметр	Описание
VID (VLAN ID)	Это идентификатор (ID) VLAN, наряду с именем VLAN, определяющий VLAN, к которой прикреплён маршрутизатор многоадресной рассылки.
VLAN Name	Это имя VLAN, к которой прикреплён 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**, необходимо кликнуть по ссылке Show All Static Router Port Entries.

Алгоритм покрывающего дерева

Коммутатор поддерживает две версии протокола покрывающего дерева (Spanning Tree): 802.1d STP, 802.1w Rapid STP. Протокол 802.1d STP появился довольно давно и знаком большинству сетевых профессионалов. Ниже представлено краткое введение в технологию и настройку протоколов 802.1d STP, 802.1w Rapid STP и 802.1s MSTP. Поскольку поддержка протокола 802.1w RSTP была добавлена относительно недавно в управляемые коммутаторы Ethernet D-Link, ниже приведено его краткое описание, а затем дано описание, как настроить 802.1d STP и 802.1w RSTP на Коммутаторе.

802.1w Rapid Spanning Tree

В Коммутаторе используются две версии протокола Spaning Tree: Rapid Spanning Tree Protocol (RSTP), определённый как IEEE 802.1w, и версия, совместимая с IEEE 802.1d STP. Протокол RSTP совместим с протоколом IEEE 802.1d, однако, при этом будут потеряны преимущества, предоставляемые протоколом RSTP.

IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) является логическим развитием протокола 802.1d STP. Протокол RSTP был разработан для преодоления некоторых ограничений, присущих протоколу STP и не позволяющих реализовать ряд функций (например, функции 3-го уровня, которые всё чаще и чаще поддерживаются коммутаторами Ethernet). Концепция протокола RSTP аналогична концепции STP, поэтому и терминология, используемая для описания этих протоколов, а также основные функции и настройки будут совпадать. Данная глава знакомит с некоторыми новшествами в STP и показывает основные различия между двумя протоколами.

Изменение состояния портов

Основные различия между двумя протоколами состоят в способе перехода портов в состояние продвижения пакетов и механизме такого перехода, относящегося к функции порта в топологии (продвижение пакетов или обратное состояние). Протокол RSTP использует состояние Discarding (отказ, отвергающий статус пересылки пакетов), в отличие от протокола 802.1d, поодерживающего три статуса отказа продвижения пакетов (отключение, блокировка, прослушивание). Хотя в STP используется три сотояния порта для отказа от пересылки пакетов, а в RSTP/MSTP для этих целей используется только статус Discarding, особых функциональных различий это не несет, поскольку порт все равно остаётся неактивным в сетевой топологии. В Таблице 7-2 показано сравнение изменения состояния портов для двух протоколов.

Все два протокола используют один и тот же механизм для вычисления топологии сети. Каждый сегмент поддерживает единственный маршрут к корневому мосту. Все мосты прослушивают BPDU-пакеты, которые отправляются с каждым Hello-пакетом. BPDU-пакеты посылаются даже в том случае, если BPDU-пакет не был принят. Состояние канала между мостами зависит от статуса портов. В конечном счете, это приводит к более быстрому обнаружению ошибок в линии и соответсвенно более быстрому изменению топологии. Недостатком 802.1d является отсутствие непосредственной обратной связи между смежными мостами.

802.1w RSTP	802.1d STP	Пересылка	Изучение
Отказ (Discarding)	Отключен (Disabled)	Нет	Нет
Отказ (Discarding)	Блокировка (Blocking)	Нет	Нет
Отказ (Discarding)	Прослушивание	Нет	Нет

	(Listening)		
Изучение (Learning)	Изучение (Learning)	Нет	Да
Продвижение пакетов (Forwarding)	Продвижение пакетов (Forwarding)	Да	Да

Таблица 7-2. Сравнение статусов портов

RSTP способен к более быстрому переходу к статусу продвижения пакетов, поскольку он не зависит от настроек таймера, а RSTP-мосты чувствительны к обратной связи от смежных RSTP-мостов. Порту теперь нет необходимости ожидать, пока топология стабилизируется, для перехода в статус продвижения пакетов. Для описания такого быстрого перехода, данный протокол вводит два новых понятия: edge port (пограничный порт) и point-to-point (P2P) порт.

Пограничный порт

Пограничный порт (Edge port) – это такой порт, который напрямую соединяется с сегментом сети, где создание петли является невозможным. Примером пограничного порта может служить порт, напрямую соединяемый с рабочей станцией. Порты, которые сконфигурированы как пограничные, переходят в состояние продвижения пакетов немедленно, минуя состояния прослушивания и изучения. Пограничный порт теряет свой статус сразу же, как только он принял BPDU-пакет, становясь при этом обычным портом spanning tree.

P2P-порт

P2P-порт также обеспечивает быстрый переход в режим продвижения пакетов. P2P-порт используется для соединения с другими мостами. При использовании протоколов RSTP все порты, работающие в дуплексном режиме, являются P2P-портами, если обратное не было задано вручную.

Совместимость 802.1d и 802.1w

RSTP позволяет работать с оборудованием, поддерживающим STP 802.1d, автоматически переводя BPDU-пакеты в формат 802.1d. Однако при использовании сегментов сети 802.1d STP на этих участках становится невозможным использование преимуществ RSTP, способного к быстрой передаче и настройке топологии.

Spanning Tree Protocol (STP) позволяет производить настройки на двух уровнях:

1. **На уровне коммутатора** – настройки будут применяться глобально.
2. **На уровне портов** - настройки будут применяться только к определенной пользователем группе портов.

Функция STP Loopback Detection

При подключении к другим коммутаторам настройки STP играют существенную роль в продавижении пакетов на порты и могут существенно улучшить пропускную способность коммутатора. Хотя иногда эта функция может необоснованно определять петли для пакетов STP BPDU, как, например, BPDU-пакеты возвращающиеся обратно от неуправляемых коммутаторов, подключенных к Коммутатору.

Когда функция обнаружения петель STP включена, Коммутатор защищен от возникновения петель между коммутаторами. Когда BPDU-пакет вернется на Коммутатор, эта функция онаружит данное событие и переведет принимающий порт в состояние отключения из-за ошибки. Далее сообщение будет перемещено в журнал Коммутатора с сообщением вида “BPDU Loopback on Port #”.

Настройка таймера Loopback

Таймер Loopback играет ключевую роль на следующем шагу решения коммутатором проблемы. Выбор любого отличного от нуля значения таймера включит механизм автообнаружения. Когда таймер истекает, коммутатор снова будет проверять, по-прежнему ли пакеты BPDU возвращаются на этот порт. Если нет, коммутатор восстановит порт как Designated Port в состояние Discarding. Если BPDU-пакеты по-прежнему возвращаются, порт останется в заблокированном состоянии, таймер будет в сброшен в заданное значение, и процесс начнется заново.

Чтобы отказаться от использования этой функции, необходимо установить значение времени Loopback Recovery в значение 0. В этом случае когда BPDU-пакет возвращается на Коммутатор, порт перейдет в состояние блокировки и будет отправлено сообщение в журнал Коммутатора. Чтобы восстановить порт, администратору необходимо выключить проблемный порт и включить его снова. Это единственный способ восстановления порта, когда параметр Loopback Recover Time установлен в значение 0.

Правила и ограничения функции Loopback Detection

- Все версии STP (STP, RSTP) поддерживают данную функцию.
- Loopback Detection может быть настроена глобально (STP Global Bridge Settings).
- Соседние коммутаторы должны поддерживать продвижение BPDU-пакетов. В противном случае данная функция будет отключена на соответствующем порту Коммутатора.
- По умолчанию функция Loopback Detection выключена на Коммутаторе.
- По умолчанию установлен таймер Loopback - 60 секунд.
- Эта настройка будет действовать только в том случае, если на интерфейсе включено STP.

Функция Loopback Detection может предотвратить петли BPDU только на назначенных портах Коммутатора. Она позволяет обнаружить петли на стороне пользователя, подключенного к пограничному порту, но не может обнаружить условия возникновения петли на выбранном корневом порту STP другого коммутатора.

Глобальные настройки STP-моста

Для работы со следующим окном откройте папку **Spanning Tree** в меню **L2 Features** и кликните по ссылке **STP Bridge Global Settings**.

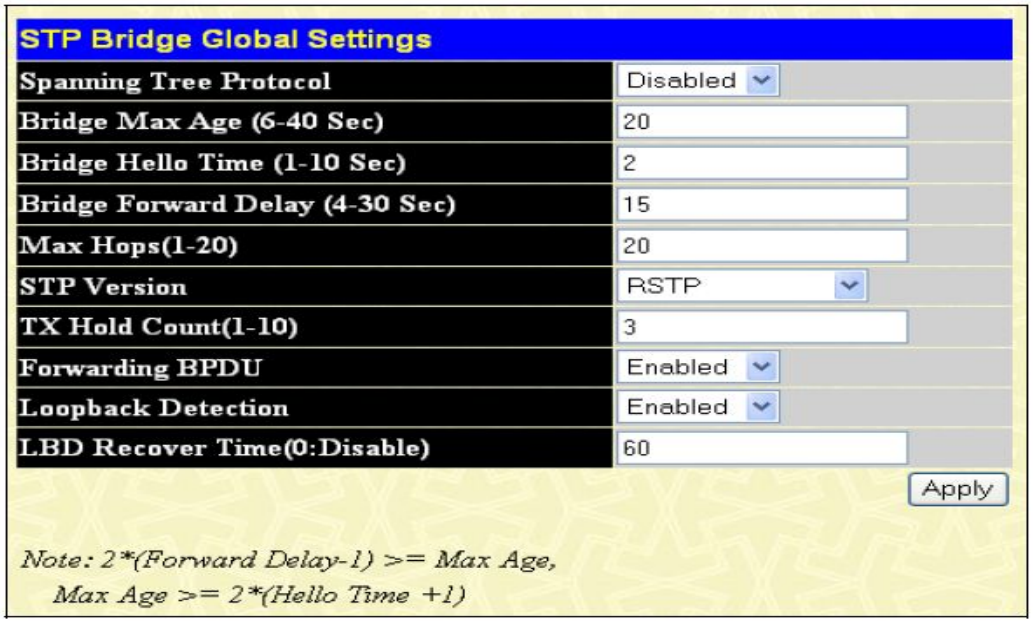


Рисунок 7- 16. Окно STP Bridge Global Settings

Можно установить следующие параметры:

Параметр	Описание
Spanning Tree Protocol	В выпадающем меню можно включить/выключить функцию STP на коммутаторе. Значение по умолчанию *Disabled* (выключено).
Bridge Max Age (6-40 сек)	Задание интервала Max Age позволяет избежать ситуации, когда устаревшая информация бесконечно блуждает по сети, мешая продвижению новой. Этот временной интервал устанавливается корневым мостом и определяет максимальное время ожидания Коммутатором BPDU-пакета от корневого моста. Если по истечении данного времени, BPDU-пакет от корневого моста так и не был получен, Коммутатор стартует свою собственную рассылку BPDU-пакетов к другим коммутаторам с тем, чтобы получить роль корневого моста. Коммутатор станет корневым мостом в том случае, если у него наименьшее значение идентификатора Bridge Identifier, по сравнению с другими коммутаторами в сети. 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 2 секунд. Этот параметр задает интервал между двумя передачами корневым коммутатором BPDU-пакетов для оповещения других коммутаторов о себе.
Bridge Forward Delay (4-30 Сек)	Данный параметр может принимать значения от 4 до 30 секунд. Это время, которое порт коммутатора находится в состоянии прослушивания при переходе от состояния блокировки к состоянию продвижения пакетов.
Max Hops (1-20)	Данный параметр задает максимальное количество шагов (хопов) между устройствами, принадлежащими одной области покрывающего дерева, при достижении которого BPDU-пакет, отправленный Коммутатором, будет считаться устаревшим. Каждый коммутатор будет уменьшать значение данного счётчика на единицу, пока этот счетчик не примет значение, равное нулю. Затем Коммутатор отбросит BPDU-пакет. Пользователь может установить значение данного счётчика от 1 до 20. Значение по умолчанию - 20.
STP Version	Выпадающее меню позволяет выбрать версию STP, которая будет использоваться. Возможны следующие значения: *STP* - Spanning Tree Protocol (STP) *RSTP* - Rapid Spanning Tree Protocol (RSTP)
TX Hold Count (1-10)	Используется для установки максимального количества Hello-пакетов, передаваемых за определенный интервал. Можно установить значение от 1 до 10. Значение по умолчанию 3.
Forwarding BPDU	Это поле может принимать значения *Enabled*(включено) или *Disabled* (выключено). Включение данного параметра позволяет пересылку STP BPDU-пакетов от других сетевых устройств. Значение по умолчанию - *Enabled*.
Loopback Detection	Эта функция позволяет временно отключить порт коммутатора, когда BPDU-пакет возвращается обратно на Коммутатор. Когда Коммутатор обнаруживает собственный BPDU-пакет, вернувшийся обратно, он определяет петлю в сети. STP автоматически блокируется, и администратору отправляется уведомление. Порт LBD STP будет восстановлен (изменен в состояние discarding) по истечении **LBD Recover Time**. Фнкция Loopback Detection будет применяться только на одном порту. С помощью выпадающего меню можно включить или выключить данную функцию. Значение по умолчанию – Enabled (включено).
LBD Recover Time (0:disable)	Это поле устанавливает время, которое STP-порт будет ожидать до восстановления состояния STP. 0 будет означать, что LBD не презапустится, пока администратор специально не изменит это. Доступны значения от *60* до *1000000* секунд. Значение по умолчанию *60* секунд.

Для применения настроек следует кликнуть по **Apply**.

Примечание: Временной интервал Hello Time не может быть больше, чем Max. Age. В противном случае возникнет ошибка конфигурации. Устанавливая данные параметры, следует придерживаться указанных ниже формул:
Max. Age ≤ 2 x (Forward Delay - 1 c)
Max. Age ≥ 2 x (Hello Time + 1 c)

Настройки STP на основе портов

Настройки STP могут быть установлены на основе портов. Чтобы просмотреть настройки порта STP, необходимо кликнуть **L2 Features > Spanning Tree > STP Port Settings**.

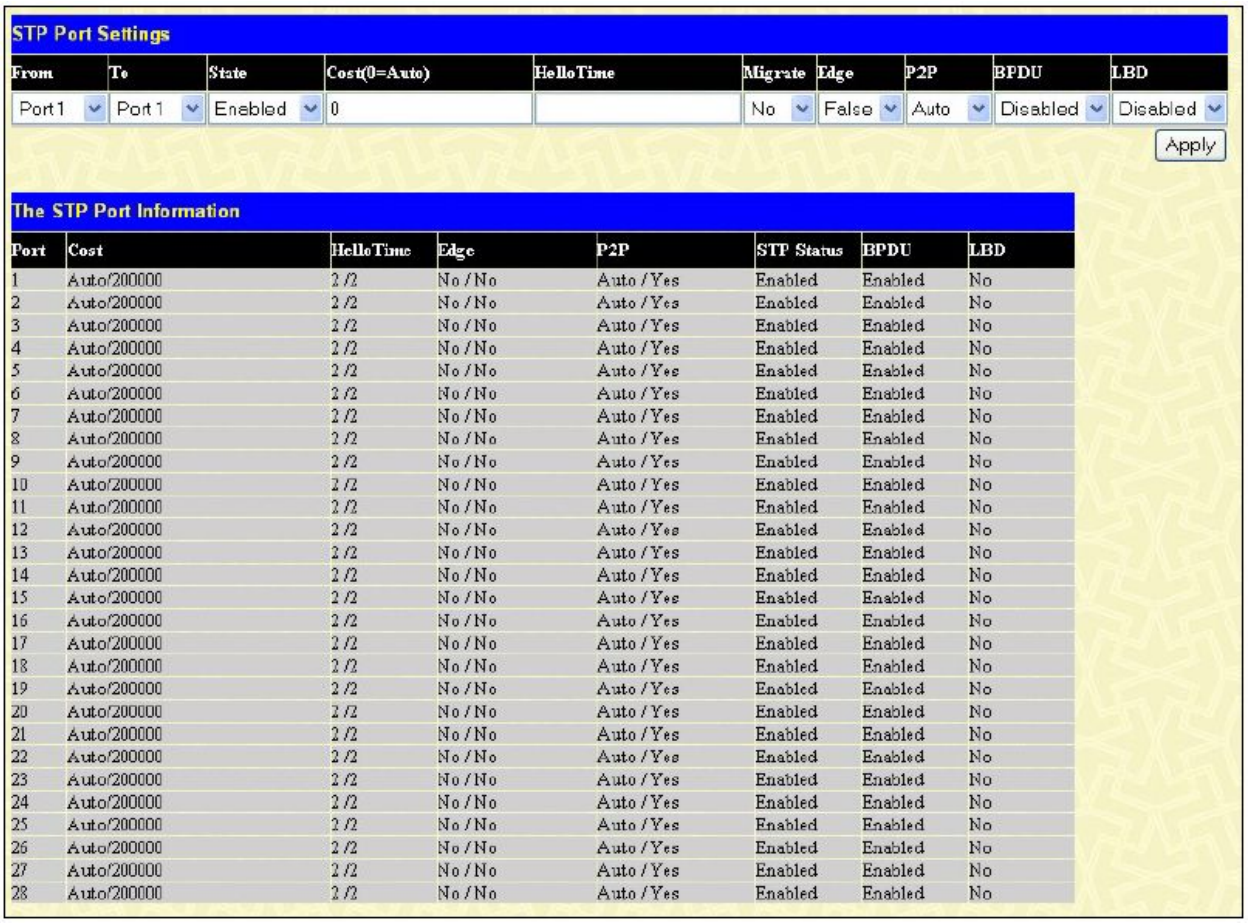


Рисунок 7- 17. Окно STP Port Settings

Помимо настройки параметров покрывающего дерева для использования на уровне коммутатора, Коммутатор позволяет настроить группы портов. При этом, каждая группа портов будет иметь свое собственное дерево с индивидуальными настройками конфигурации. Группа STP будет использовать параметры уровня коммутатора, введенные выше, а также Port Priority и Port Cost. Группа STP spanning tree работает тем же образом, что и spanning tree уровня коммутатора, просто концепция корневого моста меняется на корневой порт. Корневой порт – это порт группы, который выбирается на основе приоритетов портов и стоимости портов, для организации подключения в группе. Резервные каналы будут заблокированы точно так же, как и для покрывающего дерева уровня коммутатора. STP на уровне коммутатора блокирует резервные каналы между коммутаторами (и аналогичными сетевыми устройствами). STP на уровне портов будет блокировать резервные связи внутри STP-группы.

Рекомендуется создавать группу STP в соответствие с группой портов VLAN.

Для настройки STP на основе портов доступны следующие поля:

Параметр	Описание
From/To	Данные выпадающие меню позволяют выбрать последовательный диапазон портов для настройки.
State	Можно включить (опция Enabled) или выключить (опция Disabled) продвижение пакетов BPDU.
Cost (0 = Auto)	Данное поле определяет относительную стоимость продвижения пакетов на определенный список портов. Стоимость порта может быть установлена автоматически или может быть задано значение. По умолчанию установлено *0* (auto). *0 (auto)* - Настройка *0* для внешнего маршрута будет автоматически устанавливать скорость продвижения пакетов для заданных портов в списке для оптимальной эффективности. Стоимость порта по умолчанию: для порта 100Мбит/с = *200000,* для порта Gigabit Ethernet = *20000*. *value 1-200000000* – значение от *1* до *200000000* определяет внешнюю стоимость маршрута. Чем меньше значение, тем выше вероятность, что данный порт будет выбран для продвижения пакетов.
Hello Time	Временной интервал между передачами конфигурационных сообщений назначенным портом на другие устройства в bridged LAN. Допустимые значения лежат в интервале от *1* до *10* секунд. Значение по умолчанию равно 2 секунды. Это поле может быть изменено только в том случае, если коммутатор настроен для MSTP.
Migrate	При работе в режиме RSTP выбор yes означает, что выбранный порт будет работать RSTP BPDUs.
Edge	Выбор значения *True* в данном поле означает, что данный порт будет пограничным портом. Пограничные порты не могут создавать петли, однако пограничный порт может потерять свой статус, если при изменении топологии сети появляется возможность для образования петель. Пограничный порт обычно не получает BPDU-пакеты. Если получен пакет BPDU, то этот порт автоматически утратит статс пограничного порта. Выбор параметра *False* означает, что порт не будет иметь статус пограничного.
P2P	Выбор параметра *True* означает общий канал point-to-point (P2P). Порты P2P схожи с пограничными портами, однако у P2P-порта есть одно ограничение: необходимость работать в режиме полного дуплекса. Как и пограничные порты, порты P2P быстро переходят в состояние продвижения пакетов, как преимущество RSTP. Значение *False* в этом поле указывает, что данный порт не может иметь статус p2p. Выбор параметра *Auto* означает, что статус порта будет выбираться автоматически. Всегда, когда это возможно, будет использоваться статус p2p. Если же порт не поддерживает статус p2p (например, порт может работать только в ержиме полудуплекса), то статус p2p будет выключен *(false)*. Значение по умолчанию равно *true*.
State	Это выпадающее меню позволяет включить или выключить STP дя выбранной группы портов. Значение по умолчанию равно *Enabled*.
BPDU	Это поле может принимать значения Enabled (включено) или Disabled (выключено). При использовании опции Enabled, будет разрешено продвижение пакетов STP BPDU с других сетевых устройств. Значение по умолчанию Enabled.
LBD	Данное выпадающее меню позволяет включить (опция Enabled) или выключить (опция Disabled) функцию обнаружения петель (loop-back detection) на указанных портах. Более подробная информация по данной функции приведена в соответствующем разделе руководства.

Кликните по **Apply** для применения выполненных изменений.

Идентификация конфигурации MST

Следующие опции в окне **MST Configuration Identification** позволяют пользователю настроить копию MSTI на Коммутаторе. Эти настройки будут уникально идентифицировать копии spanning tree, установленные на Коммутаторе. Изначально Коммутатор обладает деревом *CIST* (Common Internal Spanning Tree), практически все параметры которого пользователь может изменить, за исключением только MSTI ID. Удалить CIST также нельзя. Для того чтобы открыть окно **MST Configuration Identification**, кликните **L2 Features > Spanning Tree > MST Configuration Identification:**

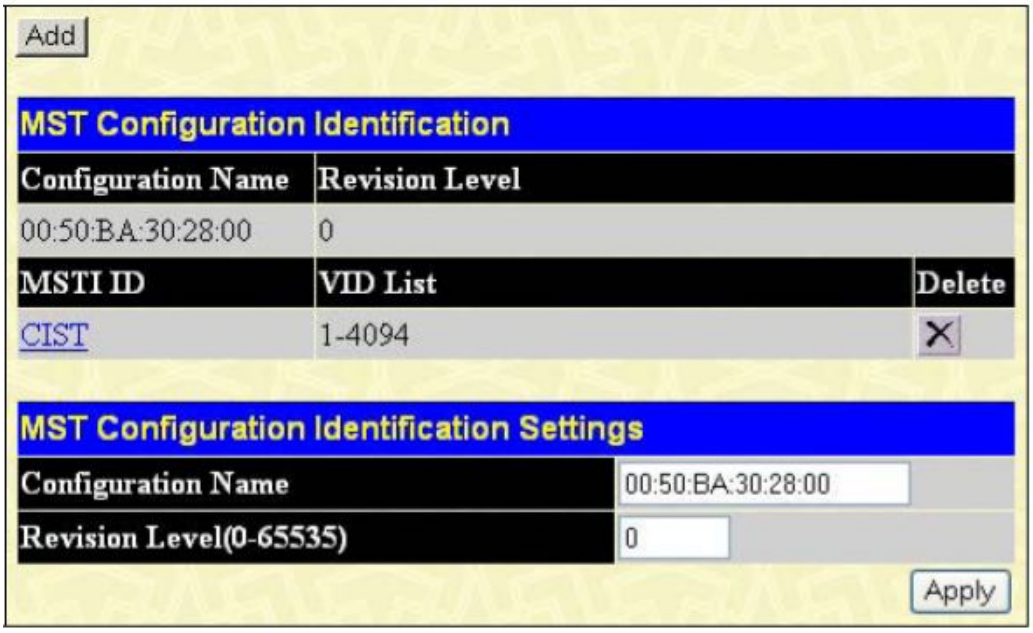


Рисунок 7- 18. Окно MST Configuration Identification

В окне, показанном выше, содержится следующая информация:

Параметр	Описание
Configuration Name	Настроенное ранее имя на Коммутаторе уникально идентифицирующее MSTI (Multiple Spanning Tree Instance). Если имя конфигурации не установлено, это поле будет отображать MAC-адрес устройства, работающего на основании протокола MSTP. Это поле может быть установлено в окне STP Bridge Global Settings.
Revision Level	Это значение, наряду с именем конфигурации будет идентифицировать регион MSTP, настроенный на Коммутаторе. Пользователь может установить значение от *0* до *65535,* значение по умолчанию равно *0*.
MSTI ID	Это поле отображает MSTI ID, установленные на Коммутаторе. Данное поле всегда будет иметь CIST MSTI, доступный для настройки, но не доступный для удаления. При нажатии на ссылку с именем откроется новое окно для настройки параметров, связанных с определенной MSTI.
VID List	В данном поле отображаются VLAN ID, связанные с определенным MSTI.

Нажатие на кнопку **Add** приведет к следующему окну для настройки:

Рисунок 7- 19. Окно Instance ID Settings – Add

Пользователь может настроить следующие параметры для создания MSTI на Коммутаторе.

Параметр	Описание
MSTI ID	Введите число от *1* до *15,* чтобы установить новый MSTI на Коммутаторе.
Type	Выбор опции *Create* позволяет создать новый MSTI. При создании нового MSTI никаие другие опции не доступны.
VID List (1-4094)	Это поле позволяет определить диапазон VID от настроенных VLAN на Коммутаторе. Поддерживаемый диапазон VID на Коммутаторе - от *1* до *4094*.

Кликните по **Apply** для применения выполненных изменений.
Чтобы задать настройки CIST, кликните по гиперссылке в окне **MST Configuration Identification**.
В результате откроется следующее окно для настройки:

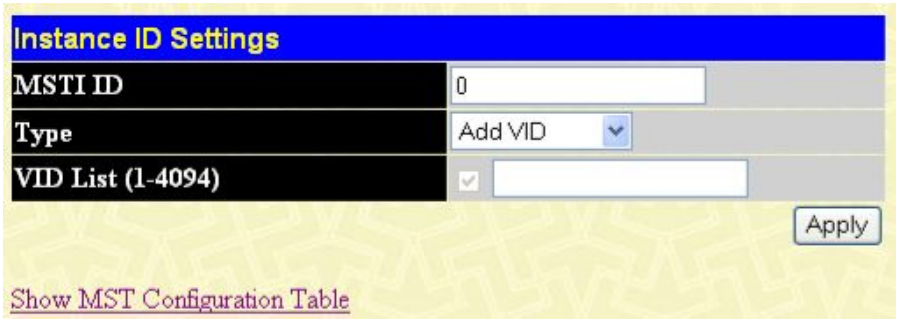


Рисунок 7- 20. Окно Instance ID Settings - CIST modify

Пользователь может задать следующие настройки CIST на Коммутаторе.

Параметр	Описание
MSTI ID	Идентификатор MSTI ID для CIST равен *0* и не может быть изменен.
Type	Это поле позволяет выбрать необходимые действия для настроек MSTI. Доступно 2 опции. *Add VID* – Выберите этот параметр, чтобы добавить VID в MSTI ID в соответствии с параметром VID List. *Remove VID* – Выберите этот параметр, чтобы удалить VID из MSTI ID в соответствии с параметром VID List.
VID List (1-4094)	Это поле позволяет определить диапазон VID от настроенных на Коммутаторе VLAN. На Коммутаторе поддерживаются VID с диапазоном от *1* до *4094*. Это поле не доступно при настройке CIST.

Кликните по **Apply** для применения выполненных изменений.

Чтобы настроить параметры созданной ранее копии MSTI, кликните по ссылке с номером MSTI ID. В результате появится следующее окно для настройки.

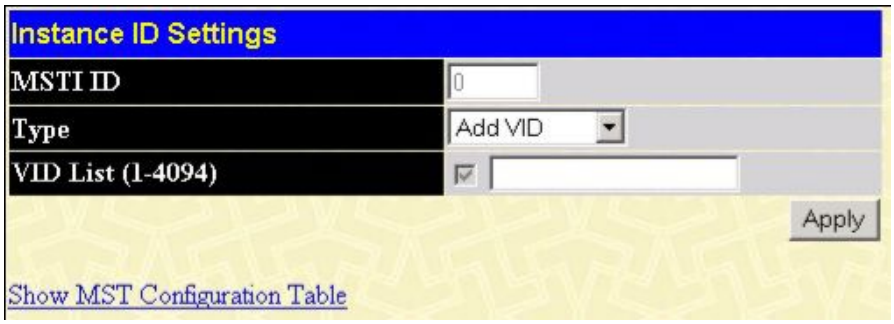


Рисунок 7- 21. Окно Instance ID Settings – Modify

Пользователь может настроить следующие параметры MSTI на Коммутаторе.

Параметр	Описание
MSTI ID	Отображает MSTI ID, установленный ранее пользователем.
Type	Это поле позволяет выбрать нужный метод изменения настроек MSTI. На выбор доступны следующие опции. *Add VID* – выберите этот параметр, чтобы добавить VID в MSTI ID. В этом случае будет доступно поле VID List. *Remove VID* – выберите этот параметр, чтобы удалить VID из MSTI ID. В этом случае будет доступно поле VID List.
VID List (1-4094)	Это поле позволяет задать диапазон VID с настроенных VLAN, установленных на Коммутаторе, которые необходимо добавить в MSTI ID. Допустимые значения от *1* до *4094*. Этот параметр может использоваться только в том случае, если в поле Type выбрано значение *Add* или *Remove*.

Кликните по **Apply** для применения выполненных изменений.

Настройки копии STP

В следующем окне отображаются MSTI, установленные на данный момент на Коммутаторе. Для работы со следующим окном кликните по **L2 Features > Spanning Tree > STP Instance Settings**:

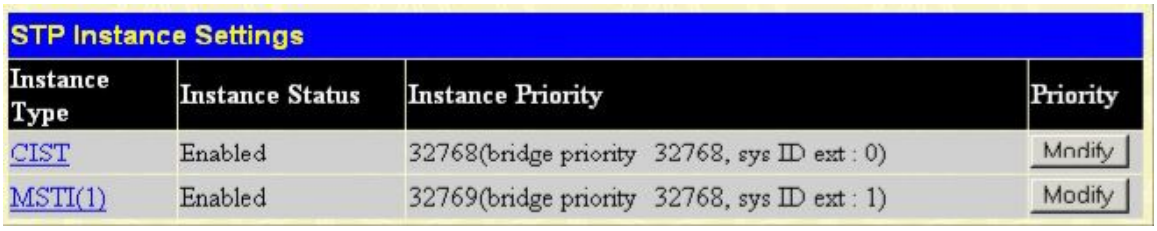


Рисунок 7- 22. Окно STP Instance Settings

Следующая информация отображается в данном окне:

Параметр	Описание
Instance Type	Отображает тип копии или копий, настроенных в данный момент на Коммутаторе. Все типы копий классифицируются по MSTI ID. CIST относится к настройкам MSTI, установленным на Коммутаторе.

Instance Status	Отображает текущий статус соответствующего MSTI ID
Instance Priority	Отображает приоритет соответствующего MSTI ID. Копия с самым маленьким значением приоритета будет назначена корневым мостом.

Кликните по **Apply** для применения выполненных изменений.
Кликните по кнопке **Modify**, чтобы изменить приоритет MSTI. В результате откроется окно I**nstance ID Settings** для настройки.

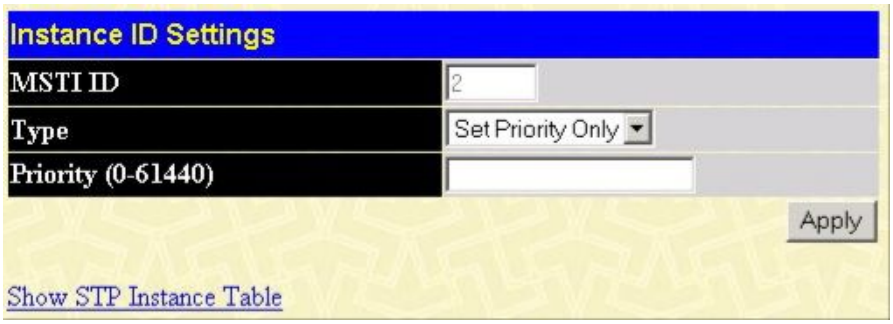


Рисунок 7- 23. Окно Instance ID Settings - modify priority

Для просмотра и изменения доступны следующие параметры:

Параметр	Описание
MSTI ID	Отображает MSTI ID изменяемой копии. Запись *0* в данном поле означает CIST (MSTI по умолчанию).
Type	В поле Type в данном окне удет постоянно выбрана опция *Set Priority Only*.
Priority (0-61440)	Введите новое значение приоритета в поле Priority. Доступные значения приоритета от *0* до *61440*.

Кликните по **Apply** для применения новых настроек приоритета.

Информация о портах MSTP

Это окно отображает текущую информацию о MSTP-порте и позволяет обновить настройки порта для MSTI ID. При возникновении петли функция MSTP будет использовать приоритет порта для выбора интерфейса, через который будут продвигаться пакеты. Чем выше приоритет интерфейса, тем больше вероятность, что данные будут передаваться через него. В случае если значения приоритетов идентичны, функция MSTP будет выбирать интерфейс с наименьшим MAC-адресом для продвижения пакетов, а другие интерфейсы с таким приоритетом при этом будут заблокированы. Помните, что чем меньше значение, тем выше приоритет. Для работы со следующим окном кликните по **L2 Features > Spanning Tree > MSTP Port Information**:

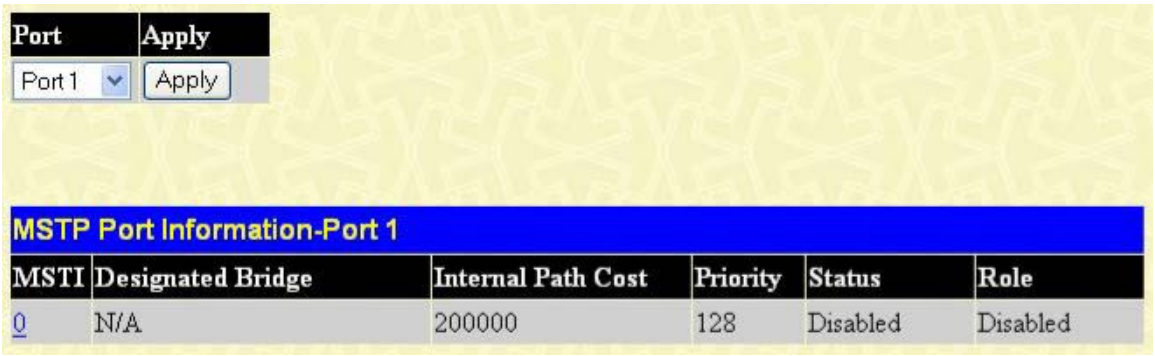


Рисунок 7- 24. Окно MSTP Port Information

Чтобы просмотреть настройки MSTI для опередеенного порта, выберите номер порта в выпадающем меню, расположенном в верхнем леовм углу экрана, и кликните по **Apply**. Чтобы

изменить настройки определенной копии MSTI, кликните по ссылке с MSTI ID. В результате появится следующее окно.

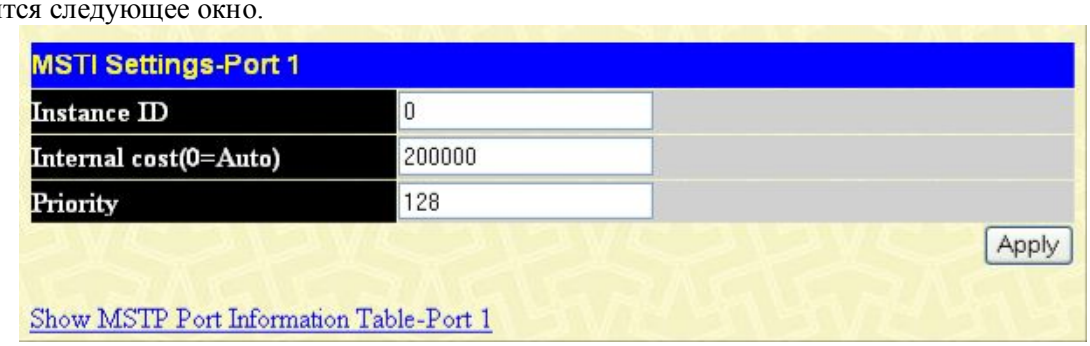


Рисунок 7- 25. Окно MSTI Settings

Для просмотра и изменения доступны следующие параметры:

Параметр	Описание
Instance ID	Отображает MSTI ID настриваемой копии spanning tree. Выбор значения 0 в этом поле означает CIST (MSTI по умолчанию).
Internal cost (0=Auto)	Этот параметр устанавливает относительную стоимость продвижения пакетов на определенные порты, когда интерфейс выбирается в копии STP. Настройка по умолчанию - 0 (auto). Доступно две опции: *0 (auto)* – Выбор этого параметра в поле *internalCost* означает автоматический выбор наиболее быстрого и подходящего для данного интерфейса маршрута. Данное значение позволяет передавать данные на скорости среды. *value 1-200000000* – выбор в этом поле значения от 1-200000000 будет устанавливать наиболее быстрый маршрут при возникновении петли. Чем меньше значение Internal cost, тем быстрее передача.
Priority	Введите значение от *0* до *240,* чтобы установить значение для интерфейса порта. Интерфейс с более высоким приоритетом будет продвигать пакеты первым. Чем меньше значение в данном поле, тем выше приоритет.

Кликните по **Apply** для применения выполненных изменений.

Раздел 8

Класс обслуживания (CoS)

Полоса пропускания порта

Приоритет по умолчанию 802.1p

Приоритет пользователя 802.1p

Работа CoS по расписанию

Настройки приоритетов

Настройки приоритетов TOS

Настройки приоритетов DSCP

Настройки приоритетов

Приоритеты на основе MAC-адресов

Для обеспечения надлежащего качества обслуживания(QoS) коммутаторы серии DES-30xx поддерживают очереди приоритетов 802.1p Quality of Service. Данная глава расскажет о применении QoS и преимуществах использования очередей приоритетов 802.1p.

Преимущества QoS

Использование IEEE 802.1p QoS позволяет приоритезировать трафик и выделить необходимую полосу пропускания для приложений, чувствительных к задержкам, включая VoIP (передача голоса по IP) и видеоконференцию. Необходимая полоса пропускания создается за счет меньшей скорости передачи данных приложений, не чувствительных к задержке. Коммутатор организует отдельные аппаратные очереди на каждом физическом порту, при этом поступающие от различных приложений пакеты получают соответствующий приоритет. Рисунок, приведенный ниже, иллюстрирует приоретизацию очередей 802.1P в коммутаторах серии DES-30xx.

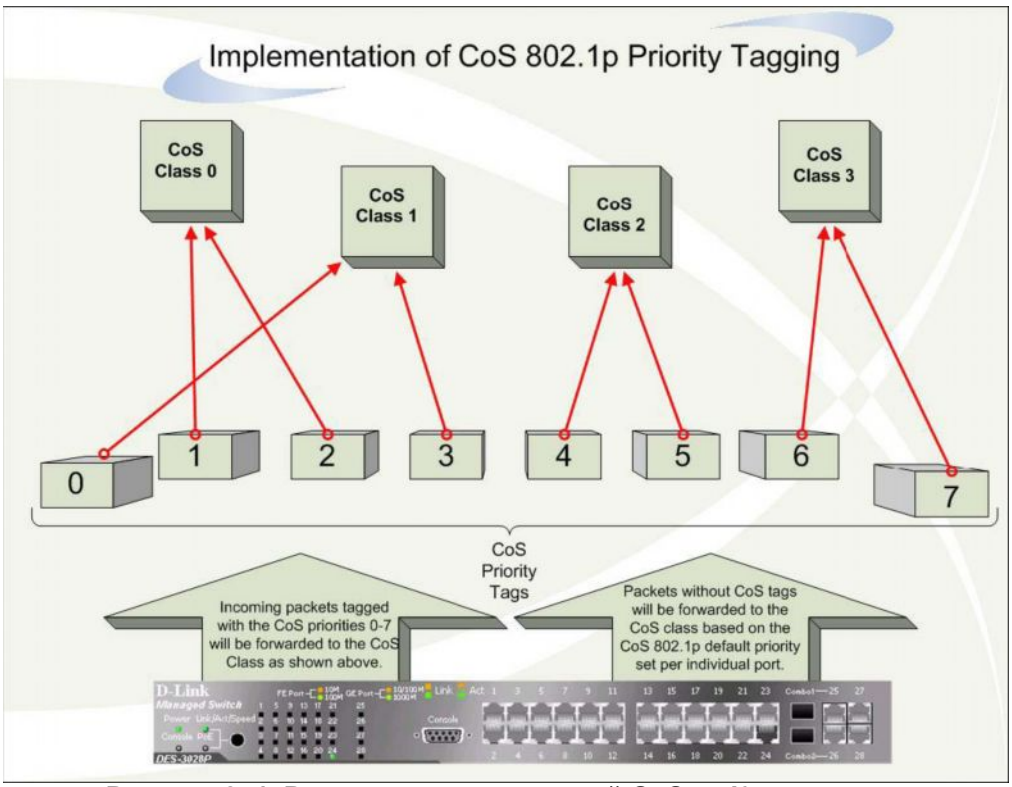


Рисунок 8- 1. Распределение очередей QoS на Коммутаторе

На приведенном выше рисунке показаны настройки приоритезации Коммутатора по умолчанию. Class 3 обладает наивысшим приоритетом среди четырёх очередей Коммутатора. Для того чтобы использовать QoS, Коммутатор должен осуществлять проверку заголовка пакета на наличие соответствующего тега. Далее тегированные пакеты отправляются в соответствующую их приоритету очередь Коммутатора.

Например, существует потребность установить видеоконференцию между двумя удалёнными компьютерами. Администратор, используя команды профиля доступа, устанавливает высокий приоритет для пакетов видео. Коммутатор на принимающей стороне проверяет пакеты на наличие тега и ставит в очередь, соответствующую приоритету пакета. В результате конечный пользователь получает информацию с максимально возможной скоростью, поскольку использование приоритезации очередей и непрерывный поток видеоданных обеспечивают оптимальное использование полосы пропускания, доступной для видеоконференции.

Понятие QoS

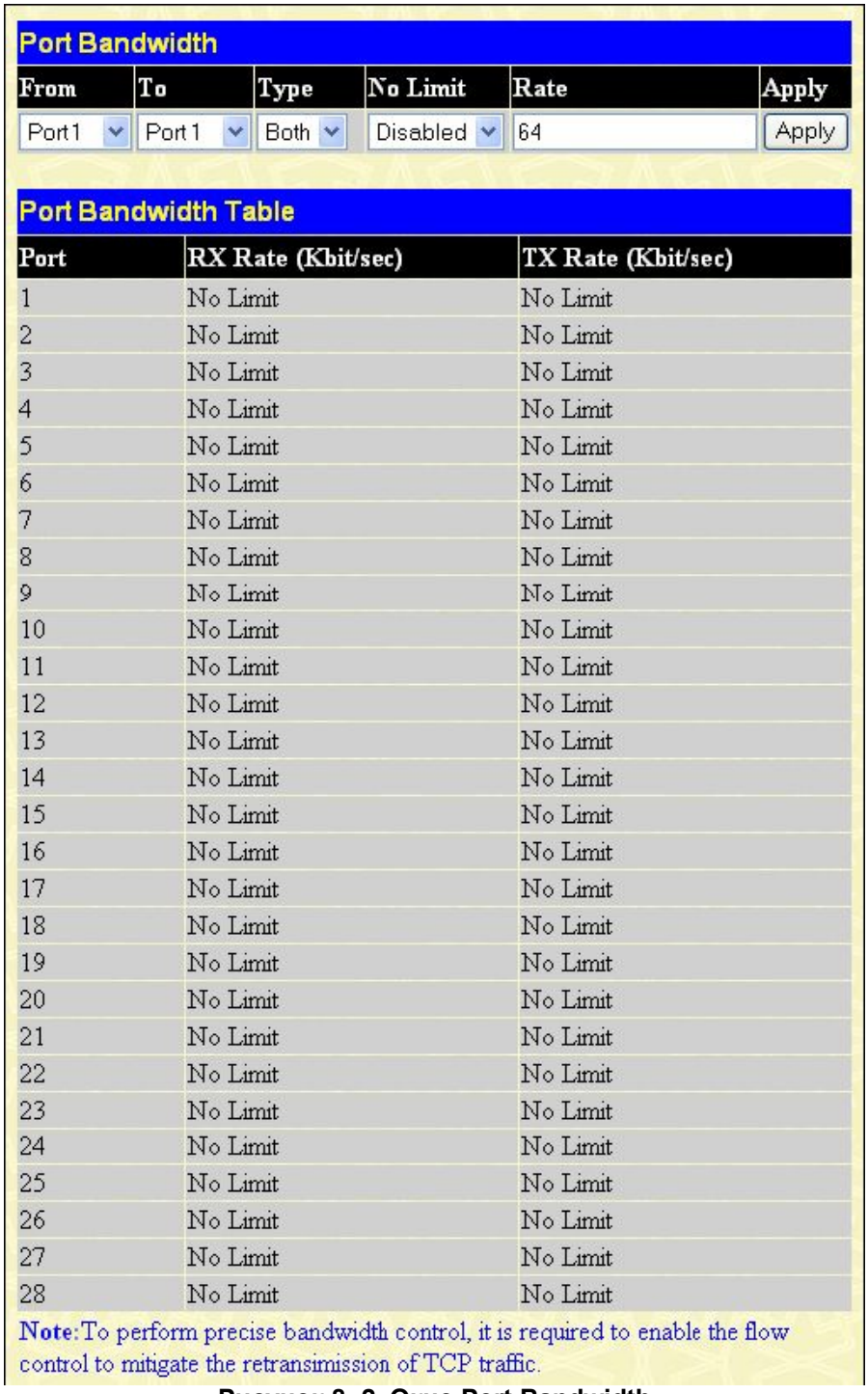
На Коммутаторе предусмотрено четыре очереди приоритетов: от 0 до 3, где 3 -очередь с наивысшим приоритетом, 0 - с наименьшим. Восемь тегов приоритета, описанные стандартом IEEE 802.1p, распределяются на Коммутаторе следующим образом:

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

При использовании строго режима (Strict mode) обработки очередей пакеты из очереди высшего приоритета всегда обслуживаются первыми. Опустошение очередей происходит, строго следуя их приоритетам. Только тогда, когда очередь более высокого приоритета пуста, обслуживаются пакеты с более низким приоритетом.
В случае использовании взвешенного кругового режима обработки очередей (weighted round robin, WRR) количество пакетов, отправленное из каждой очереди, определяется присвоенным ей взвешенным коэффициентом. Для конфигурации с 8 очередями CoS (A~H) с соответствующими взвешенными коэффициентами 8~1,пакеты будут отправляться в следующей последовательности: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1. Т.е. в то время как передано 8 пакетов из очереди A (с наивысшим приоритетом), из очереди H (с наименьшим приоритетом) передан только 1 пакет.
В алгоритме WRR если очереди CoS обладают одинаковым взвешенным коэффициентом, то каждая из них обладает равными правами продвижения пакетов.
Также в WRR если вес CoS равен 0, то пакеты из этой очереди будут обрабатываться до тех пор, пока их не останется. Другие очереди CoS, взвешенный коэффициент которых отличен от нуля, будут обрабатываться в соответствии со схемой WRR.
Следует помнить, что коммутаторы серии DES-30xx поддерживают только четыре очереди (и четыре класса обслуживания CoS) для каждого порта.

Полоса пропускания порта

Настройка управления полосой пропускания позволяет задать максимальную скорость передачи и приема данных для любого выбранного порта. Для работы с показанным ниже окном в папке **L2 Features** кликните **CoS > Port Bandwidth:**



Port Bandwidth

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
19	No Limit	No Limit
20	No Limit	No Limit
21	No Limit	No Limit
22	No Limit	No Limit
23	No Limit	No Limit
24	No Limit	No Limit
25	No Limit	No Limit
26	No Limit	No Limit
27	No Limit	No Limit
28	No Limit	No Limit

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

Рисунок 8- 2. Окно Port Bandwidth

Можно установить следующие настройки:

Параметр	Описание
From/To	Данные выпадающие меню позволяют задать диапазон портов для

	настройки.
Type	В данном выпадающем меню доступны следующие опции: *RX* (прием), *TX* (передача) и *Both*. Таким образом, определяется, будет ли ограничение скорости применяться при приеме, передаче данных или же будут сочетаться оба варианта.
no_limit	Данное выпадающее меню позволяет задать порты с неограниченной полосой пропускания. Для этого нужно указать в данном поле значение *Enabled*.
Rate	Данное поле позволяет ввести максимальную скорость в Мбит/с для выбранных портов. Доступны значения от 64 до 1024000 Кбит/с.

Для применения настроек управления полосой пропускания для выбанных портов следует кликнуть **Apply**. Результаты настройки управления полосой пропускания будут представлены в таблице **Port Bandwidth Table**.

Приоритет 802.1p по умолчанию

Коммутатор дает возможность настроить приоритет по умолчанию 802.1p для каждого порта Коммутатора. В папке **CoS** кликните по **802.1p Default Priority** для работы с окном, показанным ниже.

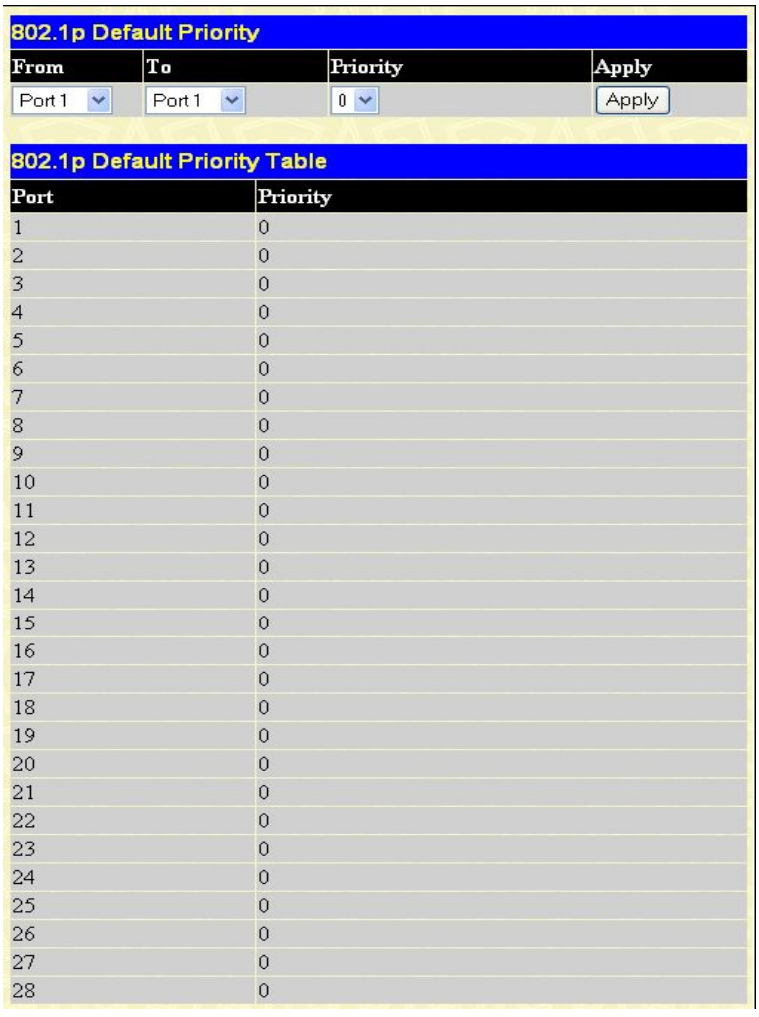


Рисунок 8- 3. Окно 802.1p Default Priority

Это окно позволяет пользователям назначить приоритет по умолчанию 802.1p любому данному порту на Коммутаторе. Очереди приоритетов нумеруются, начиная с 0, наименьшего приоритета, до 7, наивысшего приоритета. Чтобы задать новые приоритеты по умолчанию 802.1p, выберите диапазон портов в выпадающих меню **From** и **To,** а затем укажите значение приоритета от 0 до 7 в поле **Priority.**

Кликните по **Apply** для применения выполненных изменений.

Приоритет пользователя 802.1p

При использовании механизма приоритезации 802.1p пакет проверяется на наличие тега приоритета 802.1p. Исходя из значения тега, пакет назначается в очереди приоритетов. Тег приоритета может быть назначен любой из очередей.

Серия Коммутаторов DES-30xx позволяет назначать приоритет пользователя для каждого из приоритетов 802.1p. В папке **QoS** кликните по **802.1p User Priority**, после чего появится следующее окно для настройки.

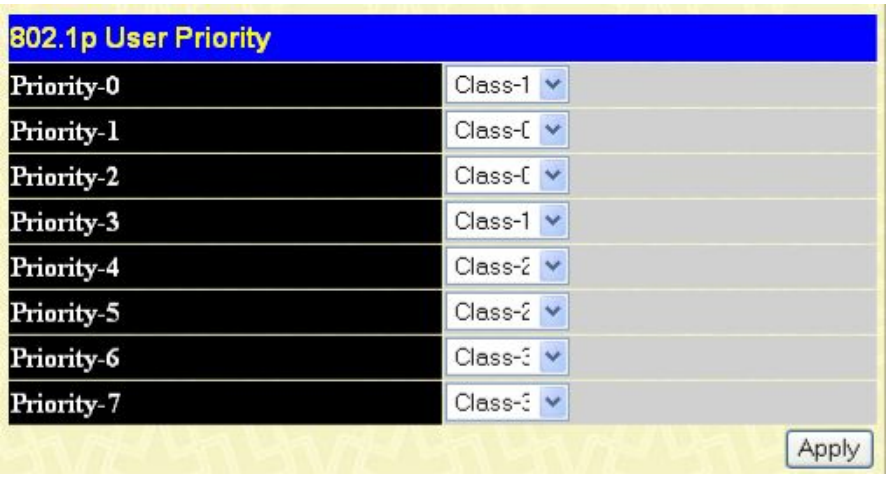


Рисунок 8- 4. Окно 802.1p User Priority

При назначении приоритета группам порта пользователи могут задать класс каждого из 4 уровней приоритетов 802.1p. Кликните по **Apply** для применения выполненных настроек.

Механизмы обработки очередей

Для работы с приведенным окном необходимо в папке **CoS** кликнуть по **QoS Scheduling Mechanism**. В выпадающем меню доступны две опции, определяющие механизм обработки очередей: **Weight Fair** и **Strict.**

Рисунок 8- 5. Окно CoS Scheduling Mechanism и CoS Scheduling Mechanism Table

ПРИМЕЧАНИЕ: По умолчанию назначен строгий алгоритм обработки очередей длянаивысшего класса (Class-3), что означает, что очередь класса 3 будет опустошаться, пока в ней не останется пакетов. Очереди других классов приоритетов будут опустошаться в соответствии с круговым циклическим алгоритмом (WRR).

Возможны следующие механизмы обработки очередей.

Параметр	Описание
Strict	При данном режиме трафик очереди с наивысшим классом обслуживания обрабатывается всегда первым. Только полсе опустошения очереди с наивысшим классом обслуживания Коммутатор перейдет к обработке трафика следующей очереди.
Weight fair	При исользовании взвешенного циклического алгоритма (*WRR*) пакеты обрабатываются в соответствии с приоритетами каждого класса обслуживаия.

Кликните по **Apply** для применения выполненных изменений.

Работа CoS по расписанию

Изменение расписания аппаратных очередей Коммутатора позволяет настроить CoS под конкретные нужды пользователя. При этом необходимо обратить особое внимание на то, как новые настройки влияют на сетевой трафик в очередях с наименьшим приоритетом. Необдуманные изменения в расписании могут привести к недопустимым уровням потерь пакетов или существенной задержке передачи. Поэтому очень важно при изменении данных настроек контролировать производительность сети, особенно в моменты пиковых нагрузок, т.к. количество «узких мест» в сети может существенно возрасти из-за неприемлемых параметров QoS. Для работы с приведенным ниже окном откройте папку **CoS** и кликните по **CoS Output Scheduling**.

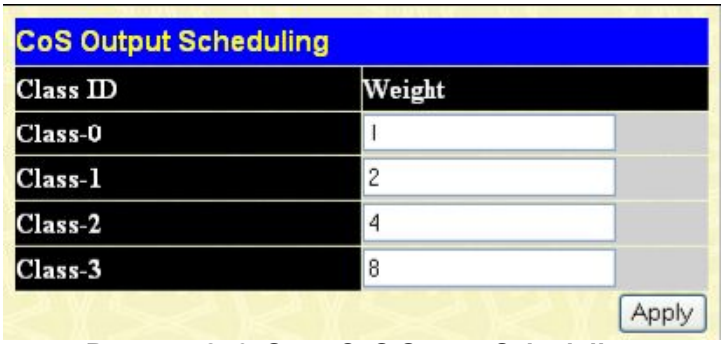


Рисунок 8- 6. Окно CoS Output Scheduling

Для принятия настроек следует кликнуть по **Apply**.

Настройки приоритета

Окно **Priority Setting** позволяет пользователям настроить приоритет CoS на основе портов. При тегировании CoS пакетов, поступающих на коммутатор, тегирование осуществляется с заданными здесь настройками. Например, если порту был назначен приорите на основе MAC-адреса, то пакет с приоритетом CoS, назначенным MAC-адресу, будет отправляться в очередь CoS, которая настроена для данного MAC-адреса. Когда настройка завершена, пользователь может просмотреть результат в окне **Priority Settings Table**. После настройки приоритетов порта пользователь может задать индивидуальные настройки CoS с помощью опций других окон, расположенных в папке **CoS**.

В папке **CoS** кликните **Priority Settings** для работы с окном, показанным ниже:

Рисунок 8- 7. Окно Priority Settings

Для настройки доступны следующие параметры:

Параметр	Описание
From/To	С помощью данных выпадающих меню пользователи могут указать порт или диапазон портов для настройки приоритетов ToS на основе значения, указанного в поле Type.
Type	Выберите основные настройки приоритета для портов, указанных в выпадающих меню. Доступны следующие опции: • **None** – Выбор этой опции очистит настройки приоритета CoS для указанных портов. • **Port Mapping** – Выбор этой опции позволяет назначить приоритеты CoS для индивидуальных портов. • **802.1p** – Выборэтой опции позволяет назначить приоритеты CoS

	приоритетам 802.1p. Это настройка по умолчанию для всех портов. • **MAC-Base –** Выбор этой опции позволяет назначить приоритеты CoS MAC-адресам. • **TOS** – Выбор этой опции позволяет назначить приоритеты CoS приоритетам ToS. • **DSCP** – Выбор этой опции позволяет назначить приоритеты CoS приоритетам DSCP.

Для принятия настроек следует кликнуть по **Apply**.

Настройки приоритета TOS

При использовании механизма приоритезации TOS/DSCP пакеты классифицируются на основе значения поля TOS/DSCP в заголовке IP-пакета. Если пакет тегирован, то он назначается в определенную очередь на основе значения тега приоритета. Тегированный приоритет может быть назначен любой из очередей. Когда используется TOS, не может использоваться DSCP. Верно и обратное.

Настройки приоритетов TOS определяются в данном окне. С помощью выпадающих меню выберите значения для **TOS** и **Class ID**.

Для работы с показанным ниже окном в папке **CoS** кликните **TOS Priority Settings**:

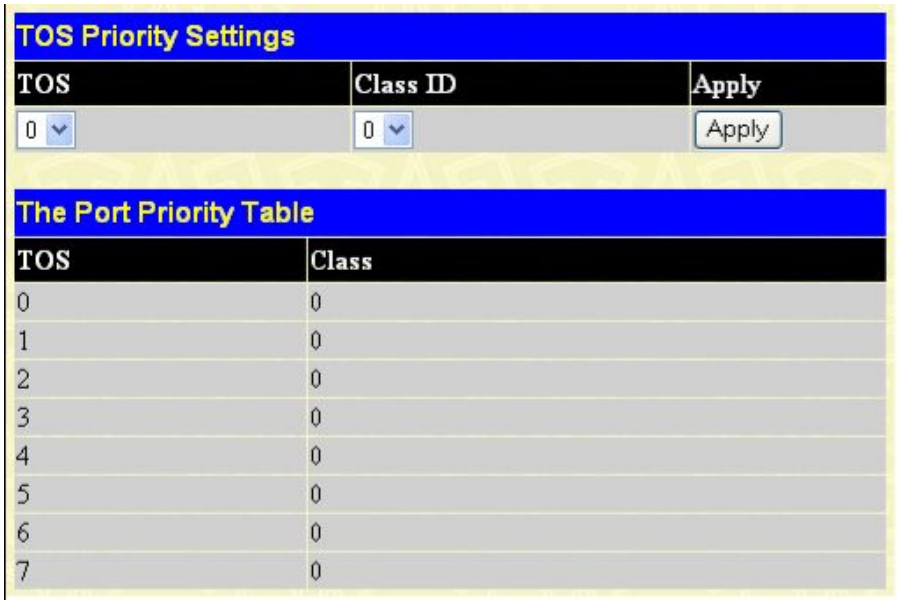


Рисунок 8- 8. Окно TOS Priority Settings

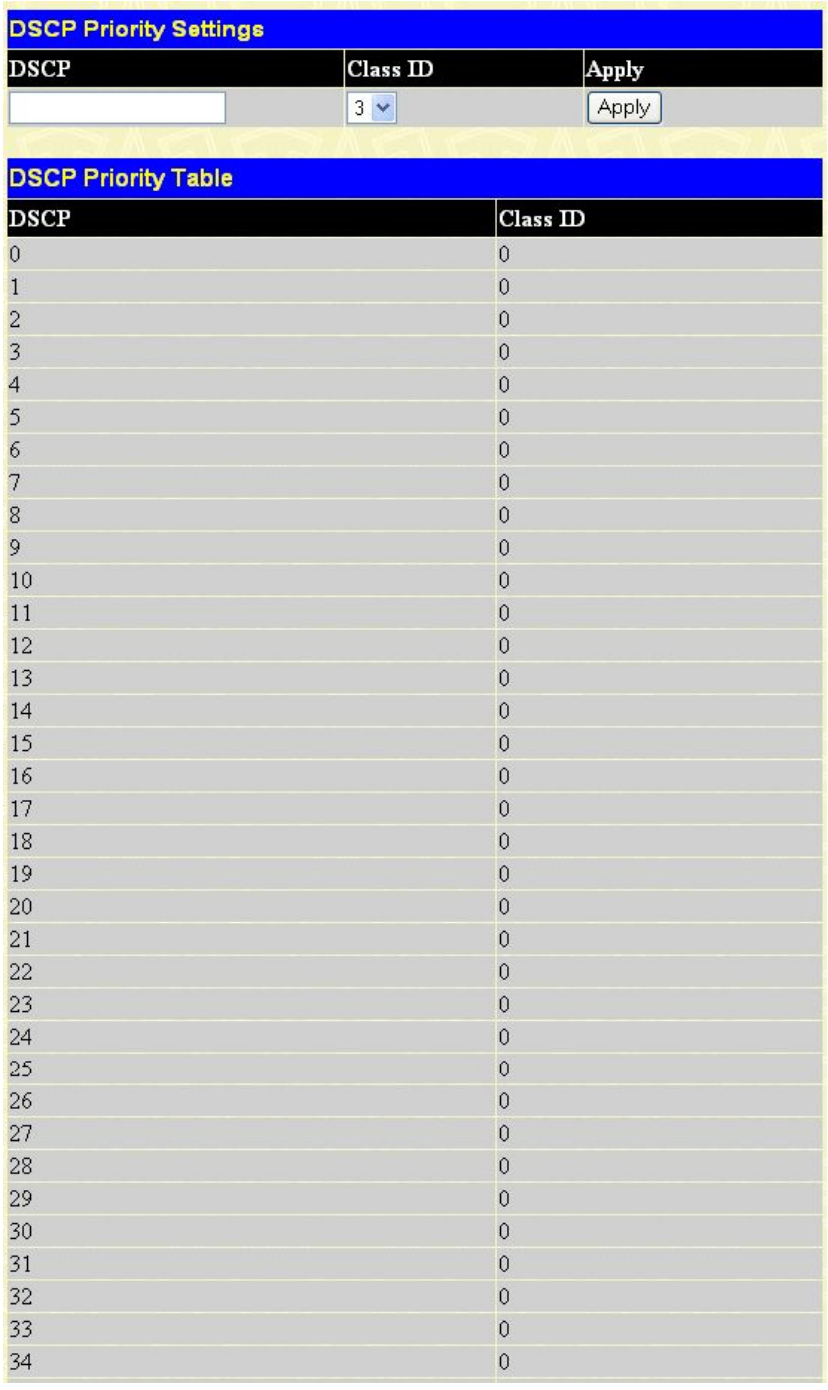
Для принятия настроек следует кликнуть по **Apply**.

Настройки приоритета DSCP

При использовании механизма приоритезации TOS/DSCP пакеты классифицируются на основе значения поля TOS/DSCP в заголовке IP-пакета. Если пакет тегирован, то он назначается в определенную очередь на основе значения тега приоритета. Тегированный приоритет может быть назначен любой из очередей. При получении пакета с тегом DSCP он будет отправлен в очередь CoS, заданную здесь. Эти настройки будут иметь силу, если настройки хотя бы одного порта используют DSCP. Когда используется DSCP, не может использоваться TOS. Верно и обратное.

В данном окне могут быть заданы настройки приоритетов DSCP. Введите значение **DSCP** и выберите значение **Class ID** (от 0 до 3).

Для работы с показанным ниже окном в папке **CoS** кликните **DSCP Priority Settings**:



DSCP Priority Settings

DSCP	Class ID	Apply
	3	Apply

DSCP Priority Table

DSCP	Class ID
0	0
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
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0
29	0
30	0
31	0
32	0
33	0
34	0

Рисунок 8- 9. Окно DSCP Priority Settings

Для принятия настроек следует кликнуть по **Apply**.

Настройка приоритетов на основе портов

При использовании механизма приоритезации на оснвое портов приоритет, назначенный каждому входящему порту, определяет очередь, в которую будут добавлены фреймы. Фреймы будут добавляться в очередь с максимальным приоритетом или минимальным.

Существует следующее ограничение, что CoS на основе портов может применяться только к Очереди 3.

Настройки приоритетов на основе портов задаются в данном окне. Выберите диапазон портов в выпадающих меню **From** и **To,** а также укажите **Class**.

Для работы с окном, показанным ниже, в папке **CoS** кликните **Port Mapping Priority Settings**:

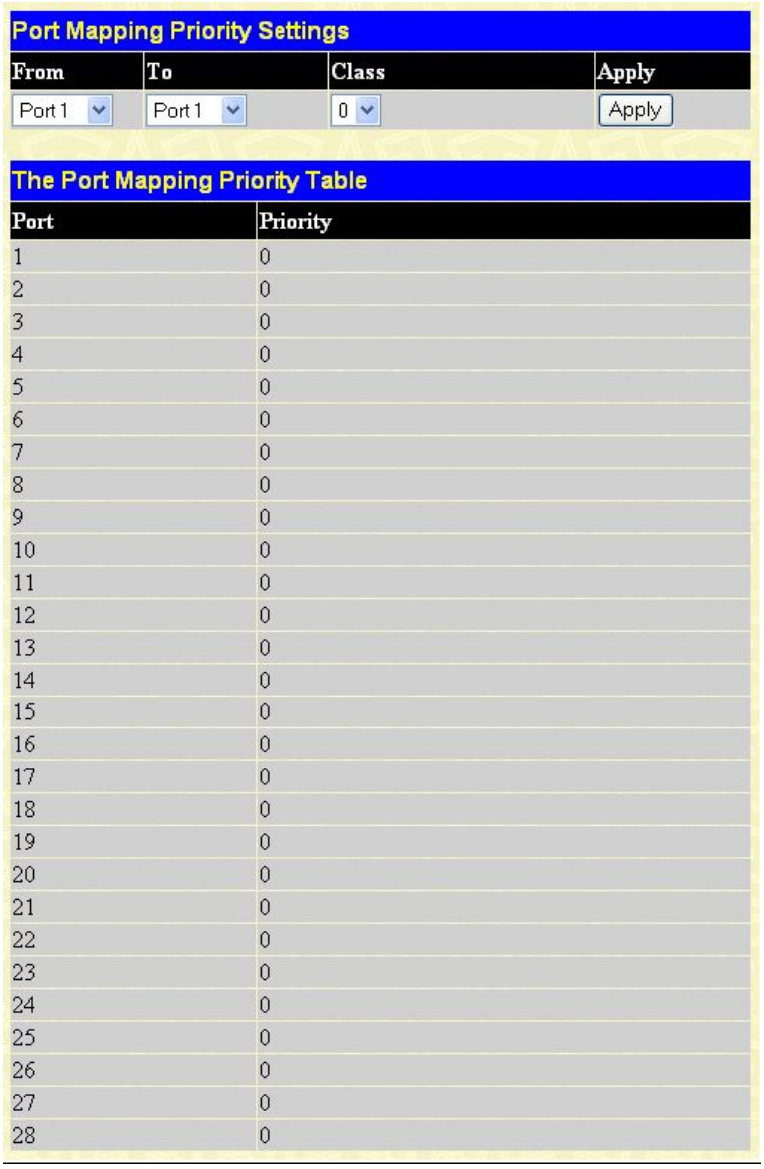


Рисунок 8- 10. Окно Port Mapping Priority Settings

Для принятия настроек следует кликнуть по **Apply**.

Приоритет на основе MAC-адресов

При использовании механизма приоритезации на основе MAC-адресов, пакеты приоритезируются на основе значения поля MAC-адрес в таблице **MAC priority table**.

Чтобы настроить MAC-адрес назначения для очереди CoS, необходимо выполнить следующие шаги:

1. Введите статический MAC-адрес назначения в базу данных Forwarding Database (FDB) Коммутатора. Для этого откройте таблицу Unicast Forwarding table в папке **Forwarding Filtering** меню **Configuration** и кликните по ссылке **Unicast Forwarding,** после чего появится окно для ввода информации.

2. После добавления MAC-адреса в FDB необходимо настроить соответствующую очередь для данного MAC-адреса назначения, используя следующее окно.

3. После установки указанных параметров необходимо открыть окно **Priority Settings,** расположенное в этой папке, и настроить порты коммутатора для **MAC Priority**. Эти порты должны быть настроены для приоритетов на основе MAC-адресов, а не для других приоритетов. По умолчанию установлен приоритет 802.1p, поэтому необходимо изменить настройку на опцию MAC Priority, чтобы данная функция работала корректно. Убедитесь, что MAC-адрес назначения подключен к порту, для которого настраивается приоритет.

Для работы с показанным ниже окном откройте папку **CoS** и кликните **MAC Priority**:

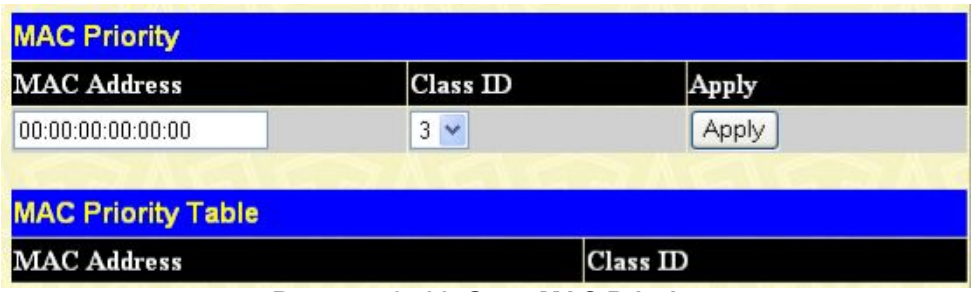


Рисунок 8- 11. Окно MAC Priority

Введите **MAC Address** назначения**,** который был введен ранее в окне **Unicast Forwarding**, а затем укажите Class ID, в который будут отправляться пакеты с указанным MAC-адресом назначения. Кликните по **Apply** для применения настроек.

Раздел 9

Списки управления доступом (ACL)

Настройка временного диапазона (Time Range)
Таблица профилей доступа
Flow Meter
CPU Interface Filtering

Настройка временного диапазона (Time Range)

Окно **Time Range** совместно с профилями доступа позволяет задать расписание, когда профили доступа будут активны на Коммутаторе. Представленное окно позволяет присвоить имя временному диапазону, а также определить дни, когда профили доступа будут активны.

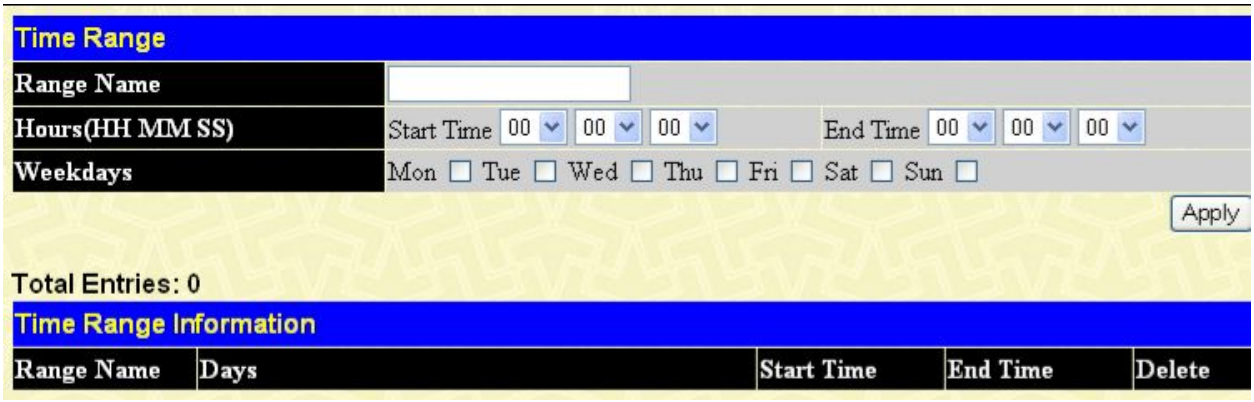


Рисунок 9- 1. Окно Time Range Settings

Кликните по **Apply** для применения выполненных изменений.

Таблица профилей доступа

Профили доступа дают возможность установить критерии, определяющие на основе информации в заголовке пакета, будет ли Коммутатор продвигать данные пакеты.

Создание профиля доступа включает в себя две основные части. Первая определяет, какую часть или части фрейма Коммутатор будет проверять, как, например, MAC-адрес источника или IP-адрес назначения. Во второй части необходимо будет ввести критерии, которые будет использовать Коммутатор, чтобы определить, что делать с фреймом. Чтобы отобразить настроенные в данный момент на Коммутаторе профили доступа, откройте папку **Configuration** и кликните по ссылке **Access Profile Table**. В результате откроется страница **Access Profile Table**, как показано ниже.

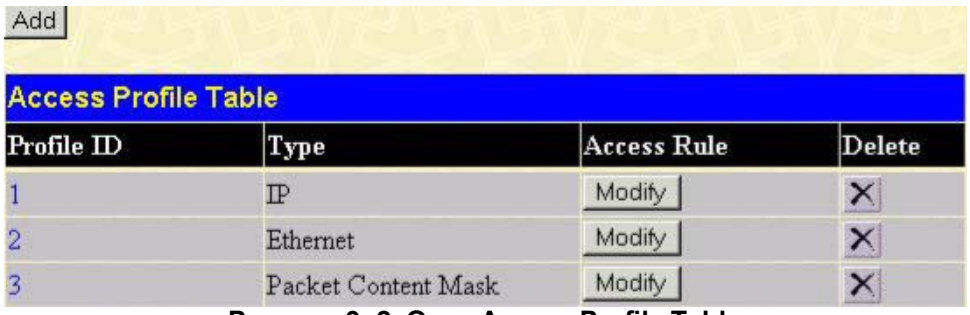


Рисунок 9- 2. Окно Access Profile Table

Чтобы добавить запись в окно **Access Profile Table**, кликните по кнопке **Add Profile**. В результате откроется окно **Access Profile Configuration**, показанное ниже. Для настройки профиля доступа доступно три окна **Access Profile Configuration:** 1. для настройки профиля на основе **Ethernet** (MAC-адреса), 2. для настройки профиля на основе **IP-адреса**, 3. для настройки профиля на основе маски содержимого пакета (**Packet Content Mask)**. Пользователь может получить доступ к различным окнам **Access Profile Configuration** с помощью выбора нужного значения в выпадающем меню **Type**. Ниже показана страница **Ethernet Access Profile Configuration**.

ПРИМЕЧАНИЕ: Profile ID задает относительный приоритет профиля доступа во избежание возникновения конфликта между правилом, созданном в одном профиле, и правилом, созданным в другом. Пожалуйста, обратитесь к разделу по командам ACL Руководства пользователя по Интерфейсу командной строки.

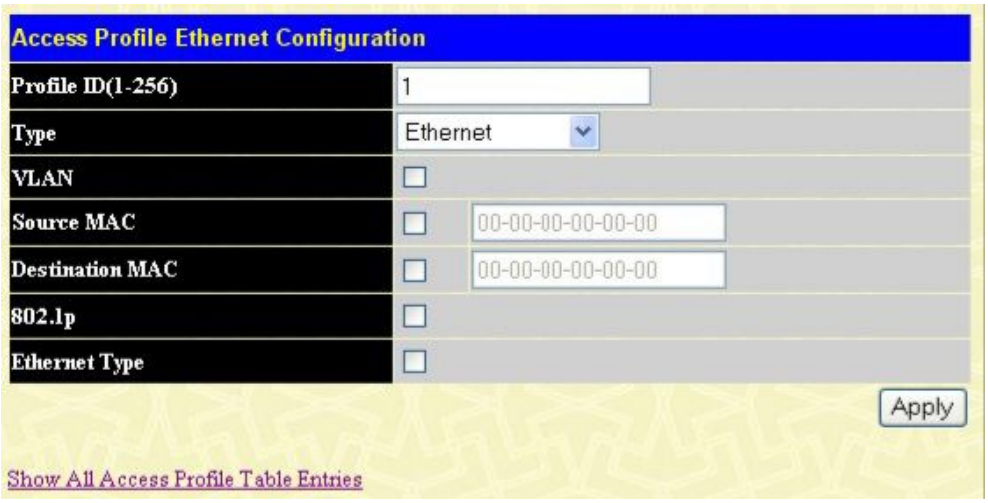


Рисунок 9-3. Окно Access Profile Configuration (Ethernet)

При выборе значения **Ethernet** в поле **Type**:

Параметр	Описание
Profile ID (1-14)	Введите уникальный идентификационный номер для данного профиля. Это поле может принимать значение от *1* до *14*.
Type	Выберите профиль на основе Ethernet (MAC-адреса), IP-адреса, содержимого пакета. В зависимости от выбранного типа профиля будут предложены соответствующие параметры для настройки: • Выбор в данном поле *Ethernet* означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. Именно этот вариант и

	будет рассмотрен в данной таблице. • Выбор в данном поле *IP* означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Выбор в данном поле *Packet Content Mask* означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
VLAN	Выбор данной опции означает, что Коммутатор будет проверять идентификатор VLAN в заголовке каждого пакета и использовать полученную информацию как единственный или один из критериев для принятия решения о продвижении пакета.
Source MAC	В случае необходимости, поставив галочку в данном поле, введите MAC-адрес источника.
Destination MAC	В случае необходимости, поставив галочку в данном поле, введите MAC-адрес назначения.
802.1p	При выборе данной опции Коммутатор будет проверять в заголовках пакетов уровень приоритета 802.1p и использовать этот приоритет для принятия решения о продвижении пакета.
Ethernet type	При выборе данной опции Коммутатор буде проверять значение типа Ethernet в заголовке каждого фрейма.

Ниже показана страница **Access Profile Configuration (IP)**.

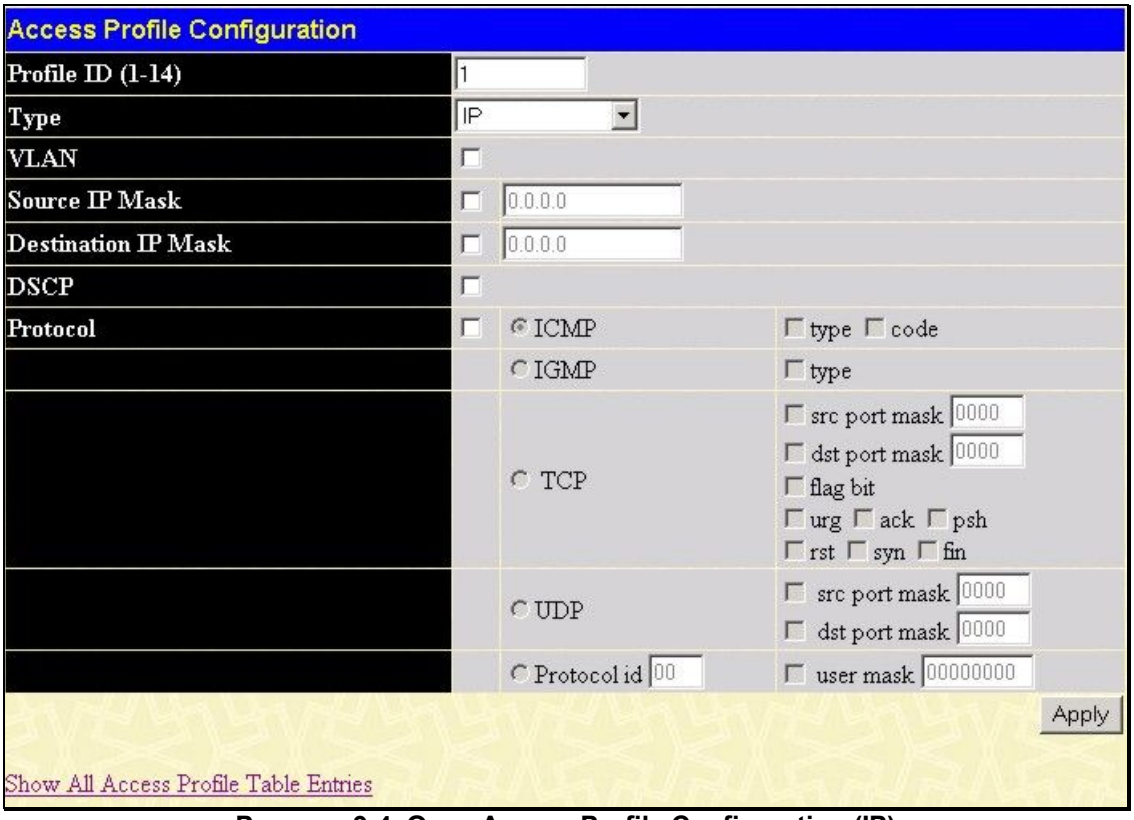


Рисунок 9-4. Окно Access Profile Configuration (IP)

Следующие параметры могут быть установлены для **IP**:

Параметр	Описание
Profile ID (1-14)	Введите уникальный идентификационный для данного профиля. Диапазон допустимых значений: от *1* до *14*.
Type	Выберите профиль на основе Ethernet (MAC-адреса), IP-адреса, содержимого пакета. В зависимости от выбранного типа профиля будут предложены соответствующие параметры для настройки: • Выбор в данном поле *Ethernet* означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. Именно этот вариант и будет рассмотрен в данной таблице. • Выбор в данном поле *IP* означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Выбор в данном поле Packet Content Mask означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
VLAN	Выбор данной опции означает, что Коммутатор будет проверять идентификато VLAN в заголовке каждого пакета и использовать полученную информацию как единственный или один из критериев для принятия решения о продвижении пакета.
Source IP Mask	В случае необходимости, поставив галочку в данном поле, введите маску источника.
Destination IP Mask	В случае необходимости, поставив галочку в данном поле, введите маску I назначения.
DSCP	При выборе данной опции Коммутатор будет проверять поле DiffServ Code в заголовках пакетов и использовать его как критерий при принятии решения о продвижении пакета.
Protocol	При выборе данной опции Коммутатор будет проверять поле типа проткола в заголовках пакетов. Далее необходимо выбрать нужный тип протокола, руководствуясь следующими принципами: При выборе опции *ICMP*- Коммутатор будет проверять заголовки пакетов на наличие Internet Control Message Protocol (ICMP) • Поставьте галочку в поле **Type,** чтобы задать, что для принятия решения будет использоваться ICMP type . Если поставить галочку в поле **Code,** то для принятия решения о продвижении пакета в профиле доступа будет использоваться поле ICMP code. При выборе опции *IGMP* Коммутатор будет проверять заголовки пакетов на наличие Internet Group Management Protocol (IGMP) • Поставьте галочку в поле **Type,** чтобы задать, что для принятия решения будет использоваться IGMP type. При выборе опции *TCP* в качестве критерия при продвижении пакетов будет использоваться номер TCP-порта, указанный в исходящем пакете. При этом необходимо, чтобы пользователь указал маску порта источника и /или маску порта назначения. Пользователь может также задать запрещенные биты флага (часть пакета, определяющая действие над пакетом). Запретив соответствующие биты флага в области TCP, пользователь может запретить таким образом и сами пакеты. Так, пользователь может запретить следующие виды пакетов: urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Для этого необходимо поставить галочку в соответствующем поле. • *src port mask* – задает в шеснадцатиричной форме (0x0-0xffff) маску TCP-порта источника, пакеты от которого будут отброшены. • *dest port mask* - определяет в шеснадцатиричной форме (0x0-0xffff) маску TCP-порта назначения, пакеты на который будут отброшены. При выборе опции *UDP* в качестве критерия при продвижении пакетов

	будет использоваться номер UDP-порта, указанный в исходящем пакете. При этом необходимо, чтобы пользователь указал маску порта источника и /или маску порта назначения. • *src port mask* – задает в шеснадцатиричной форме (0x0-0xffff) маску UDP-порта источника, пакеты от которого будут отброшены. • *dest port mask* - определяет в шеснадцатиричной форме (0x0-0xffff) маску UDP-порта назначения, пакеты на который будут отброшены. *protocol id mask* – идентификатор протокола, используемый для маски в заголовке пакета. Можно задать до 5 масок 4-го уровня для портов назначения в шестнадцатиричной форме (0x0-0xf).

Ниже показано окно настройки для **Packet Content Mask**.

Рисунок 9-5. Окно Access Profile Configuration (Packet Content Mask)

Данное окно позволяет пользователю настроить Коммутатор для маскирования заголовков пакетов, начиная с определенного байта. Для настройки **Packet Content Mask** используются следующие поля:

Параметр	Описание
Profile ID (1-14)	Введите уникальный идентификационный номер для этого профиля. Допустимые значения от *1* до *14*.
Type	Выберите профиль на основе Ethernet (MAC-адреса), IP-адреса, содержимого пакета. В зависимости от выбранного типа профиля будут предложены соответствующие параметры для настройки: • Выбор в данном поле *Ethernet* означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. Именно этот вариант и будет рассмотрен в данной таблице. • Выбор в данном поле *IP* означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Выбор в данном поле Packet Content Mask означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
Offset	Это поле указывает, с какого байта начнется маскирование заголовка пакетов. value (*0-15*) – следует задать значение в шестнадцатиричной форме для маскирования пакета с начала до 15-го байта. value (*16-31*) – следует задать значение в шестнадцатиричной форме для маскирования пакета с 16 по 31 байт. value *(32-47)* -следует задать значение в шестнадцатиричной форме для маскирования пакета с 32 по 47 байт. value *(48-63)* -следует задать значение в шестнадцатиричной форме для маскирования пакета с 48 по 63 байт. value *(64-79)* - следует задать значение в шестнадцатиричной форме для маскирования пакета с 64 по 79 байт.

Кликните по **Apply** для применения выполненных изменений.

Для установки правила для созданного ранее профиля доступа:

В папке **ACL** кликните по ссылке **Access Profile Table,** открывая **Access Profile Table**. Появится окно, показанное ниже.

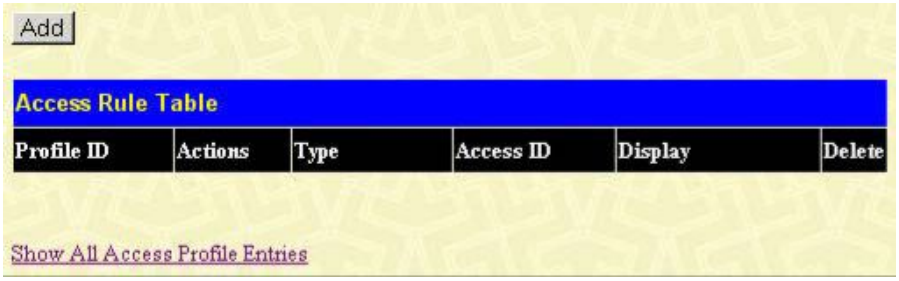


Рисунок 9-6. Окно Access Rule Table

Пользователь может осуществить быстрый поиск настроек определенного профиля доступа, введя его идентификатор в поле Access ID и кликнув Find. Чтобы отобразить все записи Access ID, кликните кнопку View All Entry.

Чтобы создать новое правило для профиля доступа, кликните по кнопке **Modify,** расположенной под заголовком **Access Rule**. Появится окно**,** показанное ниже. Чтобы удалить созданное ранее правило, кликните по соответствующей кнопке ✕.

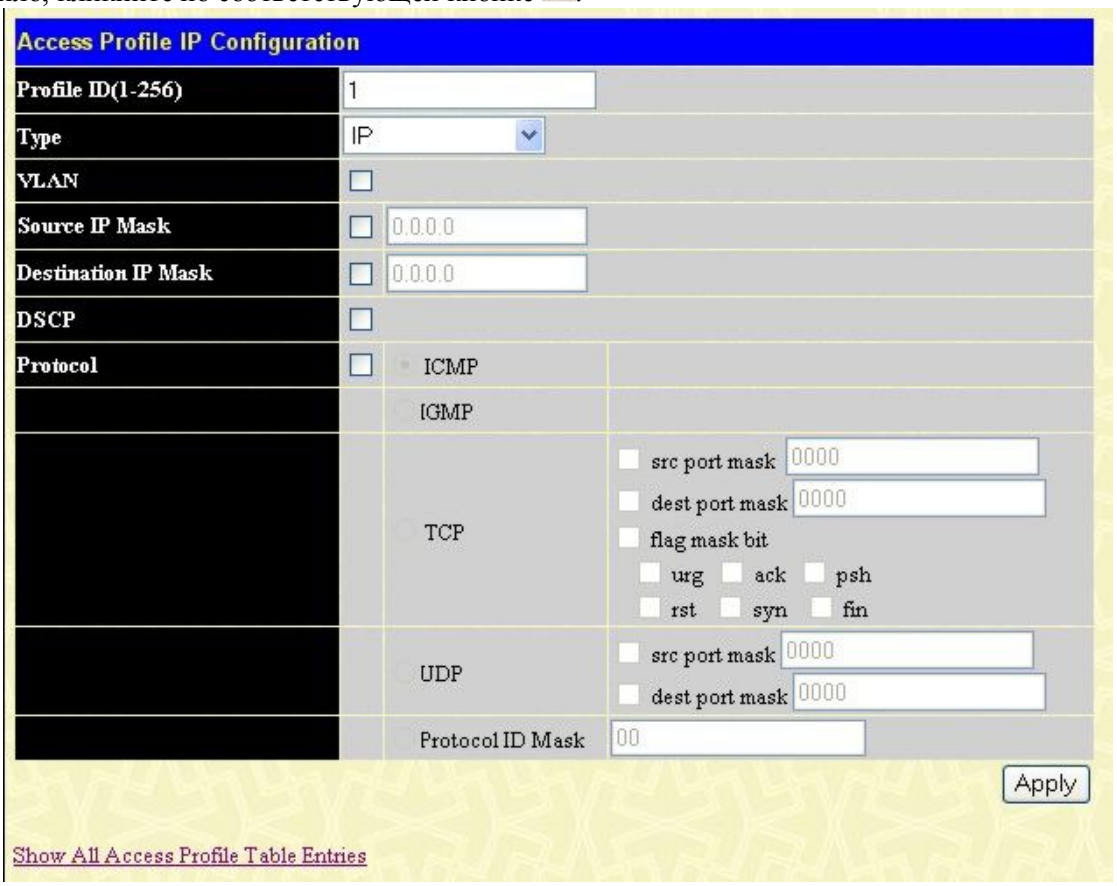


Рисунок 9-7. Окно Access Rule Configuration (IP)

Задайте следующие параметры **Access Rule Configuration** для IP:

Параметр	Описание

Profile ID	Идентификационный номер для данного профиля.
Mode	Выбор опции *Permit* позволяет определить, что пакеты, соответствующие профилю доступа, будут продвигаться Коммутатором в соответствии с добавленным правилом (см. ниже). Выбор опции *Deny* определяет, что пакеты, соответствующие профилю доступа, не будут продвигаться Коммутатором, а будут фильтроваться.
Access ID (1-256)	Введите уникальный идентификационный номер для данного доступа. Данное поле может принимать значение от *1* до *256.* • *Auto Assign* – Если отмечено это поле, то Коммутатор будет автоматически назначать Access ID для созданного правила.
Type	Выбранный профиль на основе *Ethernet* (MAC-адреса), *IP-адреса*, маски содержимого пакета. • *Ethernet* означает, что Коммутатор будет проверять информацию второго уровня в заголовке пакета. • *IP* означает, что Коммутатор будет проверять поле IP-адрес в заголовке каждого фрейма. • *Packet Content Mask* означает, что Коммутатор будет проверять заголовок пакета.
Priority (0-7)	Этот параметр задаётся, если пользователь хочет изменить приоритет по умолчанию 802.1p, предварительно установленный на Коммутаторе и использующийся для определения очереди CoS, в которую будут отправляться пакеты. При задании соответствующего значения в данном поле, пакеты принимаются Коммутатором и в соответствии с их приоритетом направляются в очередь CoS, предварительно определённую пользователем. Для получения более подробной информации об очередях приоритетов, очередях CoS и распределении приоритетов 802.1p, следует обратиться к разделу CoS данного руководства.
Replace Dscp (0-63)	Это поле позволяет пользователю ввести значение DSCP в соответствующее поле, что будет инструктировать Коммутатор проверять поле DiffServ Code в заголовке каждого пакета и использовать эту информацию как единственный или один из критериев для принятия решения о продвижении пакета. Данное поле позволяет ввести значение от 0 до 63, на которое будет заменяться исходное значение DSCP в пакетах, соответствующих выбранным критериям.
Source IP	IP-адрес источника – Введите маску IP-адреса для IP-адреса Источника.
Destination IP	IP-адрес назначения - Введите маску IP-адреса для IP-адреса Назначения.
Dscp (0-63)	Данное поле позволяет пользователю ввести значение DSCP. В этом случае Коммутатор будет проверять поле DiffServ Code в заголовке пакета и использовать его как критерий для принятия решения о продвижении пакета. Пользователь может выбрать значения от 0 до 63.
Protocol	Данное поле дает возможность изменить протокол, используемый таблицей правил доступа, в зависимости от протокола, используемого для таблицы профилей доступа.
Port Number	Введите номера портов, к которым будет применяться правило.

Чтобы просмотреть настройки корректно настроенного ранее правила, кликните кнопку View в Таблице профилей доступа, после чего появится следующее окно:

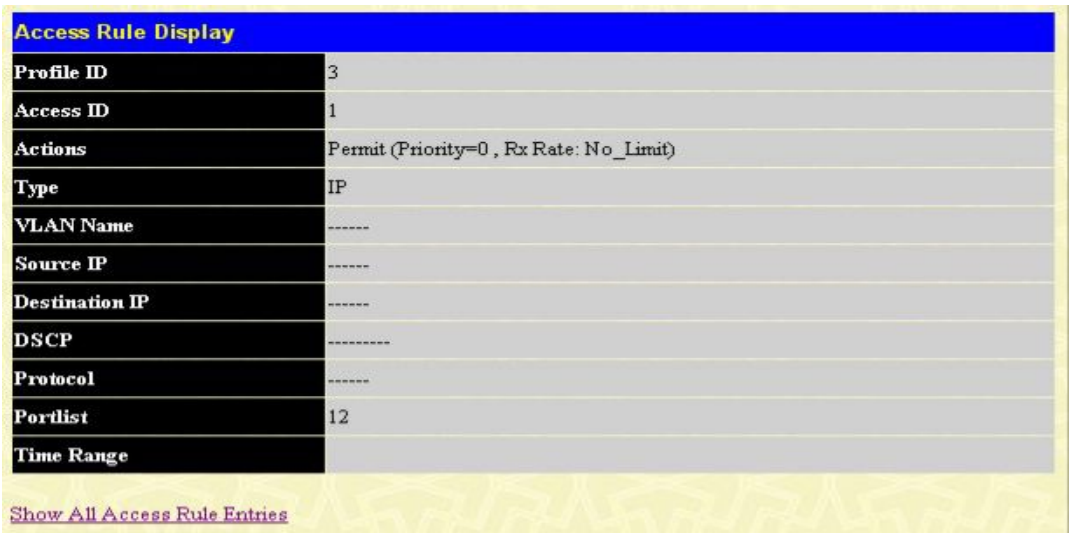


Рисунок 9- 8. Окно Access Rule Display (IP)

Чтобы настроить правило доступа Ethernet, откройте таблицу профилей доступа кликните кнопку **Modify** по соответствующей записи Ethernet. В результате откроется следующее окно:

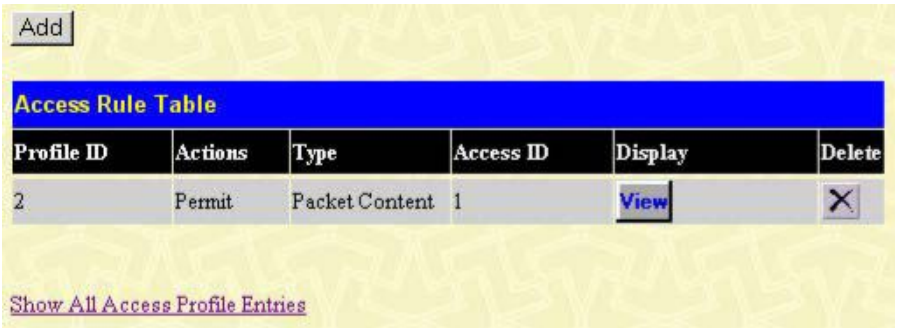


Рисунок 9- 9. Окно Access Rule Table (Ethernet)

Пользователь может осуществить быстрый поиск настроек определенного профиля доступа, введя его идентификатор в поле Access ID и кликнув Find. Чтобы отобразить все записи Access ID, кликните кнопку View All Entry.

Чтобы удалить созданное ранее правило, кликните по соответствующей кнопке .Чтобы создать новое правило для профиля доступа, кликните по кнопке **Add.**

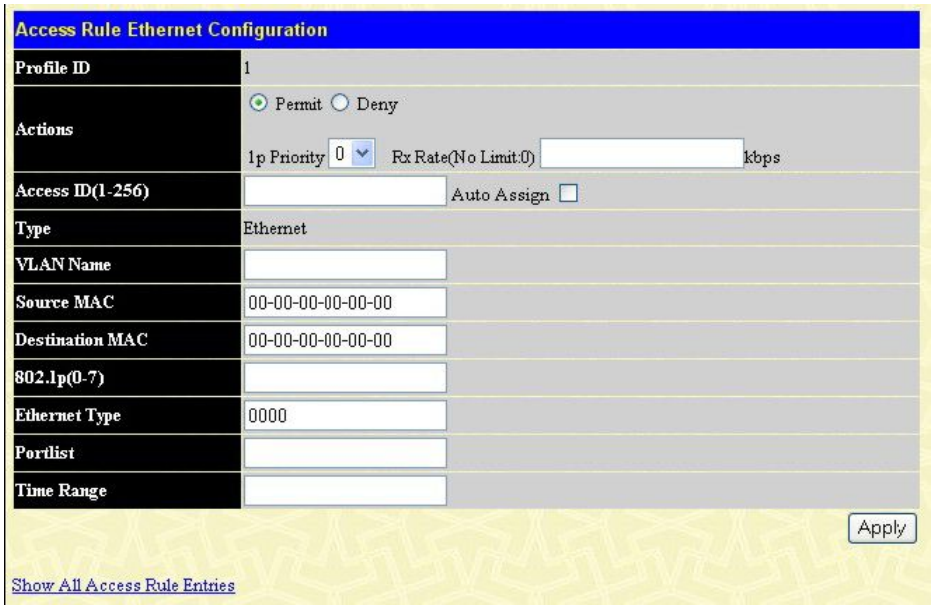


Рисунок 9- 10. Окно Access Rule Configuration(Ethernet)

Чтобы настроить правило доступа для Ethernet, задайте следующие параметры и кликните по **Apply**.

Параметры	Описание
Profile ID	Идентификационный номер для данного профиля.
Mode	Выбор опции *Permit* позволяет определить, что пакеты, соответствующие профилю доступа, будут продвигаться Коммутатором в соответствии с добавленным правилом (см. ниже). Выбор опции *Deny* определяет, что пакеты, соответствующие профилю доступа, не будут продвигаться Коммутатором, а будут фильтроваться.
Access ID	Введите уникальный идентификационный номер для данного доступа. Допустимые значения в данном поле от *1* до *128*. *Auto Assign* – Если поставлена галочка в данном поле, то это будет означать, что Коммутатор будет автоматичски назначать Access ID для создаваемого правила.
Type	Выбранный профиль на основе *Ethernet* (MAC-адреса), *IP-адреса*, *содержимого пакета*. • *Ethernet* означает, что Коммутатор будет проверять информацию второго уровня в заголовке каждого пакета. • *IP* означает, что коммутатор будет проверять IP-адрес в загловке каждого фрейма. • *Packet Content Mask* означает, что коммутатор будет проверять заголовок пакета.
Priority (0-7)	Этот параметр задаётся, если пользователь хочет изменить приоритет по умолчанию 802.1p, предварительно установленный на Коммутаторе и использующийся для определения очереди CoS, в которую будут отправляться пакеты. При задании соответствующего значения в данном поле, пакеты принимаются Коммутатором и в соответствии с их приоритетом

	направляются в очередь CoS, предварительно определённую пользователем. Для получения более подробной информации об очередях приоритетов, очередях CoS и распределении приоритетов 802.1p, следует обратиться к разделу CoS данного руководства.
VLAN Name	Позволяет ввести имя предварительно настроенной VLAN.
Source MAC	Введите MAC-адрес источника.
Destination MAC	Введите MAC-адрес назначения.
Ethernet Type	Определяет, что профиль доступа будет определяться с данным шестнадцатеричным значением 802.1Q Ethernet type (0x0-0xffff) в заголовке пакета. Значение типа Ethernet в шестнадцатеричной форме: 0x0-0xffff, что означает, что пользователь может выбрать любую комбинацию букв a-f и цифр 0-9.
Port Number	Введите номера портов, к которым будет применяться правило.

Чтобы просмотреть настройки корректно настроенного ранее правила, кликните кнопку View в Таблице профилей доступа, после чего появится следующее окно:

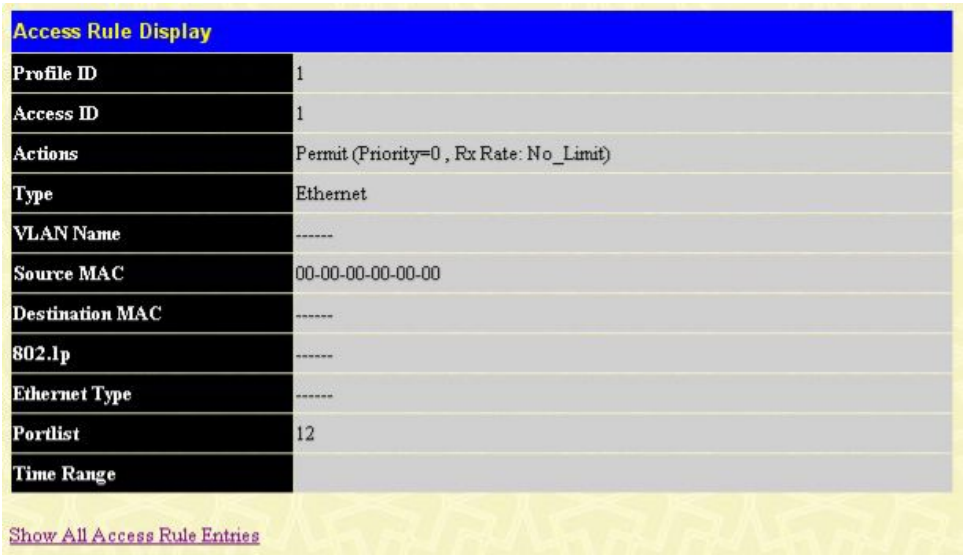


Рисунок 9- 11. Окно Access Rule Display (Ethernet)

Чтобы настроить правило доступа для маски содержимого пакета, откройте таблицу профилей доступа и кликните кнопку **Modify** для записи с маской содержимого пакета. После этого появится таблица правил доступа.

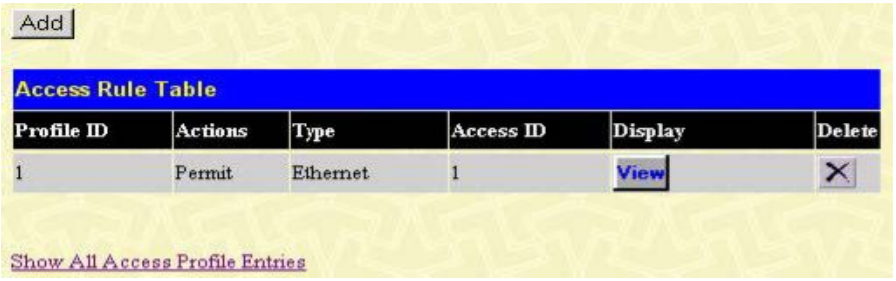


Рисунок 9- 12. Окно Access Rule Table (Packet Content Mask)

Пользователь может осуществить быстрый поиск настроек определенного профиля доступа, введя его идентификатор в поле Access ID и кликнув Find. Чтобы отобразить все записи Access ID, кликните кнопку View All Entry.

Чтобы создать новое правило для профиля доступа, кликните по кнопке **Add**. Чтобы удалить созданное ранее правило, кликните по соответствующей кнопке ✕.

Рисунок 9- 13. Окно Access Rule Packet Content Configuration

Чтобы установить правило доступа для **Packet Content Mask**, настройте следующие параметры и кликните по **Apply**.

Параметр	Описание
Profile ID	Идентификационный номер для данного профиля.
Mode	Выбор опции **Permit** определяет, что пакеты, соответствующие профилю доступа, будут продвигаться Коммутатором в соответствии с дополнительными правилами (см.ниже). Выбор опции **Deny** определяет, что пакеты, соотвествующие профилю доступа, не будут продвигаться Коммутатором, а будут отфильтровываться.
Access ID	Введите уникальный идентификационный номер для данного доступа. Этот параметр может принимать значение от *1* до *128*. **Auto Assign** – Поставив галочку в этом поле, можно настроить автоматическую установку Access ID для создаваемого правила.
Type	Выбранный профиль на основе *Ethernet* (MAC-адреса), *IP-адреса*, содержимого пакета. • *Ethernet* означает, что Коммутатор будет проверять информацию второго уровня в заголовке пакета. • *IP* означает, что Коммутатор будет проверять поле IP-адрес в заголовке

	каждого фрейма. • *Packet Content Mask* означает, что Коммутатор будет проверять заголовок пакета.
Priority (0-7)	Этот параметр задаётся, если пользователь хочет изменить приоритет по умолчанию 802.1p, предварительно установленный на Коммутаторе и использующийся для определения очереди CoS, в которую будут отправляться пакеты. При задании соответствующего значения в данном поле, пакеты принимаются Коммутатором и в соответствии с их приоритетом направляются в очередь CoS, предварительно определённую пользователем. Для получения более подробной информации об очередях приоритетов, очередях CoS и распределении приоритетов 802.1p, следует обратиться к разделу CoS данного руководства.
Offset	Это поле позволяет задать значение бита, с которого будет начинаться маскирование пакета: Можно определить значение от 0 до 76 байт.
Port Number	Введите номера портов, к которым будет применяться правило.

Чтобы просмотреть настройки корректно настроенного ранее правила, кликните кнопку View в Таблице профилей доступа, после чего появится следующее окно:

Рисунок 9- 14. Окно Access Rule Display (Packet Content)

CPU Interface Filtering

Коммутаторы серии DES-30xx оснащены функцией CPU Interface filtering, что позволяет преодолеть некоторые ограничения чипсета, а также обеспечивает дополнительный уровень безопасности. Использование этой функции повышает уровень безопасности работы Коммутатора, благодаря созданию правил управления доступом для пакетов, предназначенных для CPU Коммутатора. Аналогично рассмотренным ранее профилям доступа функция CPU

interface filtering позволяет проверять заголовки пакетов, предназначенных для CPU, на основе Ethernet, IP-адреса или маски содержимого пакета. При этом будет приниматься решение о продвижении или отбрасывании пакетов. Помимо этого Коммутатор позволяет включить или выключить функцию CPU filtering глобально на Коммутаторе, позволяя пользователям создать различные списки правил, не включая их немедленно.
Создание профиля доступа для CPU делится на две основные части. Во-первых, необходимо определить, какую часть или части фреймов Коммутатор будет проверять (например, MAC-адрес источника или IP-адрес назначения). Во-вторых, необходимо задать критерии, которые будет использовать коммутатор для определения, что делать с фреймами.

Настройки статуса CPU Interface Filtering

Следующее окно позволяет пользователю включить или выключить механизм CPU Interface Filtering с помощью выпадающего меню. Для работы с данным окном кликните **ACL > CPU Interface Filtering > CPU Interface Filtering State**. Выберите **Enabled**, чтобы включить проверку пакетов CPU Коммутатора, или **Disabled,** чтобы отключить такую проверку.

Рисунок 9- 15. Окно CPU Interface Filtering State

Таблица профилей CPU Interface Filtering

Кликните **ACL** > **CPU Interface Filtering** > **CPU Interface Filtering Table,** чтобы отобразить таблицу профилей доступа CPU, созданную на Коммутаторе. Для просмотра настроек записи кликните по ссылке соответсвующего **Profile ID**.

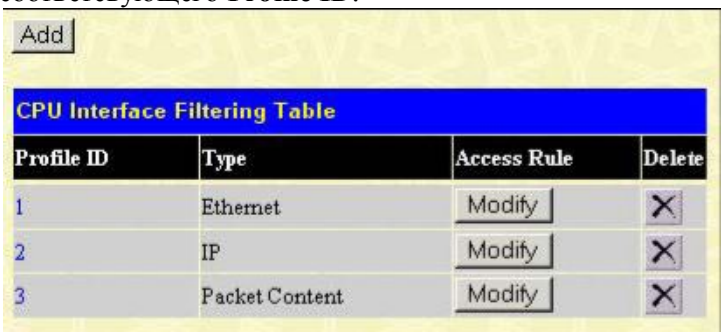


Рисунок 9- 16. Окно CPU Interface Filtering Table

Чтобы добавить запись в таблицу **CPU Interface Filtering Profile Table**, кликните по кнопке **Add**. В результате откроется окно **CPU Interface Filtering Profile Configuration**, как показано ниже. Доступно четыре варианта окон **CPU Access Profile Configuration**: одно для настройки профиля на основе **Ethernet** (на основе MAC-адреса), одно для настройки профиля на основе **IP**-адреса и одно для настройки профиля на основе маски содержимого пакета (**Packet Content Mask)**. Переключение между четырьмя окнами **CPU Access Profile Configuration** осуществляется с помощью выпадающего меню **Type**. Ниже показана страница **CPU Interface Filtering Configuration** при выборе в поле **Type** значения **Ethernet**.

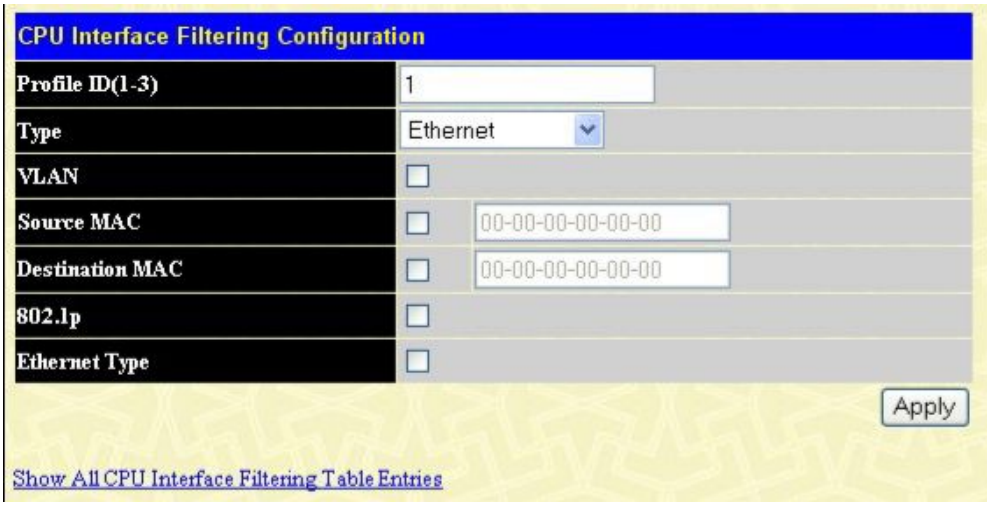


Рисунок 9- 17. Окно CPU Interface Filtering Configuration – Ethernet

Параметр	Описание
Profile ID (1-3)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Значение этого поля может быть от 1 до 3.
Type	Это поле позволяет выбрать тип профиля: на основе Ethernet (MAC-адресов), на основе IP-адресов или на основе маски содержимого пакета. В зависимости от выбранного типа профиля будут предложены соответствующие параметры для настройки: • Выбор в данном поле *Ethernet* означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. • Выбор в данном поле *IP* означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Выбор в данном поле *Packet Content Mask* означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
VLAN	Выбор данной опции означает, что Коммутатор будет проверять идентификатор VLAN в заголовке каждого пакета и использовать полученную информацию как единственный или один из критериев для принятия решения о продвижении пакета.
Source MAC	В случае необходимости, поставив галочку в данном поле, введите MAC-адрес источника.
Destination MAC	В случае необходимости, поставив галочку в данном поле, введите MAC-адрес назначения.
Ethernet type	При выборе данной опции Коммутатор будет проверять значение поля Ethernet type в каждом заголовке пакетов.

Кликните по **Apply,** чтобы ввести данную запись в память Коммутатора.

Ниже показана страница **CPU Interface Filtering Profile Configuration** при выборе в поле **Type** значения **IP**.

Рисунок 9-18. Окно CPU Interface Filtering Configuration (IP)

Для настройки доступны следующие параметры:

Параметр	Описание
Profile ID (1-3)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Значение этого поля может быть от 1 до 3.
Type	Это поле позволяет выбрать тип профиля: на основе Ethernet (MAC-адресов), на основе IP-адресов или на основе маски содержимого пакета. В зависимости от выбранного типа профиля будут предложены соответствующие параметры для настройки: • Выбор в данном поле *Ethernet* означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. • Выбор в данном поле *IP* означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Выбор в данном поле *Packet Content Mask* означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
VLAN	Выбор данной опции означает, что Коммутатор будет проверять идентификатор VLAN в заголовке каждого пакета и использовать полученную информацию как единственный или один из критериев для принятия решения о продвижении пакета.
Source IP Mask	В случае необходимости, поставив галочку в данном поле, введите маску источника.
Destination IP Mask	В случае необходимости, поставив галочку в данном поле, введите маску назначения.
DSCP	При выборе данной опции Коммутатор будет проверять поле DiffServ Code в заголовках пакетов и использовать его как критерий при принятии

	решения о продвижении пакета.
Protocol	При выборе данной опции Коммутатор будет проверять поле типа проткола в заголовках пакетов. Далее необходимо выбрать нужный тип протокола, руководствуясь следующими принципами: При выборе опции *ICMP*- Коммутатор будет проверять заголовки пакетов на наличие Internet Control Message Protocol (ICMP) • Поставьте галочку в поле **Type,** чтобы задать, что для принятия решения будет использоваться ICMP type . Если поставить галочку в поле **Code,** то для принятия решения о продвижении пакета в профиле доступа будет использоваться поле ICMP code. При выборе опции *IGMP* Коммутатор будет проверять заголовки пакетов на наличие Internet Group Management Protocol (IGMP) • Поставьте галочку в поле **Type,** чтобы задать, что для принятия решения будет использоваться IGMP type. При выборе опции *TCP* в качестве критерия при продвижении пакетов будет использоваться номер TCP-порта, указанный в исходящем пакете. При этом необходимо, чтобы пользователь указал маску порта источника и /или маску порта назначения. Пользователь может также задать запрещенные биты флага (часть пакета, определяющая действие над пакетом). Запретив соответствующие биты флага в области TCP, пользователь может запретить таким образом и сами пакеты. Так, пользователь может запретить следующие виды пакетов: urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish). Для этого необходимо поставить галочку в соответствующем поле. • *src port mask* – задает в шеснадцатиричной форме (0x0-0xffff) маску TCP-порта источника, пакеты от которого будут отброшены. • *dest port mask* - определяет в шеснадцатиричной форме (0x0-0xffff) маску TCP-порта назначения, пакеты на который будут отброшены. При выборе опции *UDP* в качестве критерия при продвижении пакетов будет использоваться номер UDP-порта, указанный в исходящем пакете. При этом необходимо, чтобы пользователь указал маску порта источника и /или маску порта назначения. • *src port mask* – задает в шеснадцатиричной форме (0x0-0xffff) маску UDP-порта источника, пакеты от которого будут отброшены. • *dest port mask* - определяет в шеснадцатиричной форме (0x0-0xffff) маску UDP-порта назначения, пакеты на который будут отброшены. *protocol id* – идентификатор протокола, используемый для маски в заголовке пакета. Можно задать маску идентификатора протокола в шестнадцатиричной форме (0x0-0xff).

Кликните по **Apply,** чтобы добавить запись в память Коммутатора.

Ниже показано окно **CPU Interface Filtering Profile Configuration** при выборе в поле **Type** значения **Packet Content Mask**.

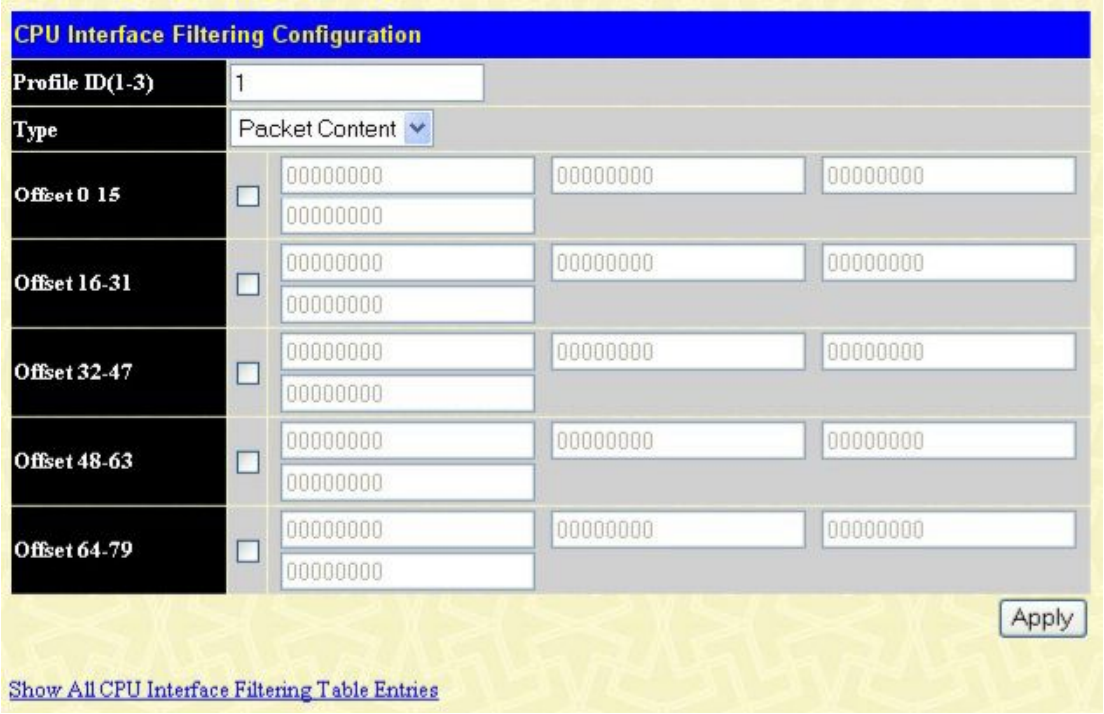


Рисунок 9- 19. Окно CPU Interface Filtering Configuration - Packet Content

Это окно позволяет пользователю Коммутатора маскировать заголовок пакета, начиная с определённого бита. При выборе в поле Type значения **Packet Content Mask** могут быть настроены следующие параметры:

Параметр	Описание
Profile ID (1-3)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Значение этого поля может быть от 1 до 3.
Type	Это поле позволяет выбрать тип профиля: на основе Ethernet (MAC-адресов), на основе IP-адресов или на основе маски содержимого пакета. В зависимости от выбранного типа профиля будут предложены соответствующие параметры для настройки: • Выбор в данном поле *Ethernet* означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. • Выбор в данном поле *IP* означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Выбор в данном поле *Packet Content Mask* означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
Offset	Это поле указывает, с какого байта начнется маскирование заголовка пакетов. • value (0-15) – следует задать значение в шестнадцатеричной форме для маскирования пакета с начала до 15-го байта. • value (16-31) – следует задать значение в шестнадцатеричной форме для маскирования пакета с 16 по 31 байт. • value (32-47) -следует задать значение в шестнадцатеричной форме для маскирования пакета с 32 по 47 байт. • value (48-63) -следует задать значение в шестнадцатеричной

	форме для маскирования пакета с 48 по 63 байт. • value *(64-79)* - следует задать значение в шестнадцатеричной форме для маскирования пакета с 64 по 79 байт.

Кликните по **Apply** для применения выполненных изменений.

Для установки правила для созданного ранее профиля доступа CPU:

В папке **ACL** кликните по **CPU Interface Filtering.** В результате откроется окно **CPU Interface Filtering Profile Table**.

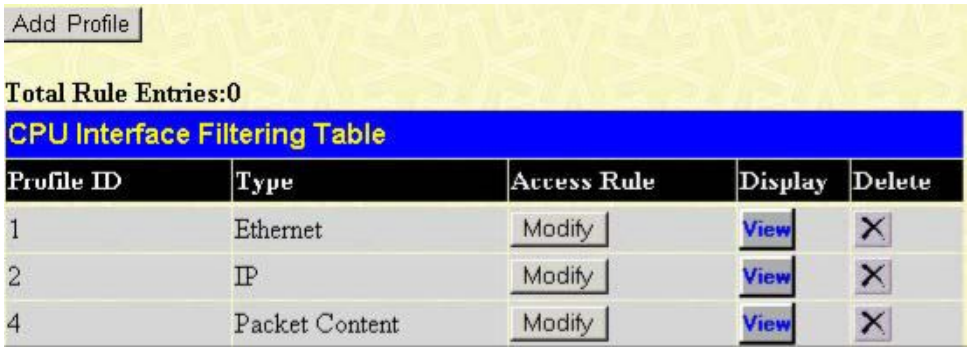


Рисунок 9- 20. Окно CPU Interface Filtering Profile Table - Add

В данном окне пользователь может добавить правило в созданный ранее профиль доступа CPU, кликнув по кнопке **Modify** для записи **Ethernet, IP** или **Packet Content Mask**.

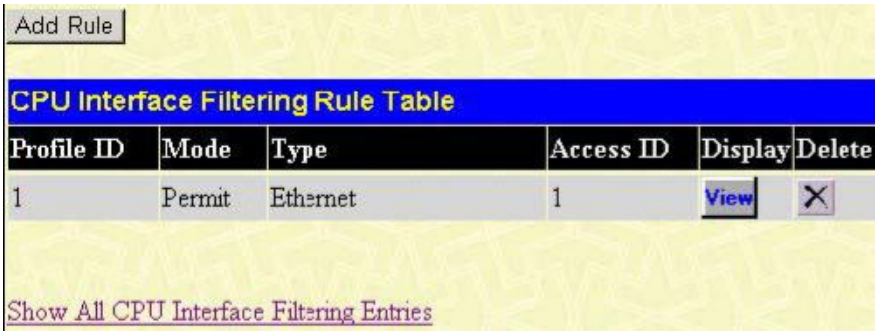


Рисунок 9- 21. Окно CPU Interface Filtering Rule Table

Кликните по кнопке **Add Rule**, чтобы добавить запись в таблицу **CPU Interface Filtering Rule Table**. В зависимости от выбранного типа (Ethernet, IP, Packet Content и IPv6) откроется соответствующее окно, как показано ниже.

Для изменения ранее созданного правила профиля доступа CPU:

Окно **CPU Interface Filtering Rule Configuration** позволяет настроить правило для созданного ранее профиля доступа CPU.

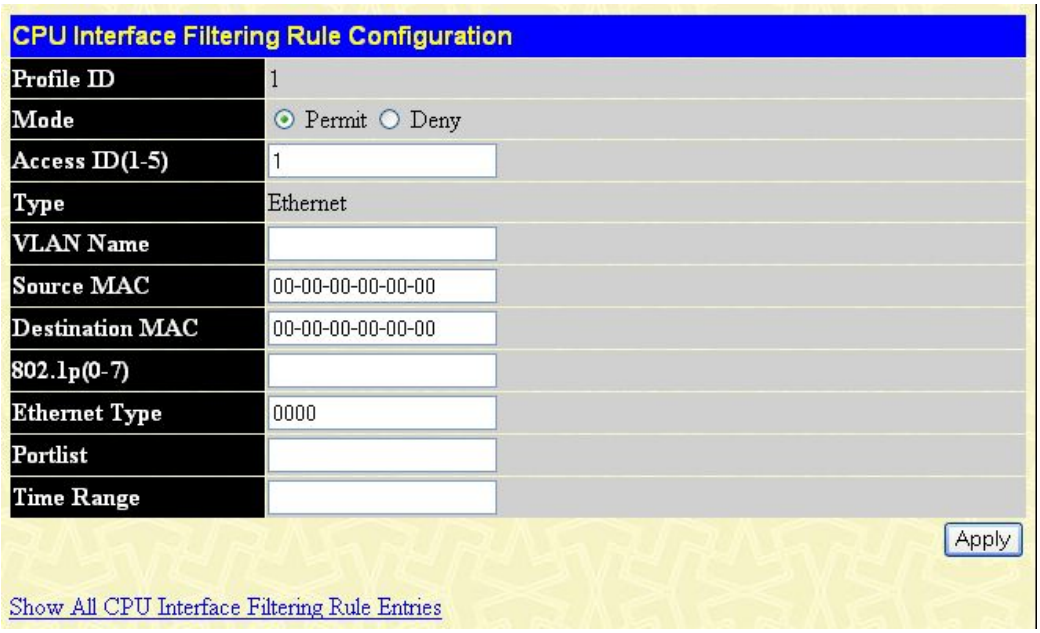


Рисунок 9- 22. Окно CPU Interface Filtering Rule Configuration – Ethernet

Для настройки правила доступа к CPU для профиля доступа на основе Ethernet необходимо задать следующие параметры и кликнуть **Apply**.

Параметр	Описание
Profile ID	Идентификационный номер профиля, доступный только для чтения.
Mode	Выбор опции *Permit* означает, что Коммутатор, следуя указанному правилу, будет продвигать пакеты, которые соответствуют добавленному профилю доступа (см. ниже). Значение *Deny* означает, что пакеты, соответствующие профилю доступа, не будут продвигаться Коммутатором, а будут отбрасываться.
Access ID	Здесь следует ввести уникальный идентификационный номер. В данном поле могут быть установлены значения от *1* до *5*.
Type	Это поле отображает тип профиля: на основе Ethernet (MAC-адресов), на основе IP-адресов или на основе маски содержимого пакета. • Значение *Ethernet* в данном поле означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. • Значение *IP* в данном поле означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Значение *Packet Content Mask* в данном поле означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
VLAN Name	Данное поле позволяет ввести имя ранее сконфигурированной VLAN.
Source MAC	Здесь следует задать MAC-адрес источника.
Destination MAC	Здесь следует задать MAC-адрес назначения.
802.1p (0-7)	Это поле позволяет задать приоритет 802.1p (значение от 0 до 7), что позволит принимать пакеты только с таким приоритетом 802.1p.
Ethernet Type	Это поле позволяет задать значение Ethernet type 802.1Q (hex 0x0-0xffff) в шестнадцатеричном виде, при обнаружении которого в заголовке пакета к

	данному пакету будет применяться профиль доступа. Поле Ethernet type может принимать значение hex 0x0-0xffff, что означает, что пользователь может выбрать любую комбинацию из букв a-f и чисел 0-9.
Port	Правило доступа CPU может быть также настроено только для отдельных портов путем ввода в данном поле номера порта Коммутатора.
Time Range	Поставьте галочку в соответствующем поле и введите имя временного диапазона, настроенное ранее в окне **Time Range**. Это позволяет установить определенное время, когда правило доступа CPU будет применяться на Коммутаторе.

Чтобы просмотреть настройки настроенного ранее правила, кликните по кнопке View в **Access Rule Table.** В результате появится следующее окно:

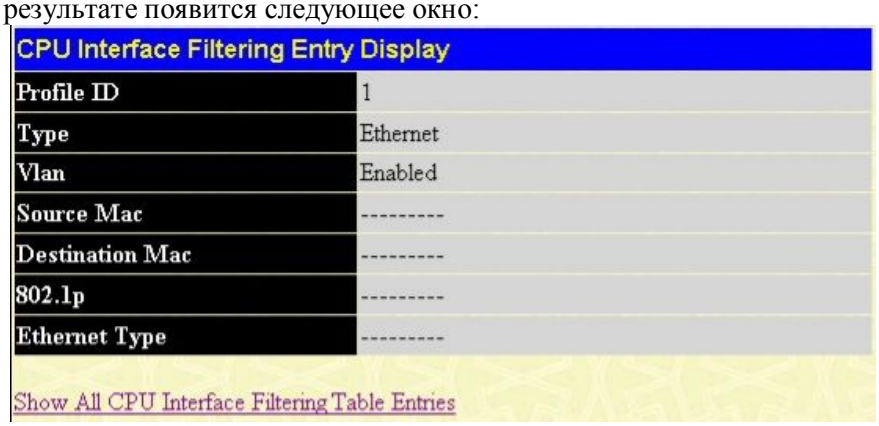


Рисунок 9- 23. Окно CPU Interface Filtering Entry Display – Ethernet

Ниже показано окно **CPU Interface Filtering Rule Table** (Type = IP).

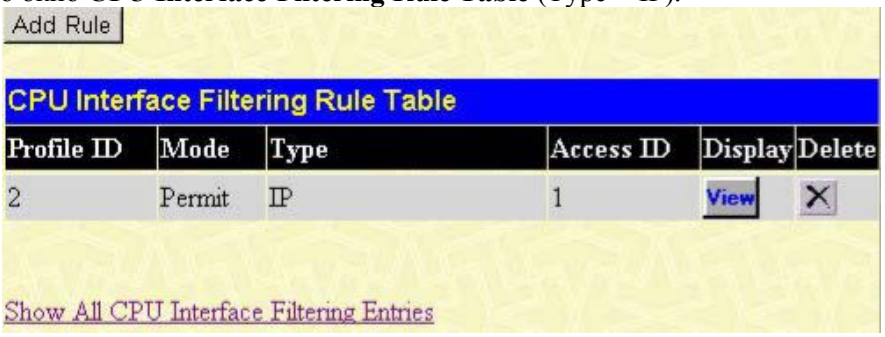


Рисунок 9- 24. Окно CPU Interface Filtering Rule Table– IP

Для создания нового правила для профиля доступа кликните по кнопке **Add**. Будет отображено новое окно. Чтобы удалить созданное ранее правило, кликните по соответствующей кнопке . Следующее окно позволяет настроить IP-правило CPU.

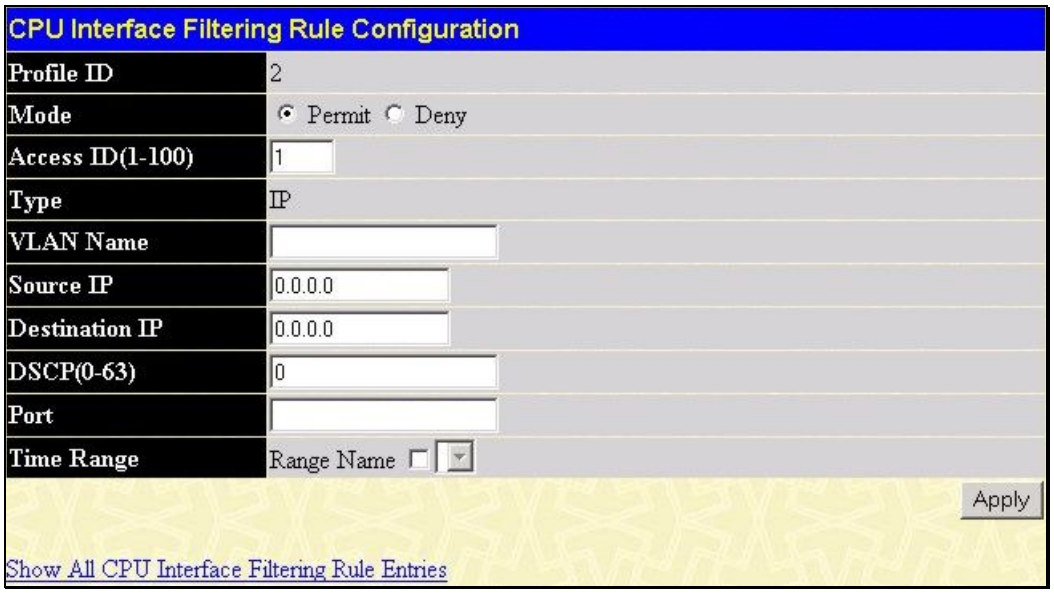


Рисунок 9- 25. Окно CPU Interface Filtering Rule Configuration – IP

В данном окне для настройки доступны следующие параметры **Access Rule Configuration**:

Параметр	Описание
Profile ID	Идентификационный номер профиля, доступный только для чтения.
Mode	Выбор опции *Permit* означает, что Коммутатор, следуя указанному правилу, будет продвигать пакеты, которые соответствуют добавленному профилю доступа (см. ниже). Значение *Deny* означает, что пакеты, соответствующие профилю доступа, не будут продвигаться Коммутатором, а будут отбрасываться.
Access ID	Здесь следует ввести уникальный идентификационный номер. В данном поле могут быть установлены значения от *1* до *5*.
Type	Это поле отображает тип профиля: на основе Ethernet (MAC-адресов), на основе IP-адресов или на основе маски содержимого пакета. • Значение *Ethernet* в данном поле означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. • Значение *IP* в данном поле означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Значение Packet Content Mask в данном поле означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.
VLAN Name	Данное поле позволяет ввести имя ранее сконфигурированной VLAN.
Source IP	Здесь следует задать IP-адреса источника.
Destination IP	Здесь следует задать IP-адреса назначения.
Dscp (0-63)	Данное поле позволяет пользователю ввести значение DSCP. В этом случае Коммутатор будет проверять поле DiffServ Code в заголовке пакета и использовать его как критерий для принятия решения о продвижении пакета. Пользователь может выбрать значения от 0 до 63.
Port	Правило доступа CPU может быть также настроено только для отдельных

	портов путем ввода в данном поле номера порта Коммутатора.
Time Range	Поставьте галочку в соответствующем поле и введите имя временного диапазона, настроенное ранее в окне **Time Range**. Это позволяет установить определенное время, когда правило доступа CPU будет применяться на Коммутаторе.

Для просмотра созданного ранее правила кликните по кнопке View в таблице **Access Rule Table**. Появится следующее окно:

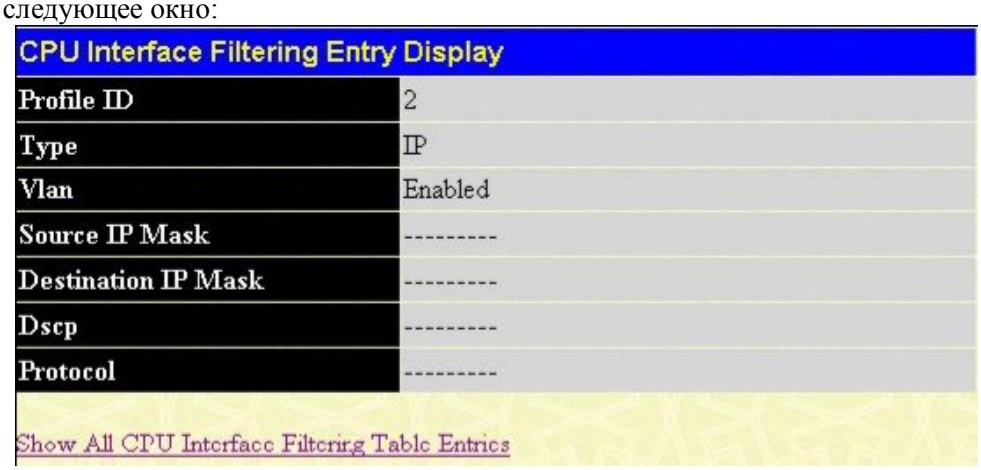


Рисунок 9- 26. Окно CPU Interface Filtering Entry Display - IP

Следующее окно **CPU Interface Filtering Rule Table** при использовании критерия содержимого пакета (Packet Content).

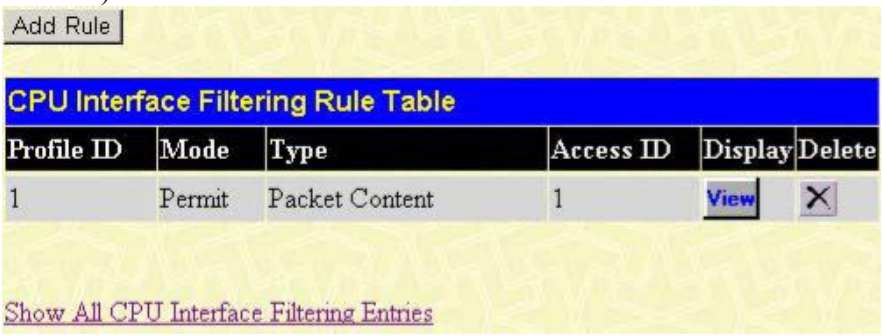


Рисунок 9- 27. Окно CPU Interface Filtering Rule Table – Packet Content

Чтобы удалить созданное ранее правило, выберите его и кликните по кнопке . Чтобы добавить новое правило доступа CPU, кликните по кнопке **Add**:

Рисунок 9- 28. Окно CPU Interface Filtering Rule Configuration - Packet Content Mask

Чтобы настроить правило доступа Ethernet, необходимо настроить следующие параметры и кликнуть по **Apply**.

Параметр	Описание
Profile ID	В этом поле отображается идентификационный номер профиля
Mode	Выбор опции *Permit* означает, что пакеты, соответствующие профилю доступа, будут продвигаться Коммутатором в соответствии с добавленными правилами (см. ниже). Выбор опции *Deny* означает, что пакеты, соответствующие профилю доступа, не будут продвигаться Коммутатором, а будут отфильтровываться.
Access ID	Введите уникальный идентификационный номер для данного доступа. Допустимый диапазон значения от *1* до *5*.
Type	Это поле отображает тип профиля: на основе Ethernet (MAC-адресов), на основе IP-адресов или на основе маски содержимого пакета. • Значение *Ethernet* в данном поле означает, что Коммутатор будет проверять заголовки пакетов 2-го уровня. • Значение *IP* в данном поле означает, что Коммутатор будет проверять IP-адрес в каждом заголовке фрейма. • Значение Packet Content Mask в данном поле означает, что Коммутатор будет выделять маску, содержащуюся в заголовке пакета.

Offset	Это поле указывает, с какого байта начнется маскирование заголовка пакетов. • *value (0-15)* – следует задать значение в шестнадцатиричной форме для маскирования пакета с начала до 15-го байта. • *value (16-31)* – следует задать значение в шестнадцатиричной форме для маскирования пакета с 16 по 31 байт. • *value (32-47)* -следует задать значение в шестнадцатиричной форме для маскирования пакета с 32 по 47 байт. • *value (48-63)* -следует задать значение в шестнадцатиричной форме для маскирования пакета с 48 по 63 байт. • *value (64-79)* - следует задать значение в шестнадцатиричной форме для маскирования пакета с 64 по 79 байт.
Port	Правило доступа CPU может быть также настроено только для отдельных портов путем ввода в данном поле номера порта Коммутатора.
Time Range	Поставьте галочку в соответствующем поле и введите имя временного диапазона, настроенное ранее в окне **Time Range**. Это позволяет установить определенное время, когда правило доступа CPU будет применяться на Коммутаторе.

Чтобы просмотреть настройки корреткно заданного ранее правила, кликните по кнопке View в таблице **Access Rule Table,** после чего появится следующее окно:

CPU Interface Filtering Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	Packet Content
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	---------
Offset 32-47	---------
Offset 48-63	---------
Offset 64-79	---------
Port	2
Time Range	Darren

Show All CPU Interface Filtering Rule Entries

Рисунок 9- 29. Окно CPU Interface Filtering Rule Display – Packet Content

Раздел 10

Безопасность

Управление трафиком
Port Security (Безопасность на уровне портов)
Таблица Port Lock Entries
SSL
SSH
802.1X
Доверенный хост (Trusted Host)
Управление аутентификацией доступа
Сегментация трафика

Управление трафиком

Многоадресные и широковещательные пакеты передаются по сети в больших количествах даже в нормальном режиме работы. Однако иногда такой трафик резко возрастает из-за хостов злоумышленников в сети или неработающих устройств, например, адаптера. Таким образом, увеличиваются проблемы с пропускной способностью Коммутатора, что, в конечном счете, может влиять на производительность всей сети. Для предотвращения пакетного шторма необходимо, чтобы Коммутатор отслеживал и контролировал ситуацию.

Отслеживание пакетного шторма позволяет определить, что в сети циркулирует слишком много пакетов. Коммутатор судит о количестве пакетов на основании пороговых величин, заданных пользователем. При обнаружении пакетного шторма Коммутатор будет отбрасывать поступающие на него пакеты до тех пор, пока пакетный шторм не прекратится. Для этого необходимо выбрать опцию **Drop** в поле **Action** показанного справа окна.

Коммутатор также сканирует и отслеживает поступающие на него пакеты с помощью счетчика микросхемы. Такой метод может быть использован только для предотвращения многоадресного и широковещательного шторма, поскольку на микросхеме предусмотрены счетчики только для таких пакетов. При обнаружении шторма (т.е. превышении установленной пороговой величины), Коммутатор закроет порты для входящего трафика, за исключением пакетов STP BPDU. Порты будут закрыты на период времени, заданный в поле CountDown.

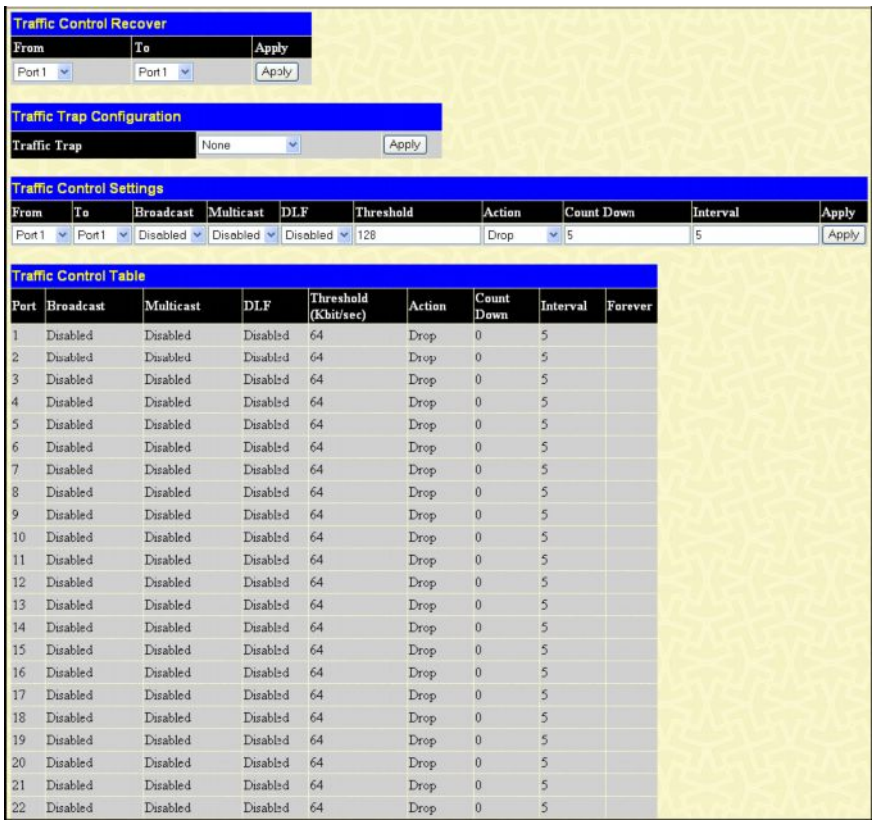


Рисунок 10- 1. Окно Traffic Control Settings

Если по истечении этого времени пакетный шторм продолжается, порт перейдет в режим **Shutdown Forever,** и будет сформировано и отправлено специальное предупреждающее сообщение. При этом порт можно будет подключить только вручную, зайдя в папку **Administration** окно **Port Configuration**, выбрав этот порт и присвоив ему статус Enabled (включено). Для использования такого варианта управления штормом необходимо выбрать опцию **Shutdown** в поле **Action** в показанном ниже окне. Для работы с данным окном кликните **Security > Traffic Control**.

Пользователь может установить следующие параметры:

Параметр	Описание
Traffic Control Recover	
From… To	Выберите порты для восстановления.
Traffic Trap Configuration	
Traffic Trap	Позволяет задать настройки отправления сообщений (Trap) при возникновении событий, касающихся шторма. Возможен выбор следующих опций: *None* – Не будет отправлять предупреждающие сообщения о шторме, независимо от события, обнаруженного механизмом управления трафиком. *Storm Occurred* – Предупреждающее сообщение о шторме будет отправляться только при обнаружении шторма. *Storm Cleared* – Предупреждающее сообщение будет отправляться только после того, как Коммутатор справился с широковещательным штормом. *Both* – Предупреждающие сообщения будут отправляться, как при обнаружении шторма, так и при его прекращении. Эта функция не может использоваться, когда используется механизм обнаружения шторма на основе аппаратного обеспечения (т.е. выбрана опция **Drop** в поле **Action**).
Traffic Control Settings	

From…To	Выберите порты на Коммутаторе для настройки функции управления штормом с помощью данных выпадающих меню.
Broadcast	Позволяет включить или выключить управление широковещательным штормом.
Multicast	Позволяет включить или выключить управление многадресным штормом.
DLF	Включает или выключает управление штормом Destination Lookup Failure (DLF). (не доступно для управления штормом на на основе программного обеспечения {Shutdown}).
Threshold	Определяет максимальное число пакетов в секунду, при котором будет активизироваться функция управления трафиком.
Action	Выберите метод управления трафиком в выпадающем меню. Доступны следующие опции: *Drop* – использует механизм управления трафиком на основе аппаратного обеспечения, что означает, что Коммутатор на аппаратном уровне будет определять возникновение пакетного шторма на основе заданного значения порога и отбрасывать пакеты, пока проблема не будет решена. *Shutdown* – использует механизм управления трафиком на основе прогаммного обеспечения. При обнаружении порт будет запрещать весь входящий трафик на порт, кроме пакетов STP BPDU, которые заинтересованы в подержании работоспособности Spanning Tree operational на Коммутаторе. Если таймер Countdown истек, а пакетный шторм продолжается, порт переводится в режим Shutdown Forever и больше не работает, пока пользователь не сбросит порт вручную с помощью настройки Storm Control Recover в верхней части окна. Выбор данной опции обязывает пользователя задать также значение в поле Interval, который будет обеспечивать выборку счетчиков пакетов с чипа Коммутатора для определения возникновения пакетного шторма.
Count Down	Таймер Count Down определяет время в минутах, которое Коммутатор будет ждать до закрытия порта, на котором обнаружен шторм трафика. Этот параметр оказывается полезным только для портов, настроенных как Shutdown в поле Action. Поэтому этот параметр не может использоваться для управления трафиком на основе аппаратного обеспечения. В данном поле может быть установлено значение *0*, *5 до 30* минут. *0* – настройка по умолчанию для данного поля, и *0* означает, что данный порт никогда не будет переходить в состояние Shutdown.
Interval	Интервал устанавливает время между количеством многоадресных и широковещательных пакетов, отправляемых с чипа коммутатора на функцию управления трафиком. Эти количества пакетов являются определяющим фактом при принятии решения при превышении входящими пакетами порогового значения. Допустимо установить интервал от *5* до *30* секунд, по умолчанию задано *5* секунд.

Кликните по **Apply** для применения выполненных настроек.

ПРИМЕЧАНИЕ: Управление трафиком не может быть реализовано на портах, на которых настроено агрегирование каналов.

ПРИМЕЧАНИЕ: Порты в режиме Shutdown forever будут иметь статус Discarding в окнах Spanning Tree, и приложения, работающие через данные порты, будут продвигать BPDU-пакеты на CPU Коммутатора.

ПРИМЕЧАНИЕ: Порты, находящиеся в режиме Shutdown Forever, будут иметь статус link down, пока пользователь не восстановит эти порты.

Port Security (Безопасность на уровне портов)

Настройка функции Port Security позволяет заблокировать динамическое изучение MAC-адресов для заданных портов (или диапазона портов). А результате текущие MAC-адреса, введённые в таблицу MAC-адресов, не могут быть изменены до тех пор, пока блокировка порта активна. Для этого необходимо выбрать в выпадающем меню поля **Admin State** значение *Enabled* и кликнуть по **Apply,** закрыв тем самым порт.

Другими словами, Port Security – это функция безопасности, которая предотвращает подключение к заблокированным портам коммутатора неавторизованных компьютеров (с MAC-адресами источников, неизвестными компьютеру до блокировки порта или портов) и получении ими доступа к сети. Для работы со следующим окном откройте папку **Security** и кликните по **Port Security**.

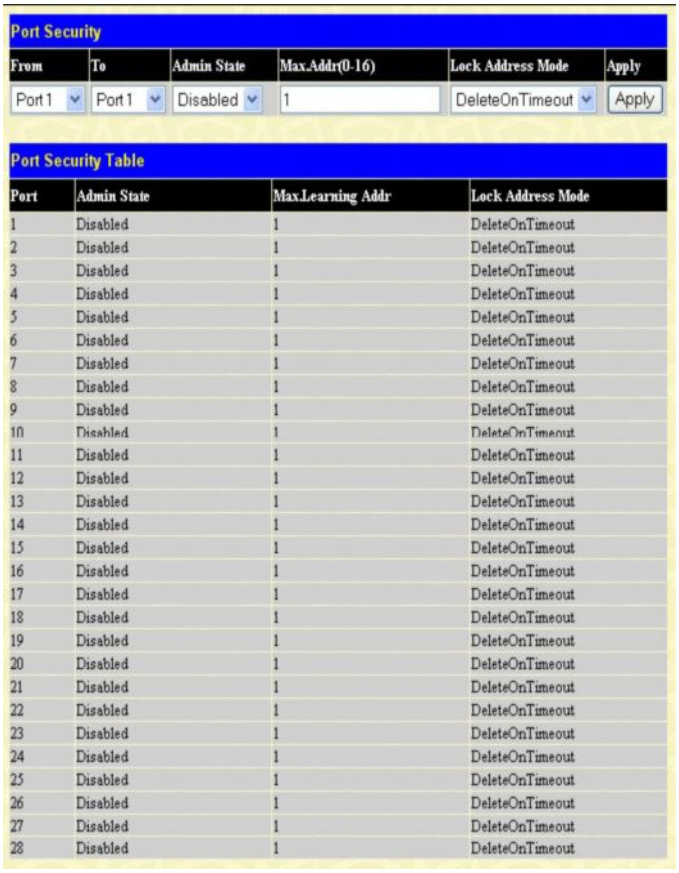


Рисунок 10- 1. Окно Port Security

Могут быть установлены следующие параметры:

Параметр	Описание
From/To	Эти выпадающие меню позволяют выбрать диапазон портов, для которых будет применяться настройка.
Admin State	Данное выпадающее меню позволяет включить/выключить функцию Port Security (закрывает таблицу MAC-адресов для помеченного порта).
Max. Learning Addr. (0-16)	Допустимое количество MAC-адресов в таблице Коммутатора для выбранной группы портов.
Lock Address Mode	Это выпадающее меню позволяет настроить режим работы таблицы блокировки MAC-адресов для выбранной группы портов: *Permanent* – заблокированные адреса не будут устаревать после истечения таймера. *DeleteOnTimeout* – заблокированные адреса будут устаревать после истечения таймера. *DeleteOnReset* – заблокированные адреса не будут устаревать до тех пор, пока Коммутатор не будет перегружен.

Кликните по **Apply** для применения выполненных изменений.

Таблица Port Lock Entries

Окно **Port Lock Entries Table** позволяет удалить запись из таблицы port security, изученной Коммутатором и ввести в базу данных продвижения пакетов. Для работы со следующим окном кликните **Security > Port Lock Entries**:

Рисунок 10- 3. Окно Port Lock Entries

Эта функция может работать только в том случае, когда в поле **Mode** окна **Port Security** выбрано значение **Permanent** или **DeleteOnReset.** Другими словами, только адреса, которые постоянно изучены Коммутатором, могут быть удалены. Когда запись определена путем ввода корректной информации в окне выше, кликните по значку ✕ под заголовком **Delete** соотвествующего MAC-адреса. Только записи, отмеченные *Secured_Permanent,* могут быть удалены. Кликните по кнопке **Next,** после чего появится следующая страница, параметры которой приведены в таблице. В этом окне содержится следующая информация:

Параметр	Описание
VID	VLAN ID записи в базе данных продвижения пакетов, которые были постоянно изучены Коммутатором.
VLAN Name	Имя VLAN для записи в таблице продвижения пакетов, которые были постоянно изучены Коммутатором.
MAC Address	MAC-адрес записи в таблице продвижения пакетов, которые были постоянно изучены Коммутатором.
Port	Идентификационный номер порта с постоянно изученным MAC-адресом.
Type	Тип MAC-адреса в таблице продвижения пакетов. Только записи, отмеченные *Secured_Permanent,* могут быть удалены.
Delete	Кликните по значку ✕ в данном поле, чтобы удалить соответствующий MAC-адрес, который был постоянно изучен Коммутатором.

Secure Socket Layer (SSL)

Secure Sockets Layer (SSL) – протокол, который обеспечивает безопасное взаимодействие между хостом и клиентом с помощью использования аутентификации, цифровых подписей и шифрования. Эти функции безопасности осуществляются с помощью *ciphersuite*. *Ciphersuite* – это строка, определяющая точные параметры шифрования, алгоритм шифрования и длину ключей, которые используются для аутентификации. C*iphersuite* состоит из трех частей:

1. **Ключ обмена (Key Exchange)**: в первой части строки cyphersuite задается используемый алгоритм открытого ключа. Коммутатор поддерживает Rivest Shamir Adleman (RSA)-алгоритм открытого ключа и Digital Signature Algorithm (DSA) – цифровую подпись -здесь используется алгоритм открытого ключа DHE DSS Diffie-Hellman (DHE). Это первая часть процесса аутентификации между хостом и клиентом, таким образом, они обмениваются ключами в поиске подходящих и установления подлинности, для того чтобы перейти к шифрованию на следующем уровне.
2. **Шифрование (Encryption)**: вторая часть *cyphersuite* задает метод шифрования, используемый для шифрования сообщения между хостом и клиентом. Коммутатор поддерживает два типа алгоритма шифрования:

- **Шифры Steam Ciphers**. В коммутаторе присутствует два типа Steam Ciphers RC4 с 40-битным ключом и RC4 со 128-битным ключом. Эти ключи используются для шифрования сообщений и должны быть одинаковы для хоста и клиента.

- **Шифры CBC Block Ciphers.** При выборе этого алгоритма зашифрованный ранее блок текста используется в шифровании текущего блока. Коммутатор поддерживает шифрование 3 DES EDE, определённое стандартом Data Encryption Standart (DES).

3. **Hash Algoritm**. Эта часть *cyphersuite* позволяет определить Message Authentification Code (код аутентификации сообщения). Этот код будет зашифрован вместе с передаваемым сообщением для того, чтобы обеспечить целостность сообщения и предотвратить взлом

защиты путём замещения оригинала. Коммутатор поддерживает два типа Hash algoritm: MD5 (Message Diggest 5) и SHA (Secure Hash Algoritm).

Эти три параметра позволяют создать трёхуровневый алгоритм шифрования для безопасной коммуникации между сервером и хостом. Пользователь может выбрать как один из вариантов cyphersuite, так и их комбинацию. Однако использование нескольких уровней cyphersuite улучшает уровень безопасности и быстродействие безопасной связи. Информация, необходимая для работы с *cyphersuite*, не поставляется с коммутатором. Ее необходимо загрузить из стороннего источника в виде файла, называемого сертификатом. Этот файл может быть загружен на Коммутатор с TFTP-сервера. Коммутатор поддерживает SSLv3 и TLSv1. Другие версии SSL могут быть несовместимы с коммутатором и привести к возникновению проблем при аутентификации и передаче сообщений между клиентом и хостом.

Загрузка сертификата

Это окно используется для загрузки сертификата для SSL-функции с TFTP-сервера. Данный файл содержит необходимую информацию для аутентификации устройств в сети. Он содержит информацию о его владельце, ключи аутентификации и цифровые подписи. Для оптимальной работы SSL-функции клиент и сервер должны обладать соответствующими файлами сертификации. Коммутатор поддерживает только файлы сертификации с расширением .der. Хотя коммутатор поставляется с предустановленным сертификатом, пользователь в зависимости от своих потребностей может произвести загрузку других сертификатов.

Ciphersuite

Приведенное ниже окно позволяет пользователю задать настройки SSL и ciphersuite на Коммутаторе. *Ciphersuite* – это строка, определяющая точные параметры шифрования, алгоритм шифрования и длину ключей, которые используются для аутентификации. В данном окне сущесвует возможность включить нужный вариант *Ciphersuite*.

При включении функции SSL, WEB-интерфейс становится неактивным. Чтобы осуществлять управление Коммутатором через Web-интерфейс с включенной функцией SSL, WEB-браузер должен поддерживать SSL-шифрование и адрес (URL) должен начинаться с http// (например, https://10.90.90.90). В противном случае будет возникать ошибка и отказ в доступе при авторизации.

Для работы со следующим окном кликните **Security > SSL**:

Рисунок 10- 4. Окно Download Certificate and Ciphersuite

Для загрузки сертификата задайте следующие парамеры и кликните по **Apply**.

Параметр	Описание
Certificate Type	Выберите тип загружаемого сертификата, который относится к серверу, ответственному за подачу сертификата. В данной реализации это поле может содержать только значение *local*
Server IP	Введите IP-адрес TFTP-сервера, с которого будет загружаться сертификат.
Certificate File Name	Введите путь и имя загружаемого файла сертификата. Этот файл должен быть с расширением .der (например, c:/cert.der).
Key File Name	Введите путь и имя загружаемого файла ключа. Этот файл должен быть с расширением .der (например, c:/cert.der).

Для настройки функции SSL на Коммутаторе настройте следующие параметры и кликните по **Apply**.

Параметр	Описание
Configuration	
SSL Status	Используйте выпадающее меню, чтобы включить или выключить SSL на Коммутаторе. Значение по умолчанию – *Disabled (выключено)*.
Cache Timeout (60-86400)	Это поле устанавливает время обмена ключами между клиентом и хостом с помощью функции SSL. Новая сессия SSL устанавливается после обмена ключами между хостом и клиентом. Установка в данном поле большего значения позволяет использовать основной ключ для SSL-соединения с определенным хостом, в результате ускоряется процесс согласования. Настройка по умолчанию 600 секунд.
Ciphersuite	
RSA with RC4 128	Выбор данной опции задает использование ключа обмена RSA, 128-битное шифрование RC4 и алгоритм шифрования MD5 Hash Algorithm. Управление

MD5	данной опцией осуществляется с помощью выпадающего меню. По умолчанию установлено значение *Enabled* (включено).
RSA with 3DES EDE CBC SHA	Выбор данной опции задает использование ключа обмена RSA, шифрование CBC Block Cipher 3DES_EDE и алгоритм шифрования MD5 Hash Algorithm. Управление данной опцией осуществляется с помощью выпадающего меню. По умолчанию установлено значение *Enabled* (включено).
DHS DSS with 3DES EDE CBC SHA	Выбор данной опции задает использование ключа обмена DHS Diffie Hellman, шифрования CBC Block Cipher 3DES_EDE и алгоритма шифрования SHA Hash Algorithm. Управление данной опцией осуществляется с помощью выпадающего меню. По умолчанию установлено значение *Enabled* (включено).
RSA EXPORT with RC4 40 MD5	Выбор данной опции задает использование ключа обмена RSA, 40-битное шифрование RC4. Управление данной опцией осуществляется с помощью выпадающего меню. По умолчанию установлено значение *Enabled* (включено).

ПРИМЕЧАНИЕ: Для получения более подробной информации по настройке SSL следует обратиться к Руководству по интерфейсу командной строки для коммутаторов серии DES-3028/28P/52/52, находящемуся на CD-диске.

ПИМЕЧАНИЕ: При выборе опции SSL переключатель на Web-интерфейс управления будет неактивным. Для того чтобы зарегистрироваться на Коммутаторе заново, адрес (URL) должен начинаться с https://. В противном случае Web-браузер выдаст ошибку и отказ в доступе.

SSH

SSH (сокращение от англ. Secure Shell) - это программа, обеспечивающая удалённую безопасную авторизацию и безопасные сетевые сервисы в современной сети.
Использование SSH позволяет осуществить удалённую авторизацию на удалённом хосте и обеспечивает безопасное выполнение команд на удалённом компьютере, благодаря использованию шифрования. SSH, оснащенный множеством средств безопасности, является незаменимым инструментом при работе в современной компьютерной сети. Ниже приводятся шаги, которые необходимо выполнить для обеспечения безопасного взаимодействия между удалённым компьютером (SSH-клиент) и Коммутатором (SSH-сервер):

1. Создайте учётную запись пользователя с правами администратора, используя окно **User Accounts** в папке **Security Management**. Процедура создания данной учетной записи ничем не отличается от создания любой другой учётной записи с правами администратора на Коммутаторе. Пароль данной учетной записи будет использоваться на Коммутаторе при установлении безопасной связи с использованием протокола SSH.
2. Настройте учётную запись с привилегиями User, определив метод идентификации пользователей для установки SSH-соединения с Коммутатором, используя окно **SSH User Authentication**. Существует три варианта авторизации пользователя: на основе хоста, пароль и открытый ключ (public key).
3. Настройте с помощью окна **SSH Algoritm** алгоритм шифрования, который будет использоваться для шифрования и дешифрования сообщений между SSH-клиентом и SSH-сервером,
4. Включите опцию SSH на Коммутаторе, используя окно **SSH Configuration**.

По выполнении данных шагов можно перейти к настройке SSH-клиента на удалённом компьютере для управления Коммутатором через безопасное соединение.

Настройка сервера SSH

Данное окно предназначено для конфигурации и просмотра настроек SSH-сервера. Для открытия данного окна кликните **Security > SSH > SSH Server Configuration**:

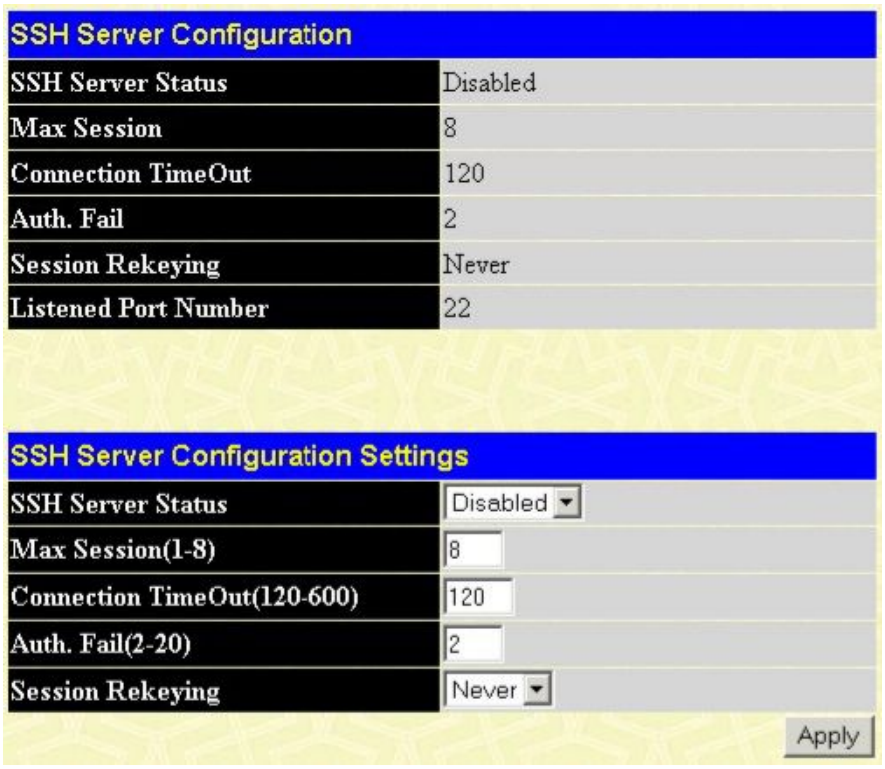


Рисунок 10- 5. Окно SSH Server Configuration

Для настройки SSH-сервера необходимо задать седующие параметры и кликнуть по **Apply**:

Параметр	Описание
SSH Server Status	Данное выпадающее меню позволяет включить/выключить функцию SSH на Коммутаторе. По умолчанию установлено значение *Disabled*.
Max Session (1-8)	Введите значение от 1 до 8 для определения количества пользователей, которые могут быть одновременно подключены к Коммутатору. По умолчанию установлено значение 8.
Time Out (120-600)	Позволяет пользователю установить тайм-аут соединения. Можно задать значение от 120 до 600 секунд. По умолчанию установлено значение 120 секунд.
Auth. Fail (2-20)	Позволяет администратору устанавливать максимальное количество попыток, которые даются пользователю для авторизации на SSH-сервере. При превышении данного лимита пользователь сможет подключиться к коммутатору, используя другое имя (логин). Данный параметр может принимать значение от 2 до 20. Значение по умолчанию 2.
Session Rekeying	Данное выпадающее меню позволяет задать временной интервал, через который Коммутатор будет менять шифрование SSH. Доступны значения: *Never, 10min, 30min и 60min*. Значение по умолчанию *Never*.

Настройки режима и алгоритма аутентификации SSH

Окно SSH Algorithm позволяет настроить нужные варианты SSH-алгоритма, использующиеся для шифрования при аутентификации. На Коммутаторе представлено четыре категории алгоритмов, и каждый из алгоритмов можно включить или выключить, используя выпадающее меню. По умолчанию, все алгоритмы включены (*Enabled*). Для работы с данным окном кликните **Security > SSH > SSH Authentication Mode and Algorithm Settings**:

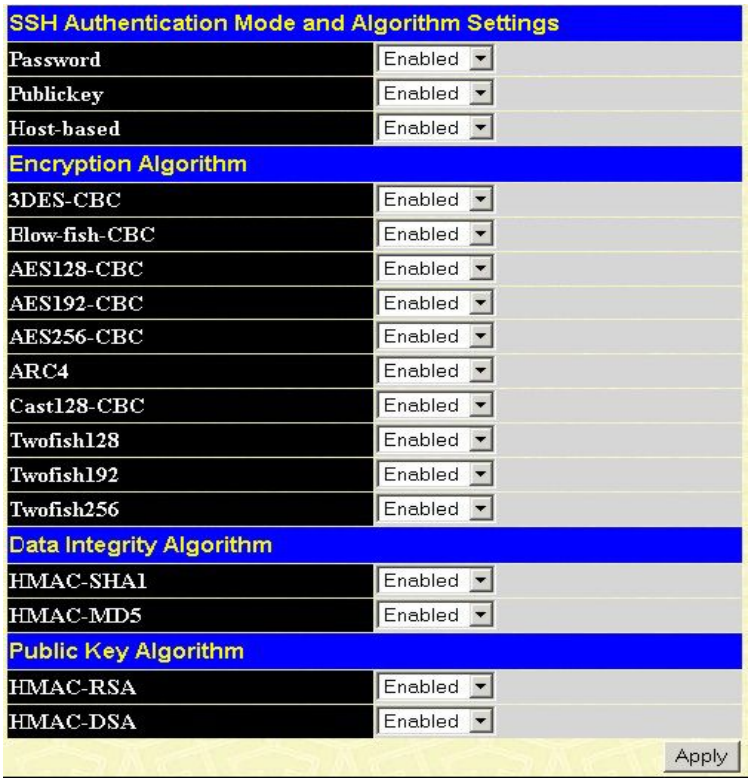


Рисунок 10-6. Окно Encryption Algorithm

Могут быть заданы следующие алгоритмы:

Параметр	Описание
SSH Authentication Mode and Algorithm Settings	
Password	Этот параметр позволяет администратору использовать локальный пароль для аутентификации на Коммутаторе. Значение по умолчанию *Enabled* (включено).
Public Key	Этот параметр необходимо включить, если администратор желает для аутентификации на Коммутаторе использовать открытый ключ, настроенный на SSH-сервере. Значение по умолчанию *Enabled*.
Host-based	Этот параметр необходимо включить, если администратор желает для аутентификации на Коммутаторе использовать компьютер. Этот параметр предназначен для пользователей Linux с настроенной аутентификацией SSH. Значение по умолчанию *Enabled*.
Encryption Algorithm	
3DES-CBC	Используйте выпадающее меню для включения или выключения алгоритма шифрования Triple Data Encryption Standard с Cipher Block Chaining. Значение по умолчанию *Enabled* (включено).
Blow-fish CBC	Используйте выпадающее меню для включения или выключения алгоритма шифрования Blowfish with Cipher Block Chaining. Значение по умолчанию *Enabled* (включено).
AES128-CBC	Используйте выпадающее меню для включения или выключения алгоритма шифрования Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. Значение по умолчанию *Enabled* (включено).
AES192-CBC	Используйте выпадающее меню для включения или выключения алгоритма шифрования Advanced Encryption Standard AES192 с Cipher Block Chaining. Значение по умолчанию *Enabled* (включено).
AES256-CBC	Используйте выпадающее меню для включения или выключения алгоритма шифрования Advanced Encryption Standard AES-256 с Cipher Block Chaining. Значение по умолчанию *Enabled* (включено).

ARC4	Используйте выпадающее меню для включения или выключения алгоритма шифрования Arcfour encryption algorithm with Cipher Block Chaining.Значение по умолчанию *Enabled* (включено).
Cast128-CBC	Используйте выпадающее меню для включения или выключения алгоритма шифрования Cast128 encryption algorithm with Cipher Block Chaining. Значение по умолчанию *Enabled* (включено).
Twofish128	Используйте выпадающее меню для включения или выключения алгоритма шифрования twofish128.Значение по умолчанию *Enabled* (включено).
Twofish192	Используйте выпадающее меню для включения или выключения алгоритма шифрования twofish192. Значение по умолчанию *Enable* (включено).
Twofish256	Используйте выпадающее меню для включения или выключения алгоритма шифрования twofish256.Значение по умолчанию *Enabled* (включено).
Data Integrity Algorithm	
HMAC-SHA1	Используйте выпадающее меню для включения или выключения механизма HMAC (Hash for Message Authentication Code) с использованием Secure Hash algorithm. Значение по умолчанию *Enabled* (включено).
HMAC-MD5	Используйте выпадающее меню для включения или выключения механизма HMAC (Hash for Message Authentication Code) с использованием MD5 Message Digest Значение по умолчанию *Enabled* (включено).
Public Key Algorithm	
HMAC-RSA	Используйте выпадающее меню для включения или выключения механизма HMAC (Hash for Message Authentication Code) с использованием алгоритма шифрования RSA. Значение по умолчанию *Enabled* (включено).
HMAC-DSA	Используйте выпадающее меню для включения или выключения HMAC (Hash for Message Authentication Code) с использованием механизма шифрования Digital Signature (Цифровая подпись). Значение по умолчанию *Enabled* (включено).

Кликните по **Apply** для применения выполненных изменений.

Аутентификация SSH-пользователя

Данное окно используется для настройки параметров для подключения пользователей к Коммутатору через SSH. Для работы с этим окном кликните **Security > SSH > SSH User Authentication Mode**.

(Note:Maximum of 8 entries.)

SSH User Authentication Mode

User Name	Auth. Mode	Host Name	Host IP
admin	Password		
user	Password		

Рисунок 10- 7. Окно SSH User Authentication Mode

Рассмотрим пример. Учетная запись “admin” была настроена ранее в окне User Accounts в папке **Administration**. Чтобы задать параметры SSH-пользователя, НЕОБХОДИМО настроить учетную запись пользователя. Для настройки параметров SSH-пользователя кликните по гиперссылке с именем пользователя в окне **Current Accounts,** после чего откроется следующее окно для настройки.

Рисунок 10- 8. Окно SSH User

Для настройки пользователем доступны следующие параметры:

Параметр	Описание
User Name	Для идентификации SSH-пользователя введите имя пользователя длиной не более 15 символов. Это имя пользователя должно быть предварительно

	настроено на Коммутаторе как учётная запись пользователя.
Auth. Mode	Администратор может выбрать одну из следующих опций для настройки авторизации пользователей при подключении к Коммутатору. *Host Based* – эта опция задает использование удалённого SSH-сервера для аутентификации пользователей. При этом пользователю необходимо будет ввести следующую информацию для идентификации: • *Host Name* – введите цифробуквенную строку не более 31 символа для идентификации удалённого SSH-пользователя. • *Host IP* – введите соответствующий IP-адрес SSH-пользователя. *Password* – эта опция задает использование для аутентификации пароля, заданного администратором. При выборе данной опции администратору понадобится ввести дважды пароль (один раз для подтверждения). *Public Key* – эта опция задает использование для аутентификации на SSH-сервере открытый ключ.
Host Name	Введите цифробуквенную строку не боле 31 символа для идентификации удалённого SSH-пользователя. Этот параметр используется только при выборе Host Based в поле Auth. Mode.
Host IP	Введите соответствующий IP- адрес SSH-пользователя. Этот параметр используется только при выборе Host Based в поле Auth. Mode.

Кликните по **Apply** для применения выполненных изменений.

ПРИМЕЧАНИЕ: Для настройки параметров аутентификации SSH-пользователя на Коммутаторе, учётная запись пользователя должна быть сконфигурирована заранее. Для получения более подробной информации о настройке локальных учётных записей пользователя на Коммутаторе обратитесь к разделу «Учетные записи пользователей» в данном Руководстве.

Аутентификация 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.

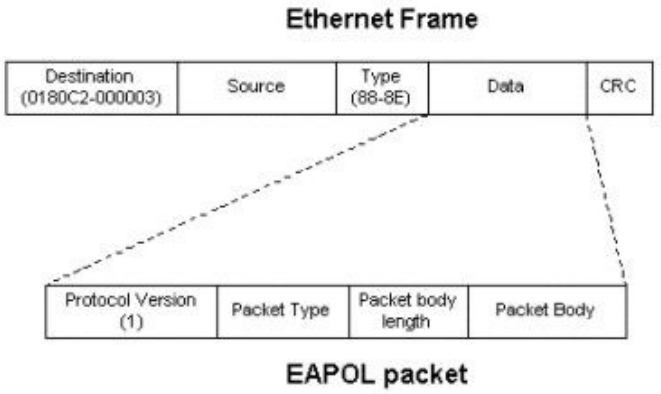


Рисунок 10- 9. Структура пакета EAPOL

Благодаря использованию данного метода, неавторизованные устройства не смогут подключиться к сети LAN через порт, к которому подключен пользователь. Пакеты EAPOL являются единственным трафиком, который может быть передан через определенный порт, пока не будет получена авторизация. Управление доступом 802.1X использует три роли, каждая из которых важна для создания и поддержания стабильной работы метода безопасности Управления доступом.

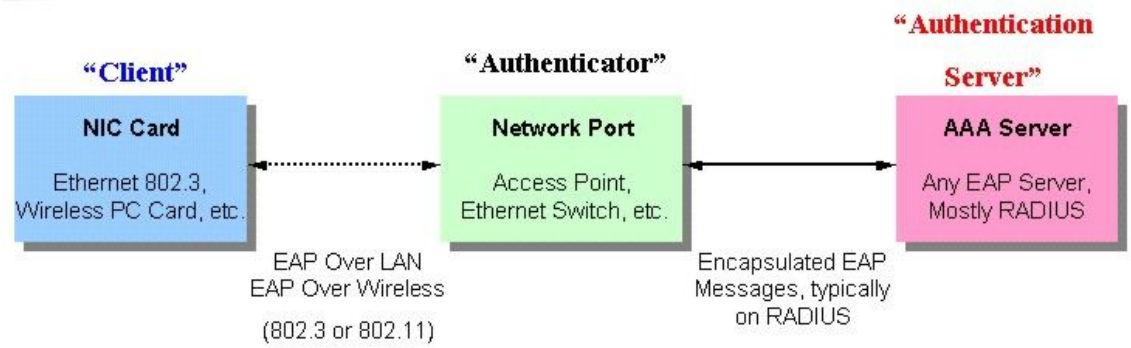


Рисунок 10- 10. Три функции протокола 802.1x

Все эти компоненты и их основные функции будут более подробно рассмотрены далее.

Сервер аутентификации

Сервер аутентификации – это внешнее устройство, включенное в одну сеть с клиентом и аутентификатором. На сервере аутентификации должно быть установлено программное обеспечение RADIUS-сервера. Помимо этого необходимо правильно настроить сервер аутентификации на Коммутаторе (Аутентификаторе). Основная функция Сервера аутентификации (RADIUS) состоит в аутентификации клиентов, подключенных к портам коммутатора, до того, как они получат доступ к каким-либо сервисам, предоставляемым коммутатором в локальной сети. Сервер аутентификации должен осуществить проверку подлинности клиента, пытающегося получить доступ к сети. Это происходит путем обмена секретной информацией (пакеты EAPOL) между сервером RADIUS и клиентом. Далее Сервер аутентификации информирует коммутатор, нужно или нет предоставлять данному клиенту доступ к локальной сети и/или сервисам коммутатора.

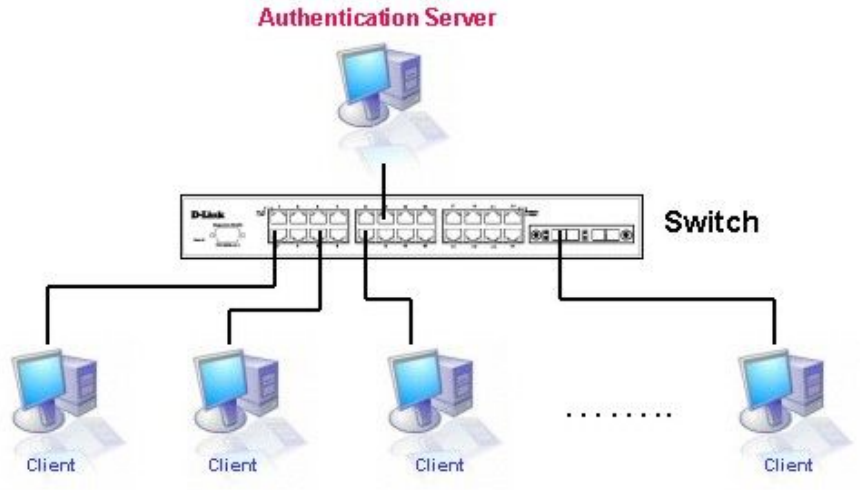


Рисунок 10- 11. Сервер аутентификации

Аутентификатор

Аутентификатор (Коммутатор) является посредником между сервером аутентификации и клиентом. При использовании протокола 802.1x Аутентификатор выполняет две задачи: запрос и получении от клиента информации аутентификации с помощью пакетов EAPOL, а затем проверка данной информации с помощью сервера аутентификации. Получив ответ от сервера аутентификации, аутентификатор пересылает ответ клиенту.

Для правильной настройки аутентификатора необходимо выполнить три шага.

1. Активировать 802.1X на устройстве *Enabled*. (**DES-30xx Web Management Tool**)
2. Настроить 802.1X на порту (**Security** / **802.1X** / **Configure 802.1X Authenticator Parameter**)
3. Настроить параметры RADIUS-сервера на Коммутаторе. (**Security** / **802.1X** / **Authentic RADIUS Server**)

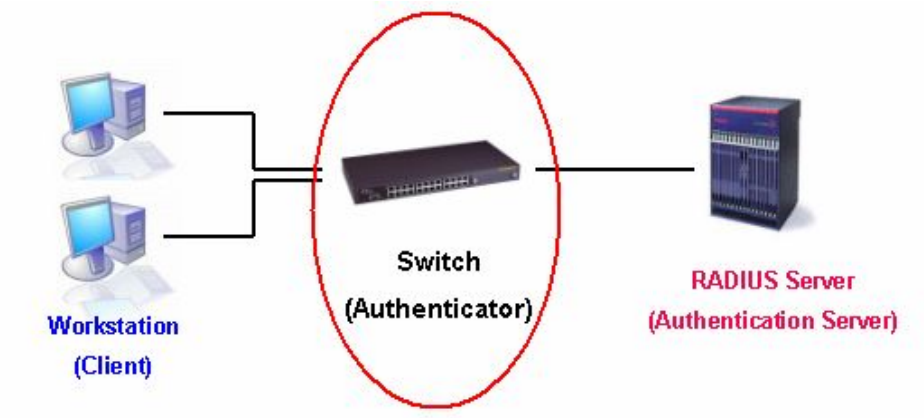


Рисунок 10- 12. Аутентификатор

Клиент

Клиент – это рабочая станция, которая запрашивает доступ к локальной сети или сервисам коммутатора. На всех рабочих станциях должно быть установлено программное обеспечение 802.1x. Для пользователей Windows XP программное обеспечение уже встроено в операционную систему, пользователям других ОС придется установить ПО отдельно. Клиент с помощью пакетов EAPOL запрашивает доступ к локальной сети или коммутатору и получает от коммутатора ответ.

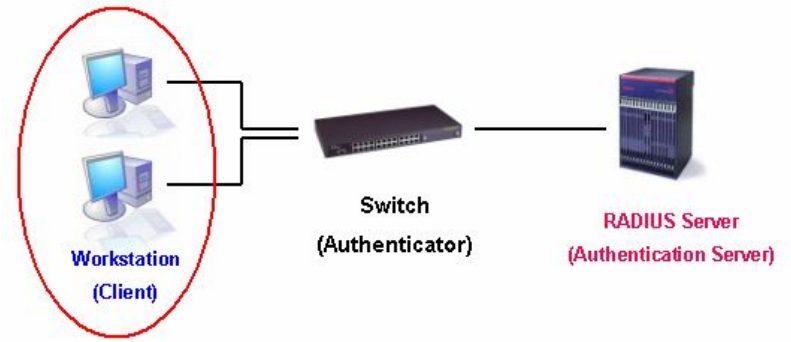


Рисунок 10- 13. Клиент

Процесс аутентификации

Благодаря использованию трех основных компонентов, описанных выше, протокол 802.1x обеспечивает надежный и безопасный способ авторизации и аутентификации пользователей, пытающихся получить доступ к сети. До завершения аутентификации через порты коммутатора может проходить только трафик EAPOL. Порт находится в неавторизованном состоянии до тех пор, пока клиенту не будет разрешен доступ после введения правильного имени пользователя и пароля (и MAC-адреса при аутентификации 802.1x на основе MAC-адресов). После этого порт переходит в авторизованное состояние, и через него может передаваться нормальный трафик. На следующем рисунке пердставлено более подробное объяснение процесса аутентификации.

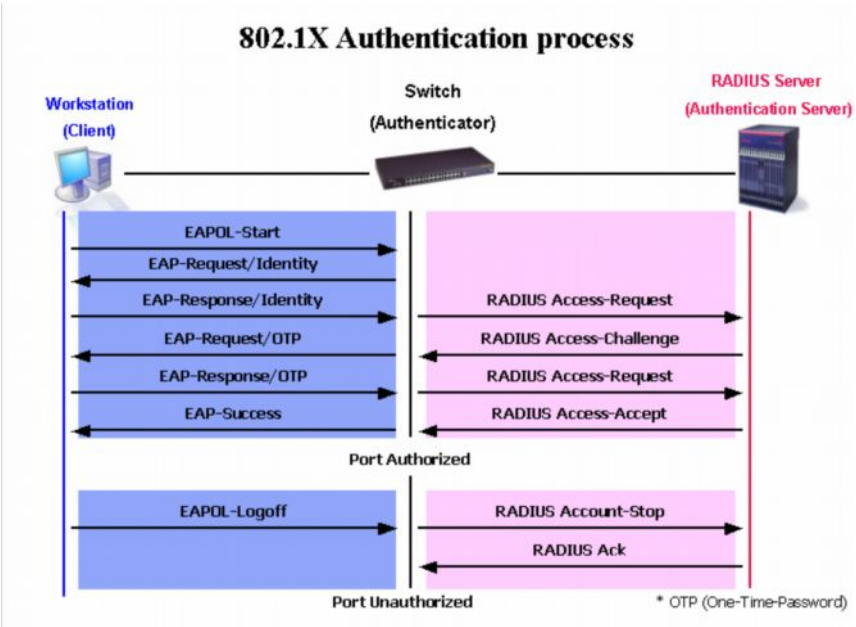


Рисунок 10-14. Процесс аутентификации 802.1X

Реализация 802.1x на оборудовании D-Link дает возможность сетевым администраторам выбирать между двумя типами аутентификации:

1. Аутентификация на основе портов – С того момента как клиент прошел авторизацию на определённом порту, любой другой клиент, подключённый к этому же порту, может получить доступ к сети.

2. Аутентификация на основе MAC-адресов – В данном случае проверяются с помощью сервера RADIUS не только учётные данные пользователей, но и достигнуто ли максимальное количество разрешённых на порту MAC-адресов. Если достигнуто, то новый MAC-адрес блокируется.

Понятие аутентификации 802.1X на основе портов и MAC-адресов

Стандарт 802.1x ориентирован прежде всего на усиление безопасности соединения точка-точка в локальных сетях. Любой сегмент сети в такой инфраструктуре обладает не более, чем двумя подключёнными устройствами, одним из которых является Bridge Port. Bridge Port обнаруживает присоединение активного устройства к удалённому концу линии или изменение состояния устройства с активного на неактивное. При возникновении таких событий может быть проверен статус авторизации порта или инициирован процесс аутентификации присоединённого устройства, если порт не был авторизован ранее. Таким образом работает аутентификация на основе портов (Port-Based Network Access Control).

Аутентификция на основе портов

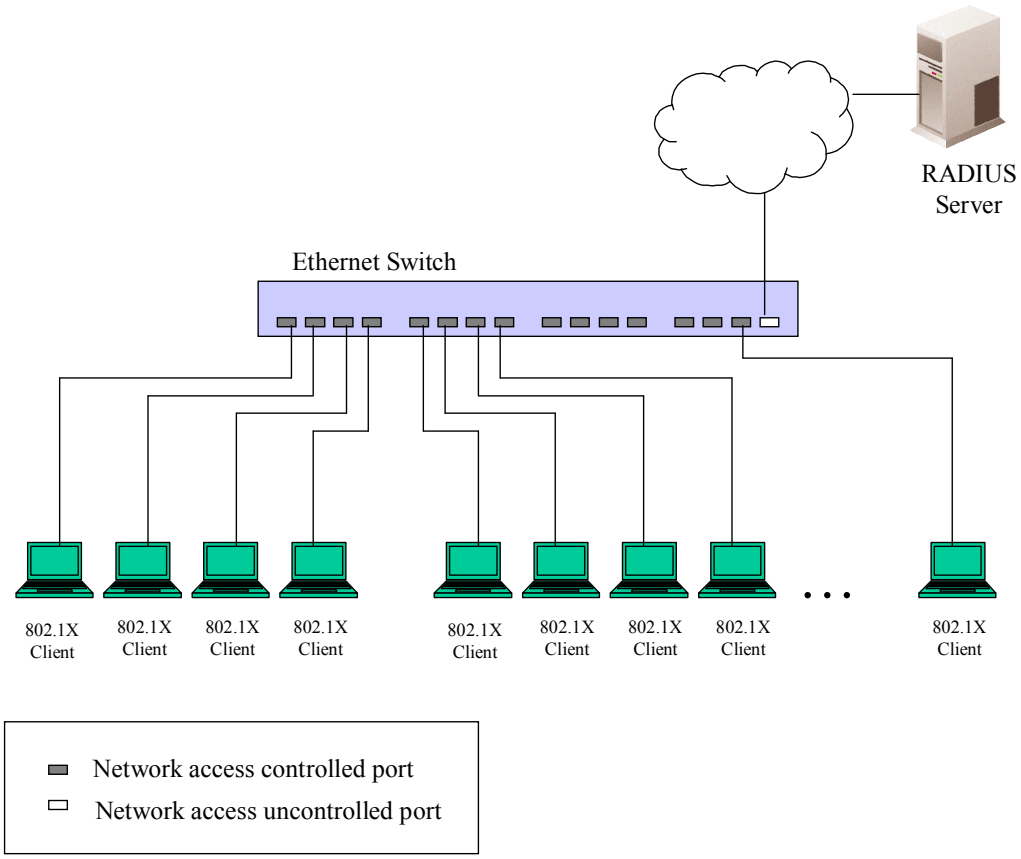


Рисунок 10-15. Пример типичной конфигурации Port-Based (на основе портов)

После успешного прохождения Клиентом аутентификаци порт переходит в авторизованное состояние, и для передачи последующего трафика по данному порту аутентификация не требуется. Это происходит до тех пор, пока не произойдёт событие, в результате которого порт перейдет в неавторизованное состояние. Следовательно, если к порту подключен 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 не обеспечивается надлежащая безопасность подключения.

Аутентификация на основе MAC-адресов

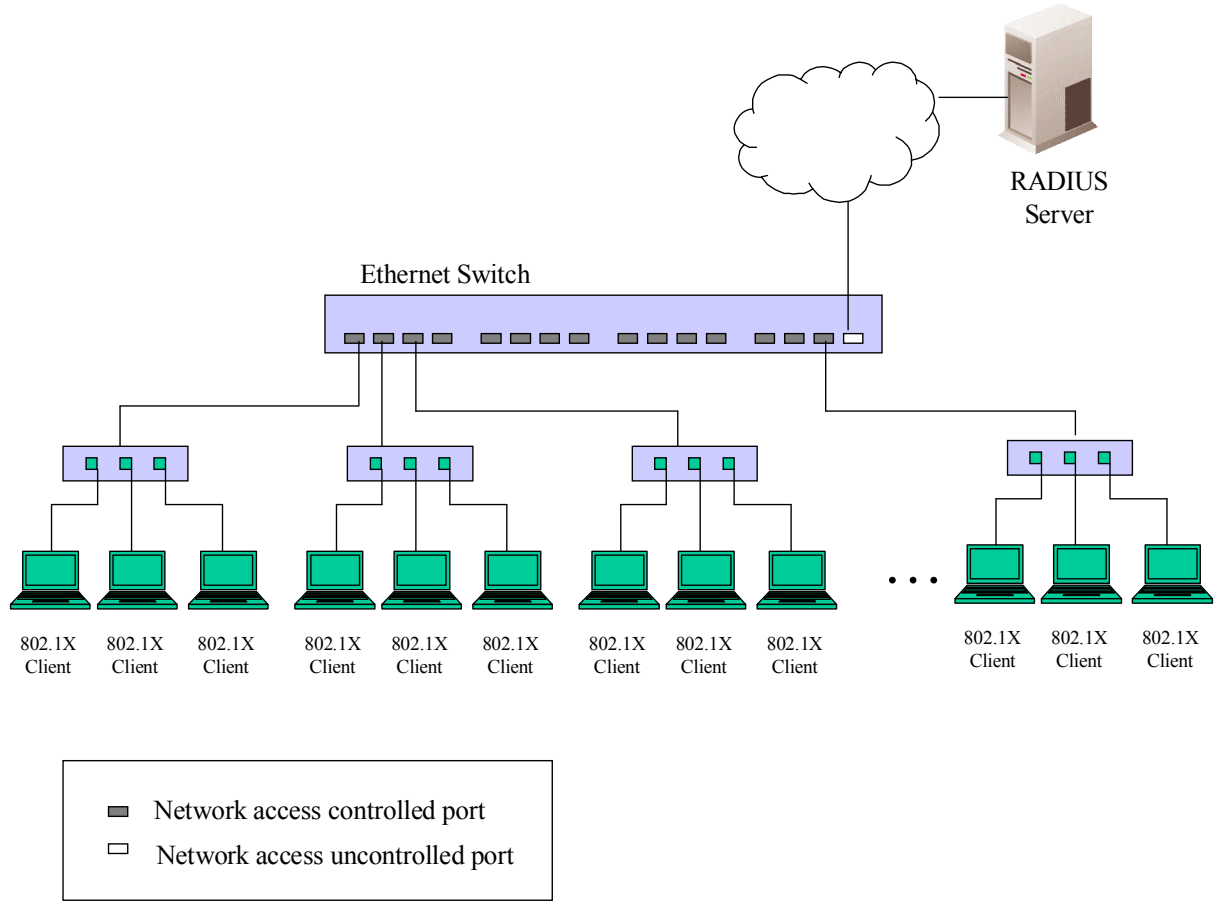


Рисунок 10-16. Пример типичной конфигурации MAC-Based (на основе MAC-адресов)

Для того чтобы успешно применять аутентификацию 802.1x в сегменте LAN, необходимо создать «виртуальные» порты для каждого устройства в сегменте LAN, для которого необходим доступ к LAN. Коммутатор будет рассматривать один физический порт, к которому подключен сегмент LAN, в качестве нескольких виртуальных портов, для каждого из которых будет отдельно контролироваться статус авторизации. Коммутатор изучает MAC-адреса подключенных устройств и создаёт для каждого из них свой виртуальный порт. В результате каждое устройство получает возможность получить доступ к LAN через свой виртуальный порт.

Guest VLANs

Поддержка 802.1x позволяет устройствам, не поддерживающим или несовместимым с данным стандартом (как, например, компьютер, работающий с операционной системой Windows 98 или более ранними версиями операционной системы), получить доступ к сети с ограниченными правами. Кроме того, некоторые пользователи («гости») могут получить ограниченный доступ к сети, не проходя полной авторизации. Все это реализовано на коммутаторах благодаря поддержке опции Guest VLAN 802.1x. К этим сетям будут получать доступ пользователи, имеющие ограниченные права доступа, и характеристики таких сетей будут отличаться от других VLAN в сети. Для создания Guest 802.1x VLAN сначала необходимо создать на сети VLAN с ограниченными правами доступа, а затем определить ее как Guest VLAN 802.1x. Далее администратор должен создать учетные записи «гостей», подключающихся к коммутатору, чтобы они могли получить доступ в Guest VLAN при подключении к коммутатору. Для получения доступа к VLAN назначения при подключении к коммутатору клиент должен пройти аутентификацию либо локально, либо с помощью удаленного сервера RADIUS. После успешного завершения аутентификации клиента он может быть принят в target VLAN (VLAN назначения) с стандартными правами доступа. Если аутентификация не прошла успешно, то клиент будет возвращен в исходную VLAN. Если клиент не прошел аутентификацию, он будет перемещен в Guest VLAN, где, он будет иметь ограниченные права доступа. Приводимый рисунок позволит лучше разобраться в процессах, происходящих в Guest VLAN.

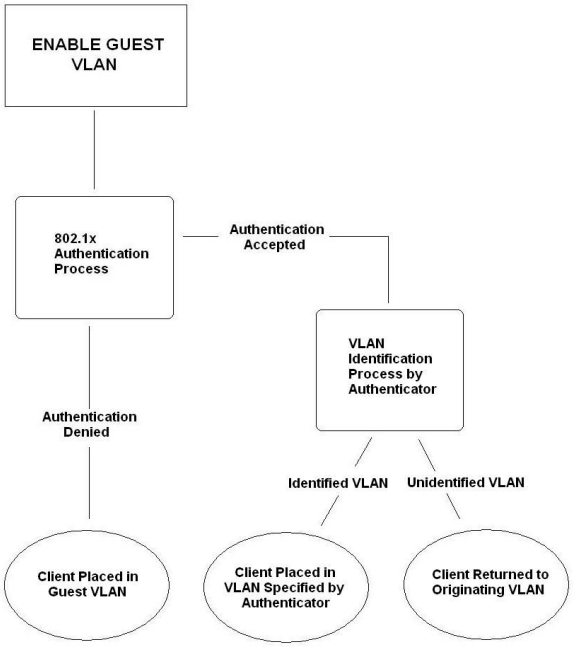


Рисунок 11- 2. Процесс аутентификации Guest VLAN

Ограничения при использовании Guest VLAN

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

Настройка 802.1x Guest VLAN

В меню **Security** откройте папку **802.1X** и кликните по **Configure 802.1X Guest VLAN.** В результате отобразится следующее окно для настройки пользователем. Следует помнить, что для настройки Guest 802.1X VLAN пользователю необходимо сначала настроить стандартную VLAN, которой затем можно будет присвоить статус Guest VLAN в показанном ниже окне.

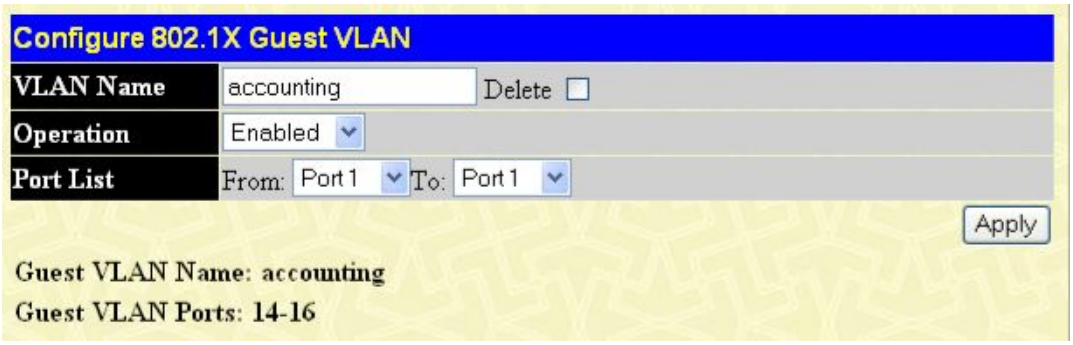


Рисунок 10- 18. Окно Guest VLAN Settings

Могут быть настроены следующие поля, чтобы включить опцию guest 802.1X VLAN:

Параметр	Описание
VLAN Name	Введите настроенное ранее имя VLAN, которой необходимо присвоить статус Guest 802.1X VLAN.
Operation	При настройке Guest 802.1X VLAN в данном поле доступно две опции: *Enabled* – при выборе этой опции порты, представленные в списке ниже, будут добавлены в Guest VLAN. Убедитесь, что данные порты добавлены в данную VLAN. В противном случае появится сообщение об ошибке. *Disabled* – при выборе данной опции порты, представленные в списке ниже, будут исключены из Guest VLAN. Убедитесь, что данные порты добавлены в данную VLAN. В противном случае появится сообщение об ошибке.
Port List	Выберите нужные порты Guest VLAN.

Кликните по **Apply** для применения введенных настроек guest 802.1X VLAN. Только одна VLAN может быть назначена как 802.1X Guest VLAN.

Настройка параметров аутентификатора 802.1X

Для задания настроек аутентификатора 802.1X кликните **Security > 802.1X > 802.1X Authenticator Settings**:

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
19	both	auto	30	60	30	30	2	3600	no
20	both	auto	30	60	30	30	2	3600	no
21	both	auto	30	60	30	30	2	3600	no
22	both	auto	30	60	30	30	2	3600	no
23	both	auto	30	60	30	30	2	3600	no
24	both	auto	30	60	30	30	2	3600	no
25	both	auto	30	60	30	30	2	3600	no
26	both	auto	30	60	30	30	2	3600	no
27	both	auto	30	60	30	30	2	3600	no
28	both	auto	30	60	30	30	2	3600	no

Рисунок 10-19. Окно 802.1X Authenticator Settings

Чтобы задать настройки только для определенных портов, кликните по соответствующей ссылке с номером порта**.** В результате отобразится следующее окно для настройки:

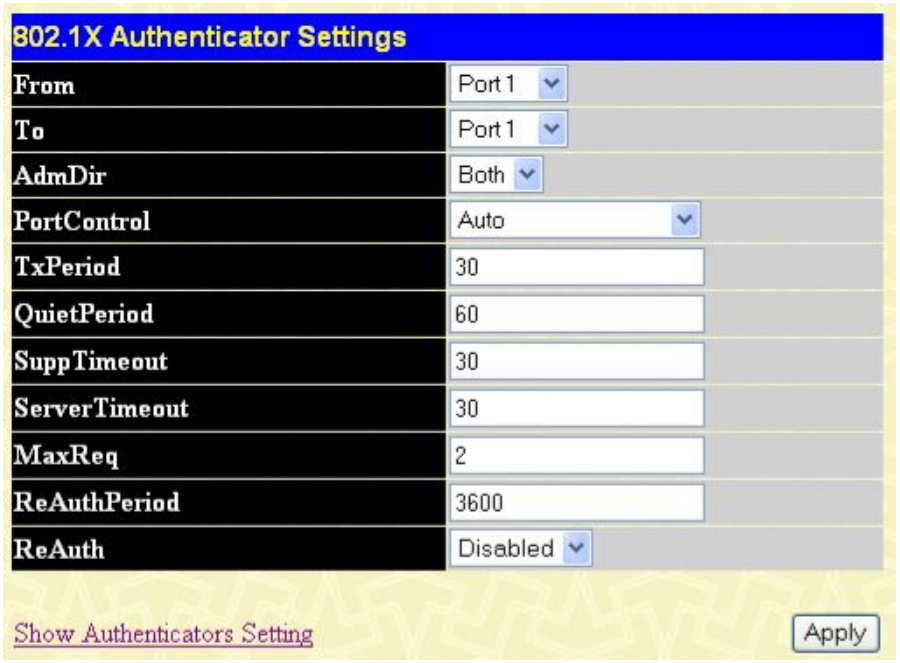


Рисунок 10-20. Окно 802.1X Authenticator Settings (Modify)

Данное окно содержит опции для настройки следующих параметров:

Параметр	Описание
From [ ] To [ ]	Данные выпадающие меню позволяют ввести порт (или порты) для настройки.
AdmDir	В данном поле пользователь может выбрать вид трафика, подлежащего контролю. Для выбора доступны опции: *in* или *both*. При выборе опции *in* будет осуществляться контроль только исходящего трафика для портов заданного выше диапазона. При выборе опции *both* будет осуществляться контроль как исходящего, так и входящего трафика для портов заданного выше диапазона.
PortControl	Это поле позволяет управлять статусом авторизации порта. При выборе опции *forceAuthorized* аутентификация 802.1X выключается, и порт всегда находится в авторизованном состоянии и может передавать и принимать трафик 802.1X, не запрашивая аутентификацию клиента. При выборе опции *forceUnauthorized* порт всегда будет оставаться в неавторизованном состоянии, игнорируя все попытки клиента аутентифицироваться. Коммутатор не обеспечивает аутентификацию клиента через данный интерфейс. При выборе опции *Auto* аутентификация 802.1X включена, и порт изначально находится в неавторизованном состоянии, и через него доступна передача и прием только EAPOL-фреймов. Процесс аутентификации запускается при активности на порту или принятии стартового EAPOL-фрейма. Тогда Коммутатор запрашивает у клиента аутентификацию и начинает передавать аутентификационные сообщения между клиентом и сервером аутентификации. Значение по умолчанию - *Auto.*
TxPeriod	Здесь устанавливается периодичность TxPeriod аутентификации PAE. Это значение определяет периодичность передачи клиенту пакета EAP Request/Identity. Значение по умолчанию равно *30* секунд.
QuietPeriod	Данное поле позволяет установить пользователю период в секундах, в течение которого Коммутатор будет оставаться в неактивном состоянии после неудачной аутентификации клиента. Значение по умолчанию равно 60 секунд.
SuppTimeout	Это значение определяет период таймаута при обмене сообщениями между Аутентификатором и клиентом. Значение по умолчанию 30 секунд.
ServerTimeout	Это значение определяет период таймаута при обмене сообщениями между Аутентификатором и сервером аутентификации. Значение по умолчанию равно 30 секунд.

MaxReq	Максимальное количество попыток запроса EAP от клиента, до того как истечёт время аутентификации. Значение по умолчанию равно 2.
ReAuthPeriod	Заданное в этом поле значение определяет период в секундах между периодическими повторными запросами аутентификации. Значение по умолчанию равно *3600* секунд.
ReAuth	Данное выпадающее меню позволяет включить (*Enabled*) или выключить (*Disabled*) повторную аутентификацию для выбранного диапазона портов. Значение по умолчанию *Disabled*.

Кликните по **Apply** для применения выполненных изменений конфигурации.

Локальные пользователи 802.1X

В папке **Security** откройте папку **802.1X** и кликните по **802.1X User**, чтобы открыть окно **802.1X User**. Данное окно позволяет установить различных локальных пользователей на Коммутаторе.

Рисунок 10- 21. Окно Local Users Configuration

Введите **User Name**, **Password**, а также подтверждение пароля. Настроенные должным образом локальные пользователи отобразятся в таблице **Local Users Table** в том же окне.

Инициализация портов при аутентификации 802.1X на основе портов

Существующие настройки 802.1X на основе портов и MAC-адресов отображаются и доступны для настройки в представленном ниже окне.
Для работы с этим окном кликните **Security > 802.1X > Initialize Port(s)**:

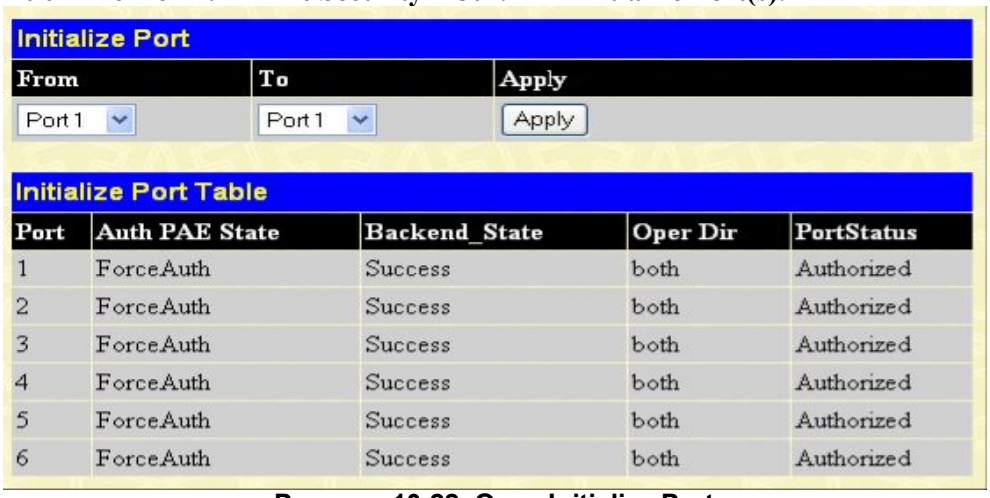


Рисунок 10-22. Окно Initialize Port

Это окно позволяет инициализировать порт или группу портов. В нижней части окна в **Initialize Port Table** отображается текущий статус порта (-ов).
В данном окне отображается следующая информация:

Параметр	Описание
From and To	Выбираются порты для инициализации.
Auth PAE State	В поле **Auth PAE State** будет отображаться одно из следующих значений: *Initialize, Disconnected,Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth* или *N/A.*
Backend State	В поле **Backend Authentication State** будет отображаться одно из следующих значений: *Request, Response,Success, Fail, Timeout, Idle, Initialize* или *N/A.*
Port	Это поле, доступное только для чтения, содержит номер порта Коммутатора.

Port Status	Статус контролируемого порта может быть *Authorized, Unauthorize* или *N/A.*

Инициализация портов для 802.1X на основе MAC-адресов

Для инициализации портов для 802.1x на основе MAC-адресов пользователю необходимо сначала установить аутентификацию 802.1X на основе MAC-адресов в окне **DES-30xx Web Management Tool**.

Кликните по **Security > 802.1X > Initialize Port(s),** чтобы открыть следующее окно:

Рисунок 10-23. Окно Initialize Ports (MAC based 802.1X)

Для инициализации портов выберите нужный диапазон портов с помощью полей **From** и **To**. Затем пользователю необходимо задать MAC-адрес для инициализации, введя его в поле **MAC Address** и поставив галочку в соответствующее поле. Для начала инициализации кликните по **Apply**.

ПРИМЕЧАНИЕ: Пользователю сначала необходимо глобально включить 802.1X в окне **DES-30xx Web Management Tool** до инициализации портов. До включения 802.1X информация в таблице **Initialize Ports Table** не доступна для просмотра.

Повторная аутентификация портов для 802.1X на основе портов

Это окно позволяет осуществить повторную аутентификацию порта или группы портов. Для этого необходимо задать диапазон портов с помощью выпадающих меню **From** и **To**, а затем кликнуть по **Apply**.

Кликните по **Security > 802.1X > Reauthenticate Port(s),** чтобы открыть окно **Reauthenticate Port(s)**:

Рисунок 10-24. Окно Reauthenticate Port и Reauthenticate Port Table

Это окно отображает следующую информацию:

Параметр	Описание
Port	Данное поле отображает номер повторно аутентифицирующегося порта.
Auth State	В поле **Authenticator State** будет отображаться одно из следующих значений: *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth* и *N/A*.
BackendState	В поле **Backend State** будет отображаться одно из следующих значений: *Request, Response, Success, Fail, Timeout, Idle, Initialize* и *N/A*.
OperDir	Определяет направление контроля: In (входящий трафик) или Both (входящий / исходящий трафик).
PortStatus	Статус контролируемого порта может быть *Authorized, Unauthorized* или *N/A*.

ПРИМЕЧАНИЕ: Пользователю необходимо сначала включить глобально 802.1X с помощью окна **DES-30xx Web Management Tool** перед инициализацией портов. Информация в таблице **Initialize Ports Table** не доступна для просмотра до включения 802.1X.

Повторная аутентификация портов для 802.1X на основе MAC-адресов

Чтобы повторно аутентифицировать порты в соответствии с аутентификацией MAC 802.1X, пользователю необходимо сначала включить 802.1X на основе MAC-адресов в окне **DES-30xx Web Management Tool**. Кликните **Security > 802.1X > Reauthenticate Port(s),** чтобы открыть следующее окно:

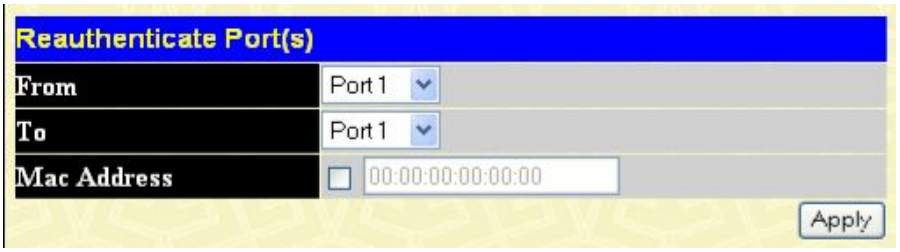


Рисунок 10- 25. Окно Reauthenticate Ports – MAC based 802.1x

Для повторной аутентификации портов сначала выберите Коммутатор в стеке с помощью выпадающего меню, а затем выберите диапазон портов с помощью выпадающих меню **From** и **To**. Затем пользователю необходимо задать MAC-адрес для повторной аутентификации, введя его в поле **MAC Address** и поставив галочку в соответствующем поле. Для начала повторной аутентификации кликните **Apply**.

Сервер аутентификации RADIUS

Функция RADIUS Коммутатора позволяет облегчить централизованное управление пользователями, а также обеспечить защиту от хакерских атак и шпионских программ. Web-менеджер предлагает пользователю три окна для настройки.

Кликните **Security** > **802.1X** > **RADIUS Server,** чтобы открыть окно **RADIUS Server,** показанное ниже:

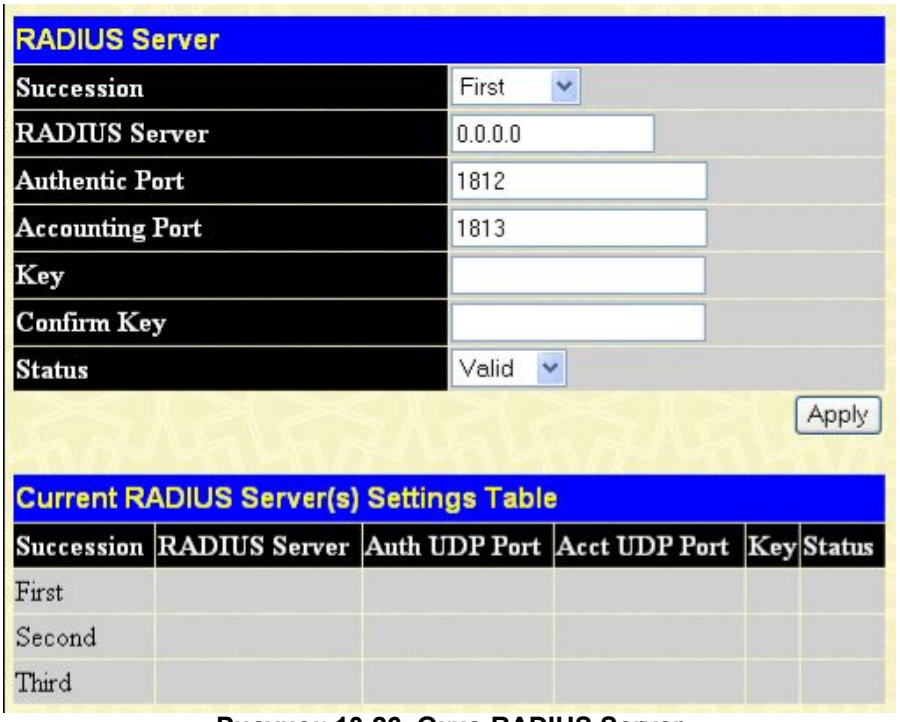


Рисунок 10-26. Окно RADIUS Server

В этом окне отображается следующая информация:

Параметр	Описание
Succession	Выберите нужный RADIUS-сервер для настройки: *First, Second* или *Third*.

RADIUS Server	Установите IP-адрес RADIUS-сервера.
Authentic Port	Установите UDP-порт сервера аутентификации RADIUS. По умолчанию установлен порт *1812*.
Accounting Port	Установите UDP-порт сервера учетных записей RADIUS. По умолчанию установлен порт *1813*.
Key	Установите тот же ключ, что и для RADIUS-сервера.
Confirm Key	Введите подтверждение ключа для RADIUS-сервера.
Status	Данное поле позволяет установить статус RADIUS-сервера как *Valid* (включен) или *Invalid* (выключен).

Доверенный хост (Trusted Host)

Зайдите в папку **Security** и кликните по ссылке **Trusted Host**; появится следующее окно.

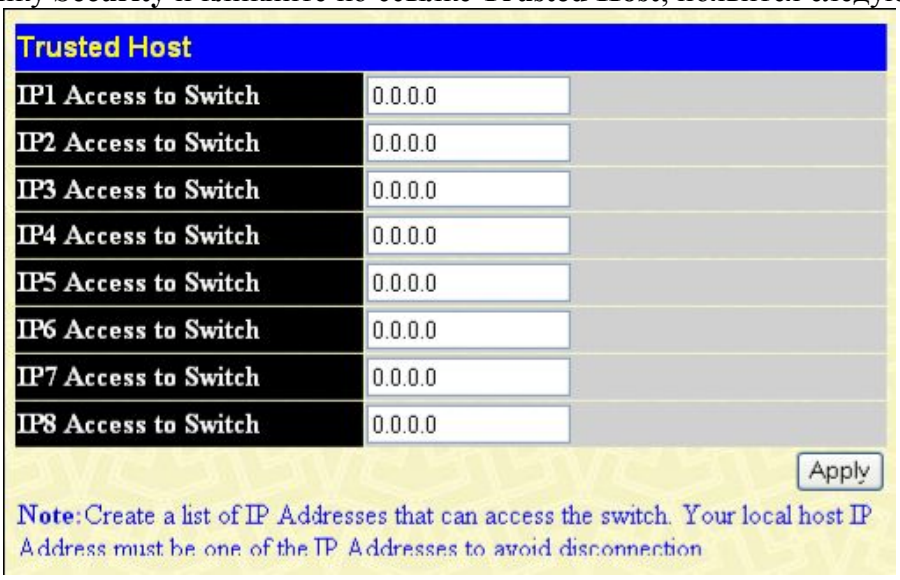


Рисунок 10- 27. Окно Trusted Host

Данное окно позволяет разрешить удаленным станциям управление коммутатором. При выборе одной или более управляющих станций только станциям с указанными IP-адресами будет разрешено управление через Web-менеджер или Telnet. Чтобы определить IP-настройки управляющей станции, введите IP-адрес**,** а затем кликните по кнопке **Apply**.

Управление аутентификацией доступа

Поддержка Коммутаторами протоколов TACACS/XTACACS/TACACS+/RADIUS обеспечивает безопасный доступ к Коммутатору. При регистрации пользователю будет предложено ввести пароль. При включенной опции аутентификации TACACS/XTACACS/TACACS+/RADIUS Коммутатор обратится к серверу TACACS/XTACACS/TACACS+/RADIUS для проверки пользователя. Если подлинность пользователя подтверждена, то он получит доступ к Коммутатору. В настоящее время существует три версии протокола безопасности TACACS. Все они поддеживаются программным обеспечением Коммутатора:

- **TACACS** (Terminal Access Controller Access Control System) – обеспечивает проверку пароля и аутентификацию пользователя, а также отправляет уведомления о пользовательских действиях в целях безопасности через один или несколько централизованных TACACS-серверов, используя UDP-протокол для передачи пакетов.
- **Extended TACACS (XTACACS) –** Расширение протокола TACACS с возможностью обеспечения большего числа типов запросов аутентификации и большего числа типов кодов

ответов, по сравнению с TACACS. XTACACS для передачи пакетов также использует протокол UDP.

- **TACACS+ (Terminal Access Controller Access Control System plus**) – предоставляет детализированное управление доступом для аутентификации сетевых устройств. TACACS+ позволяет передавать аутентификационные команды через один и более централизованных серверов. Протокол TACACS+ обеспечивает шифрование трафика между коммутатором и TACACS+-сервером и использует более надежный протокол TCP для доставки данных.

Для нормальной работы функции безопасности TACACS/XTACACS/TACACS+/RADIUS необходимо также настроить TACACS/XTACACS/TACACS+/RADIUS-сервер на сервере аутентификации и задать на нем имена пользователей и пароли для аутентификации. Тогда при вводе имени пользователя и пароля, коммутатор обратится за подтверждением подлинности к TACACS/XTACACS/TACACS+/RADIUS-серверу, который ответит одним из трех сообщений:

- Сервер подтверждает имя пользователя и пароль, и пользователю предоставляется доступ к коммутатору с привилегиями пользователя.
- Сервер не принимает имя пользователя и пароль, пользователю отказано в доступе к коммутатору.
- Сервер не отвечает на запрос. В данном случае коммутатор выжидает заданный таймаут и переходит к следующему настроенному способу подтверждения в списке.

Коммутатор оснащен четырьмя встроенными группами серверов аутентификации ***Authentication Server Groups,*** по одной на каждый из протоколов TACACS, XTACACS, TACACS+, RADIUS. Эти группы используются для аутентификации пользователей, пытающихся получить доступ к коммутатору. Пользователи располагают серверы аутентификации в группе серверов аутентификации в предпочтительном порядке. Когда пользователи попытаются получить доступ к коммутатору, он сначала обратится к первому серверу аутентификации в списке. Если аутентификации не произойдет, то далее Коммутатор обратится к второму серверу в списке и т.д. Группа серверов аутентификации может содержать серверы, работающие по одному протоколу. Например, в группе серверов аутентификации TACACS могут быть только серверы TACACS. Администратор может установить до шести различных методов аутентификации в списке методов для аутентификации (TACACS/XTACACS/TACACS+/RADIUS/local/none). Эти методы должны быть занесены в список в приоритетном порядке. Пользователь может задать до 8 вариантов аутентификации. Когда пользователь будет пытаться получить доступ к коммутатору, коммутатор выберет первый метод из указанных в списке. Коммутатор будет перебирать методы аутентификации в списке до тех пор, пока не получит аутентификацию или е дойдет до конца списка.

Пожалуйста, обратите внимание, что пользователям будет предоставляться доступ к коммутатору с уровнем привилегий User. Для получения доступа с уровнем привилегий Admin, необходимо открыть окно **Enable Admin** и ввести пароль, который был ранее настроен на коммутаторе администратором.

ПРИМЕЧАНИЕ: Протоколы TACACS, XTACACS и TACACS+ не поддерживают совместимость друг с другом. Поэтому Коммутатор и сервер должны быть идентично настроены и использовать один и тот же протокол. (Например, если на коммутаторе установлена аутентификация TACACS, то и на сервере должен использоваться тот же протокол TACACS).

Настройки политики и параметров аутентификации

Показанное ниже окно позволяет администратору включить политику аутентификации для пользователей, пытающихся получить доступ к коммутатору. Когда данная политика включена, устройство проверяет список методов регистрации (Login Method List) и выбирает метод аутентификации пользователя при регистрации.

Для работы со следующим окном нажмите **Security > Access Authentication Control > Authentication Policy and Parameter Settings**:

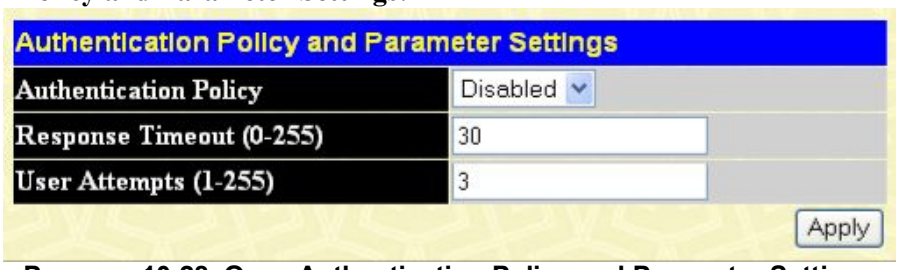


Рисунок 10-28. Окно Authentication Policy and Parameter Settings

Могут быть установлены следующие параметры:

Параметр	Описание
Authentication Policy	Данное выпадающее меню позволяет включить (Enabled) и выключить (Disabled) политику аутентификации на Коммутаторе.
Response Timeout (0-255)	Данное поле позволяет задать время ожидания от пользователя информации аутентификации. Доступны значения от 0 до 255 секунд. По умолчанию установлено 30секунд.
User Attempts (1-255)	Данная команда задает максимальное количество попыток получения аутентификации пользователями на Коммутаторе. Пользователям, исчерпавшим установленное количество попыток, будет отказано в доступе к Коммутатору и дальнейшие попытки аутентификации будут заблокированы. Пользователям Интерфейса командной строки CLI будет предоставлено 60 секунд перед следующей попыткой аутентификации. Пользователи Telnet и Web-интерфейса будут отключены от коммутатора. Существует возможность установить количество попыток от 1 до 255 (по умолчанию их 3).

Кликните по **Apply** для применения выполненных изменений.

Настройки аутентификации приложений

Данное окно используется для настройки приложений, с помощью которых осуществляется управление коммутатора (консоль, Telnet, SSH, Web-интерфейс), и для регистрации на уровне пользователя и уровне администратора (Enable Admin), следуя настроенному ранее списку методов. Для работы с данным окном нажмите: **Security > Access Authentication Control > Application Authentication Settings**:

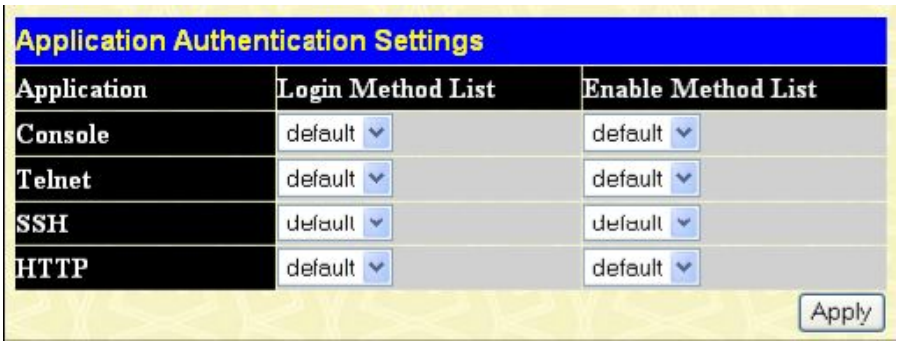


Рисунок 10-29. Окно Application Authentication Settings

Могут быть установлены следующие параметры:

Параметр	Описание

Application	Списки приложений управления Коммутатора. Пользователь может настроить Login Method List и Enable Method List для аутентификации пользователей, использующих интерфейс командной строки, Telnet, SSH и WEB (HTTP)-интерфейс.
Login Method List	С помощью выпадающего меню настройте стандартную регистрацию на уровне пользователя, используя ранее настроенный список методов. Пользователь может использовать список методов по умолчанию (default) или другой, настроенный пользователем. Более подробная информация доступна в окне **Login Method Lists** в этом разделе.
Enable Method List	С помощью выпадающего меню настройте стандартную регистрацию на уровне пользователя, используя ранее настроенный список методов. Пользователь может использовать список методов по умолчанию (default) или другой, настроенный пользователем. Более подробная информация доступна в окне **Enable Method Lists** в этом разделе.

Кликните по **Apply** для применения выполненных изменений настроек.

Группа серверов аутентификации

Данное окно позволяет пользователям настроить на коммутаторе группу серверов аутентификации (***Authentication Server Groups)***. Группа серверов – это способ, используемый для группировки TACACS/XTACACS/TACACS+/RADIUS-серверов в определенную пользователем категорию для аутентификации с помощью списка методов. Тип группы серверов определяется используемым протоколом, или же пользователь может самостоятельно настроить группу серверов. Коммутатор поддерживает четыре встроенные группы серверов аутентификации, которые доступны для изменения настроек, но не могут быть удалены. В каждую группу может быть внесено до 8 серверов аутентификации. Для просмотра следующего окна, нажмите **Security > Access Authentication Control > Authentication Server Group**:

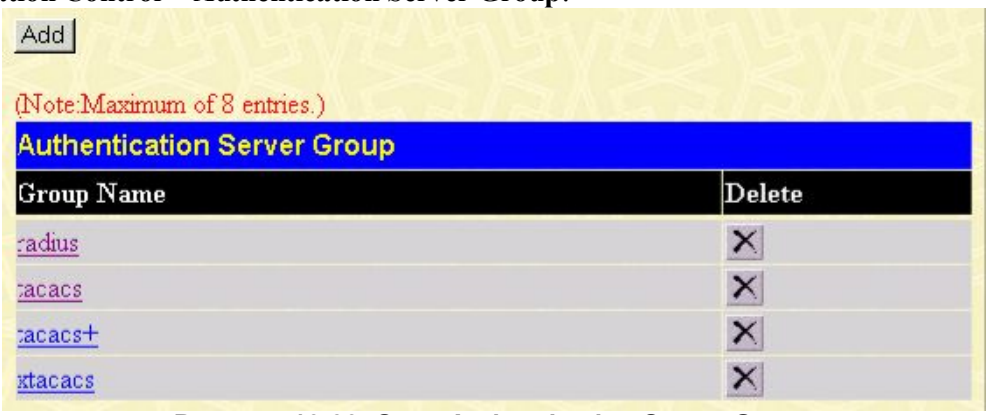


Рисунок 10-30. Окно Authentication Server Group

В данном окне отображаются существующие на коммутаторе группы серверов аутентификации. Как говорилось ранее, Коммутатор поддерживает четыре группы серверов аутентификации. Эти группы нельзя удалить, но можно изменить их настройки. Для этого необходимо кликнуть по гиперссылке имени группы, после чего отобразится следующее окно.

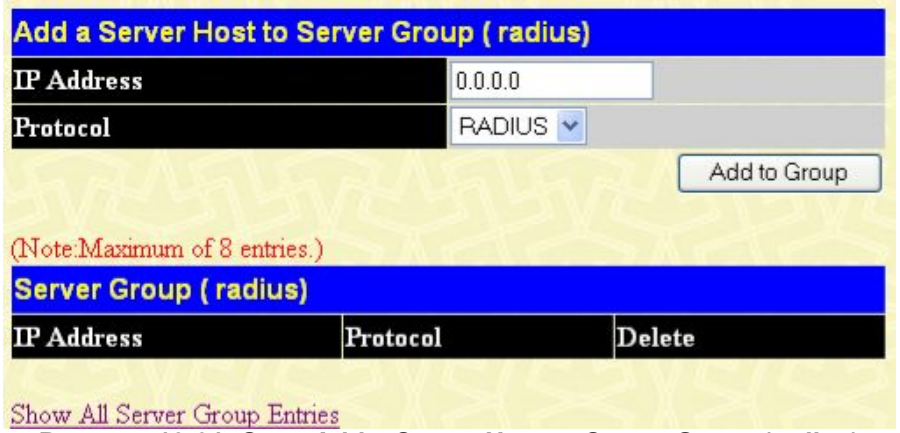


Рисунок 10-31. Окно Add a Server Host to Server Group (radius)

Чтобы добавить хост сервера аутентификации в список, введите его IP-адрес в поле IP Address, выберите протокол, связанный с IP-адресом хоста сервера аутентификации, и кликните по **Add to Group,** чтобы добавит данный хост сервера аутентификации в группу.

Чтобы добавить определенную пользователем группу в список, кликните по кнопке Add в окне **Authentication Server Group.** В результате появится следующее окно:

Рисунок 10-32. Окно Authentication Server Group Table Add Settings

Для идентификации пользовательской группы серверов аутентификации введите название группы длиной не более 15 буквенно-цифровых символов и кликните по *Apply*. Новое имя группы, заданное пользователем, появится в окне **Authentication Server Group**.

ПРИМЕЧАНИЕ: Пользователь должен настроить серверы аутентификации, используя окно **Authentication Server Hosts**, прежде чем добавить их в список. Серверы аутентификации должны быть настроены согласно протоколам, определенным центральным удаленным сервером. После этого данная функция будет работать надлежащим образом.

ПРИМЕЧАНИЕ: Протоколы TACACS/XTACACS/TACACS+ являются различными протоколами и не поддерживают совместимость друг с другом. Поэтому встроенные группы серверов аутентификации TACACS/XTACACS/TACACS+ могут включать только серверы с заданным протоколом.

Серверы аутентификации

Это окно позволяет установить хосты серверов аутентификации для протоколов безопасности TACACS/XTACACS/TACACS+/RADIUS на Коммутаторе. Когда пользователь пытается получить доступ к коммутатору по заданной политике аутентификации, коммутатор отправляет аутентификационные пакеты на удаленный TACACS/XTACACS/TACACS+/RADIUS-сервер. TACACS/XTACACS/TACACS+/RADIUS-сервер подтвердит или отклонит запрос и отправит коммутатору соответствующее сообщение. На одном физическом сервере одновременно могут работать более одного протокола аутентификации, однако следует помнить, что протоколы TACACS/XTACACS/TACACS+/RADIUS не поддерживают совместимоть друг с другом. Максимальное число поддерживаемых серверов 16. Для работы со следующим окном нажмите **Security > Access Authentication Control > Authentication Server Host**:

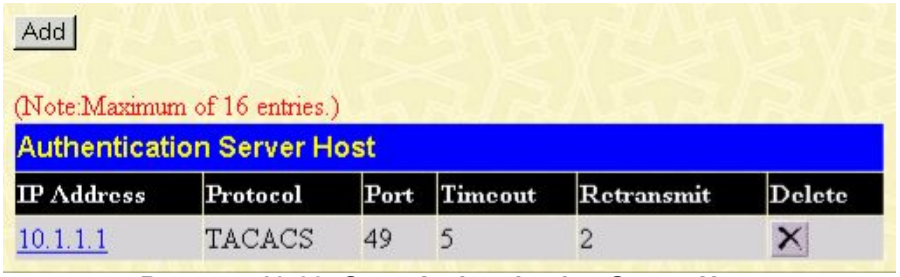


Рисунок 10-33. Окно Authentication Server Host

Для добавления сервера аутентификации кликните по кнопке **Add**, в результате откроется следующее окно:

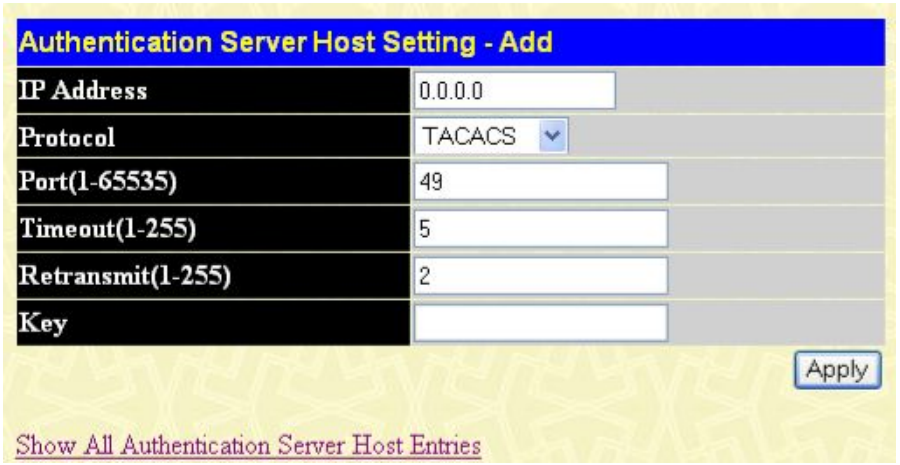


Рисунок 10-34. Окно Authentication Server Host Setting – Add

Чтобы отредактировать настройки сервера аутентификации, кликните по ссылке IP-адреса, после чего появится следующее окно:

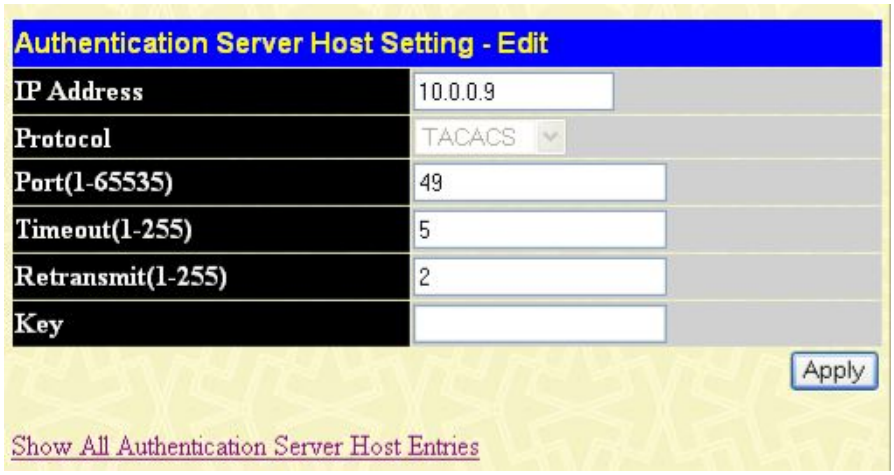


Рисунок 10-35. Окно Authentication Server Host Setting – Edit

Настройте следующие параметры, чтобы добавить сервер аутентификации:

Параметр	Описание
IP Address	IP-адрес внешнего сервера аутентификации, который предполагается добавить.
Protocol	Данное выпадающее меню позволяет ввести протокол, используемый сервером. Пользователь может выбрать один из следующих протоколов: ▪ TACACS – выбор данной опции означает, что сервер будет использовать протокол TACACS. ▪ XTACACS - выбор данной опции означает, что сервер будет использовать протокол XTACACS. ▪ TACACS+ - выбор данной опции означает, что сервер будет использовать протокол TACACS+. ▪ RADIUS - выбор данной опции означает, что сервер будет использовать протокол RADIUS.
Port (1-65535)	Введите номер виртуального порта протокола аутентификации для сервера. Доступный диапазон значений 1-65535. По умолчанию для TACACS/XTACACS/TACACS+-серверов задан номер порта 49, а для RADIUS-сервера 1813. Но для обеспечения большего уровня безопасности пользователь может настроить уникальный номер порта.
Timeout (1-255)	Введите время (в секундах), в течение которого коммутатор будет ожидать ответ от сервера на запрос аутентификации. По умолчанию данное значение равно 5 секундам.
Retransmit (1-255)	В данном поле введите, сколько раз устройство будет повторно отправлять запросы аутентификации, если TACACS-сервер не отвечает.

Key	Ключ аутентификации используется только для настройки серверов TACACS или RADIUS. Необходимо ввести буквенно-цифровую строку не более 254 символов.

Кликните по **Apply,** чтобы добавить сервер.

ПРИМЕЧАНИЕ: На одном физическом сервере одновременно могут работать более одного протокола аутентификации, однако, протоколы TACACS/XTACACS/TACACS+/RADIUS различны и не поддерживают совместимость друг с другом.

Список методов регистрации

Показанное ниже окно позволяет настроить определенный пользователем или созданный по умолчанию список методов регистрации (Login Metod Lists), который будет использоваться при регистрации пользователей на коммутаторе. Последовательность методов аутентификации в списке влияет на порядок аутентификации. Например, если пользователь введет последовательность методов TACACS-XTACACS–local, то коммутатор сначала отправит запрос аутентификации к первому серверу TACACS в группе серверов. Не получив ответа от этого сервера, коммутатор отправляет запрос на аутентификацию второму TACACS-серверу в группе серверов и т.д., пока не дойдет до конца списка или не получит ответ на запрос аутентификации. Если аутентификация так и не произошла, то коммутатор отправит запрос серверу XTACACS (следующий протокол, указанный в списке). Если аутентификация не произошла и по XTACACS, то для аутентификации пользователя будет использоваться локальная база, установленная на коммутаторе. Когда используется локальный метод, уровень привилегий будет зависеть от настроенной на коммутаторе привилегии локальной учетной записи.

Такая регистрация позволяет пользователю получить только привилегию уровня «User». Для получения привелегий уровня **Admin** необходимо воспользоваться окном **Enable Admin,** в котором необходимо ввести пароль, настроенный администратором ранее. (Для получения более подробной информации, касающейся окна Enable Admin, обратитесь, пожалуйста, к соответствующей главе данного Руководства). Для работы со следующим окном нажмите **Security > Access Authentication Control > Login Method Lists**:

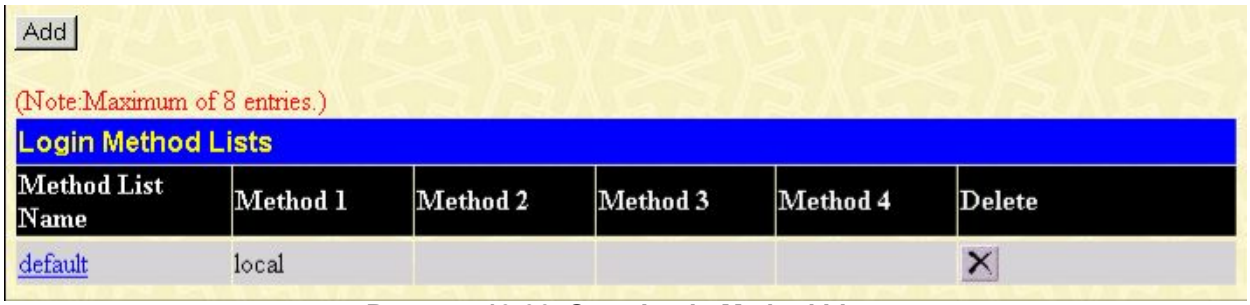


Рисунок 10-36. Окно Login Method Lists

Коммутатор поддерживает один список методов (default), который не может быть удален, однако его настройки доступны для изменения. Для удаления списка методов регистрации, определенного пользователем, кликните по соответствующему значку ✕ под заголовком **Delete** напротив соответствующей записи. Для изменения настроек списка методов регистрации кликните по гиперссылке Method List Name. Для настройки нового списка методов кликните по кнопке **Add**. В результате обоих действий появится следующее окно для настройки:

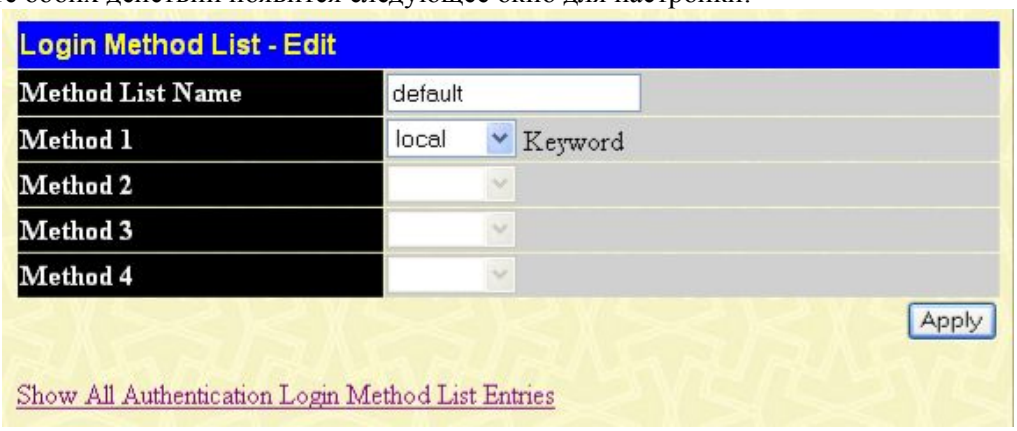


Рисунок 10-37. Окно Login Method List - Edit (default)

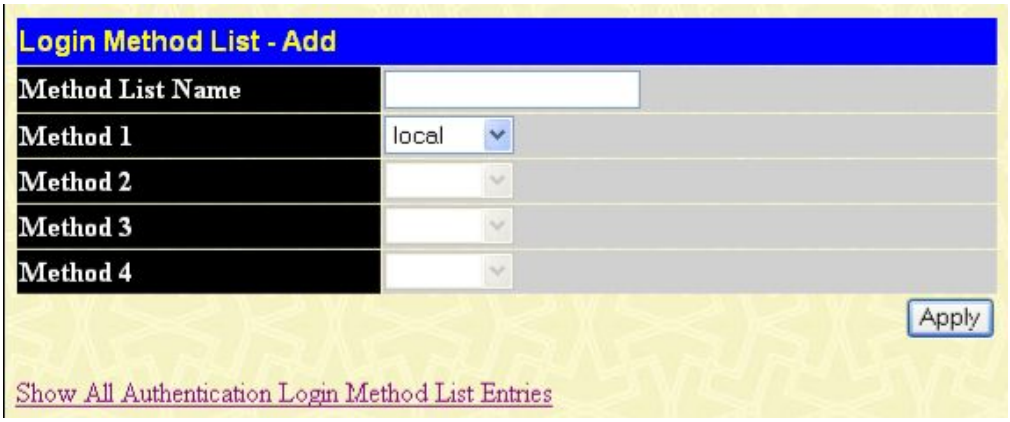


Рисунок 10-38. Окно Login Method List – Add

Для задания списка методов регистрации установите следующие параметры и кликните по **Apply**:

Параметр	Описание
Method List Name	Введите название списка методов, определенного пользователем, длиной не более 15 символов.
Method 1, 2, 3, 4	Пользователь может добавить в данный список методов один метод или комбинацию (до 4) из следующих методов аутентификации: ▪ *tacacs* – для аутентификации пользователя с помощью протокола TACACS с внешнего TACACS-сервера. ▪ *tacacs+* - для аутентификации пользователя с помощью протокола TACACS+ с внешнего TACACS+-сервера. ▪ *Radius* - для аутентификации пользователя с помощью протокола RADIUS с внешнего RADIUS-сервера. ▪ *server_group* – для аутентификации пользователя в соответствии с определенной пользователем группой серверов, настроенной ранее на коммутаторе. ▪ *local* – для аутентификации пользователя с помощью локальной базы данных, настроенной на коммутаторе. ▪ *none* – для отсутствия аутентификации.

Enable Method Lists

Окно **Enable Method List Settings** позволяет настроить списки методов аутентификации для перехода от привилегии уровня пользователя до привилегии уровня администратора (Admin), используя методы аутентификации на коммутаторе. Аутенцифицировавшись и получив привилегию уровня User на коммутаторе, пользователь може повысить уровень своих привилегий до Admin, пройдя соответствующую аутентификацию. Коммутатор поддерживает до восьми списков Enable Method List, один из которых установлен по умолчанию. Установленный по умолчанию Enable Method List доступен для изменения, но не может быть удален.
Последовательность методов аутентификации в списке влияет на порядок аутентификации.
Например, при задании последовательности методов TACACS – XTACACS – Local Enable коммутатор отправит запрос аутентификации сначала на первый TACACS-сервер в группе серверов, затем, если аутентификация не произошла, на второй TACACS-сервер в группе серверов и т.д., пока не дойдет до конца списка. Далее аналогично произойдет и серверами XTACACS.
Если аутентификации по XTACACS не произошло, то для аутентификации пользователя будет использоваться пароль Local Enable (локальный пароль), установленный на коммутаторе. Успешно прошедшая аутентификация с помощью любого из этих методов даст пользователю привилегию уровня «Admin».

ПРИМЕЧАНИЕ: Рекомендации по настройке локального пароля доступны далее в соответствующем разделе данного Руководства.

Для работы со следующим окном нажмите **Security > Access Authentication Control > Enable Method Lists**:

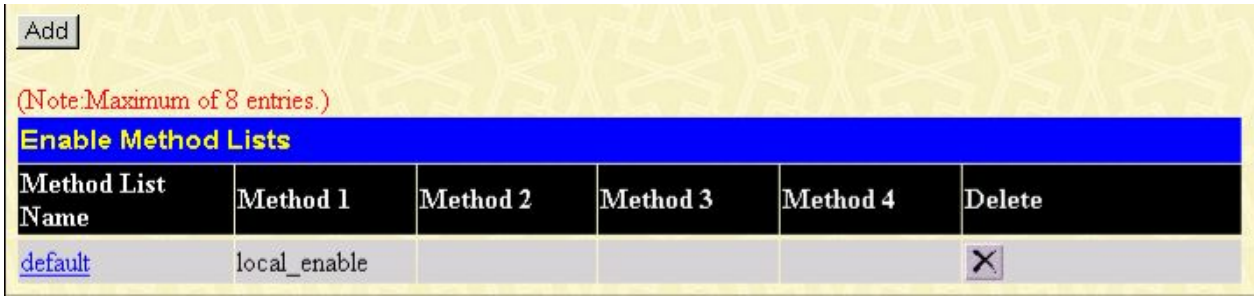


Рисунок 10-39. Окно Enable Method Lists

Для удаления списка Enable Method List, созданного пользователем, нажмите ✕ под заголовком Delete напротив соответствующей записи, которую хотите удалить. Для изменения существующего Enable Method List нажмите на соответствующую гиперссылку Method List Name. Чтобы добавить новый Enable Method List, кликните по кнопке **Add**. Данные действия приведут к открытию следующего окна:

Рисунок 10-40. Окно Enable Method List - Edit

Рисунок 10-413. Окно Enable Method List - Add

Чтобы определить Enable Login Method List, установите следующие параметры и кликните по **Apply**:

Параметр	Описание
Method List Name	Введите название списка методов, определенного пользователем, длиной не более 15 символов.
Method 1, 2, 3, 4	Пользователь может добавить один метод или комбинацию (до 4) из следующих методов аутентификации к данному списку методов: ▪ *local_enablel* - для аутентификации пользователя с помощью локального пароля. ▪ *none* – для отсутствия аутентификации. ▪ *Radius* - для аутентификации пользователя с помощью протокола RADIUS с внешнего RADIUS-сервера ▪ *tacacs* – для аутентификации пользователя с помощью протокола TACACS с внешнего TACACS-сервера. ▪ *tacacs+* - для аутентификации пользователя с помощью протокола TACACS+ с внешнего TACACS+-сервера.

	▪ *server_group* – для аутентификации пользователя в соответствии с определенной пользователем группой серверов, настроенной ранее на коммутаторе.

Настройка локального пароля (Local Enable Password)

Данное окно позволяет настроить локальный пароль (locally enable password), позволяющий перейти от привилегий уровня пользователя к привилегиям уровня администратора (Enable Admin). При использовании метода «local_enable» для повышения привилегии от уровня пользователя до уровня администратора (Admin) пользователю будет предложено ввести пароль, который локально установлен на коммутаторе. Для работы со следующим окном нажмите **Security > Access Authentication Control > Configure Local Enable Password**:

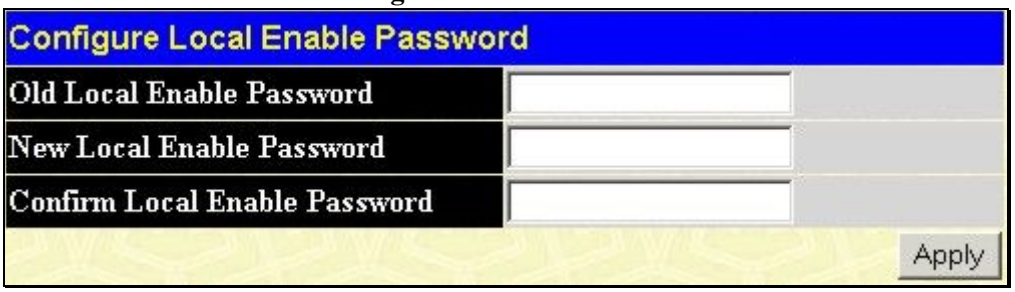


Рисунок 10-42. Окно Configure Local Enable Password

Для настройки локального пароля установите следующие параметры и кликните **Apply**.

Параметр	Описание
Old Local Enabled	Чтобы сменить существующий локальный пароль на новый, необходимо ввести в данном поле действующий пароль.
New Local Enabled	Данное поле позволяет задать новый локальный пароль длиной не более 15 символов.
Confirm Local Enabled	Подтвердите ввод нового пароля. Введение в данном поле пароля, отличного от пароля в поле New Local Enabled, приведет к появлению сообщения об ошибке.

Enable Admin

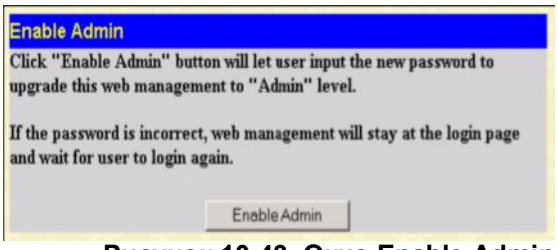


Рисунок 10-43. Окно Enable Admin

Окно **Enable Admin** позволяет пользователям, зарегистрировавшимся на коммутаторе с привилегиями уровня User, повысить привилегии до уровня Admin. Для этого пользователю необходимо всего лишь открыть данное окно и ввести нужный пароль для аутентификации. Данная функция позволяет осуществить аутентификацию на основе протоколов TACACS/XTACACS/TACACS+/RADIUS, заданной пользователем группы серверов. Также возможна аутентификация на основе локальнолй базы данных (локальная учетная запись на коммутаторе) или отсутствие аутентификации. При использовании протоколов XTACACS и TACACS пользователю необходимо создать специальную учетную запись на сервере с именем пользователя «enable» и паролем, заданным администратором, для поддержки функции «enable». Эта функция становится недоступна, когда функция политики аутентификации выключена. Когда появится данное окно, нажмите кнопку **Enable Admin**, возникнет показанное ниже диалоговое окно, где пользователю необходимо будет ввести имя пользователя и пароль для аутентификации. При корректном вводе данных пользователь получит привилегии уровня администратора.

Рисунок 10-44. Диалоговое окно Enter Network Password

Сегментация трафика

Сегментация трафика используется для ограничения трафика от одного порта Коммутатора к группе его других портов (при использовании одного Коммутатора) или к группе портов другого коммутатора в стеке (по технологии Single IP). Этот метод сегментации трафика аналогичен используемой технологии для ограничения трафика в VLAN, но ограничения при сегментации трафика еще более строгие. При использовании сегментации пакеты передаются по сети таким образом, чтобы не вызвать перегрузку CPU Master-коммутатора.

В папке **Security** кликните по **Traffic Segmentation**. Откроется окно, показанное ниже.

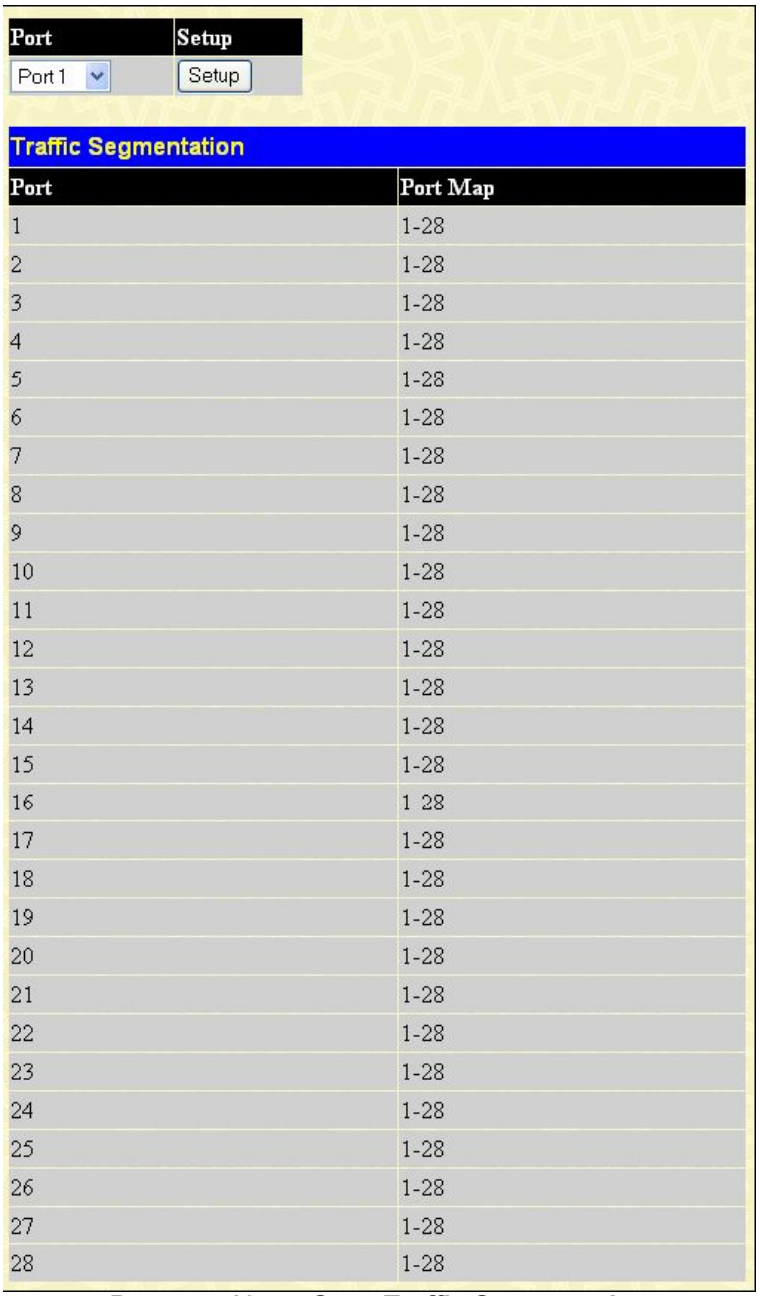


Рисунок 10-45. Окно Traffic Segmentation

Чтобы задать принимающие порты для данного порта, выберите в выпадающем меню нужный порт и кликните **Setup**. Появится окно, показанное ниже.

Рисунок 10- 46. Окно Setup Forwarding Ports

Данное окно позволяет задать комбинацию передающего и принимающих портов для каждого порта, выбранного с помощью выпадающего меню **Port**. Комбинация передающего и разрешенных принимающих портов передается в таблицу **Traffic Segmentation Table** после нажатия на кнопку **Apply**.

Раздел 11

Мониторинг

Использование CPU
Использование порта
Пакеты
Ошибки
Размер пакетов
MAC-адрес
Системный журнал коммутатора
Группа IGMP Snooping
Порт маршрутизатора
Статические настройки ARP
Таблица сессий
Управление доступом порта

Использование CPU

Окно **CPU Utilization** отображает процентное соотношение использования CPU. Для работы с данным окном откройте папку **Monitoring** и кликните по ссылке **CPU Utilization**.

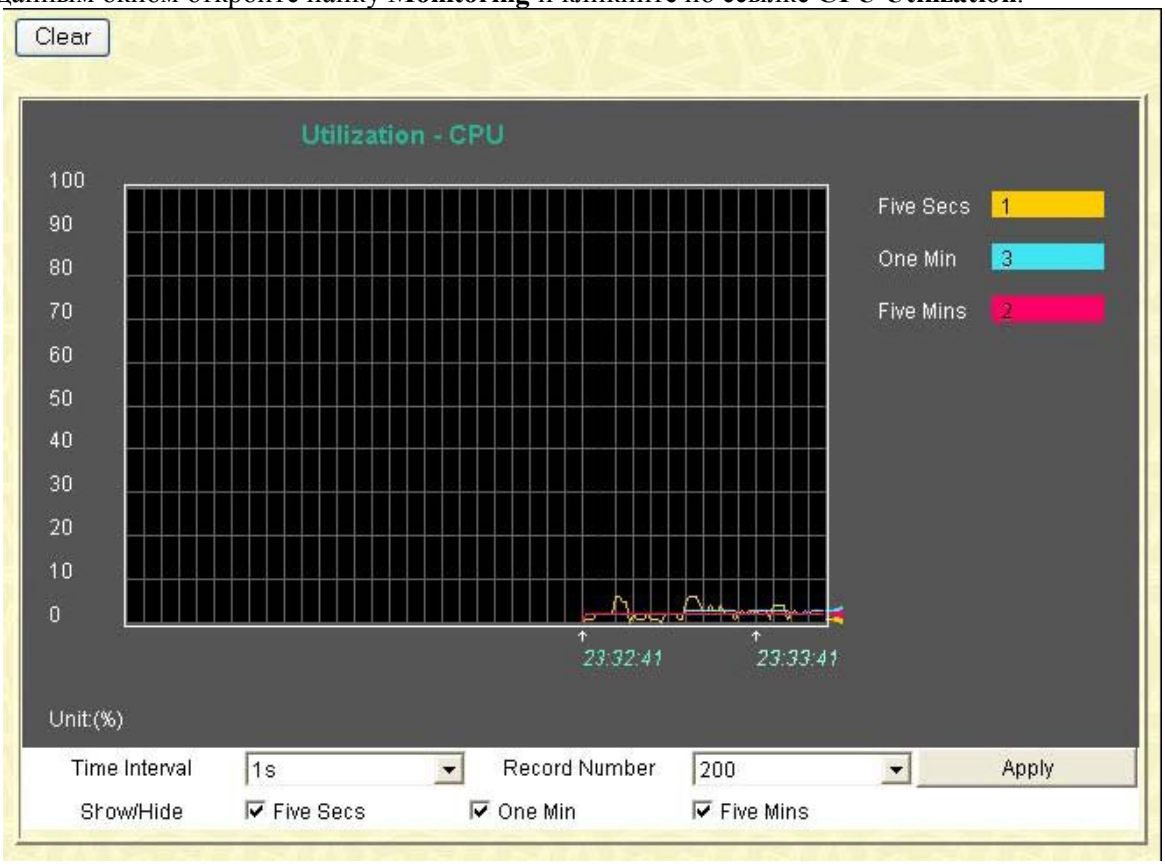


Рисунок 11.1 – Окно CPU Utilization

Нажмите **Apply** для того, чтобы настройки вступили в силу. Окно автоматически обновит статистику по параметрам, описанным ниже:

Параметр	Описание
Time Interval	Выберите желаемое значение временного интервала от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1s.
Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное

	значение по умолчанию равно 200.
Show/Hide	Данное поле позволяет отследить и сравнить использование CPU через пять секунд (*Five Secs)*, одну минуту (*One Min)* и пять минут (*Five Min)*. Поставив галочки сразу в трех полях, можно увидеть три графика различных цветов (опции *Five Secs* соответствует желтый цвет, *One Min* – голубой, *Five Min* –розовый).
Clear	Кликнув по этой кнопке, можно очистить статистику по всем счетчикам в данном окне.

Использование порта

Функция Port Utilization (Использование порта) является еще одним важным инструментом мониторинга состояния сети. 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.**

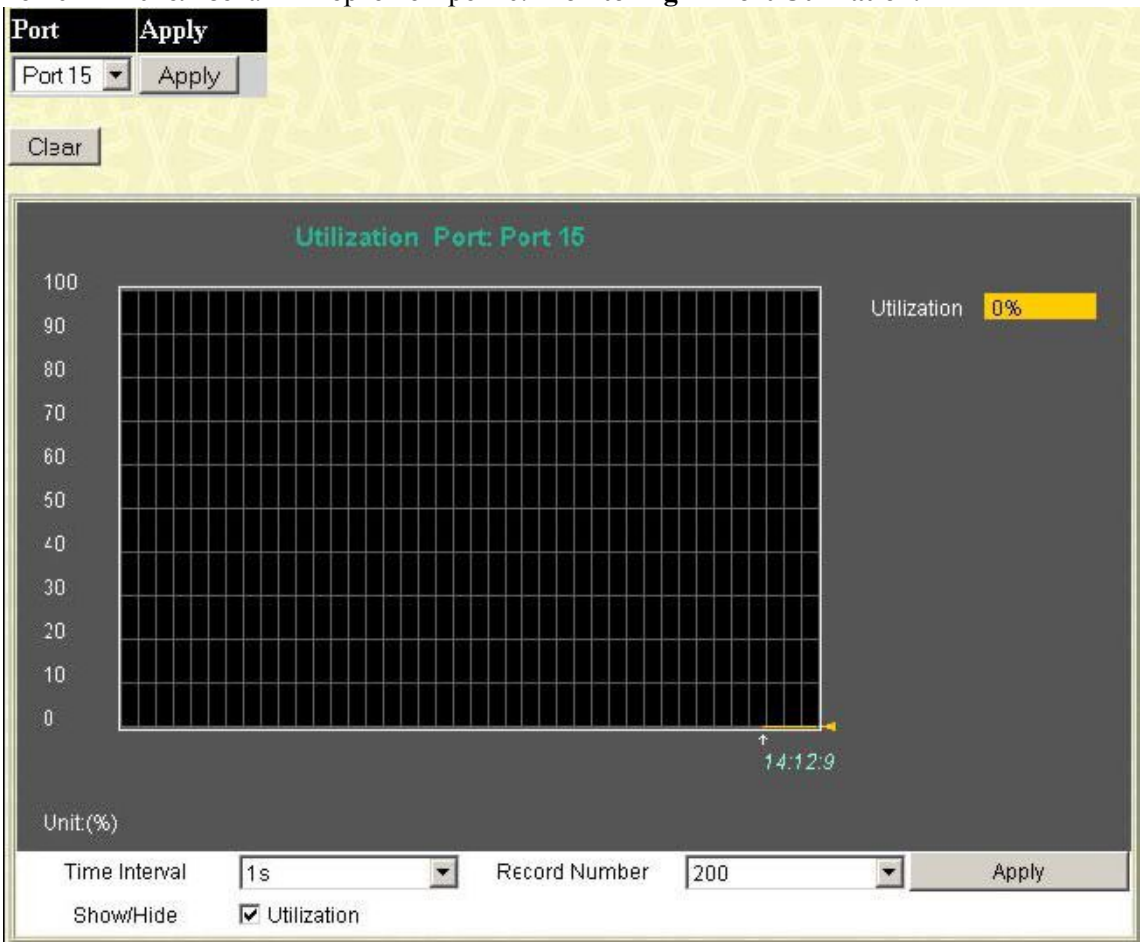


Рисунок 11.2 – Окно Port Utilization

Выберите номер порта в выпадающем меню и кликните по **Apply** для отображения диаграммы использования выбранного порта.

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с. Этот параметр указывает временной интервал, через который будет проводиться измерение использования порта.
Record Number	В этом поле необходимо указать значение от 20 до 200 (по умолчанию указано 200). Этот параметр задает, сколько раз будет измеряться значение использования порта с заданным временным интервалом (Time Interval).

Show/Hide	Отметьте, нужно или нет отобразить использование.
Clear	Кликнув по этой кнопке, можно очистить статистику по всем счетчикам в данном окне.

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

Пакеты

Web-интерфейс управления позволяет просматривать различные статистики по пакетам, как в графическом виде, так и в виде таблицы. Так, пользователь может просмотреть статистику по полученным пакетам, отправленным пакетам, а также многоадресным, одноадресным и широковещательным пакетам, полученным коммутатором. Ниже данные статистики будут рассмотрены более подробно.

Полученные пакеты(RX)

Для просмотра статистики по пакетам, полученным коммутатором, нажмите: **Monitoring ⇨ Packets ⇨ Received (RX).** Выберите порт для просмотра статистики с помощью выпадающего меню **Port**.

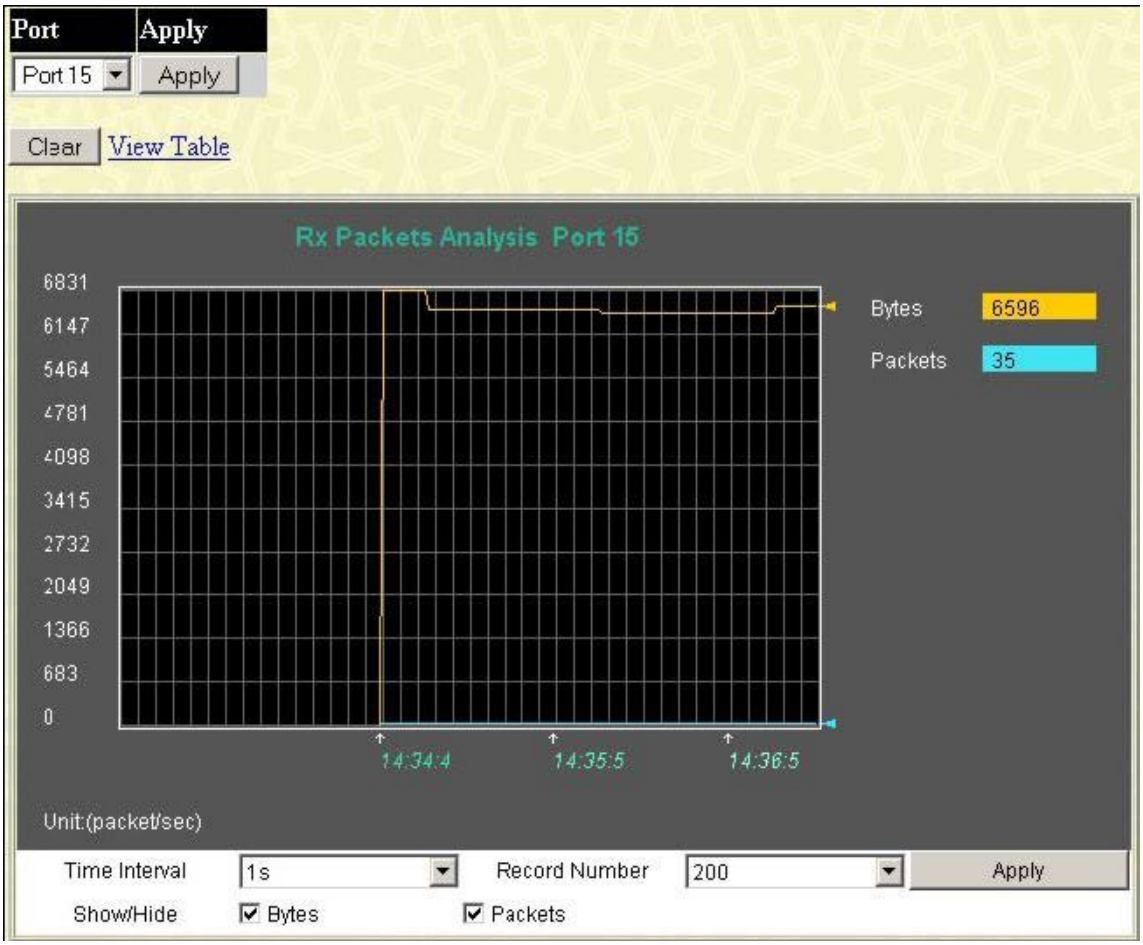


Рисунок 11.3 – Окно Rx Packets Analysis (график зависимости для байт и пакетов)

Чтобы просмотреть таблицу **Received Packets Table**, кликните по ссылке View Table, в результате отобразится следующая таблица:

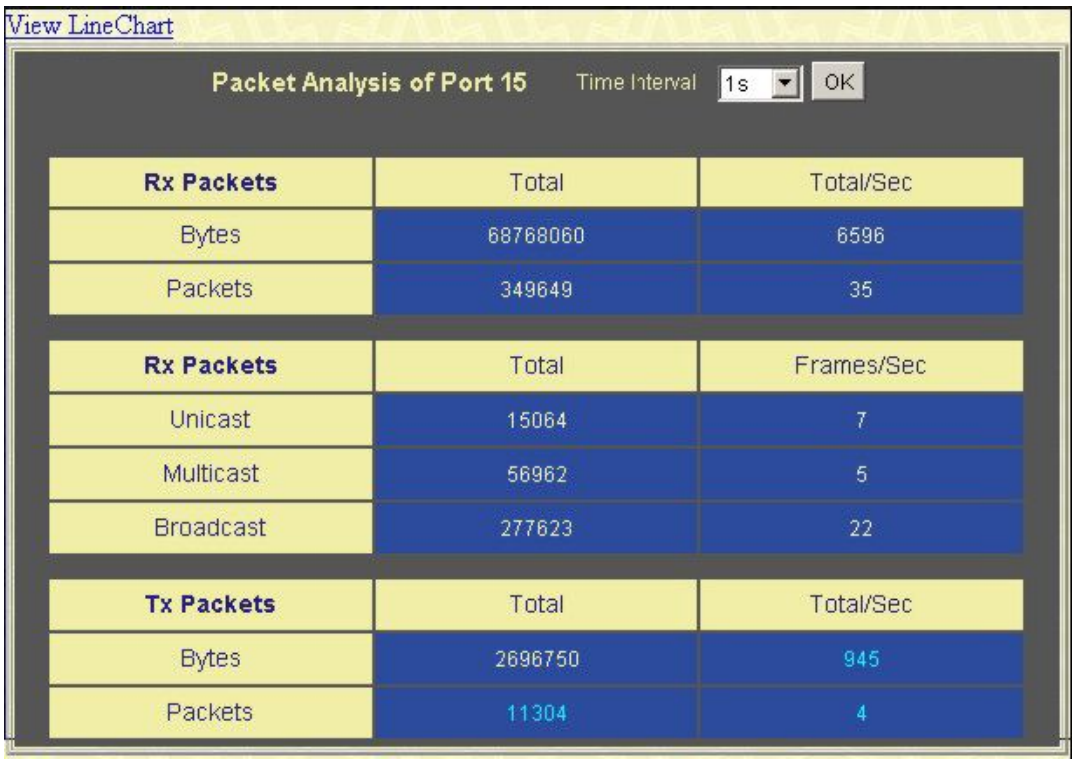


Рисунок 11.4 – Окно Rx Packets Analysis» (таблица зависимости для байт и пакетов)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с.
Record Number	Этот параметр задает, сколько раз будет измеряться количество пакетов с заданным временным интервалом (Time Interval). Данное значение по умолчанию равно 20.
Bytes	Подсчитывает число байт, полученных на порту.
Packets	Подсчитывает число пакетов, полученных на порту.
Unicast	Отображает количество полученных пакетов unicast без ошибок.
Multicast	Отображает количество полученных многоадресных пакетов без ошибок.
Broadcast	Отображает количество полученных широковещательных пакетов без ошибок.
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.

Полученные одноадресные, многоадресные и широковещательные пакеты (RX)

Для просмотра графика одноадресных, многоадресных и широковещательных пакетов, полученных коммутатором, нажмите: **Monitoring ⇨ Packets ⇨UMB Cast (RX).**

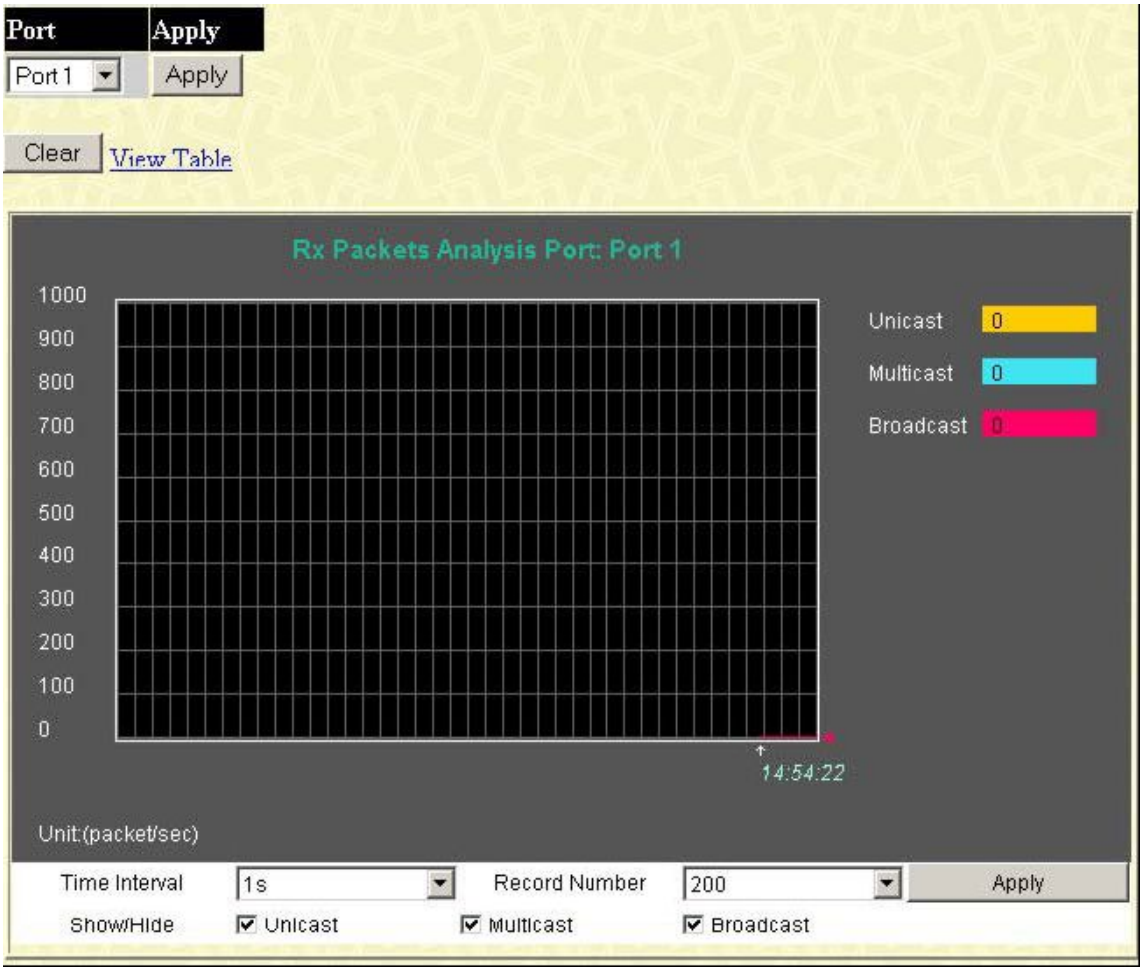


Рисунок 11.5 – Окно Rx Packets Analysis (график зависимости для одноадресных, многоадресных и широковещательных пакетов, полученных Коммутатором)

Для просмотра данной зависимости в виде таблицы кликните по ссылке View Table:

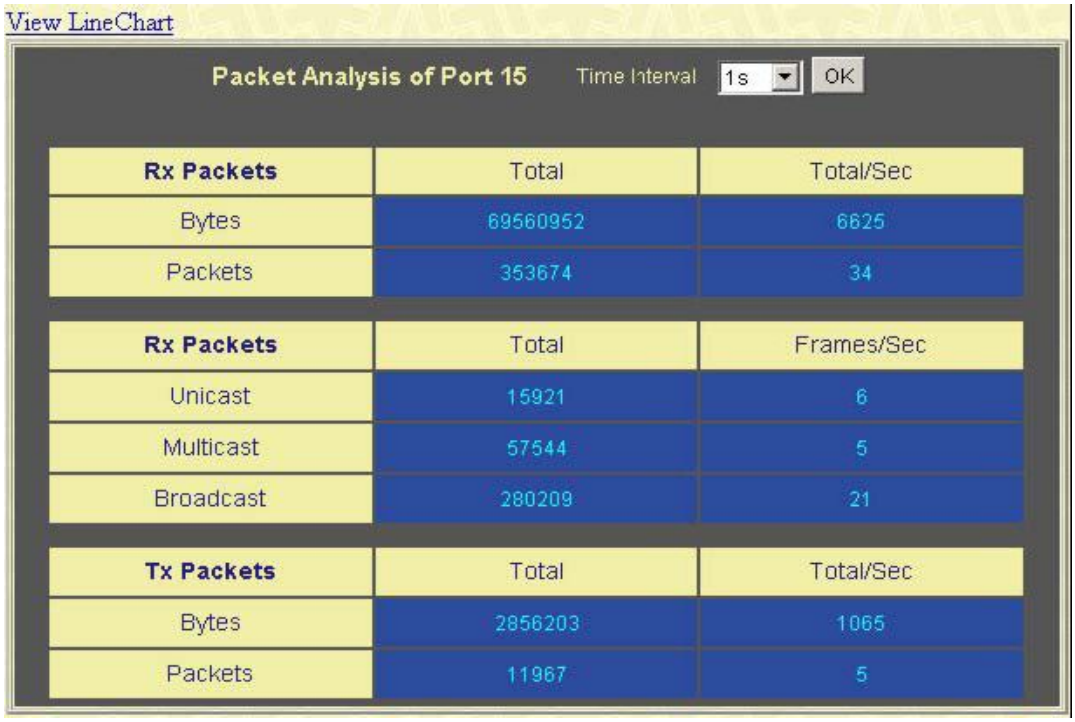


Рисунок 11.6 – Окно Rx Packets Analysis (таблица зависимости для одноадресных, многоадресных и широковещательных пакетов, полученных Коммутатором)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с.
Record Number	Этот параметр задает, сколько раз будет измеряться количество пакетов с заданным временным интервалом (Time Interval). Данное значение по умолчанию равно 20.
Unicast	Отображает количество полученных пакетов unicast без ошибок.
Multicast	Отображает количество полученных многоадресных пакетов без ошибок.
Broadcast	Отображает количество полученных широковещательных пакетов без ошибок.
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.

Отправленные пакеты (TX)

Для просмотра статистики по пакетам, отправленным коммутатором, нажмите: **Monitoring ⇨ Packets ⇨Transmitted (TX).** Укажите порт для просмотра статистики с помощью выпадающего меню **Port**.

Рисунок 11.7 – Окно Tx Packets Analysis (график зависимости для байт и пакетов)

Для просмотра количества переданных коммутатором пакетов TX в виде таблицы, кликните по ссылке View Table:

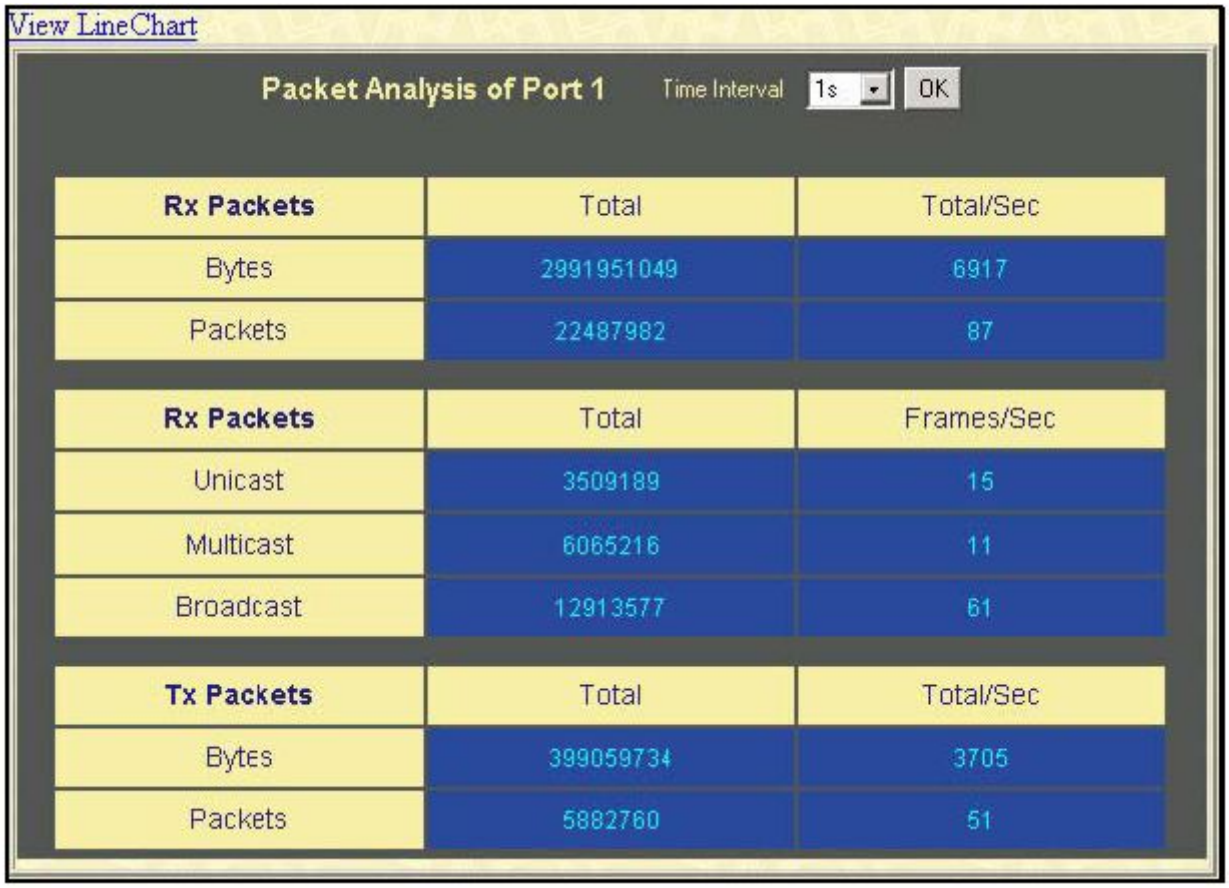


Рисунок 11.8 – Окно Tx Packets Analysis (таблица зависимости количества для байт и пакетов)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1с. Через данный временной интервал каждый раз будет измеряться количество пакетов.
Record Number	Этот параметр задает, сколько раз будет измеряться количество пакетов с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка. Данное значение по умолчанию равно 20.от 20 до 200. Данное значение по умолчанию равно 20.
Bytes	Подсчитывает число байт, отправленных с данного порта.
Packets	Подсчитывает число пакетов, отправленных с данного порта.
Show/Hide	Отметьте, нужно ли отображать байты и пакеты или нет.
Unicast	Отображает количество отправленных пакетов unicast без ошибок.
Multicast	Отображает количество отправленных многоадресных пакетов без ошибок.
Broadcast	Отображает количество отправленных широковещательных пакетов без ошибок.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Ошибки

Web-интерфейс управления позволяет просматривать статистику ошибок по порту, собранную агентом управления коммутатора, как в графическом виде, так и в виде таблицы. Далее остановимся на этом более подробно.

Ошибки в полученных коммутатором пакетах (RX)

Для просмотра следующего графика, отражающего количество ошибок в полученных Коммутатором пакетах, кликните по ссылке **Received (RX)** в папке **Errors** меню **Monitoring**. С помощью выпадающего меню **Port** выберите нужный порт.

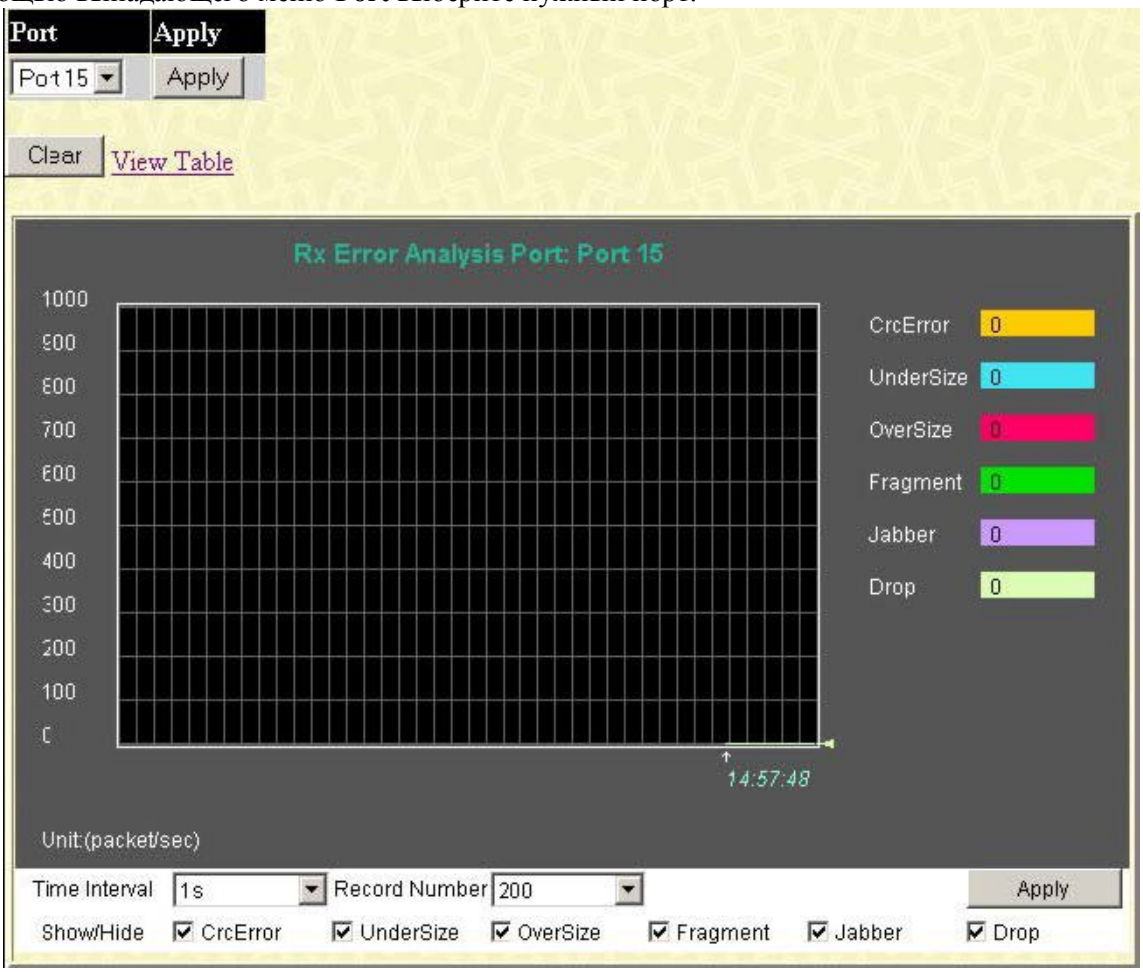


Рисунок 11.9 – Окно Rx Error Analysis (график зависимости)

Чтобы увидеть табличное отражение данной зависимости, кликните по ссылке View Table**:**

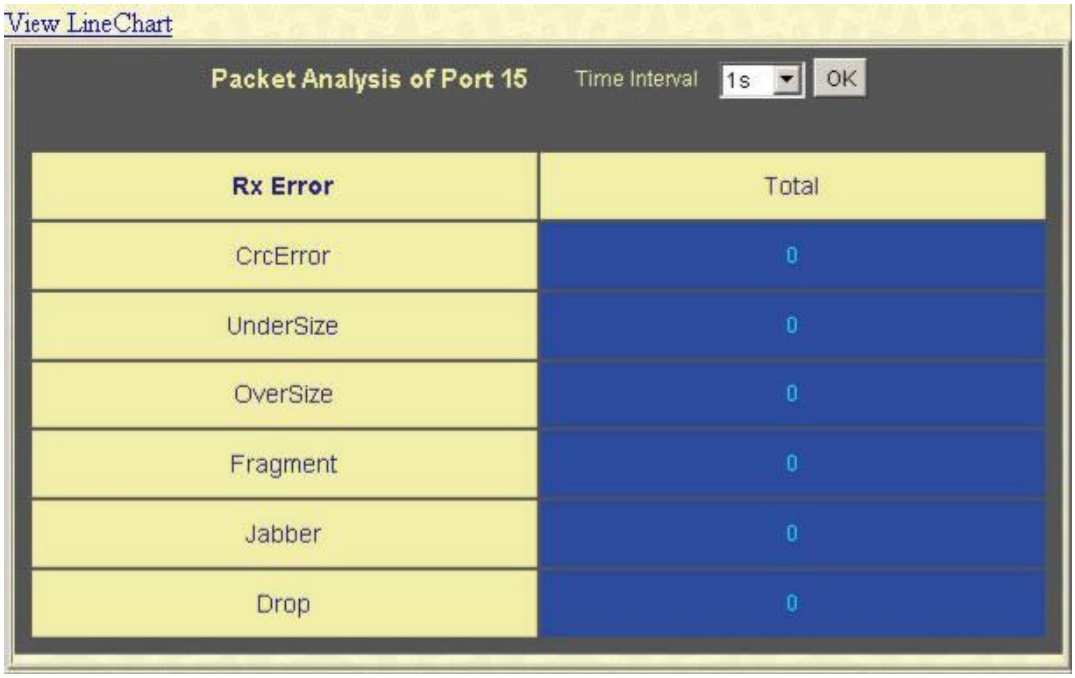


Рисунок 11.10 – Окно Rx Error Analysis (таблица)

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 1с.
Record Number	Этот параметр задает, сколько раз будет измеряться количество ошибок с заданным временным интервалом (Time Interval). Данное значение по умолчанию равно 20.
Crc Error	Подсчитывает количество пакетов, не прошедших проверку с помощью циклического избыточного кода.
Under Size	Количество обнаруженных пакетов длиной меньше, чем минимально допустимый размер пакета в 64 байт и верным значением CRC последовательности. Пакеты недостаточной длины обычно указывают на наличие коллизии.
Over Size	Количество пакетов, длиной более 1518 байт, или в случае фрейма VLAN, длиной менее значения MAX_PKT_LEN, равного 1522 байт.
Fragment	Количество пакетов, длиной меньше 64 байт, а также или неправильным значением CRC, что обычно свидетельствует о коллизиях.
Jabber	Количество пакетов, длиной более значения MAX_PKT_LEN, равного 1522 байт.
Drop	Количество пакетов, удаленных данным портом с момента последнего перезапуска коммутатора.
Show/Hide	Отметьте, нужно ли отображать или нет ошибки Crc Error, Under Size, Over Size, Fragment, Jabber и Drop.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Ошибки в отправленных коммутатором пакетах (TX)

Кликните по ссылке **Transmitted (TX)** в папке **Error** меню **Monitoring,** чтобы просмотреть следующий график ошибок в пакетах, полученных Коммутатором. С помощью выпадающего меню **Port** выберите нужный порт.

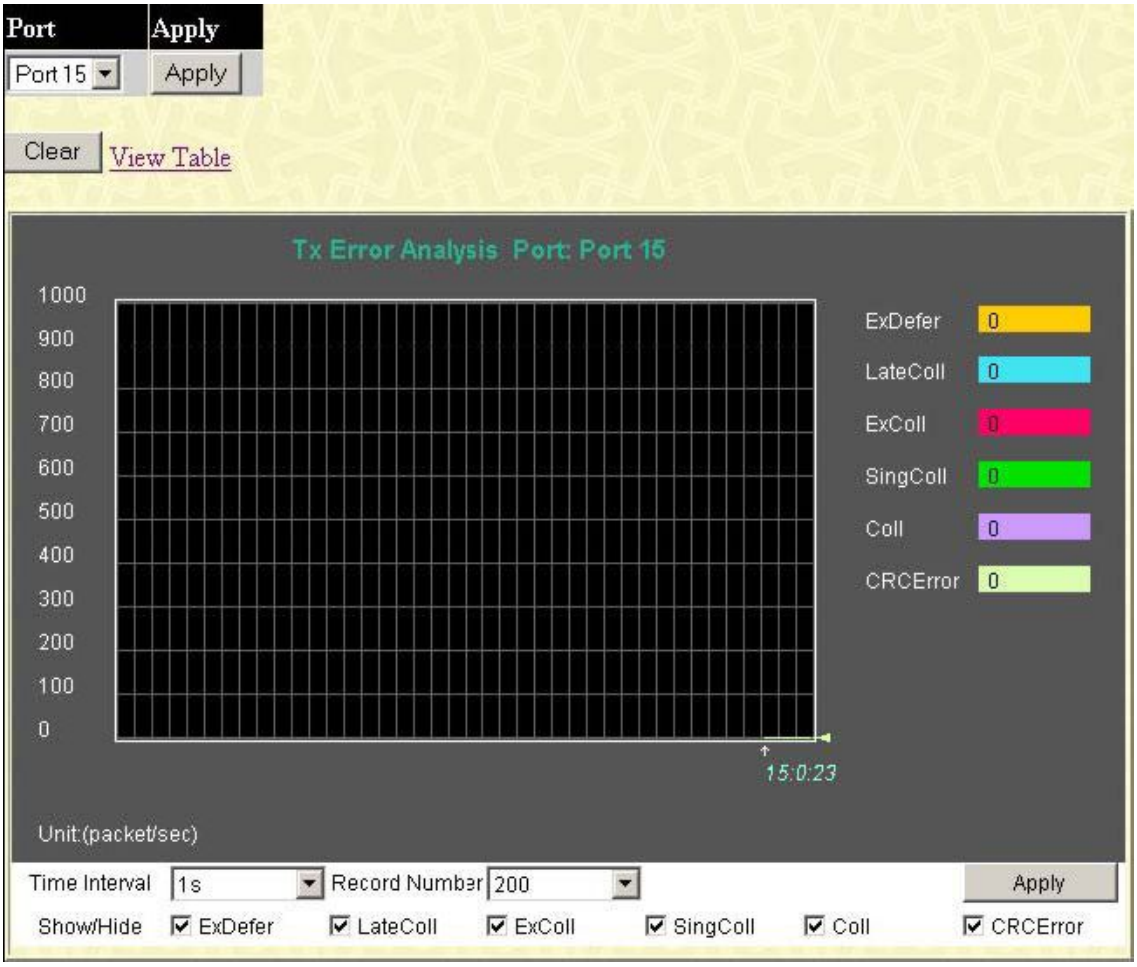


Рисунок 11.11 – Окно Tx Error Analysis (график зависимости)

Чтобы увидеть статистику по ошибкам в отправленных коммутатором пакетах в виде таблице, кликните по ссылке View Table**:**

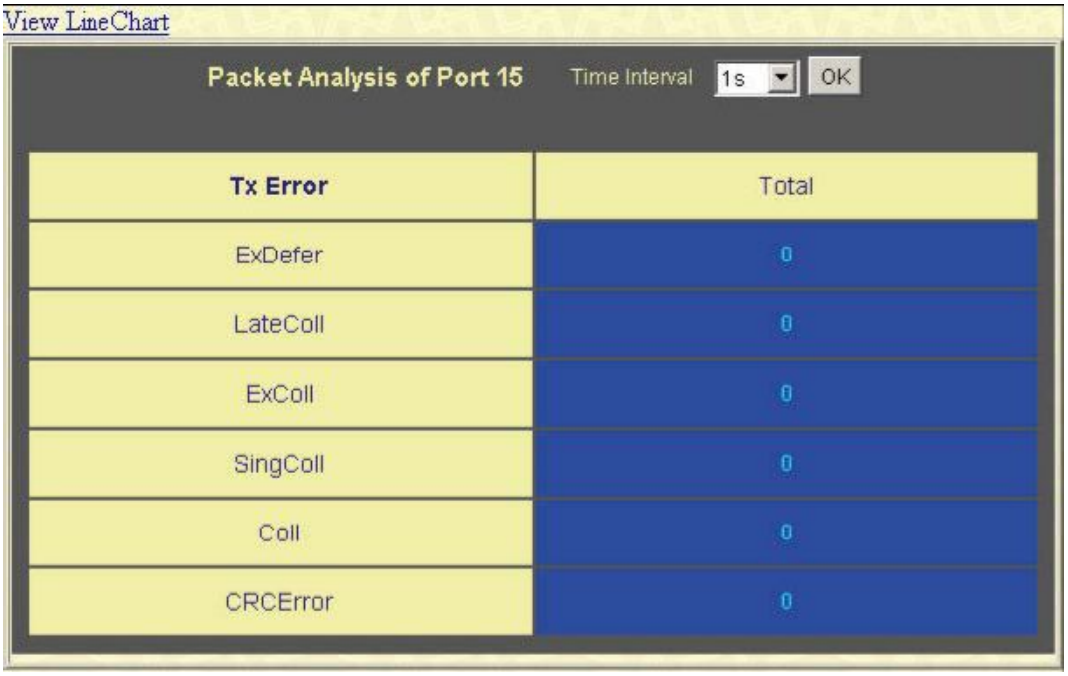


Рисунок 11.12 – Окно Tx Error Analysis (таблица)

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 1с.
Record Number	Этот параметр задает, сколько раз будет измеряться количество ошибок с заданным временным интервалом (Time Interval). Данное значение по умолчанию равно 20.
ExDefer	Счетчик, отображающий количество пакетов, которые были задержаны во время первой попытки передачи по определенному интерфейсу из-за того, что среда была занята.
LateColl	Счетчик, отображающий количество раз, когда коллизия при передаче пакета была обнаружена позже, чем за 512 битовых интервала.
ExColl	Excessive Collisions – чрезмерные коллизии. Количество пакетов, не переданных из-за чрезмерных коллизий
SingColl	Single Collision Frames – кадры с одиночными коллизиями. Количество успешно отправленных пакетов, которые были задержаны во время передачи из-за более, чем одной коллизии.
Coll	Оценка общего числа коллизий в данном сегменте сети.
Show/Hide	Отметьте, нужно ли отображать или нет значение соответствующих счетчиков ExDefer, LateColl, ExColl, SingColl и Coll.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Размер пакета

Web-интерфейс управления позволяет просматривать как в графическом виде, так и в виде таблицы, статистику по размеру полученных коммутатором пакетам. При этом в зависимости от размера пакетов выделяется 6 групп. С помощью выпадающего меню **Port** выберите нужный порт.

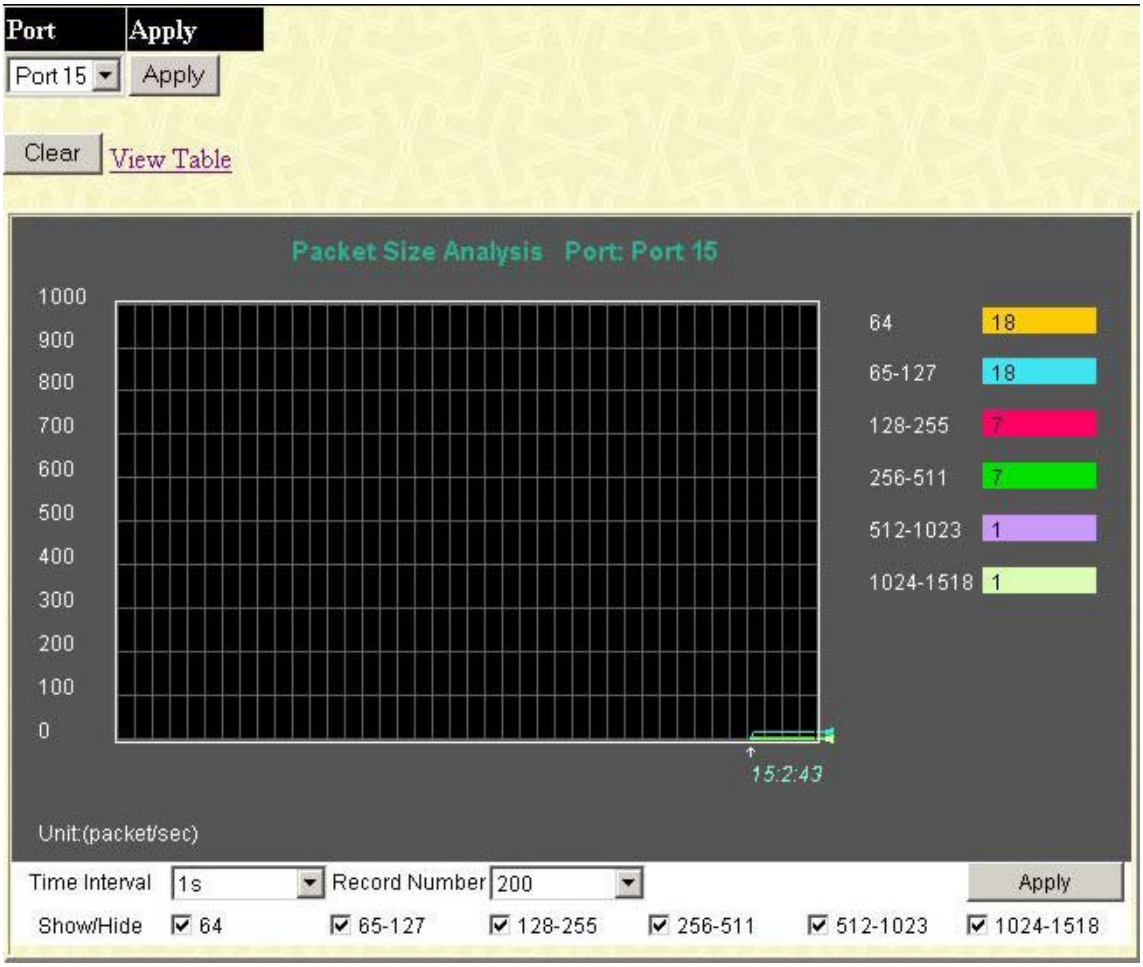
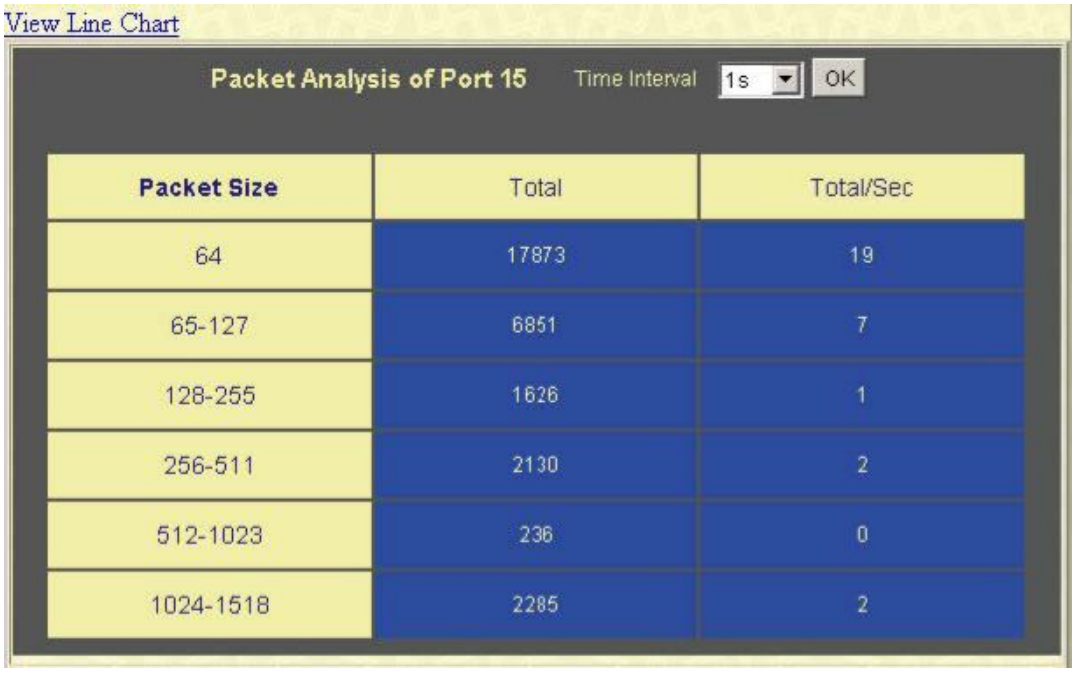


Рисунок 11.13 – Окно Rx Size Analysis (график зависимости)

Чтобы просмотреть ту же статистику в табличном виде, кликните по ссылке **View Table**:



Packet Size	Total	Total/Sec
64	17873	19
65-127	6851	7
128-255	1626	1
256-511	2130	2
512-1023	236	0
1024-1518	2285	2

Рисунок 11.14 – Окно Rx Size Analysis (таблица)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите желаемое значение временного интервала от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 1s.

Record Number	Выберите количество раз опрашивания коммутатора от 20 до 200. Данное значение по умолчанию равно 200.
64	Общее число полученных пакетов (включая «битые» пакеты), длиной 64 байт (исключая кадрирующие биты, но включая байты FCS).
65-127	Общее число полученных пакетов (включая «битые» пакеты), длиной от 65 до 127 байт (исключая кадрирующие биты, но включая байты FCS).
128-255	Общее число полученных пакетов (включая «битые» пакеты), длиной от 128 до 255 байт (исключая кадрирующие биты, но включая байты FCS).
256-511	Общее число полученных пакетов (включая «битые» пакеты), длиной от 256 до 511 байт (исключая кадрирующие биты, но включая байты FCS).
512-1023	Общее число полученных пакетов (включая «битые» пакеты), длиной от 512 до 1023 байт (исключая кадрирующие биты, но включая байты FCS).
1024-1518	Общее число полученных пакетов (включая «битые» пакеты), длиной от 1024 до 1518 байт (исключая кадрирующие 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-адреса

Динамическую таблицу MAC-адресов можно просмотреть в таблице, представленной ниже. Когда коммутатор изучает связь между MAC-адресом и номером порта, он делает запись в данной таблице. Эти записи используются для продвижения пакетов через коммутатор.

Для просмотра таблицы с MAC-адресами в меню **Monitoring** кликните ссылку **MAC Address Table.**

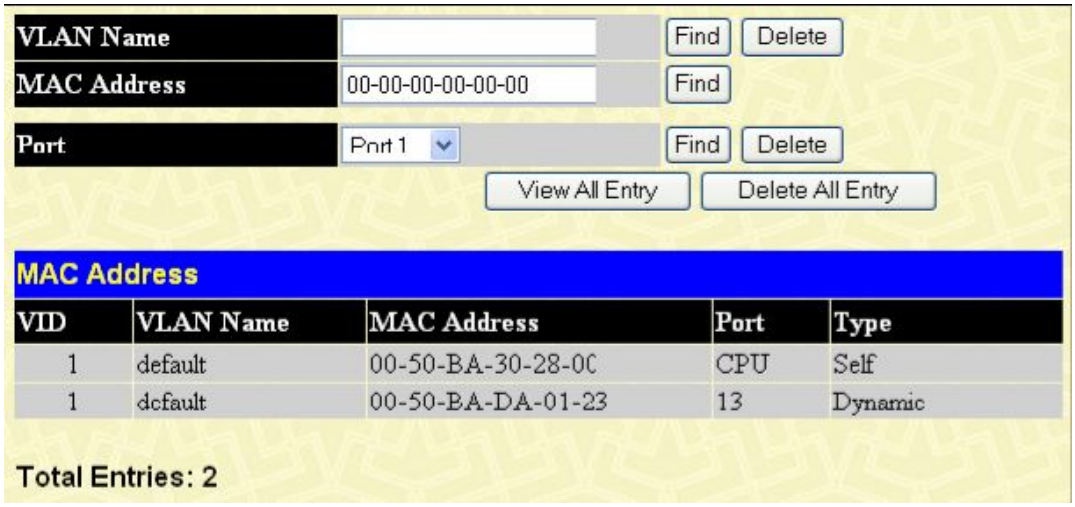


Рисунок 11.15 – Окно MAC Address Table

Можно настроить или просмотреть следующие поля:

Параметр	Описание
VLAN ID	Данное поле позволяет осуществлять быстрый поиск в таблице продвижения пакетов по заданному VLAN ID.
MAC Address	Данное поле позволяет осуществлять быстрый поиск в таблице продвижения пакетов по заданному MAC-адресу.
Port	Выберите нужный порт в данном выпадающем меню.
Find	Задав в соответствующем поле порт,VLAN ID или MAC-адрес и кликнув по данной кнопке Find, возможен быстрый переход к нужной строке.

VID	VLAN ID виртуальной сети VLAN, членом которой является данный порт.
MAC Address	MAC-адрес в таблице продвижения пакетов.
Port	Порт, которому соответствует MAC-адрес, указанный в соответствующем поле.
Learned	Данное поле задает способ, каким коммутатор узнает MAC-адрес. Возможны следующие опции: Dynamic, Self, Static.
Type	Описывает метод, который использует Коммутатор для обнаружения MAC-адресов. Возможные опции: Dynamic, Self и Static.
Next	Кликните по данной кнопке для перехода к следующей странице таблицы.
View All Entry	Нажав на эту кнопку, пользователь может просмотреть все записи таблицы адресов.
Delete All Entry	Пользователь может удалить все записи таблицы адресов, нажав на эту кнопку.

Журнал коммутатора (Switch Log)

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

Рисунок 11.16 – Окно Switch Log

Коммутатор может записывать информацию о нештатных событиях в своем собственном журнале, на определенной станции для получения сообщений SNMP trap и на персональном компьютере с подлюченной консолью. Кликните по кнопке **Next** для перехода к следующей странице журнала. Нажатие на кнопку **Clear** приводит к очистке журнала Коммутатора.

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.

ЗАМЕЧАНИЕ: Для получения более подробной информации о возможных записях в журнале коммутатора, пожалуйста, обратитесь к Приложению C данного Руководства.

Группа IGMP Snooping

Использование IGMP Snooping позволяет коммутатору считывать IP-адрес многоадресной группы и соответствующий MAC-адрес из IGMP-пакетов, проходящих через коммутатор. Количество IGMP-отчетов, которые были просмотрены, отображаются в поле Reports. Для просмотра таблицы **IGMP Snooping Table** кликните **IGMP Snooping Group** в меню **Monitoring.**

Рисунок 11- 17. Окно IGMP Snooping Group

Для удобства пользователя предусмотрена возможность быстрого поиска в IGMP Snooping Table по VLAN ID (VID). Для этого необходимо ввести нужный VID в верхнем левом углу окна и кликнуть по кнопке **Search**.

Можно просмотреть следующие поля:

Параметр	Описание
VLAN Name	Имя VLAN многоадресной группы.
Multicast Group	IP-адрес многоадресной группы.
MAC Address	MAC-адрес многоадресной группы.
Reports	Общее количество отчетов, полученных для данной группы.
Port Map	Отображаются соответствующие порты.

Примечание: Для настройки IGMP Snooping на коммутаторе в папке **L2 Features** выберите **IGMP Snooping.** Примеры настройки, а также другую информацию, касающуюся IGMP Snooping, можно найти в разделе 7 данного Руководства.

Поиск порта маршрутизатора

В данном окне отображается, какой из портов Коммутатора настроен как порт маршрутизатора. Порт маршрутизатора, настроенный пользователем (с помощью консоли или Web-интерфейса управления) отображается как статический порт маршрутизатора и обозначается S. D определяет динамически настроенный порт маршрутизатора. Для работы с данным окном откройте папку **Monitoring** и кликните по ссылке **Browse Router Port**.

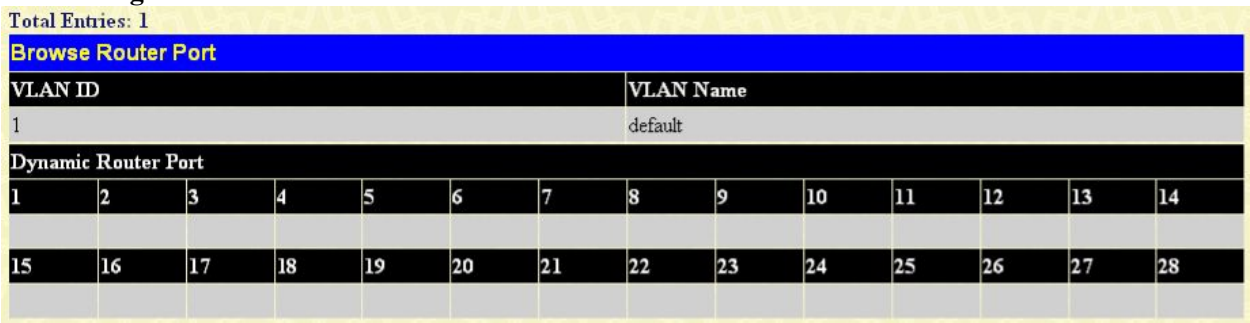


Рисунок 11.18 – Окно Browse Router Port

Статические настройки ARP

Окно **Browse ARP Table** доступно в меню **Monitoring**. Это окно отображает текущие записи ARP на Коммутаторе. Чтобы очистить таблицу **ARP Table**, кликните **Clear All.**

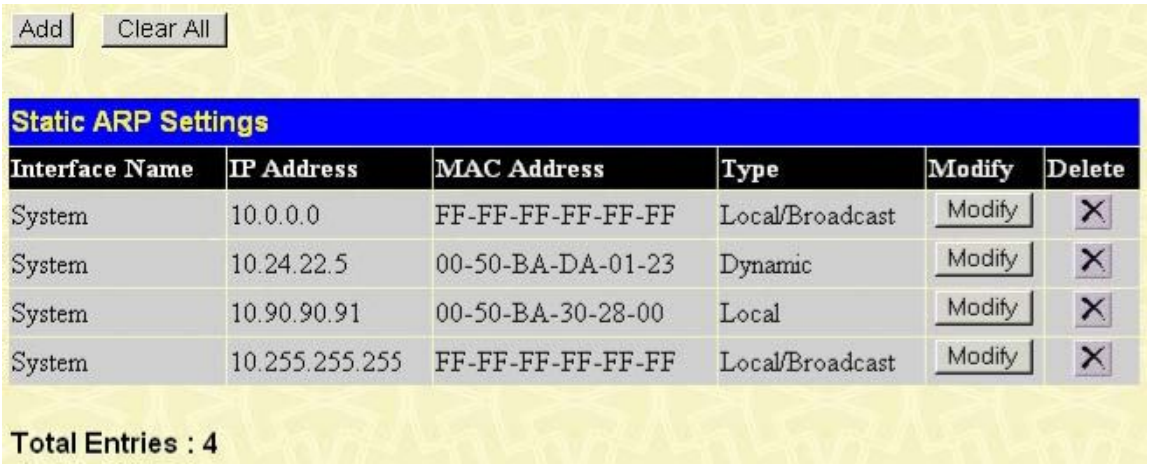


Рисунок 11- 19. Окно Static ARP Settings

Чтобы добавить запись в таблицу **Static ARP Settings**, кликните кнопку **Add**.

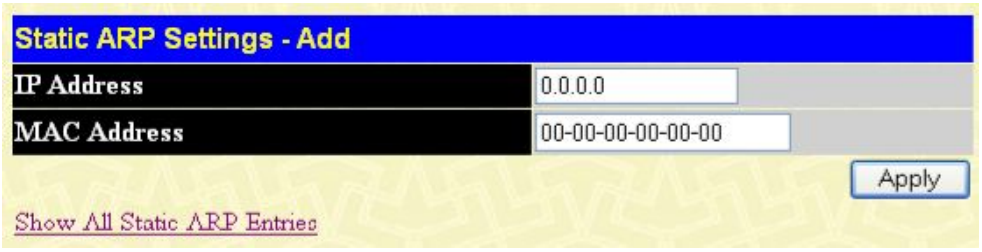


Рисунок 11- 20. Окно Static ARP Settings – Add

Чтобы изменить запись, выберите ее в таблице ARP Settings table и кликните **Modify**.

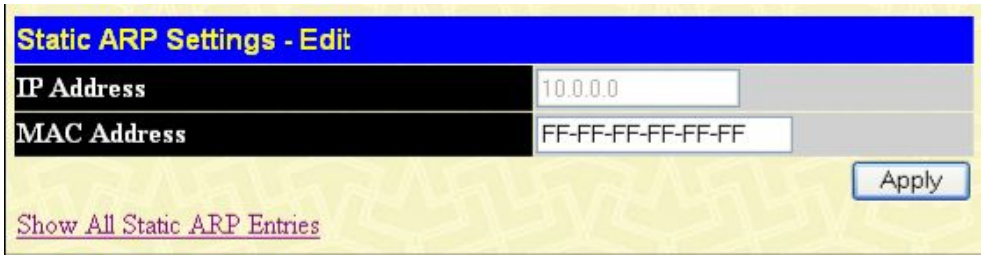


Рисунок 11- 21. Окно Static ARP Settings – Edit

Таблица сессий

Таблице сессий позволяет просмотреть подробную информацию о текущих сессиях на Коммутаторе. Здесь отображается такая информация как Session **ID** пользователя, время исходной регистрации **Login Time**, время жизни **Live Time**, настройка соединения на коммутаторе (поле **From)**, уровень **Level** и имя пользователя **Name.** Чтобы оновить информацию в окне, кликните **Reload**.

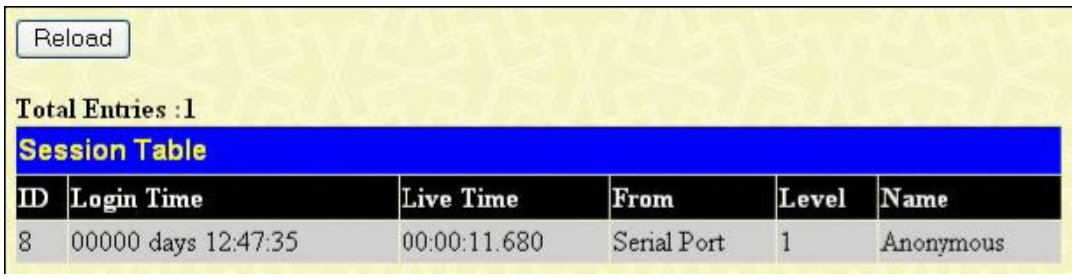


Рисунок 11- 22. Окно Session Table

Управление доступом на базе портов

Следующие экраны предназначены для мониторинга статистики 802.1X на Коммутаторе на основе портов. Чтобы просмотреть окна **Port Access Control**, откройте папку Monitorin и кликните по **Port Access Control**. Мониторинг может осуществляться с помощью шести экранов.

ПРИМЕЧАНИЕ: Окна **Authenticator State, Authenticator Statistics**, **Authenticator Session Statistics** и **Authenticator Diagnostics** не могут быть просмомотрены на Коммутаторе, если 802.1X не включен на основе портов или MAC-адресов. Чтобы включить 802.1X, перейдите в меню **DES-30xx Web Management Tool.**

Аутентификация с помощью внешнего сервера RADIUS

Эта таблица содержит информацию, указывающую на активность клиента аутентификации RADIUS на клиентской стороне протокола аутентификации RADIUS. Каждой строке в таблице соответствует свой сервер аутентификации RADIUS. Для работы с окном **RADIUS Authentication** кликните **Monitoring > Port Access Control > RADIUS Authentication**.

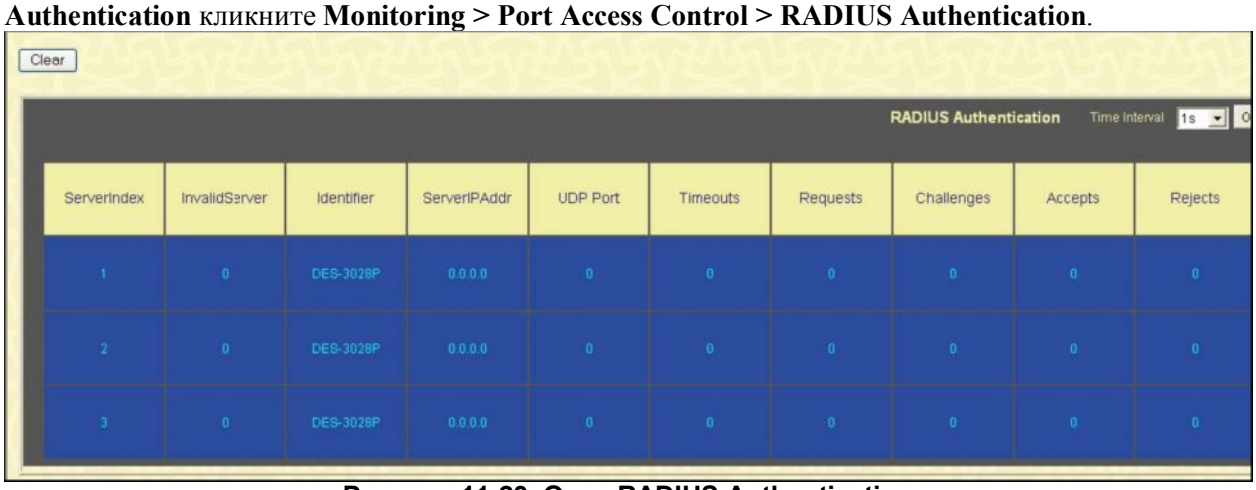


Рисунок 11-23. Окно RADIUS Authentication

Пользователь может также выбрать нужный временной интервал для обновления статистики от *1s* до *60s*, где "s" означает секунды. Значение по умолчанию равно 1 секунде. Чтобы сбросить существующую статистику, кликните по кнопке *Clear* в верхнем левом углу.
Для просмотра доступны следующие параметры:

Параметр	Описание
ServerIndex	Идентификационный номер, назначенный серверу аутентификации RADIUS.
UDP Port	UDP-порт, который использует клиент для отправки запросов на данный сервер.
Timeouts	Количество таймаутов аутентификации для данного сервера. По истечении таймаута клиент может повторить попытку запроса на данный сервер, отправить запрос на другой сервер или прекратить попытки запроса учетной записи. Повторный запрос на тот же сервер учитывается как повторная передача, так же как и истечение таймаута. Отправка запроса на другой сервер учитывается как запрос Request, так же как и истечение таймаута.
Requests	Количество пакетов RADIUS Access-Request, отправленных на данный сервер. Это число не включает повторные передачи.
Challenges	Количество пакетов RADIUS Access-Challenge (корректных или некорректных), полученных с данного сервера.

Accepts	Количество пакетов RADIUS Access-Accept (корректных ил некорректных), полученных с данного сервера.
Rejects	Количество пакетов RADIUS Access-Reject (корректных или некорректных), полученных с данного сервера.
RoundTripTime	Временной интервал (в сотнях секунд) между пакетами Access-Reply/Access-Challenge и Access-Request, который совпадает с данным сервером аутентификации RADIUS.
AccessRetrans	Количество пакетов RADIUS Access-Request, повторно переданных на данный сервер аутентификации RADIUS.
PendingRequests	Количество пакетов RADIUS Access-Request, предназначенных для данного сервера, которые ее не получили ни таймаута, ни ответа. Эта переменная увеличивается при отправке Access-Request и уменьшается по мере приема Access-Accept, Access-Reject или Access-Challenge, таймаута или повоторной передачи.
AccessResponses	Количество некорректных пакетов RADIUS Access-Response, полученных с данного сервера. Данное поле включает пакеты с некорректной длиной. Пакеты с неверным значением аутентификатора или атрибутов сигнатур, не включаются в это число.
BadAuthenticators	Количество пакетов RADIUS Access-Response, содержащих некорректные атрибуты authenticator или Signature и полученных с данного сервера.
UnknownTypes	Количество пакетов RADIUS неизвестного типа, которые были получены с данного сервера на порт аутентификации.
PacketsDropped	Количество пакетов RADIUS, полученных с данного сервера на аутентификационный сервер и отброшенных по некоторым другим причинам.

Учетные записи RADIUS

Это окно отображает управляющие объекты, используемые для управления учетными записями RADIUS и статически связянными с ними клиентами. В данном окне каждому ряду соответствует сервер аутентификации RADIUS. Для работы с окном **RADIUS Accounting** кликните **Monitoring > Port Access Control > RADIUS Accounting**.

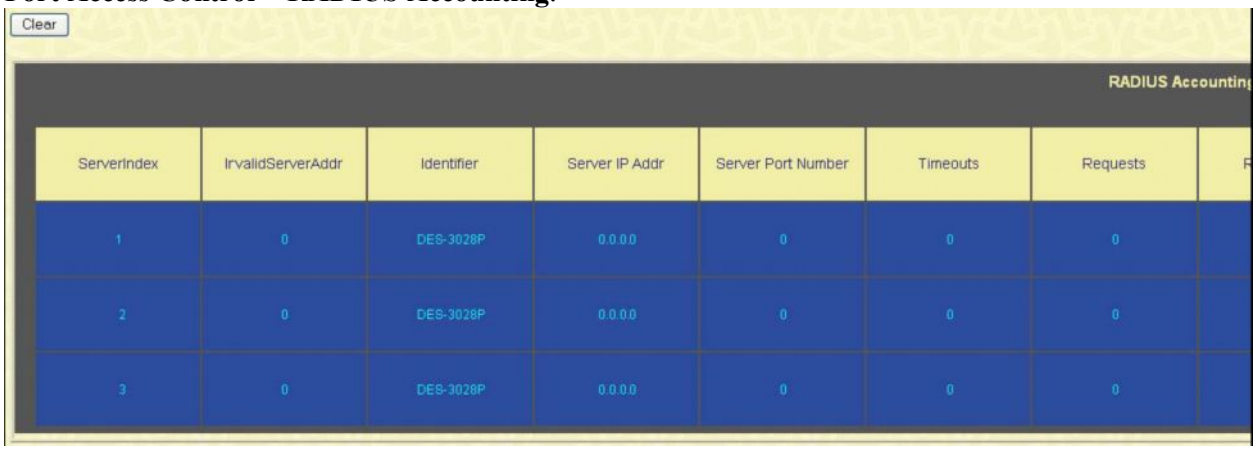


Рисунок 11-24. Окно RADIUS Accounting

Пользователь может выбрать нужный интервал для обновления статистики от *1s* до *60s*, где “s” означает сеунды. Значение по умолчанию равно 1 с. Чтобы сбросить всю показанную статистику, кликните по кнопке *Clear* в верхнем левом углу.

Для просмотра доступны следующие поля:

Параметр	Описание
Server IP Addr	IP-адрес, назначенный серверу RADIUS.
UDP Port	UDP-порт, который использует клиент для отправки запросов на данный сервер.
Timeouts	Количество таймаутов аутентификации для данного сервера. По истечении таймаута клиент может повторить попытку запроса на данный сервер, отправить запрос на другой сервер или прекратить попытки запроса учетной записи. Повторный запрос на тот же сервер учитывается как повторная передача, так же как и истечение таймаута. Отправка запроса на другой сервер учитывается как запрос Request, так же как и истечение таймаута.
Requests	Количество пакетов RADIUS Access-Request, отправленных на данный сервер. Это число не включает повторные передачи.
Responses	Количество принятых от данного сервера RADIUS пакетов через порт запроса учетных записей.
RoundTripTime	Интервал между последним пакетом Accounting-Response и соответствующим ему пакетом Accounting-Request от сервера.
AccessRetrans	Количество пакетов Accounting-Request, повторно отправленных на данный сервер учетных записей RADIUS.
PendingRequests	Количество пакетов Accounting-Request, отправленных на данный сервер RADIUS, время ожидания ответа которых еще не истекло, и еще не был получен ответ. Эта переменная инкрементируется при каждой отправке пакета Accounting-Request и декрементируется при приеме пакета Accounting-Response, по истечении времени ожидания или при повторной передаче.
MalformedResponses	Количество некорректных пакетов Accounting-Response RADIUS, полученных от данного сервера. Сюда входят пакеты некорректной длины. Пакеты с некорректным аутентификатором и пакеты неизвестного типа не входят в это число.
BadAuthenticators	Количество полученных с данного сервера RADIUS пакетов Accounting-Response с некорректным атрибутом аутентификатора.
UnknownTypes	Количество пакетов RADIUS неизвестного типа, которые были получены с данного сервера на порт учетной записи.
PacketsDropped	Количество пакетов RADIUS, которые были получены с данного сервера на порт учетной записи и отброшены по некоторым другим причинам.

Диагностика Аутентификатора

Эта таблица содержит диагностическую информацию, относящуюся к действиям Аутентификатора, относящуюся к порту. Запись в данной таблице появляется для каждого порта, поддерживающего функцию аутентификации. Чтобы просмотреть окно **Authenticator Diagnostics**, кликните **Monitoring > Port Access Control > Authenticator Diagnostics**.

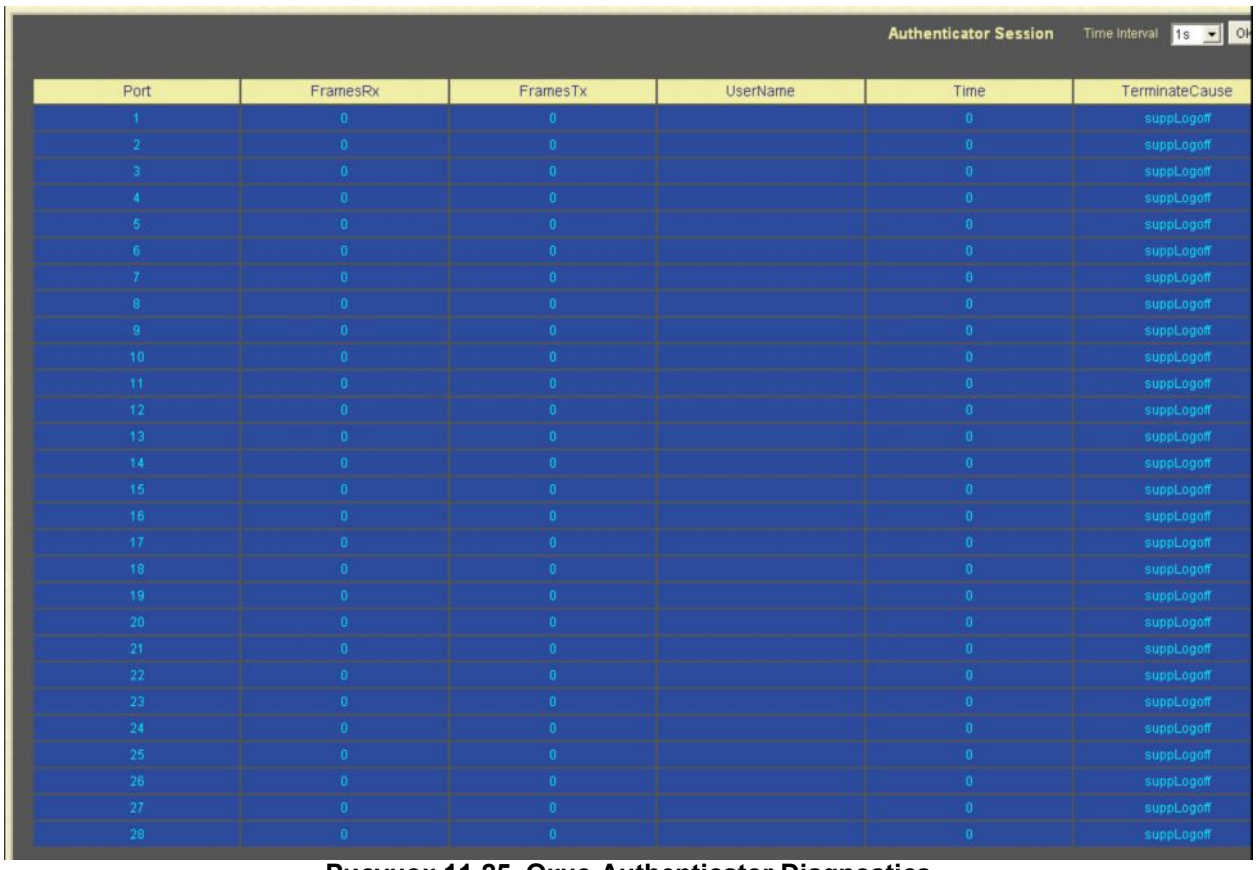


Рисунок 11-25. Окно Authenticator Diagnostics

Пользователь может выбрать желаемый временной интервал для обновления статистики (от *1s* до *60s*, где “s” означает секунды). Значение по умолчанию -1 секунда.

Для просмотра доступны следующие поля:

Параметр	Описание
Port	Идентификационный номер, назначенный портом системой, к которой принадлежит порт.
EntersConnecting	Считает количество переходов в состояние CONNECTING из любого другого.
EapLogOffsConnecting	Считает количество переходов из состояния CONNECTING в состояние DISCONNECTED в результате получения сообщения EAPOL-Logoff.
EntersAuthenticating	Считает количество переходов из состояния CONNECTING в состояние AUTHENTICATING в результате получения сообщения EAP-Response/Identity от Supplicant.
SuccessAuthenticating	Считает количество переходов из состояния AUTHENTICATING в состояние AUTHENTICATED в результате статуса Backend Authentication, указывающего на успешную аутентификацию Supplicant (authSuccess = TRUE).
TimeoutsAuthenticating	Считает количество переходов из состояния AUTHENTICATING в состояние ABORTING в результате статуса Backend Authentication, указывающего на таймаут аутентификации (authTimeout = TRUE).
FailAuthenticating	Считает количество переходов из состояния AUTHENTICATING в состояние HELD в результает статуса Backend Authentication, указывающего на ошибку аутентификации (authFail = TRUE).
ReauthsAuthentic	Считает количество переходов из состояния AUTHENTICATING в состояние ABORTING в результате зпроса повторной аутентификации (reAuthenticate =

ating	TRUE).
EapStartsAuthenticated	Считает количество переходов из состояния AUTHENTICATING в состояние ABORTING в результает сообщения EAPOL-Start, полученного от Supplicant.
EapLogOffAuthenticated	Считает количество переходов из состояния AUTHENTICATING в состояние ABORTING в результате сообщения EAPOL-Logoff, полученного от Supplicant.
ReauthsAuthenticated	Считает количество переходов из состояния AUTHENTICATED в состояние CONNECTING в результате запроса повторной аутентификации (reAuthenticate = TRUE).
EapStartsAuthenticated	Считает количество переходов из состояния AUTHENTICATED в состояние CONNECTING в результате сообщения EAPOL-Start, полученного от Supplicant.
EapLogOffAuthenticated	Считает количество переходов из состояния AUTHENTICATED в состояние DISCONNECTED в результате сообщения EAPOL-Logoff, полученного от Supplicant.
Responses	Считает количество отправленных пакетов начального запроса доступа на сервер аутентифкации (например, выполнение записи sendRespToServer в состоянии RESPONSE). Указывает на попытку Аутентификатора взаимодействовать с Сервером Аутентификации.
AccessChallenges	Считает количество полученных пакетов initial Access-Challenge от сервера Аутентификации (например, aReq принимает значение TRUE в результате выхода из состояния RESPONSE). Укзазывает, что сервер аутентификации взаимодействует с Аутентификатором.
OtherReqToSupp	Считает количество отправленных пакетов EAP-Request (не включая Identity, Notification, Failure или Success) на Supplicant (например, выполнение txReq на запис в состоянии REQUEST). Указывает на выбор Аутентификатором метода EAP.
ResponsesFromSupplicant	Число полученных ответов от Supplicant в ответ на исходный EAP-Request, причем этот ответ не должен быть EAP-NAK (например, rxResp становится TRUE в результате перехода из состояния REQUEST в состояние RESPONSE, причем ответ не должен быть типа EAP-NAK). Указывает, что Supplicant может отвечать на выбранный метод EAP Аутентификатора.
AuthSuccesses	Считает количество полученных сообщений Accept от сервера Аутентификации (например, aSuccess принимает значение TRUE в результате перехода из сосотояния RESPONSE в состояние SUCCESS). Указывает, что Supplicant успешно Authentication Server.
AuthFail	Считает количество полученных сообщений Reject от сервера аутентификации (например, aFail принимает значение TRUE, вызванное переходом из состояния RESPONSE в состояние FAIL). Указывает, что Supplicant не прошел аутентификацию на сервере аутентификации.

Статистика сессий Аутентификатора

Эта таблица содержит таблицу статистики сессий для Аутентификатора PAE с привязкой к определенному порту. Запись появляется в таблице для каждого порта с поддержкой функции Аутентификатора. Для просмотра **Authenticator Session Statistics** кликните по **Monitoring > Port Access Control > Authenticator Session Statistics**.

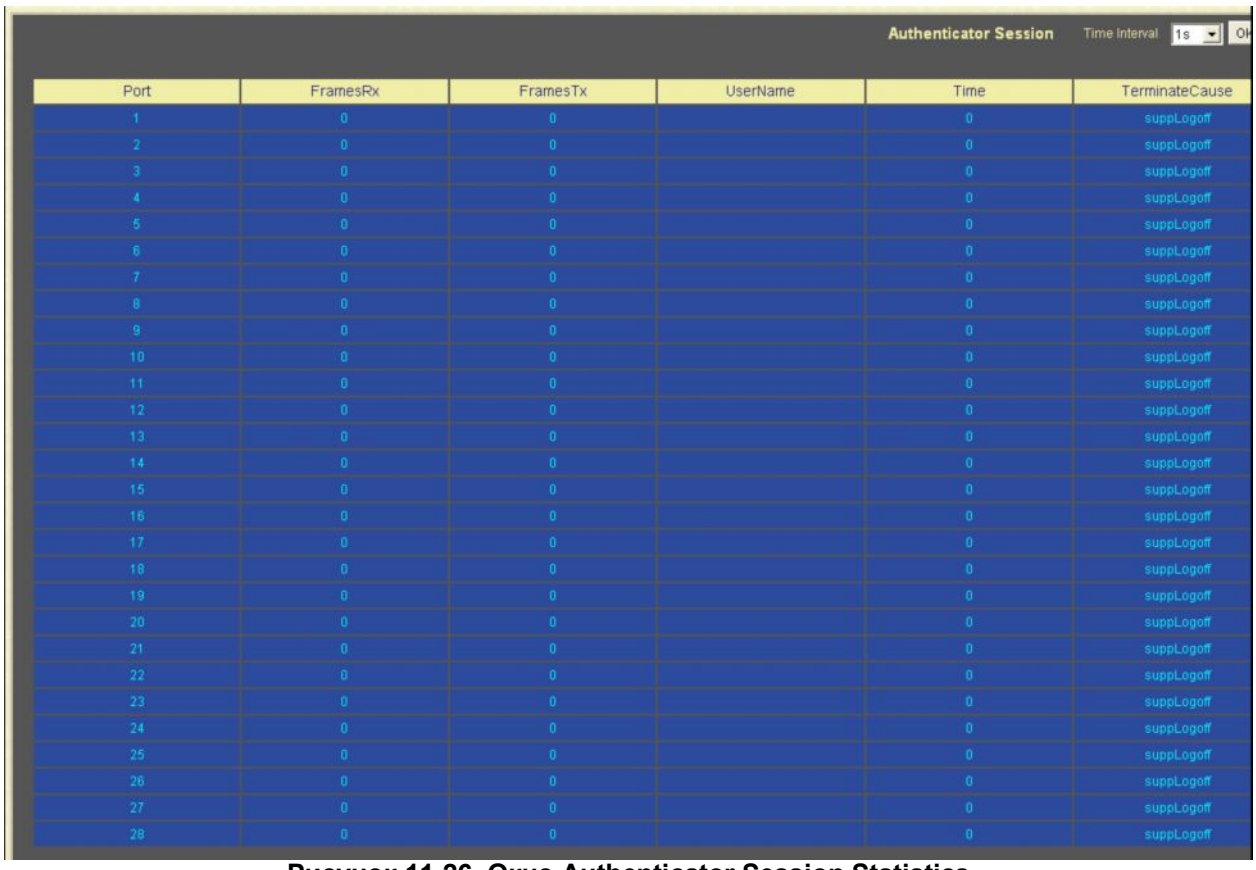


Рисунок 11-26. Окно Authenticator Session Statistics

Пользователь может выбрать нужный временной интервал для обновления статистики от *1s* до *60s*, где “s” означает секунды. Значение по умолчанию 1 секунда.

Для просмотра доступны следующие поля:

Параметр	Описание
Port	Идентификационный номер, назначенный порту системой, которой данный порт принадлежит.
Frames Rx	Количество фреймов данных пользователя, полученных на данном порту в течение сессии.
Frames Tx	Количество фреймов данных пользователя, переданных на данном порту в течение сессии.
UserName	Имя пользователя, служащее для идентификации Supplicant PAE.
Time	Продолжительность сессии в секундах.
Terminate Cause	Причина окончания сессии. Выделяют восемь возможных причин окончания сессии. 1) Supplicant Logoff 2) Ошибка на порту 3) Supplicant Restart 4) Ошибка повторной аутентификации 5) AuthControlledPortControl установлено в значение ForceUnauthorized 6) Реинициализация порта 7) Порт выключен администратором 8) Еще не завершена
Octets Rx	Количество октетов, полученных во фреймах данных пользователя на

	данном порту в течение сессии.
Octets Tx	Количество октетов, переданных в фреймах анных пользователя, на данном порту в течение сессии.
ID	Уникальный идентификатор сессии в форме печатной строки ASCII длиной как минимум 3 символа.
Authentic Method	Метод аутентификации, используемый для установки сессии. Доступны следующие методы аутентификации: (1) Remote Authentic Server – Сервер аутентификации является внешним по отношению к системе Аутентификатора. (2) Local Authentic Server – Сервер аутентификации расположен внутри системы Аутентификатора.

Статистика Аутентификатора

Эта таблица содержит статистичекие объекты для Authenticator PAE, привязанные к каждому порту. Эти записи поддерживают функцию Аутентификатора. Чтобы просмотреть статистику аутентификтаора, кликните по **Monitoring > Port Access Control > Authenticator Statistics.**

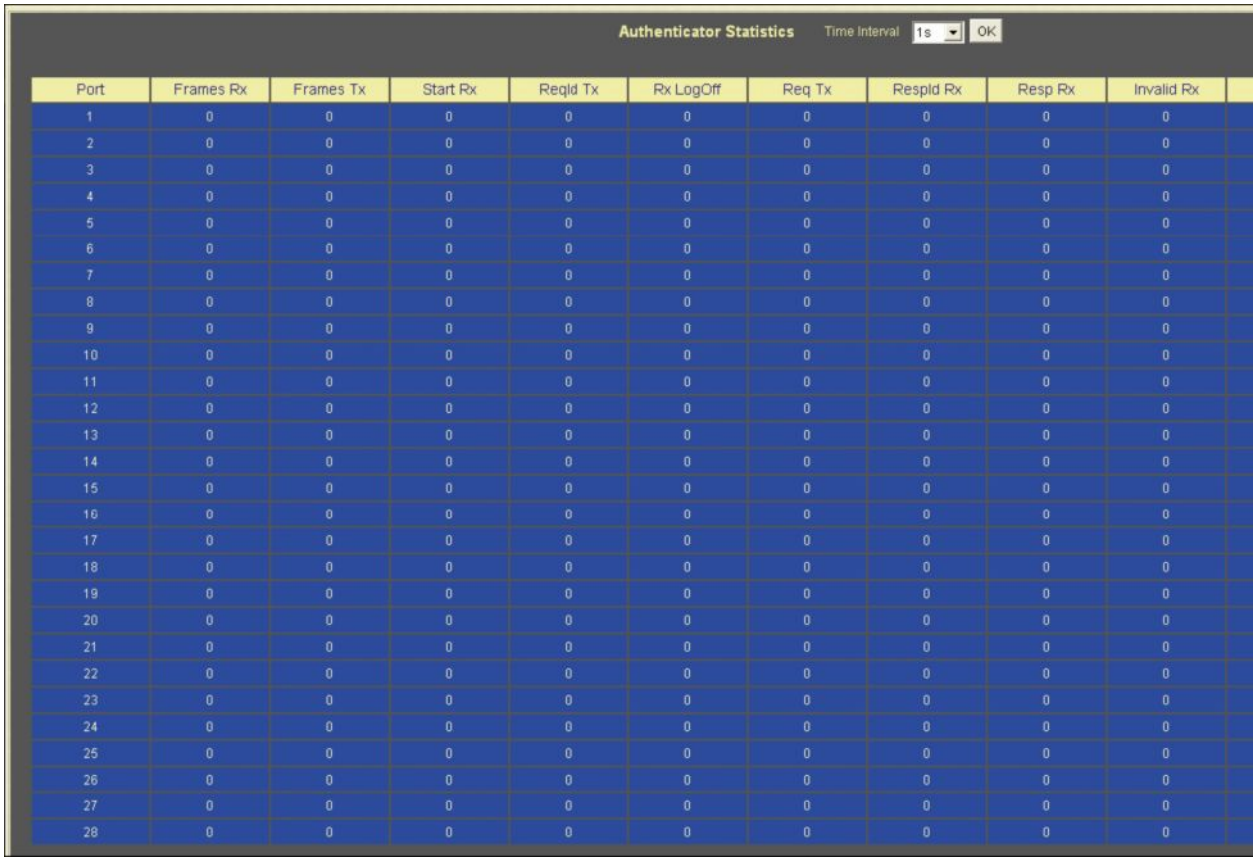


Рисунок 11-27. Окно Authenticator Statistics

Пользователь может также выбрать нужный временной интервал обновления статистики от *1s* до *60s*, где “s” означает секунды. Значение поумолчанию 1 секунда.

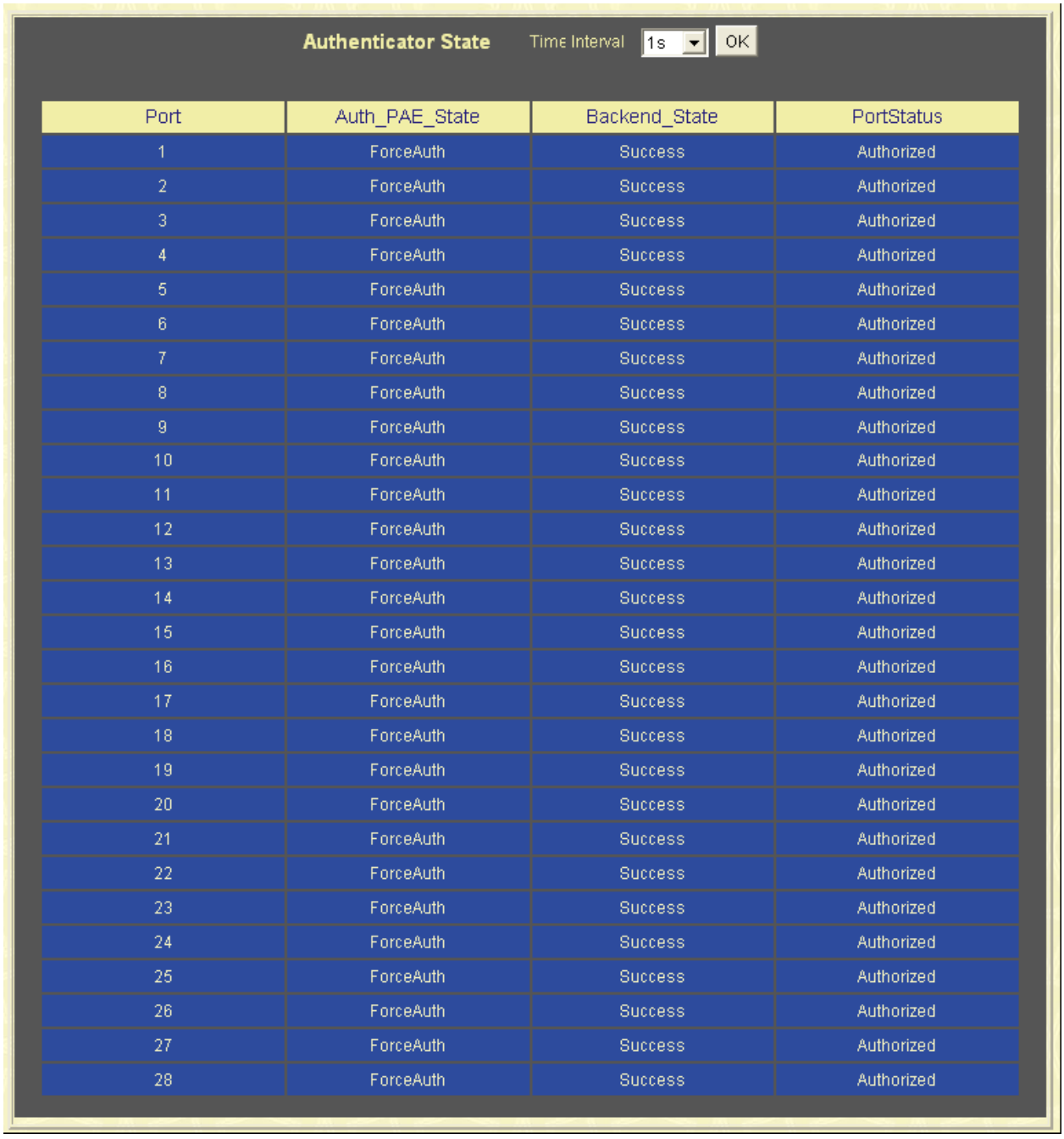
Для просмотра доступны следующие параметры:

Параметр	Описание
Port	Идентификационный номер, назначенный порту системой, к которой относится порт.
Frames Rx	Количество корректных фреймов EAPOL, полученных Аутентификатором.
Frames Tx	Количество фреймов EAPOL, переданных Аутентификатором.
Rx Start	Количество стартовых фреймов EAPOL, полученных Аутентификатором.
TxReqId	Количество фреймов EAP Req/Id, которые были переданы данным Аутентификатором.
RxLogOff	Количество фреймов EAPOL Logoff, полученных данным Аутентификатором.
Tx Req	Количество фреймов запроса EAP (отличаются от фреймов Rq/Id), которые были переданы данным Аутентификатором.
Rx RespId	Количество фреймов EAP Resp/Id, которые были получены данным Аутентификатором.
Rx Resp	Количество корректных фреймов ответа EAP (отличаются от фреймов Resp/Id), которые были получены данным Аутентификатором.
Rx Invalid	Количество полученных данным Аутентификатором фреймов EAPOL, в которых не распознается тип фрейма.
Rx Error	Количество полученных данным Аутентификатором фреймов EAPOL, в

	которых поле Packet Body Length (Длина тела пакета) не корректно.
Last Version	Номер версии протокола для большинства недавно полученных фреймов EAPOL.
Last Source	MAC-адрес Источника для большинства недавно полученных фреймов EAPOL.

Состояние аутентификатора

В показанном ниже окне отображается статус Аутентификатора для каждого порта**.** Для просмотра таблицы **Authenticator State** нажмите **Monitoring ⇨ Port Access Control ⇨Auth State.**



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
19	ForceAuth	Success	Authorized
20	ForceAuth	Success	Authorized
21	ForceAuth	Success	Authorized
22	ForceAuth	Success	Authorized
23	ForceAuth	Success	Authorized
24	ForceAuth	Success	Authorized
25	ForceAuth	Success	Authorized
26	ForceAuth	Success	Authorized
27	ForceAuth	Success	Authorized
28	ForceAuth	Success	Authorized

Рисунок 11.28 – Окно Authenticator State

Пользователь может выбрать нужный интервал обновления статистики от 1s до 60s, где “s” означает секунда. Значение по умолчанию 1 секунда.

Сброс настроек коммутатора (функция Reset)

Окно Reset позволяет сбросить настройки коммутатора. Однако очень важно выбрать нужную опцию, поскольку от этого многое зависит.

Примечание: Только функция **Reset System** позволит ввести в долговременную память коммутатора заводские параметры по умолчанию после автоматического перезапуска коммутатора. 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.

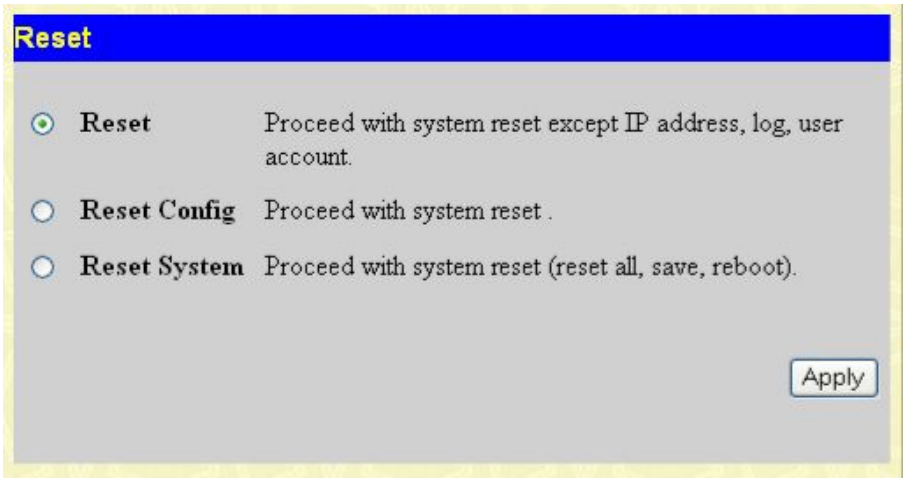


Рисунок 11- 29. Окно Reset

Перезапуск коммутатора

Следующее окно используется для перезапуска коммутатора.

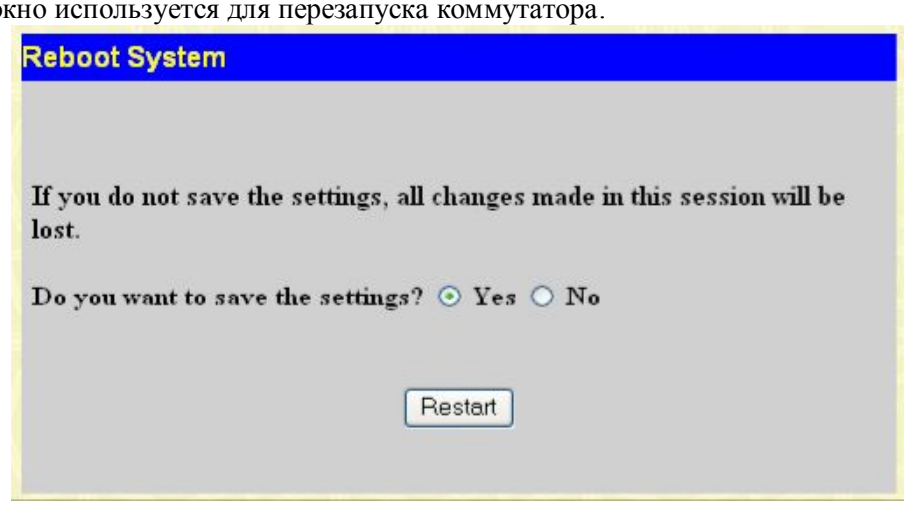


Рисунок 11.30 - Окно Reboot System

При выборе опции **Yes** коммутатор сохранит текущую конфигурацию в энергонезависимой памяти до перезапуска коммутатора.

При выборе опции **No** текущая конфигурация не будет сохранена перед перезапуском коммутатора. При этом, вся информация, введенная с последнего сохранения настроек (**Save Changes),** будет утрачена.

Кликните по кнопке **Restart** для перезапуска коммутатора.

Сохранение изменений

Коммутатор обладает двумя видами памяти: оперативная RAM и постоянная (энергонезависимая) NV-RAM. Выполняемые настройки записываются в RAM и вступают в силу после нажатия на кнопку **Apply**. При этом настройки вступают в силу и записываются в оперативную память RAM. Однако для вступления в силу некоторых настроек, требуется перезапуск коммутатора. Если настройки не были сохранены в памяти NV-RAM, то во время перезапуска коммутатора они сотрутся, и коммутатор вернется к настройкам, сохраненным в NV-RAM. Поэтому очень важно сохранить все настройки в энергонезависимую память перед перезапуском Коммутатора.
Для сохранения выполненных изменений в настройках в энергонезависимой памяти NV-RAM кликните по кнопке **Save** в окне **Save Changes.**

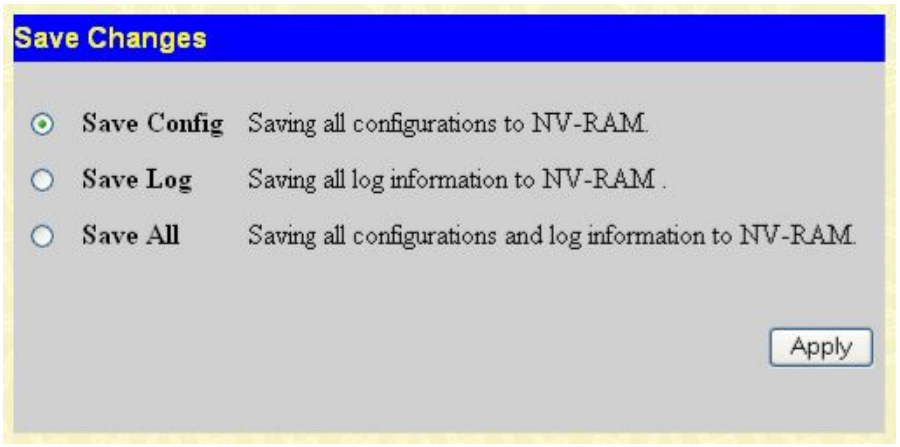


Рисунок 11- 31. Окно Save Changes

Выход из системы (Logout)

Кликнув по кнопке **Logout** в окне **Logout,** можно немедленно покинуть интерфейс настройки.

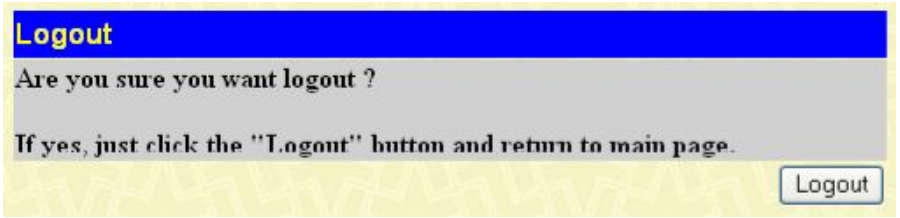


Рисунок 11.32 – Окно Logout

Приложение А
Техническая спецификация

Основные	
Протоколы	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”) IEEE 802.1D Spanning Tree IEEE 802.1S/W Spanning Tree IEEE 802.1Q VLAN Очереди приоритетов IEEE 802.1p Управление доступом к сети на основе портов IEEE 802.1x Агрегирование каналов IEEE 802.3ad Управление потоком в режиме полного дуплекса IEEE 802.3x Автосогласование NWay IEEE 802.3 IEEE 802.3af (только для моделей с поддержкой PoE)
Трансиверы	Поддерживаемые трансиверы SFP (Mini GBIC) - DEM-310GT (1000BASE-LX) - DEM-311GT (1000BASE-SX) - DEM-314GT (1000BASE-LH) - DEM-315GT (1000BASE-ZX) - DEM-210 (одномодовое волокно, 100Base-FX) - DEM-211 (многомодовое волокно, 100Base-FX) Поддерживаемые трансиверы WDM: DEM-330T (TX-1550/RX-1310нм), до 10 км, одномодовое волокно DEM-330R (TX-1310/RX-1550нм), до 10 км, одномодовое волокно DEM-331T (TX-1550/RX-1310нм), до 40 км, одномодовое волокно DEM-331R (TX-1310/RX-1550нм), до 40 км, одномодовое волокно
Стандарты	CSMA/CD
Скорость передачи данных: **Ethernet** **Fast Ethernet** **Gigabit Ethernet**	Полудуплекс Дуплекс 10 Мбит/с 20 Мбит/с 100Мбит/с 200 Мбит/с N/a 2000 Мбит/с
Топология	Звезда
Сетевые кабели	Cat.5 Enhanced для 1000BASE-T UTP Cat.5, Cat. 5 Enhanced для 100BASE-TX UTP Cat.3, 4, 5 для 10BASE-T EIA/TIA-568 100 Ом экранированная витая пара (STP)(100м)
Количество портов	DES-3028/DES-3028P: 24 порта 10/100Base-T 2 комбо-порта 1000Base-T/SFP 2 порта 1000Base-T DES-3052/DES-3052P: 48 портов 10/100Base-T 2 комбо-порта 1000Base-T/SFP 2 порта 1000Base-T

Физические параметры и условия эксплуатации	
Внутренний источник питания	На входе: DES-3028/DES-3052 - 100~240В переменного тока 0,5А, 50~60 Гц DES-3052P - 100~240 В переменного тока 5А, 50~60 Гц DES-3028P - 100~240 В переменного тока 2,9А, 50~60 Гц

	На выходе: DES-3028/DES-3052: 12В, 3,3 А (макс.) DES-3028P: 12В, 3,3 А / 50 В, 3,7А (макс.) DES-3052P: 12В,10,5 А / 50 В, 7, 5А (макс.)
Потребляемая мощность	DES-3028 – 25 Вт DES-3052 – 26 Вт DES-3028P – 217 Вт DES-3052P – 395 Вт
Вентиляторы DC	DES-3028/DES-3052 – Нет вентиляторов DES-3028P – один вентилятор 8,5 см и один 17 см DES-3052P – один вентилятор 5см, один 8,3 см и один вентилятор 17см
Рабочая температура	От 0 до 40С
Температура хранения	От -40 до 70С
Влажность	От 5% до 95% без образования конденсата
Размеры	DES-3028: 441 x 207 x 44 мм DES-3028P/3052/3052P: 441 x 309 x 44 мм
Вес	DES-3028 – 2,36 кг DES-3028P – 4,5 кг DES-3052 – 3,85 кг DES-3052P – 5,70 кг
Электромагнитное излучение (EMI)	CE class A, FCC Class A, C-Tick, VCCI
Безопасность	CB Report, UL

Производительность	
Метод коммутации	Store-and-forward
Размер буфера пакетов	512 кБ на устройство
Скорость фильтрации/ продвижения пакетов	14 881 pps (для 10Мбит/с) 148 810 pps (для 100Мбит/с) 1 488 100 pps (для 1Гбит/с)
Изучение MAC - адресов	Автоматическое обновление. Поддержка 8К MAC-адресов
Очереди приоритетов	4 очереди приоритетов на порт.
Время жизни таблицы MAC-адресов	Максимальнвый помежуток: 10-1000000 с. По умолчанию 300 с.

Функционал PoE	
Число портов с	DES-3028P: 12 портов

<table>
<tr><td>поддержкой PoE</td><td>DES-3052P: 24 порта</td></tr>
<tr><td>Питание PoE</td><td>DES-3028P:
На порт 15,4 Вт (по умолчанию),
Выходная мощность для DES-3028P: 185Вт
Потребляемая мощность: 225Вт (макс.)
DES-3052P:
На порт 15,4Вт (по умолчанию),
Выходная мощность для DES-3052P: 370Вт
Потребляемая мощность: 500Вт (макс.)</td></tr>
<tr><td>Спецификация PoE</td><td>1. Питание устройств до 15,4Вт на порт в соответствии со стандартом IEEE 802.3af
2. Функция автоматического обнаружения и распознавания подключения устройств PoE и немедленное включение их питания
3. Автоматическое выключение порта, если ток на порту превышает 350мА. При этом другие порты остаются активными.
4. Активная защита от короткого замыкания: автоматическое обнаружение портов при обнаружении короткого замыкания. При этом другие порты остаются активными.
5. Устройства PoE должны поддерживать получение питания в соответствии со следующей классификацией.
<table>
<tr><th>Класс</th><th>Применение</th><th>Максимальная мощность, потребляемая устройством</th></tr>
<tr><td>0</td><td>По умолчанию</td><td>От 0,44 до 12,95 Вт</td></tr>
<tr><td>1</td><td>Опционально</td><td>От 0,44 до 3,84 Вт</td></tr>
<tr><td>2</td><td>Опционально</td><td>От 3,84 до 6,49 Вт</td></tr>
<tr><td>3</td><td>Опционально</td><td>От 6,49 до 12,95 Вт</td></tr>
<tr><td>4</td><td>Не поддерживается</td><td>Зарезервировано</td></tr>
</table>
6. PSE должно обеспечивать питание согласно следующей классификации:
<table>
<tr><th>Класс</th><th>Применение</th><th>Максимальная мощность</th></tr>
<tr><td>0</td><td>По умолчанию</td><td>15,4 Вт</td></tr>
<tr><td>1</td><td>Опционально</td><td>4,0 Вт</td></tr>
<tr><td>2</td><td>Опционально</td><td>7,0 Вт</td></tr>
<tr><td>3</td><td>Опционально</td><td>15,4 Вт</td></tr>
<tr><td>4</td><td>Зарезервировано</td><td>15,4 Вт</td></tr>
</table>
7. DES-3028P/DES-3052P соответствует Alternative A стандарта распределния контактов PSE, согласно которой питание отправляется через контакты 1,2,3,6 8-контактного UTP-кабеля Кат.5.
8. DES-3028P/DES-3052P может работать совместно со всеми устройтсвами D-Link с поддержкой 802.3af PoE
9. DES-3028P/DES-3052P может работать со всеми устройствами D-Link (точки доступа, IP-камеры и IP-телефоны) без поддержки 802.3af PoE через DWL-P50</td></tr>
</table>

Приложение B
Записи системного журнала

В следующей таблице представлены возможные записи в Системном журнале и их значение.

Категория	Описание события	Содержимое записи	Уровень события
system	Запуск системы	**System started up**	Critical
	Сохранение конфигурации во Flash-памяти	**Configuration saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Сохранение журнала во Flash-памяти	**System log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Сохранение конфигурации ижурнала во Flash-памяти	**Configuration and log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
up / download	Успешное обновление программного обеспечения	**Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Программное обеспечение обновить не удалось	**Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning
	Конфигурационный файл успешно загружен	**Configuration successfully downloaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Загрузить конфигурационный файл не удалось	**Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning
	Конфигурационный файл успешно сохранен	**Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Сохранить конфигурационный файл не удалось	**Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning
	Журнал коммутатора успешно сохранен	**Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Не удалось сохранить журнал коммутатора	**Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning
Interface	Соединение на порту	**Port <portNum> link up, <link state>**	Informational
	Отсутствие соединения на порту	**Port <portNum> link down**	Informational
Console	Успешная регистрация через консоль	**Successful login through Console (Username: <username>)**	Informational

Категория	Описание события	Содержимое записи	Уровень события
	Не удалось зарегистрироваться через консоль	**Login failed through Console**	Warning
	Выход из системы через консоль	**Logout through Console (Username: <username>)**	Informational
	Время сессии консоли истекло	**Console session timed out (Username: <username>)**	Informational
Web	Успешная регистрация через Web-интерфейс	**Successful login through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Не удалось зарегистрироваться через Web-интерфейс	**Login failed through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning
	Выход из системы через Web-интерфейс	**Logout through Web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Успешная регистрация через SSL	**Successful login through Web (SSL) (Username: <string>, IP: <ip>, MAC: <mac>)**	Informational
	Выход из системы через SSL	**Logout through Web (SSL) Username: <string>, IP: <ip>, MAC: <mac>)**	Informational
	Зарегистрироваться через SSL не удалось	**Login failed through Web (SSL) (Username: <string>, IP: <ip>, MAC: <mac>)**	Warning
	Таймаут сессии SSL	**Web(SSL) session timed out (Username: <username>)**	Informational
Telnet	Успешная регистрация через Telnet	**Successful login through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Зарегистрироваться через Telnet не удалось	**Login failed through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning
	Выход из системы через Telnet	**Logout through Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Время сессии Telnet истекло	**Telnet session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
SNMP	Полученный SNMP-запрос содержит некорректную community string	**SNMP request received from <ipAddress> with invalid community string!**	Informational
STP	Топология изменилась	**Topology changed**	Informational
	Выбран новый маршрут	**New Root selected**	Informational
	BPDU Loop Back на порту	**BPDU Loop Back on Port <portNum>**	Warning
	Включение протокола Spanning Tree	**Spanning Tree Protocol is enabled**	Informational
	Выключение	**Spanning Tree Protocol is**	Informational

Категория	Описание события	Содержимое записи	Уровень события
	протокола Spanning Tree	**disabled**	
SSH	Успешная регистрация через SSH	**Successful login through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Зарегистрироваться через SSH не удалось	**Login failed through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning
	Выход из системы через SSH	**Logout through SSH (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	Время сессии SSH истекло	**SSH session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational
	SSH-сервер включен	**SSH server is enabled**	Informational
	SSH-сервер выключен	**SSH server is disabled**	Informational
AAA	Политика аутентификации включена	**Authentication Policy is enabled (Module: AAA)**	Informational
	Политика аутентификации выключена	**Authentication Policy is disabled (Module: AAA)**	Informational
	Регистрация через консоль аутентифицирована в соответствии с локальным методом (local)	**Successful login through Console authenticated by AAA local method (Username: <username>)**	Informational
	Регистраця через консоль не аутентифицирована в соответствии с локальным методом (local)	**Login failed through Console authenticated by AAA local method (Username: <username>)**	Warning
	Регистрация через Web-интерфейс аутентифицирована в соответствии с локальным методом (local)	**Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через Web-интерфейс не аутентифицирована в соответствии с локальным методом (local)	**Login failed through Web from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через Web (SSL) аутентифицирована в соответствии с локальным методом (local)	**Successful login through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через	**Login failed through Web (SSL)**	Warning

Категория	Описание события	Содержимое записи	Уровень события
	Web (SSL) не аутентифицирована в соответствии с локальным методом (local)	**from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	
	Регистрация через Telnet аутентифицирована в соответствии с локальным методом (local)	**Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через Telnet не аутентифицирована в соответствии с локальным методом (local)	**Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через SSH аутентифицирована в соответствии с локальным методом (local)	**Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через SSH не аутентифицирована в соответствии с локальным методом (local)	**Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через консоль аутентифицирована в соответствии с методом none	**Successful login through Console authenticated by AAA none method (Username: <username>)**	Informational
	Регистрация через Web-интерфейс аутентифицирована в соответствии с методом none	**Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>,**	Informational
	Регистрация через Web(SSL) аутентифицирована в соответствии с методом none	**Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через Telnet аутентифицирована в соответствии с методом none	**Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через SSH аутентифицирована в соответствии с методом none	**Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational

Категория	Описание события	Содержимое записи	Уровень события
	Регистрация через консоль аутентифицирована Сервером аутентификации	**Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational
	Регистрация через консоль не аутентифицирована Сервером аутентификации	**Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)**	Warning
	Регистрация через консоль не аутентифицирована из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning
	Регистрация через Web-интерфейс аутентифицирована Сервером аутентификации	**Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через Web-интерфейс не аутентифицирована Сервером аутентификации	**Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через Web-интерфейс не аутентифицирована из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через Web (SSL) аутентифицирована Сервером аутентификации	**Successful login through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через Web (SSL) не аутентифицирована Сервером аутентификации	**Login failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через Web (SSL) не аутентифицирована из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning

Категория	Описание события	Содержимое записи	Уровень события
	Регистрация через Telnet аутентифицирована Сервером аутентификации	**Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через Telnet не аутентифицирована Сервером аутентификации	**Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через Telnet не аутентифицирована из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через SSH аутентифицирована Сервером аутентификации	**Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Регистрация через SSH не аутентифицирована Сервером аутентификации	**Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Регистрация через SSH не аутентифицирована из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через консоль аутентифицировано методом local_enable (локальный пароль)	**Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)**	Informational
	Выполнение команды Enable Admin через консоль не аутентифицировано методом local_enable (локальный пароль)	**Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)**	Warning
	Выполнение команды Enable	**Successful Enable Admin through Web from <userIP>**	Informational

Категория	Описание события	Содержимое записи	Уровень события
	Admin через Web-интерфейс аутентифицировано методом local_enable (локальный пароль)	**authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	
	Выполнение команды Enable Admin через Web-интерфейс не аутентифицировано методом local_enable (локальный пароль)	**Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через Web (SSL) аутентифицировано методом local_enable (локальный пароль)	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через Web (SSL) не аутентифицировано методом local_enable (локальный пароль)	**Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через Telnet аутентифицировано методом local_enable (локальный пароль)	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через Telnet не аутентифицировано методом local_enable (локальный пароль)	**Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через SSH аутентифицировано методом local_enable (локальный пароль)	**Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через SSH	**Enable Admin failed through SSH from <userIP> authenticated by**	Warning

Категория	Описание события	Содержимое записи	Уровень события
	не аутентифицировано методом local_enable (локальный пароль)	**AAA local_enable method (Username: <username>, MAC: <macaddr>)**	
	Выполнение команды Enable Admin через консоль аутентифицировано методом none	**Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)**	Informational
	Выполнение команды Enable Admin через Web-интерфейс аутентифицировано методом none	**Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через Web (SSL) аутентифицировано методом none	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через Telnet аутентифицировано методом none	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через SSH аутентифицировано методом none	**Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через консоль аутентифицировано сервером аутентификации	**Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)**	Informational
	Выполнение команды Enable Admin через консоль не аутентифицировано сервером аутентификации	**Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)**	Warning
	Выполнение команды Enable Admin через консоль не аутентифицировано сервером аутентификации из-	**Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning

Категория	Описание события	Содержимое записи	Уровень события
	за таймаута или несоответствующей конфигурации сервера аутентификации		
	Выполнение команды Enable Admin через Web-интерфейс аутентифицировано сервером аутентификации	**Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через Web-интерфейс не аутентифицировано сервером аутентификации	**Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через Web-интерфейс не аутентифицировано сервером аутентификации из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через Web (SSL) аутентифицировано сервером аутентификации	**Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через Web (SSL) не аутентифицировано сервером аутентификации	**Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через Web (SSL) не аутентифицировано сервером аутентификации из-за таймаута или несоответствующей конфигурации	**Enable Admin failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning

Категория	Описание события	Содержимое записи	Уровень события
	сервера аутентификации		
	Выполнение команды Enable Admin через Telnet аутентифицировано сервером аутентификации	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через Telnet не аутентифицировано сервером аутентификации	**Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через Telnet не аутентифицировано сервером аутентификации из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через SSH аутентифицировано сервером аутентификации	**Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Informational
	Выполнение команды Enable Admin через SSH не аутентифицировано сервером аутентификации	**Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**	Warning
	Выполнение команды Enable Admin через SSH не аутентифицировано сервером аутентификации из-за таймаута или несоответствующей конфигурации сервера аутентификации	**Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning
	Таймаута сервера аутентификации	**AAA server <serverIP> (Protocol: <protocol>) connection failed**	Warning
Port Security	Количество изученных адресов	**Port security violation (Port: <portNum>, MAC: <macaddr>)**	Warning

Категория	Описание события	Содержимое записи	Уровень события
	функции Port Security достигло максимума, и новые адреса не могут быть изучены.		
IP and Password changed	Изменение управляющего IP-адреса.	**Management IP address was changed by (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Informational
	Изменение пароля	**Password was changed by (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Informational
Safeguard Engine	Функция Safeguaard Engine работает в нормальном режиме	**SafeGuard Engine enters NORMAL mode**	Informational
	Функция Safeguaard Engine работает в режиме фильтрации трафика	**SafeGuard Engine enters EXHAUSTED mode**	Warning
Packet storm	Обнаружен широковещательный шторм	**Broadcast storm is occurring (port: <id>)**	Warning
	Широковещательный шторм прекращен	**Broadcast storm has cleared (port: <id>)**	Informational
	Обнаружен многоадресный шторм	**Multicast storm is occurring (port: <id>)**	Warning
	Многоадресный шторм прекращен	**Multicast storm has cleared (port: <id>)**	Informational
	Выключение порта из-за пакетного шторма	**Port (port: <id>) is cuurently shut down due to a packet shtorm**	Warning

Приложение D
Длина кабелей

В данной таблице приводится максимальное значение длины кабеля в зависимости от типа среды.

Стандарт	Тип среды	Максимальная протяжённость
Mini-GBIC	1000BASE-LX, одномодовый оптический модуль 1000BASE-SX, многомодовый оптический модуль 1000BASE-LH, одномодовый оптический модуль 1000BASE-ZX, одномодовый оптический модуль	10 км 550 м 40 км 80 км
1000BASE-T	UTP-кабель категории 5e UTP-кабель категории 5 (1000 Мбит/с)	100 м
100BASE-TX	UTP-кабель категории 5 (100 Мбит/с)	100 м
10Base-T	UTP-кабель категории 3 (10 Мбит/с)	100м

Глоссарий

1000BASE-LX: технология Gigabit Ethernet, использует многомодовое волокно, дальность прохождения сигнала без повторителя до 550 м.

1000BASE-SX: технология Gigabit Ethernet, использует многомодовое волокно, дальность прохождения сигнала без повторителя до 10 км.

100BASE-FX: Fast Ethernet с помощью оптоволоконного кабеля.

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

10BASE-T: Спецификация IEEE 802.3i для сетей Ethernet с использованием неэкранированного кабеля на основе скрученных пар ("витая пара").

aging: Автоматическое удаление из базы данных Коммутатора записей, которые устарели или утратили свою актуальность.

ATM: Asynchronous Transfer Mode (асинхронный режим передачи). Протокол передачи, ориентированный на соединение и основанный на использовании пакетов (ячеек) фиксированной длины. ATM рассчитан на передачу различных типов трафика, включая голос, данные и видео.

Автоматическое согласование (auto-negotiation): функция порта, которая позволяет ему сообщать свои параметры скорости, режима и управление потока. При соединении со станцией, также поддерживающей автоматическое согласование, оптимальные установки определяются автоматически.

Магистральный порт (**backbone port):** порт, который не распознает адреса устройств, получает все фреймы с нераспознанными адресами. Этот порт используется для соединения Коммутатора с магистралью сети. Магистральные порты также известны как назначенные downlink-порты.

Магистраль сети (backbone): Часть сети, по которой передается основной трафик между сегментами сети.

Полоса пропускания (bandwidth): характеризует количесво информации, которое может передать канал, измеряется в битах в секунду. Полоса пропускания для технологии Ethernet равна 10Мбит/с, для Fast Ethernet – 100Мбит/с.

baud rate: скорость коммутации в линии, скорость линии между сегментами сети.

BOOTP: Протокол BOOTP позволяет автоматически назначать IP-адрес соответствующему MAC-адресу при запуске устройства. Кроме того, протокол позволяет назначить маску подсети и шлюз по умолчанию для данного устройства.

Мост (bridge): Устройство, соединяющее локальные или удаленные сети при использовании протоколов высоких уровней модели OSI.

Широковещание (broadcast): Отправка сообщений на все устройства назначения в сети.

Широковещательный шторм (broadcast storm): Множество одновременных широковещательных рассылок в сети, которые, как правило, поглощают доступную полосу пропускания сети и могут вызвать отказ сети.

Консольный порт (console port): Порт на коммутаторе, к которому подключается терминальное или модемное соединение. Он преобразует параллельное представление данных на

последовательное, которое используется при передаче данных. Этот порт чаще используется для выделенного локального управления.

CSMA/CD: Carrier sense multiple access/collision detection. Метод канального доступа, использующий стандарты Ethernet и IEEE 802.3, где устройства передают данные только тогда, когда канал передачи данных не занят в течение некоторого периода времени. Когда два устройства передают данные одновременно, возникает коллизия. В этом случае конфликтующие устройства передают информацию повторно через выбранный случайным образом временной интервал.

Коммутация центра обработки данных (data center switching): точка агрегации в корпоративной сети, где коммутатор предоставляет высокопроизводительный доступ к серверной ферме, высокоскоростное соединение и контрольную точку для обеспечения управления сетью и безопасности.

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

Fast Ethernet: 100Мбитная технология, разработанная на основе Ethernet. Использует тот же протокол CSMA/CD для передачи данных.

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

Продвижение (forwarding): Процесс продвижения пакета к месту его назначения посредством сетевого устройства**.**

Полный дуплекс (full duplex): Возможность одновременной передачи и приема пакетов, и в результате удвоение потенциальной пропускной способности канала.

Полудуплекс (half duplex): Возможность передачи и приема пакетов, но не одновременно, в отличие от режима полного дуплекса.

IP-адрес (IP address): Уникальный идентификатор устройств, подключенных к сети с помощью протокола TCP/IP. Адрес записывается как 4-х байтовое значение с разделением точками, включает номер сети, а также может дополнительно включать номера подсети и номер хоста.

IPX: Протокол, обеспечивающий взаимодесйствие в сети NetWare

Локальная сеть (LAN): Сеть, соединяющая такие устройства как компьютеры, принтеры, сервера, покрывающая относительно небольшую площадь (часто не больше этажа или здания). Характеризуется высокой скоростью передачи данных и маленким количеством ошибок.

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

Скорость линии (line speed): смотри baud rate.

Основной порт (main port): Основной порт отказоустойчивой линии, обычно используемый для продвижения трафика в нормальных эксплуатационных режимах.

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

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

База управляющей информации (MIB): База данных, в которой хранятся параметры и характеристики управления устройством. Эта база данных ведется протоколом сетевого управления SNMP. Каждый коммутатор ведет совю собсвенную базу MIB.

Многоадресная рассылка (multicast): Передача пакета заданному подмножеству сетевых адресов. Эти адреса задаются в поле адреса приемника (Destination address field).

Протокол (protocol): набор правил, используемый для соединения устройств в сети. Эти правила задают формат пакета, временные интервалы, последовательность и контроль ошибок.

Отказоустойчивый канал (resilient link): пара портов, настроенные таким образом, что при выходе одно из них из строя, его функции принимает на себя другой порт. Смотрите также Основной порт (main port) и standby port.

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

Удаленный мониторинг (RMON): Модуль SNMP MIB II, который позволяет мониторить и управлять устройством, обрабатывая до 10 различных потоков информации.

Резервный источник питания (RPS): устройство, подключаемое к коммутатору для обеспечения резервного питания.

SLIP - Serial Line Internet Protocol: протокол, позволяющий передвать IP-информацию поверх последовательных соединений.

SNMP - Simple Network Management Protocol: Простой протокол сетевого управления, изначально использовавшийся только в сетях TCP/IP. Сейчас SNMP широко используется в компьютерах и сетевом оборудовании и позволяет управлять многими параметрами сети и конечными станциями.

Spanning Tree Protocol (STP): Проткол покрывающего дерева, позволяющий избежать образование петель в сетях. При использовании проткола STP обеспечиваются резервные пути для прохождения трафика, в то же время, в сети не образуются петли.

Стек (stack): Группа сетевых устройств, которые объединены в группу, образуя единое логическое устройство.

standby port: порт в отказоустойчивом канале, который возьмет на себя передачу данных в случае выхода из строя основного порта.

Коммутатор (switch): устройство, которое фильтрует, продвигает и рассылает пакеты, основываясь на адресе их доставки. Коммутатор изучает адреса, связанные с каждым своим портом, и заносит полученные данные в таблицы. Продвижение пакетов происходит на основе данных, представленных в данной таблице.

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

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

TFTP - Trivial File Transfer Protocol: протокол, позволяющий передавать файлы (такие как обновление программного обеспечения) с удалённого устройства, используя возможности управления коммутатора.

UDP - User Datagram Protocol: протокол Интернета, позволяющий программному приложению на одном устройстве отправлять датаграммы программному приложению другого устройства.

VLAN (Виртуальная LAN): объединение устройств в логическую группу независимо от размещения устройства и топологии сети. При этом взаимодействие устройств практически идентично взаимодействию в обычной сети LAN.

Канал виртуальный LAN (VLT): соединение Коммутатор-коммутатор, которое передаёт трафик всех VLAN-ов на каждый коммутатор.

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