Руководство пользователя

Коммутаторы серии DES-3500 xStack™
Управляемые стекируемые коммутаторы
Fast Ethernet 2 уровня
Release 5

СОДЕРЖАНИЕ

Предисловие.....vii
Предполагаемые читатели.....viii
Условные обозначения.....viii
Замечания, предупреждения, предостережения.....viii
Инструкция по безопасности..... ix
Предостережения безопасности ix
Общие меры безопасности для устройств, устанавливаемых в стойку..... x
Защита от электростатического разряда..... xi
Введение.....1
Описание коммутатора..... 1
Технические характеристики 2
Порты.....3
Компоненты передней панели.....3
Светодиодные индикаторы.....3
Описание задней панели.....5
Описание боковой панели.....5
Гигабитные комбо-порты.....6
Установка.....8
Комплект поставки..... 8
Перед началом работы..... 8
Настольное размещение коммутатора..... 8
Монтаж коммутатора в стойку..... 9
Монтаж коммутатора в стандартную 19" стойку..... 10
Включение электропитания (переменный ток).....11
Отключение электричества.....11
Подключение DES-3526DC к источнику постоянного тока..... 11
Подключение коммутатора..... 12
Подключение коммутатора к конечному узлу..... 12
Подключение коммутатора к концентратору или коммутатору..... 13
Подключение коммутатора к магистрали сети или серверу..... 14
Введение в управление коммутатором..... 15
Функции управления..... 15
Web-интерфейс управления..... 15
Управление через SNMP-протокол..... 15
Подключение к консольному порту коммутатора (RS-232 DCE)..... 15
Первое подключение к коммутатору..... 17
Защита паролем..... 17
Настройка SNMP..... 19
Traps 20
Базы управляющей информации MIB.....20
Назначение IP-адреса..... 20
Подключение устройств к коммутатору..... 22
Настройка коммутатора через Web-интерфейс..... 23
Введение..... 23
Регистрация в Web-интерфейсе управления..... 23
Пользовательский Web-интерфейс..... 24
Поля Web-интерфейса пользователя.....24
Опции, доступные через Web-интерфейс..... 25
Настройка Коммутатора..... 26
Информация о Коммутаторе..... 26
IP-адрес.....27
Расширенные настройки.....29
Настройка портов.....31
Описание портов.....33

Зеркалирование портов…… 34
Агрегирование каналов 35
Понятие группы агрегированных каналов 35
Настройки порта LACP 38
MAC-уведосление 40
Глобальные настройки MAC-уведомления 40
Настройки MAC-уведомления на порту 40
IGMP 41
IGMP Snooping 42
Создание записи о статических портах маршрутизатора 43
Запрещенные порты для подключения маршрутизатора 44
Многоадресная VLAN IGMP 45
Алгоритм покрывающего дерева 48
802.1s MSTP 48
802.1w Rapid Spanning Tree 48
Изменение состояния портов в протоколах STP, MSTP, RSTP 49
Пограничный порт 49
P2P-порт 50
Совместимость 802.1d/802.1w/802.1s 50
Глобальные настройки STP-моста 50
Таблица конфигурации MST 53
Настройки MSTI 55
Настройки копии STP 56
Информация о портах MSTP 57
Функция Loopback Detection 60
Продвижение и фильтрация пакетов (папка Forwarding Filtering) 62
Продвижение пакетов на заданный Unicast-адрес (Unicast Forwarding) 62
Multicast Forwarding 63
Режим фильтрации порта многоадресной рассылки 64
Виртуальные локальные сети (VLAN) 65
Понятие приоритета IEEE 802.1p 65
Описание VLAN 66
Замечания по реализации функции VLAN в коммутаторах серии DES-3500 … 66
IEEE 802.1Q VLAN 66
Теги 802.1Q VLAN 68
Идентификатор порта VLAN ID 68
Тегирующие и нетегирующие порты 70
Фильтрация входящих пакетов (Ingress Filtering) 70
VLAN по умолчанию 70
Port-based VLAN (на основе портов) 71
Сегментация VLAN 71
Асимметричные VLAN 71
VLAN и группы агрегированных каналов 72
Статическая запись VLAN 72
Настройки GVRP 74
Управление трафиком 76
Port Security(безопасность на уровне портов) 79
QoS 81
Преимущества QoS 82
Понятие QoS 83
Полоса пропускания порта 85
Работа по расписанию 86
Приоритет 802.1p по умолчанию 86
Приоритет пользователя 802.1p 87
Сегментация трафика 87
Задание уровня проблемы для отправки сигнала предупреждения 88
Системный журнал 89

Настройки SNTP..... 90
Настройки времени..... 90
Часовые пояса и DST..... 91
Таблица профилей доступа..... 93
Настройка таблицы профилей доступа..... 93
CPU Interface Filtering..... 108
Таблица профилей CPU Interface Filtering..... 109
Port Access Entity (802.1X) 122
Аутентификация 802.1x на основе портов и MAC-адресов..... 122
Сервер аутентификации.....122
Аутентификатор.....123
Клиент.....124
Процесс аутентификации..... 124
Аутентификация на основе портов..... 124
Аутентификация на основе MAC-адресов..... 126
Настройка утентификатора..... 127
Система управления PAE..... 129
Port Capability 129
Инициализация портов при аутентификации 802.1x на основе портов.....130
Инициализация портов при аутентификации 802.1x на основе MAC-адресов.....131
Повторная аутентификация портов для 802.1x на основе портов.....131
RADIUS-сервер..... 132
Guest VLAN..... 133
Ограничения при использовании Guest VLAN.....134
IP-MAC Binding(Связка IP-MAC)..... 135
Режим ACL..... 135
Настройка IP-MAC Binding для портов..... 138
Таблица IP-MAC Binding..... 138
Блокировка из-за несоответствия связки IP-MAC..... 140
Настройка ограничения диапазона IP-адресов многоадресной рассылки..... 140
Настройка профиля ограничения диапазона IP-адресов многоадресной рассылки 141
Настройка статуса ограниченного диапазона IP-адресов многоадресной рассылки..... 141
Настройка ограниченного диапазона IP-адресов многоадресной рассылки..... 143
Построение IP-сетей 3 уровня..... 145
Статическая таблица ARP..... 145
DHCP/BOOTP Relay..... 147
Глобальная настройка DHCP / BOOTP Relay на Коммутаторе.....147
Реализация Option 82 в коммутаторах серии DES-3500 xStack.....149
Настройки интерфейса DHCP/BOOTP Relay.....150
Управление.....151
Задание безопасных IP-адресов 151
Учетные записи пользователей.....151
Привилегии пользователей «Admin», «Operator» и «User» Privileges 153
Управление аутентификацией доступа..... 153
Настройки политики и параметров.....154
Настройка аутентификации приложений.....154
Настройка группы серверов аутентификации.....155
Серверы аутентификации..... 157
Списки методов регистрации (Login Method Lists)..... 159
Enable Method Lists 161
Локальный пароль..... 162
Enable Admin (Включение привилегий уровня Администратора)..... 163
Secure Socket Layer (SSL)..... 164
Загрузка сертификата..... 165
Настройка Ciphersuite..... 165
Secure Shell (SSH) 167
Настройка SSH..... 167

SSH Algorithm (SSH-алгоритм)..... 168
Аутентификация SSH-пользователя..... 170
SNMP-менеджер..... 171
Настройки SNMP……..... 171
Traps 172
Базы управляющей информации MIB.....173
Таблица SNMP-пользователей..... 173
Таблица просмотра SNMP (SNMP View Table) 175
Таблица групп SNMP (SNMP Group Table)..... 176
Таблица конфигурации SNMP Community..... 177
Таблица хоста SNMP..... 178
SNMP Engine ID 179
Safeguard Engine..... 180
Фильтрация…..... 183
Настройка сортировки DHCP-серверов..... 183
Настройка фильтрация DHCP-клиента..... 184
Настройка фильтрации NetBIOS..... 185
Мониторинг..... 188
Использование порта……..... 188
Использование CPU……..... 189
Пакеты..... 190
Полученные пакеты (RX)..... 190
Полученные одноадресные, многоадресные и широковещательные пакеты (RX) 191
Отправленные пакеты (TX)..... 193
Ошибки..... 194
Ошибки в полученных коммутатором пакетах (RX)..... 195
Ошибки в отправленных коммутатором пакетах(TX) 197
Размер пакета..... 199
MAC-адреса……..... 200
Журнал коммутатора..... 202
Группа IGMP Snooping..... 203
Таблица IGMP Snooping Forwarding..... 204
Статус VLAN..... 204
Порт маршрутизатора..... 205
Контроль доступа по портам..... 206
Состояние аутентификатора 206
Функции уровня 3……..... 208
Просмотр таблицы ARP..... 208
Статус Safeguard Engine..... 208
Техническая эксплуатация…..... 210
Сервисы TFTP..... 210
Загрузка программного обеспечения с TFTP-сервера..... 210
Загрузка конфигурационного файла..... 211
Сохранение конфигурационного файла на TFTP-сервере..... 211
Загрузка журнала коммутатора на TFTP-сервер..... 212
Поддержка нескольких версий программного обеспечения..... 212
Информация о программном обеспечении..... 212
Настройка образа программного обеспечения..... 213
Ping Test 214
Сохранение изменений..... 215
Сброс настроек коммутатора (функция Reset)..... 215
Reset System..... 216
Reset Config 216
Перезапуск коммутатора..... 216
Выход из системы (Logout)..... 217
Технология D-Link Single IP Management 218
Обзор технологии Single IP Management (SIM)..... 218

Обновление технологии SIM до версии v1.6.....219
Подключение функции SIM через Web-интерфейс..... 220
Топология сети..... 221
Значки устройств..... 223
Нажатие правой кнопки мыши..... 224
Группировка иконок.....224
Значок управляющего коммутатора.....225
Значок члена группы.....226
Значок коммутатора CaS…….....226
Линейка меню..... 227
File ….....228
Group 228
Device 228
View.....228
Help….....228
Обновление программного обеспечения для членов SIM-группы..... 229
Сохранение / восстановление конфигурационных файлов.....229
Загрузка файла журнала коммутатора.....230
Техническая спецификация..... 231
Кабели и коннекторы..... 233
Записи системного журнала..... 234
Длина кабелей 249
Глоссарий..... 250

Предисловие

Руководство пользователя для коммутаторов серии DES-3500 состоит из нескольких разделов, в которых приводятся инструкции по настройке и примеры конфигурации. Ниже приводится краткий обзор разделов:

Раздел 1, Введение - Описание коммутатора и его свойств.

Раздел 2, Установка- Помогает осуществить установку коммутатора, а также содержит описание передней, задней панелей и индикаторов коммутатора. Также в этом раздел содержатся инструкции, как подключить питание постоянного тока к Коммутатору серии DES-3500.

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

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

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

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

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

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

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

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

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

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

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

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

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

Предполагаемые читатели

Руководство пользователя для коммутаторов ***серии DES-3500*** содержит необходимую информацию для настройки и управления коммутатором. Это руководство предназначено преимущественно для администраторов сети, знающих принципы сетевого управления и терминологию.

Условные обозначения

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

Замечания, предупреждения и предостережения

ЗАМЕЧАНИЕ содержит важные указания, помогающие наиболее эффективно использовать устройство.

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

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

Инструкция по безопасности

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

⚠ Предостережения безопасности

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

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

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

• Используйте только подходящие силовые кабели. Если нужный кабель не входил в комплект поставки, то приобретите силовой кабель, который одобрен для использования в вашей стране. Силовой кабель должен соответствовать характеристикам напряжения и тока, необходимым для данного устройства. Характеристики напряжения и тока кабеля должны быть больше, чем мощность, указанная на

устройстве.

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

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

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

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

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

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

- Установите источник питания до 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 коммутатора
Технические характеристики
Порты
Компоненты передней панели
Описание боковой панели
Описание задней панели
Комбо-порты Gigabit Ethernet

Серия коммутаторов DES-3500 – это стекируемые коммутаторы 2 уровня Fast Ethernet серии D-Link xStack. Коммутаторы семейства xStack 10/100 Мбит/с поддерживают стекирование по технологии SIM и обеспечивают необходимую отказоустойчивость, гибкость сети, плотность портов, требуемую безопасность и максимальную пропускную способность. При этом эти коммутаторы снабжены удобным интерфейсом управления, что по достоинству оценят сетевые профессионалы.

Данное руководство описывает установку, эксплуатацию и настройку коммутаторов серии DES-3500 xStack. Эти коммутаторы идентичны в настройках и по основным аппаратным средствам, соответственно большая часть информации в данном руководстве будет универсальной для всех коммутаторов этой серии (DES-3526, DES-3526DC, DES-3550). 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.

Пожалуйста, обратите внимание, что если оборудование было куплено за пределами Европы, то читателю будут заметны определенные внешние различия между самим коммутатором и его изображением его лицевой панели в этом руководстве.

Описание коммутатора

Коммутаторы серии DES-3500 снабжены портами под неэкранированную витую пару (UTP), обеспечивающими выделенную полосу пропускания 10 или 100 Мбит/с. Коммутатор оснащен 24 (для DES-3526, DES-3526DC) или 48 портами (для DES-3550) 10/100Base-TX, поддерживающими автоматическое определение полярности MDI-X/MDI-II. Они могут быть использованы для подключения ПК, принтеров, серверов, концентраторов, маршрутизаторов, коммутаторов и другого сетевого оборудования. Данные порты на основе стандартной витой пары идеально подходят для сегментирования сетей на малые подсети для получения улучшенных характеристик. Каждый порт 10/100 Мбит/с может обеспечить пропускную способность до 200 Мбит/с в полнодуплексном режиме.

Помимо этого коммутатор снабжен двумя комбо-портами 1000Base-T/Mini-GBIC(SFP), которые идеально подходят для подключения к серверу или магистрали сети.

Данный коммутатор позволяет реализовывать в сети некоторые из наиболее распространенных мультимедийных и видео приложений одновременно с другими пользовательскими приложениями без создания, так называемых, «узких мест». Встроенный интерфейс командной строки может быть использован для настройки приоритезации очередей, виртуальных локальных сетей (VLAN), групп агрегированных каналов, мониторинга по портам и скорости по портам.

Примечание: Далее в руководстве все устройства (DES-3526, DES-3526DC, DES-3550) будут упоминаться как «Коммутатор» или «коммутатор серии DES-3500». Кроме тех моментов, где между ними существуют различия.

Технические характеристики

• IEEE 802.3 10BASE-T
• IEEE 802.3u 100BASE-TX
• Приоритезация очередей IEEE 802.1p
• Управление потоком в полнодуплексном режиме согласно IEEE 802.3x
• Агрегирование портов (LACP) согласно IEEE 802.3ad
• Управление доступом IEEE 802.1x на основе портов и MAC-адресов
• Поддержка VLAN IEEE 802.1Q
• Поддержка протоколов IEEE 802.1D Spanning Tree, IEEE 802.1W Rapid Spanning Tree and IEEE 802.1s
• Списки управления доступом (ACL)
• Управление через единый IP-адрес (SIM)
• Аутентификация с помощью TACACS, XTACACS and TACACS+
• Поддержка двух копий ПО (Dual Image)
• Протокол SNTP
• MAC Notification
• Ассиметричные VLAN
• Просмотр использования системы и портов
• Журнал регистраций
• Размер таблицы MAC-адресов 8К
• Буфер пакетов 16 Мбайт
• Группы VLAN на основе портов
• Гибкое агрегирование портов
• IGMP Snooping
• SNMP
• Secure Sockets Layer (SSL) и Secure Shell (SSH)
• Зеркалирование портов
• База управляющей информации (MIB) для:
• RFC1213 MIB II
• RFC1493 Bridge
• RFC1757 RMON
• RFC1643 Ether-like MIB
• RFC2233 Interface MIB
• Private MIB
• RFC2674 for 802.1p
• IEEE 802.1x MIB
• Консольный порт RS-232 DCE
• Индикаторы для каждого порта
• Высокопроизводительная коммутация, позволяющая осуществлять продвижение и фильтрацию пакетов со скоростью соответствующей среде передачи: максимум 14 881 пакетов/с для каждого порта Ethernet 10Мбит/с, максимум 148 810 пакетов/с для каждого порта 100Мбит/с Fast Ethernet.
• Поддержка режимов полного и полудуплекса для соединений 10 и 100Мбит/с. В режиме полного дуплекса порт коммутатора может одновременно передавать и принимать данные. Этот режим используется для соединения с конечными станциями и коммутаторами, поддерживающими данный режим. Соединение с концентраторами должны осуществляться в режиме полудуплекса.
• Поддержка управления широковещательным штормом:
• Неблокирующая схема коммутации store and forward с автоматическим выбором скорости и протокола.
• Поддержка управления входящей / исходящей скоростью на основе портов.
• IP-MAC Port Binding
• Эффективный механизм распознавания адресов и создания таблицы адресов
• Поддержка Safeguard Engine

Порты

- 24 (для DES-3526, DES-3526DC) или 48 (для DES-3550) портов 10/100Base-TX(MDI-X/MDI-II) для подключения конечных станций, серверов, концентраторов и других сетевых устройств. Эти порты поддерживают автоматическое определение скорости передачи данных (10 Мбит/с/100 Мбит/с) и режима работы (дуплексный / полудуплексный), а также настройку управления потоком (в полудуплесном режиме – метод обратного давления, в дуплексном режиме – 802.1x).
- Два комбо-порта 1000BASE-T/Mini-GBIC(SFP) для гибкого подключения к другому коммутатору, серверу или магистрали сети.
- Порт RS-232 DCE (консольный порт) для настройки и управления коммутатором через подключение к консольному терминалу или ПК, используя эмуляционную терминальную программу.

Примечание: Покупателям, заинтересовавшимся в управляющем программном обеспечении SNMP корпорации D-Link «D-View», советуем посетить сайт D-Link (www.dlink.ru) и скачать программное обеспечение и руководства.

Компоненты передней панели

Передняя панель коммутатора содержит светодиодные индикаторы:

- питания;
- портов под витую пару со скоростью 10/100 Мбит/с;
- двух комбо-портов 1000BASE-T Mini-GBIC.

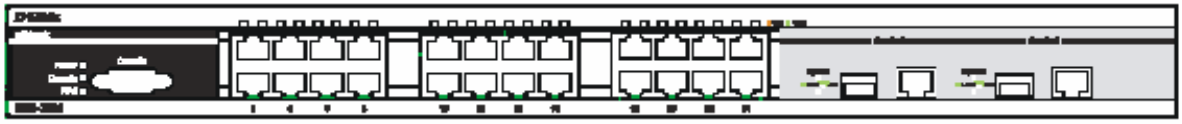


Рисунок 1.1 – Вид передней панели коммутатора DES-3526

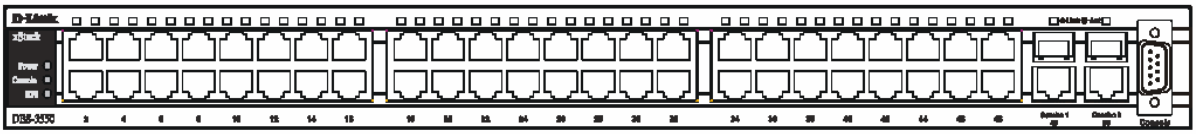


Рисунок 1.2 – Вид передней панели коммутатора DES-3550

Коммутатор DES-3526DC не поддерживает резервный блок питания, поэтому на передней панели отсутствует индикатор RPS.

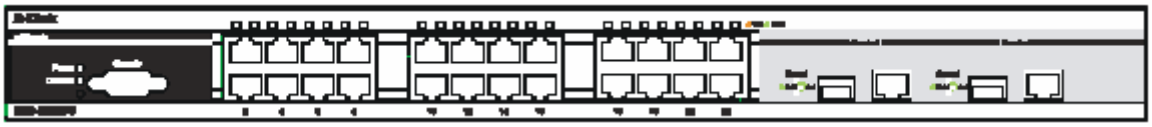


Рисунок 1.3– Вид передней панели коммутатора DES-3526DC

Все светодиодные индикаторы отображают статус коммутатора и сети.

Светодиодные индикаторы

У коммутатора есть светодиодные индикаторы питания, консоли, резервного блока питания RPS (только для DES-3526/DES-3550), портов. На рисунке 1.3 показано расположение

светодиодных индикаторов, а в представленной ниже таблице описаны индикаторы и соответствующие им значения.

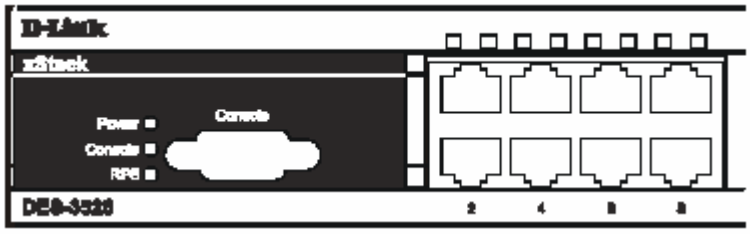


Рисунок 1.4 – Светодиодные индикаторы на коммутаторе DES-3526

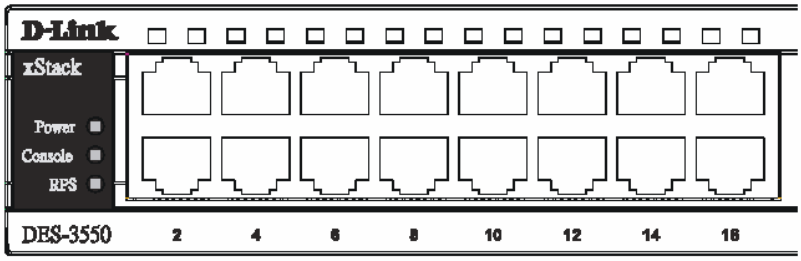


Рисунок 1.5 – Светодиодные индикаторы на коммутаторе DES-3550

Светодиодный индикатор	**Описание**
Power	После включения коммутатора индикатор питания будет гореть зеленым цветом, показывая готовность устройства к работе. В случае отключения питания, индикатор будет темного цвета.
Console	Данный индикатор будет мигать во время самотестирования при включении питания Power-On Self Test (POST). После того, как самотестирование будет завершено, индикатор станет темным. Индикатор будет гореть постоянным зеленым цветом в случае удаленного либо местного управления коммутатором через консольный порт RS-232 с помощью «прямого» последовательного кабеля.
RPS (только для DES-3526/DES-3550)	Данный индикатор будет гореть, когда будет использоваться резервный блок питания, в противном случае он будет темным.
Ports LEDs	Один ряд индикаторов расположен над каждым портом на передней панели. Данные индикаторы портов будут гореть двумя различными цветами для скорости передачи 10Мбит/с и 100Мбит/с: ▪ Желтый – для скорости 10 Мбит/с. Постоянный цвет говорит о текущей активности на порту, мигающий цвет свидетельствует об установленном соединении. ▪ Зеленый - для скорости 100 Мбит/с. Постоянный цвет говорит об активности на порту, мигающий цвет свидетельствует об установленном соединении.
100M/10M	Индикаторы будут гореть постоянным зеленым цветом при передаче данных через порт на скорости 100 Мбит/с.
Gigabit ports	Два порта Mini GBIC коммутатора оснащены своими собственными индикаторами: Speed – данный индикатор будет гореть постоянным зеленым цветом при передаче данных на скорости 1000 Мбит/с. Когда индикатор темного цвета, то через порт передаются данные на скорости 10/100 Мбит/с Link/Act – данный индикатор горит постоянным зеленым цветом, в случае когда канал установлен. Мигающий индикатор свидетельствует о текущей активности порта. Темный индикатор говорит об отсутствии активности на

	порту.

Описание задней панели

На задней панели коммутатора DES-3526 и DES-3550 есть разъем питания переменного тока.

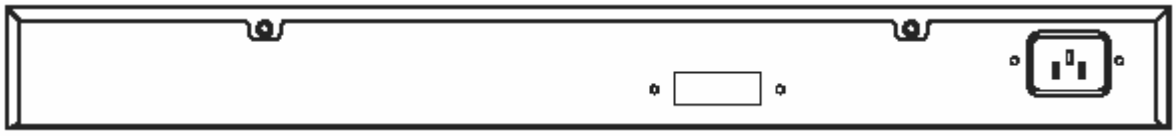


Рисунок 1.6 – Вид задней панели коммутатора DES-3526

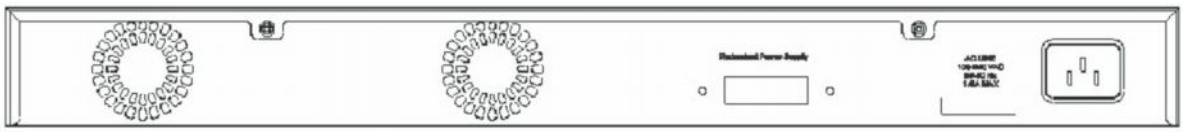


Рисунок 1.7 – Вид задней панели коммутатора DES-3550

Разъем питания переменного тока представляет собой стандартный трехконтактный разъем под шнур питания. В данный разъем поместите один конец шнура питания с разъемом типа «мама», другой конец с разъемом типа «папа» вставьте в розетку. Коммутатор автоматически отрегулирует настройки питания под потребляемое напряжение в диапазоне 100 ~ 240 В переменного тока с частотой 50 ~ 60 Гц.

Один конец шнура питания вставьте в разъем питания коммутатора, а другой конец в гнездо ближайшей розетки. На задней панели также есть выход для дополнительного внешнего источника питания. В случае пропадания питания, немедленно заработает резервный источник питания.

Рисунок 1.8 – Вид задней панели коммутатора DES-3526DC

На задней панели коммутатора DES-3526DC есть выход, предназначенный для питания постоянным током. В данном разделе приводятся подробные инструкции по инсталляции.

Описание боковой панели

На правой боковой панели коммутатора находится вентилятор, на левой боковой панели вентилятор и теплоотвод. Вентилятор используется для рассеивания тепла. Для той же цели служит и теплоотвод. Не закрывайте эти отверстия и оставьте по 6 дюймов (1 дюйм = 2,54 см, 6 дюймов = 15,24 см) свободного пространства вокруг задней и боковых панелей коммутатора. Напоминаем, что без правильно организованного теплового рассеивания и циркуляции воздуха, системные компоненты могут перегреться, что, в свою очередь, может привести к нарушению работы устройства.

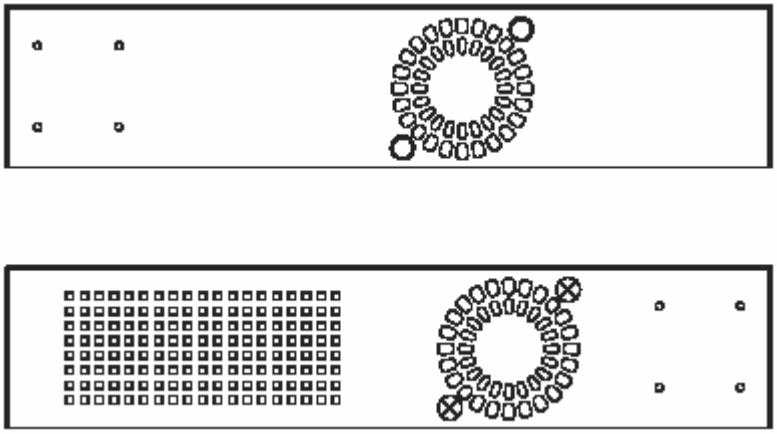


Рисунок 1.9 – Боковые панели коммутаторов DES-3526/DES-3526DC

Рисунок 1.10 – Боковые панели коммутаторов DES-3550

Гигабитные комбо-порты

В дополнение к 24 (или 48) портам 10/100 Мбит/с коммутатор также оснащен двумя гигабитными Ethernet комбо-портами, т.е. двумя портами, выполненными под медную витую пару 1000BASE-T, и двумя портами Mini-GBIC. Посмотрите на представленный ниже рисунок по включению Mini-GBIC модулей в соответствующие порты. Пожалуйста, обратите внимание, что из одной пары портов (всего две пары портов) под медную витую пару и под оптические модули Mini-GBIC можно использовать только один порт. GBIC-порт будет всегда обладать наивысшим приоритетом.

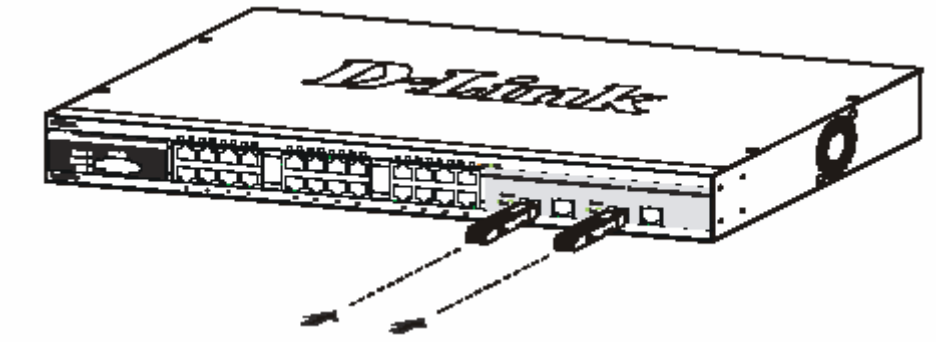


Рисунок 1.11 – Включение в коммутатор модулей Mini-GBIC для DES-3526

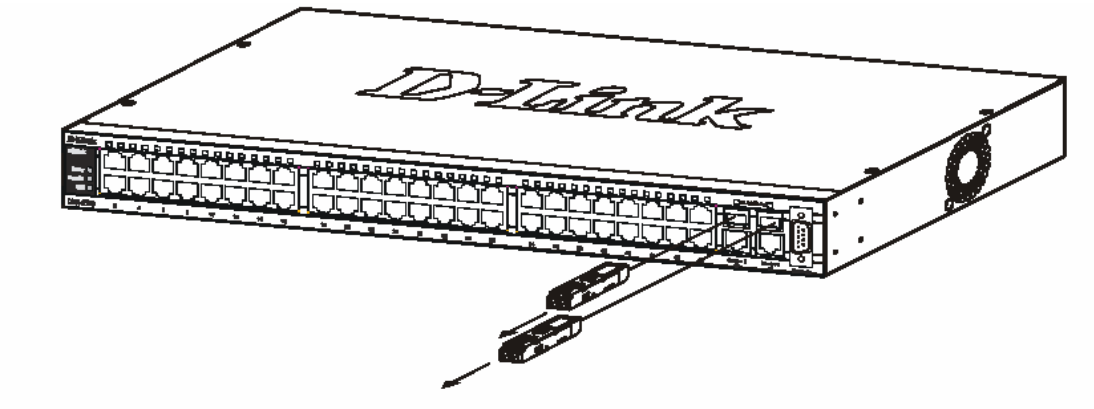


Рисунок 1.12 – Включение в коммутатор модулей Mini-GBIC для DES-3550

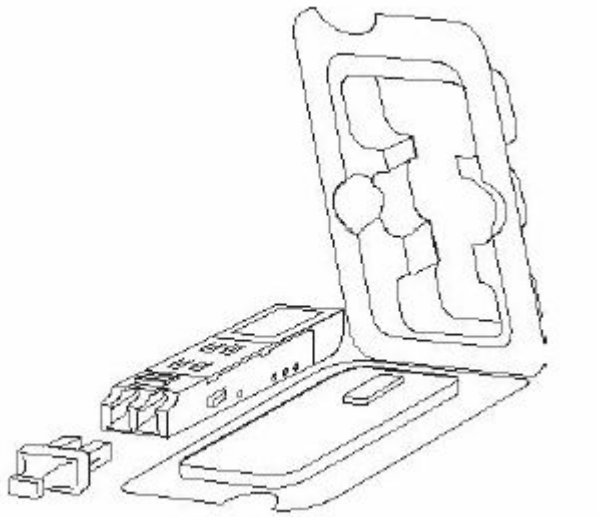


Рисунок 1.13 – Установка модулей Mini-GBIC

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-3500 xStack
- Один шнур питания переменного тока (AC) (кроме DES-3526DC)
- Данное руководство пользователя
- Регистрационная карточка
- 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, 3 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 (только для DES-3526).
- 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.

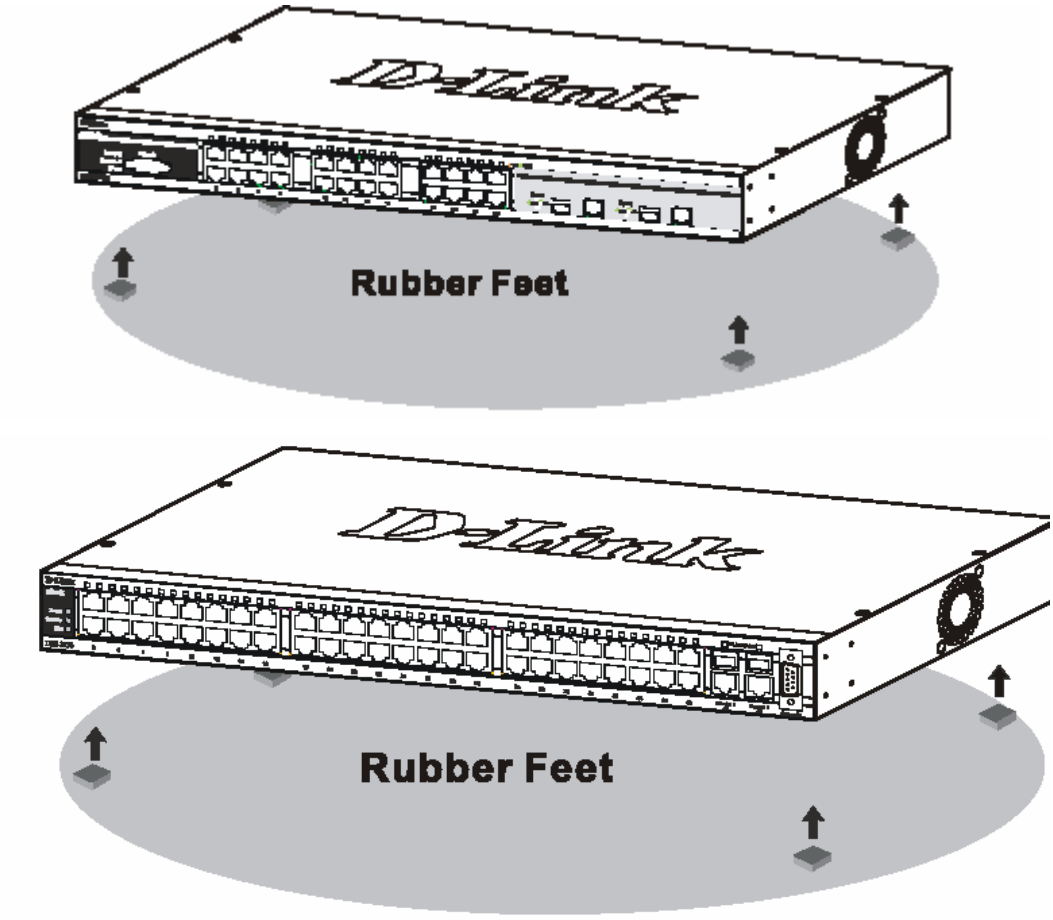


Рисунок 2.1 – Подготовка коммутатора DES-3526 и DES-3550 к установке на стол или полку

Монтаж коммутатора в стойку

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

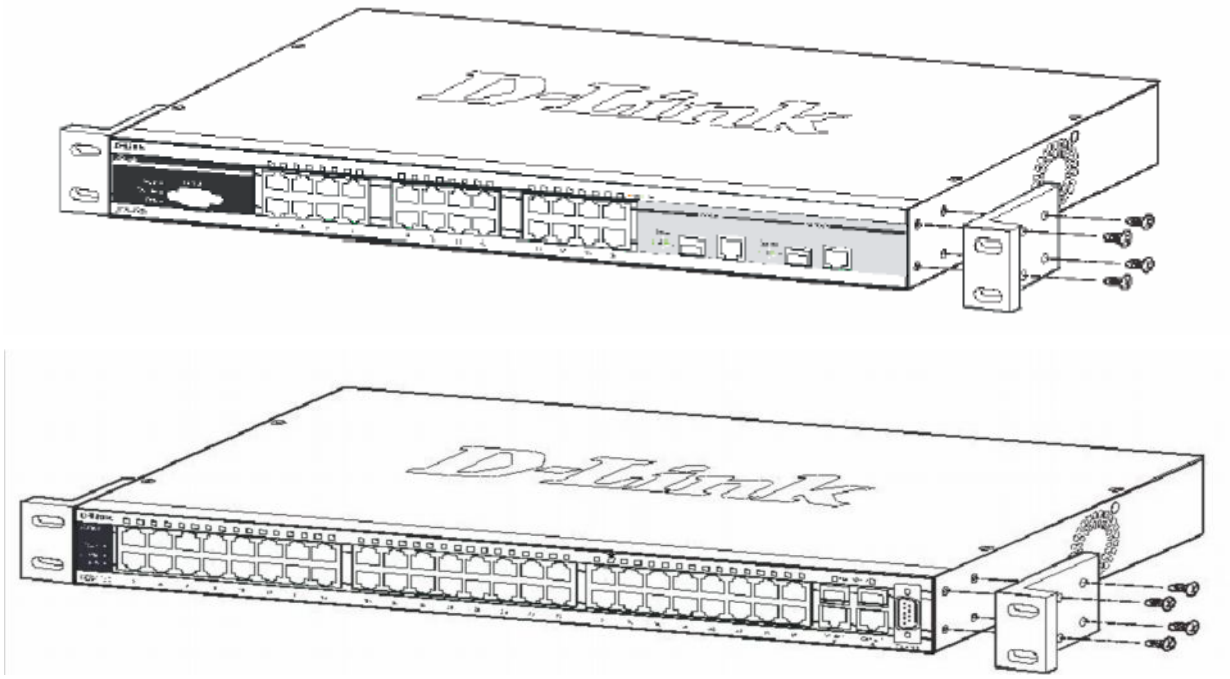


Рисунок 2.2 – Прикрепление петлей к коммутаторам DES-3526 и DES-3550

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 и рисунке 2.4.

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.

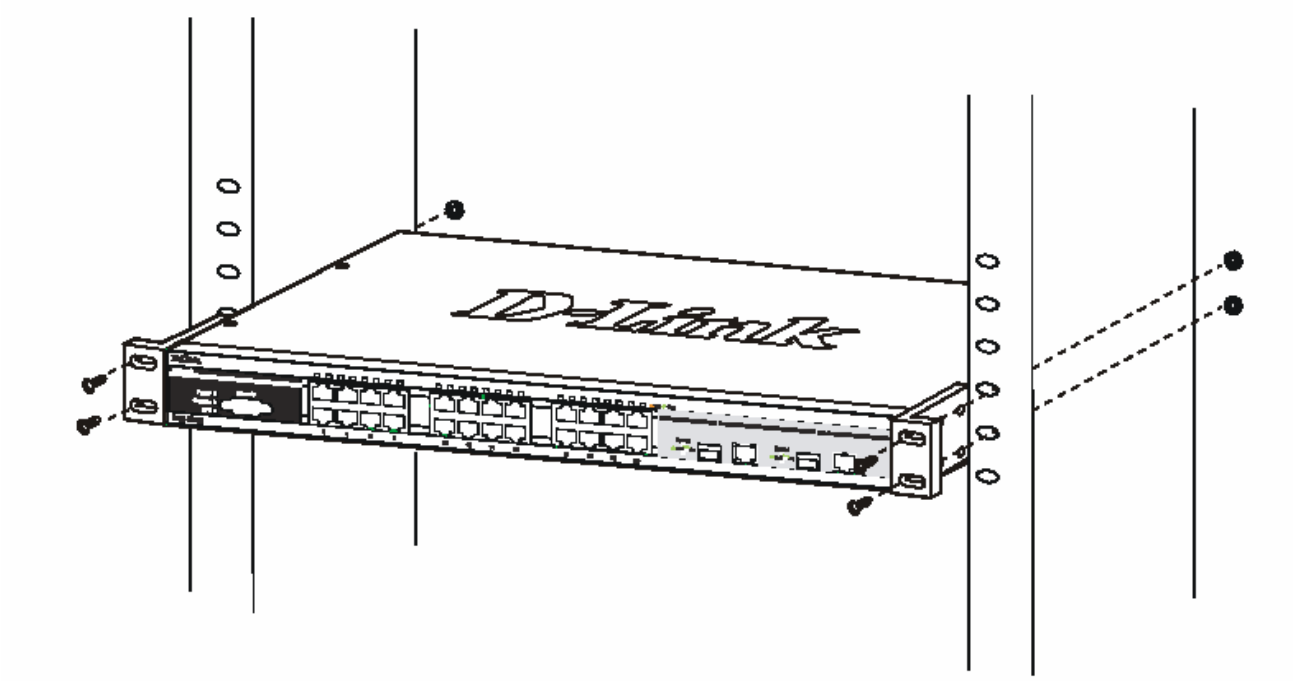


Рисунок 2.3 – Монтаж коммутатора DES-3526 в стойку

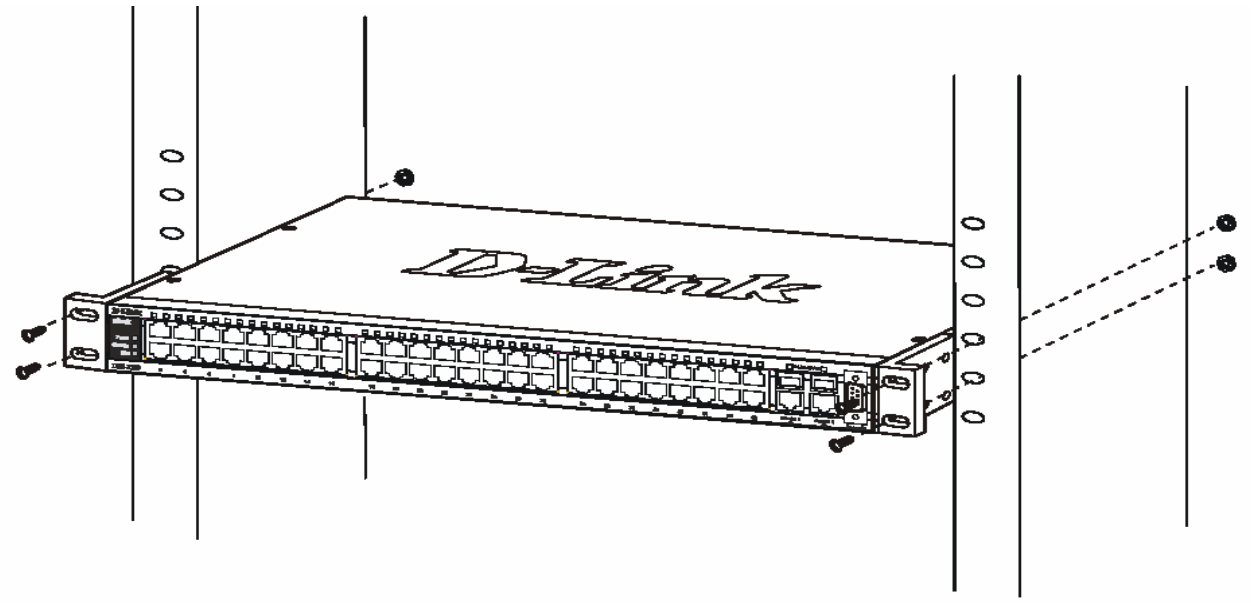


Рисунок 2.4 – Монтаж коммутатора DES-3550 в стойку

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.

Подключение DES-3526DC к источнику постоянного тока

Для подключения DES-3526DC к источнику постоянного тока, следуйте приведенным ниже рекомендациям.

Рисунок 2.4 – Подключение блока питания к источнику постоянного тока

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

Раздел 3 - Подключение коммутатора

Подключение коммутатора к конечному узлу

Подключение коммутатора к концентратору или коммутатору

Подключение коммутатора к магистрали сети или серверу

Примечание: Все 24 (48 для DES-3550) высокопроизводительных порта NWay Ethernet могут поддерживать как MDI-II, так и MDI-X-соединения.

Подключение коммутатора к конечному узлу

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

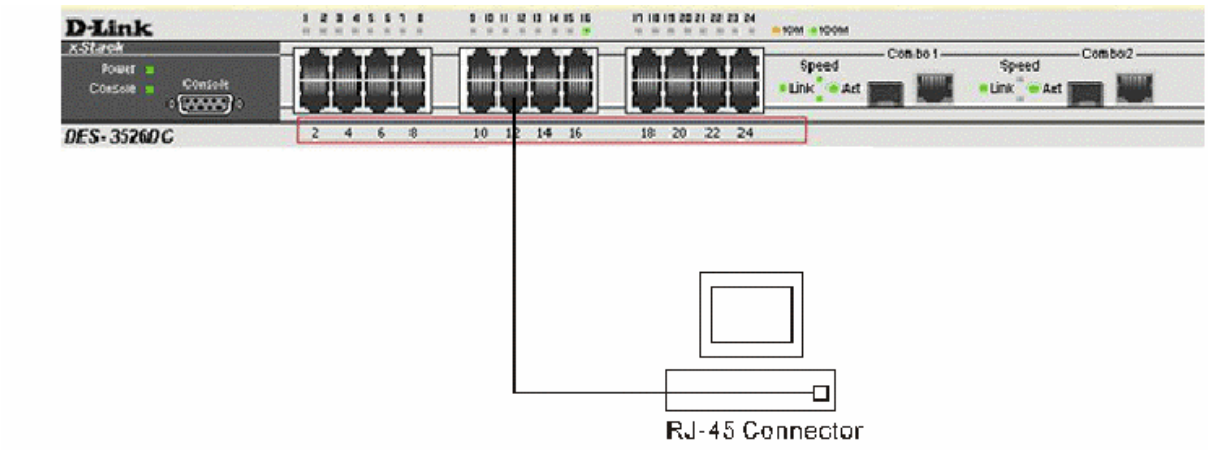


Рисунок 3.1 – Подключение коммутатора DES-3526DC к конечному узлу

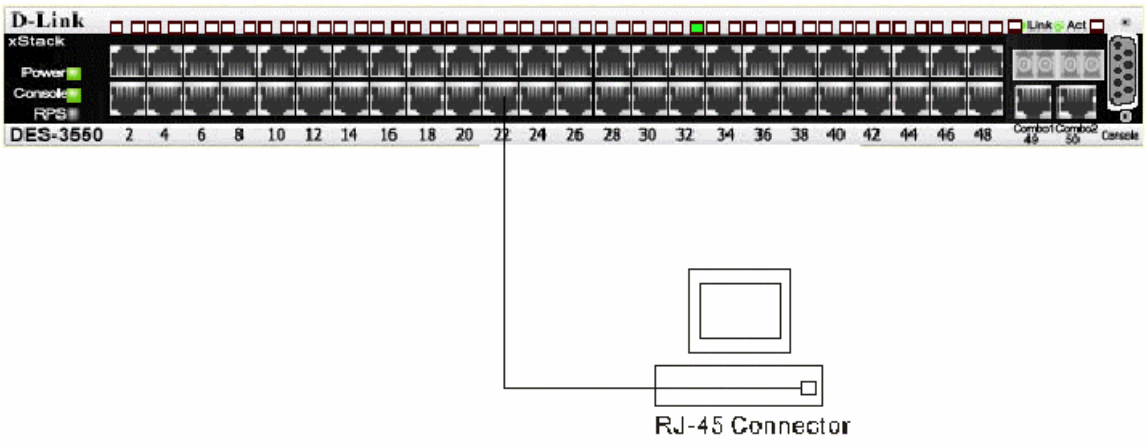


Рисунок 3.2 – Подключение коммутатора DES-3550 к конечному узлу

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 обыкновенного кабеля.

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

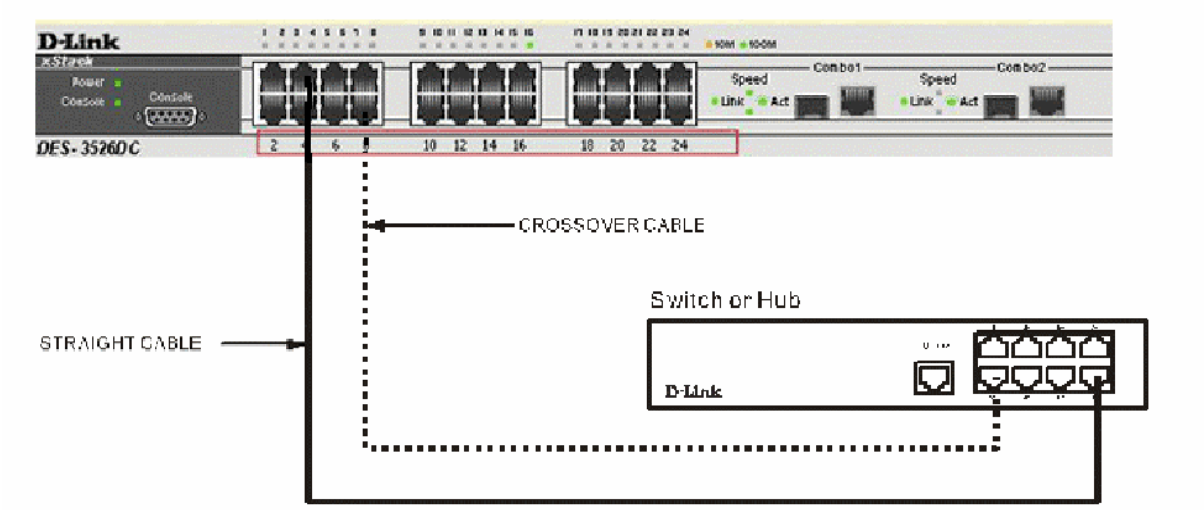


Рисунок 3.3 – Коммутатор DES-3526DC, подключенный к обыкновенному (не Uplink) порту концентратора или коммутатора с помощью прямого или кроссового кабеля

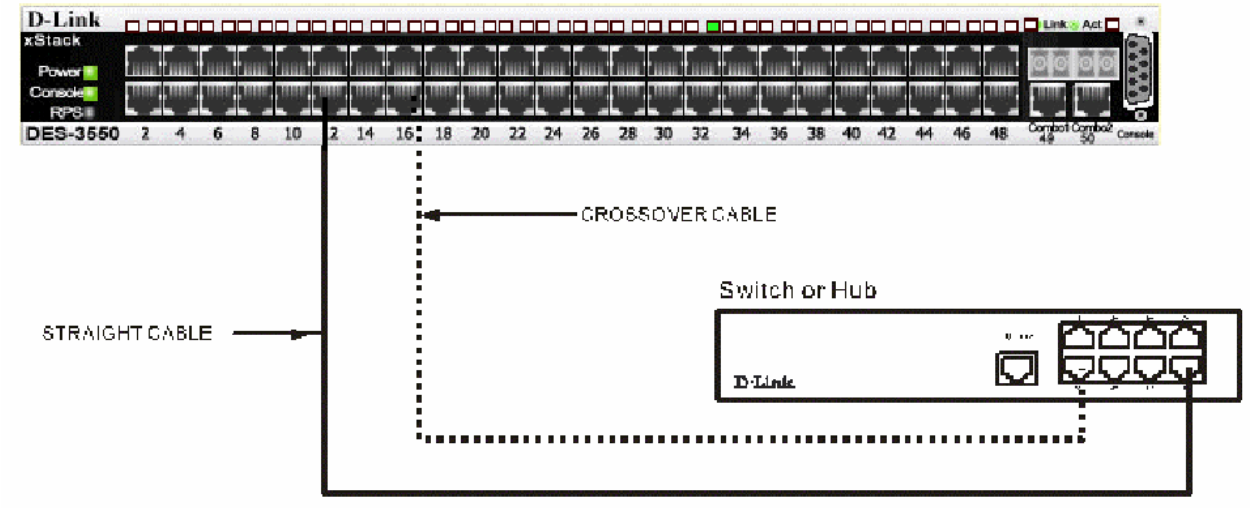


Рисунок 3.4 – Коммутатор DES-3550, подключенный к обыкновенному (не Uplink) порту концентратора или коммутатора с помощью прямого или кроссового кабеля

Подключение коммутатора к магистрали сети или серверу

Два комбо-порта Mini–GBIC идеально подходят для uplink-подключения к магистрали сети или серверу. Медные порты работают на скоростях 1000, 100 или 10 Мбит/с в дуплексном или полудуплексном режимах. Порты, выполненные под волоконно-оптический кабель, могут работать на скорости 1000 Мбит/с в дуплексном режиме.

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

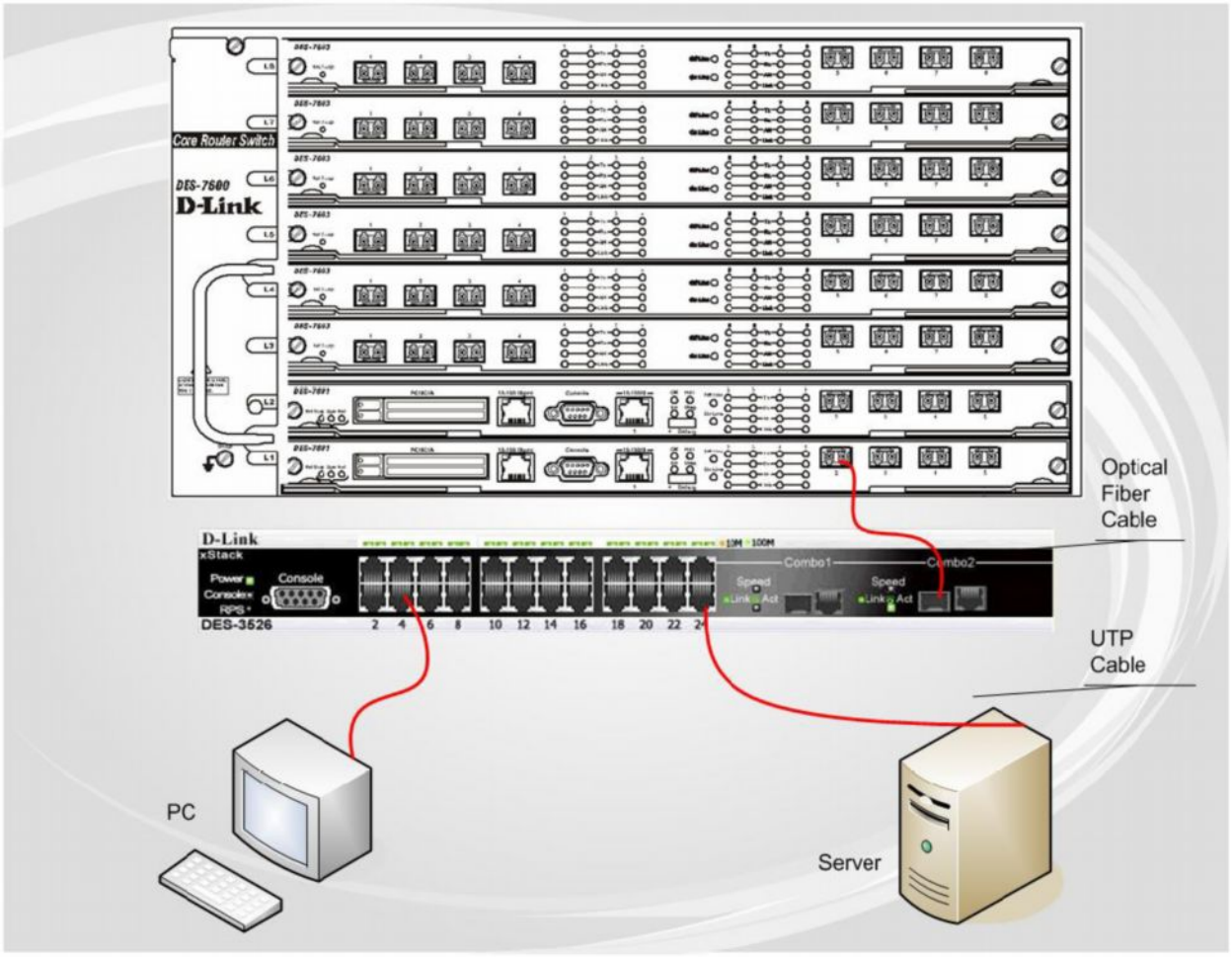


Рисунок 3.5 – Подключение коммутатора серии DES-3500 к серверу

Раздел 4 - Введение в управление коммутатором

Функции управления
Web-интерфейс управления
Управление через SNMP-протокол
Подключение к консольному порту коммутатора (RS-232 DCE)
Первое подключение к коммутатору
Защита паролем
Настройка SNMP
Назначение IP-адреса
Подключение устройств к коммутатору

Функции управления

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 и выше) или Microsoft Internet Explorer (версия 5.0).

Управление через SNMP- протокол

Также можно управлять коммутатором с помощью консольной программы, совместимой с SNMP-протоколом. Коммутатор поддерживает 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-3500***, 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 в 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-3526:admin#,** как это показано ниже.

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

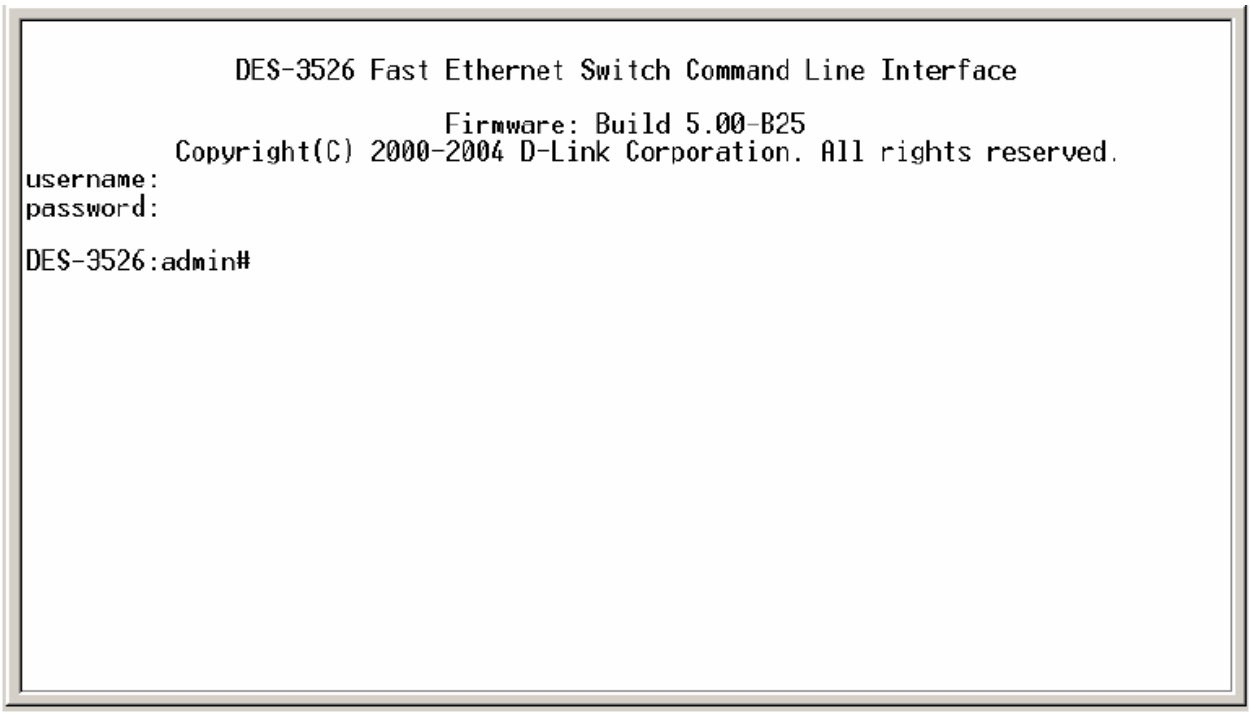


Рисунок 4.2 – Командная строка

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-3500 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-3526:admin#create account operator 2
Command: create account operator 2

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

DES-3526:admin#
```

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-3500 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:

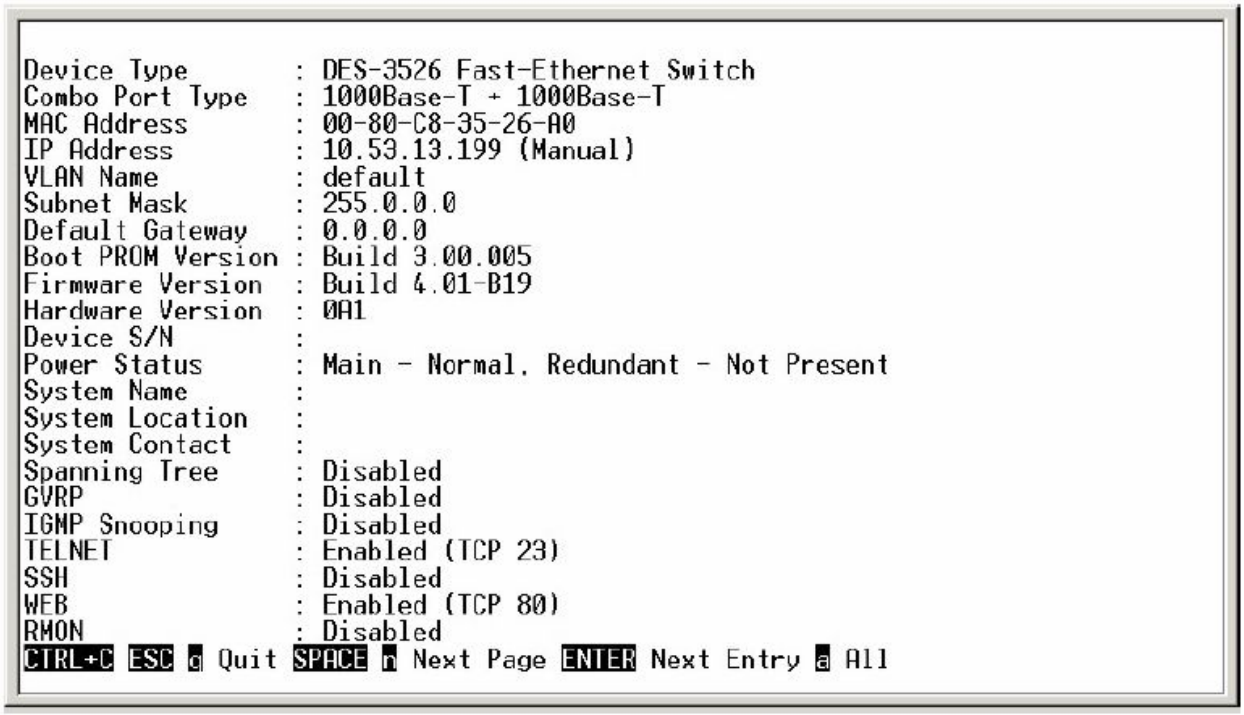


Рисунок 4.3 – Демонстрация команды

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

IP-адрес коммутатора должен быть установлен до 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.

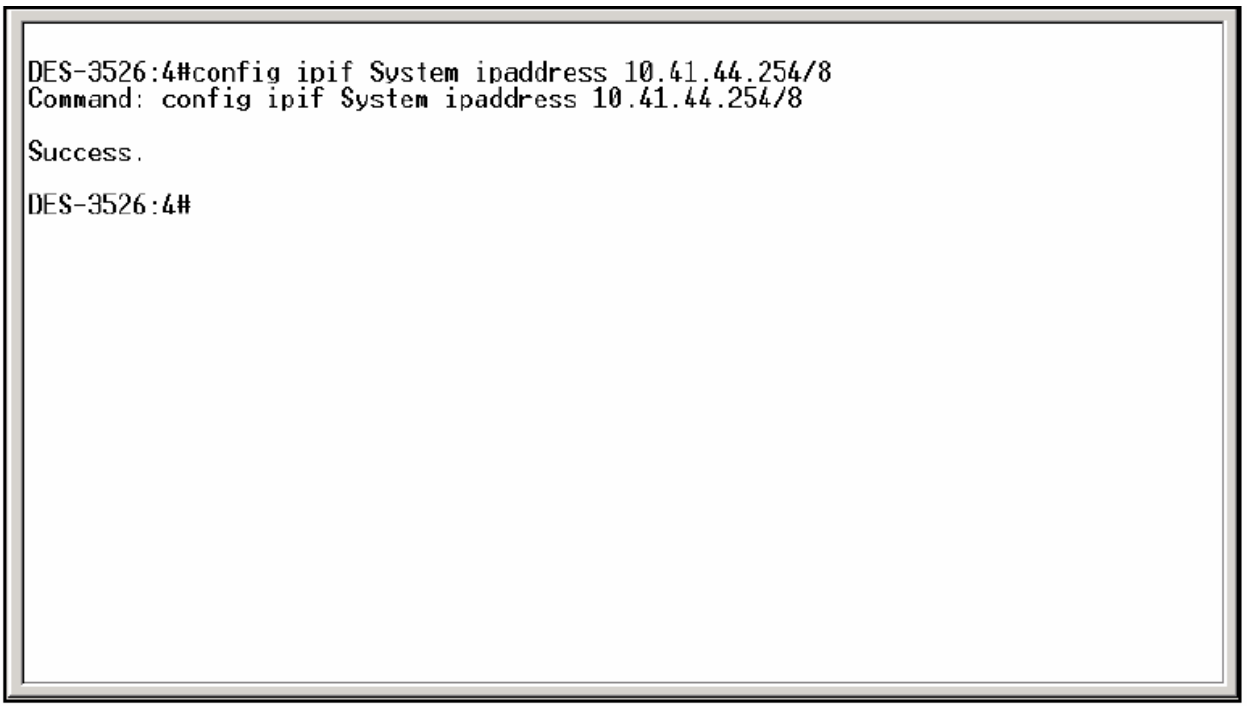


Рисунок 4.4 – Назначение IP-адреса коммутатору

В приведенном выше примере коммутатору назначен IP-адрес 10.41.44.254 с маской подсети 255.0.0.0. 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.

Подключение устройств к коммутатору

После назначения IP-адреса можно подключать устройства к коммутатору.
Для подключения устройства к порту для SFP-передатчика:

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

Предупреждение: При установке соединения через SFP-передатчик, соответствующий порт 10/100/1000Base-T будет заблокирован (речь идет о комбо-портах коммутатора 10/100/1000Base-T/SFP).

Раздел 5 - Настройка коммутатора через Web-интерфейс

Введение
Регистрация в Web-интерфейсе управления
Пользовательский Web-интерфейс
Поля пользовательского интерфейса

Введение

Все программные функции коммутатора серии DES-3500 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.

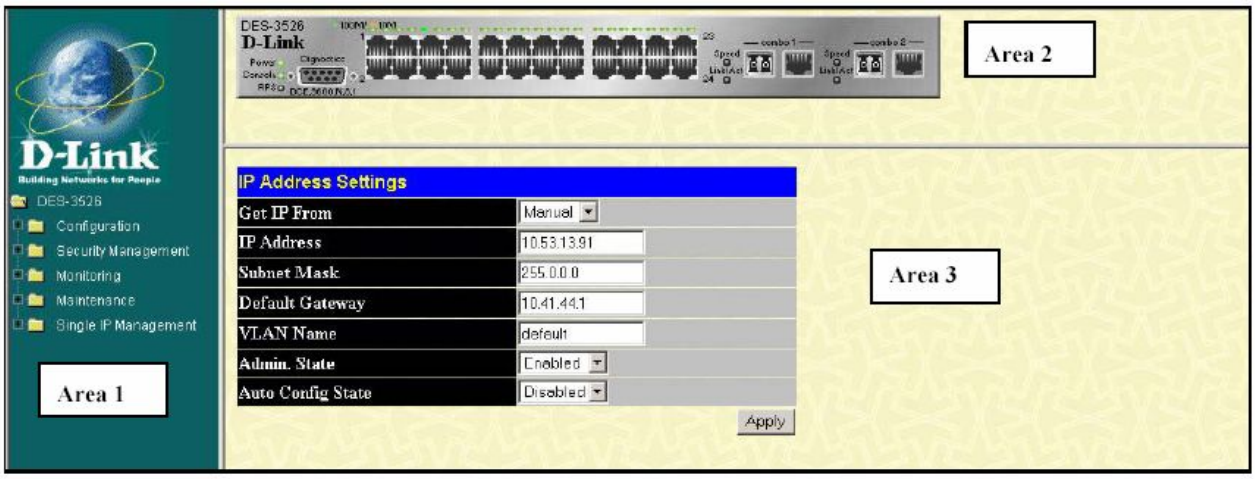


Рисунок 5.3 – Главная страница Web-менеджера

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:

Configurations (Настройки) – содержит опции, позволяющие настроить IP Address (IP-адрес), Switch Information (Информацию о коммутаторе), Advanced Settings (Расширенные настройки), Port Configuration (Настройки порта), IGMP, Spanning Tree, Forwarding Filtering, VLANs, Port Bandwidth (Полосу пропускания порта), SNTP Settings (Настройки SNTP), Port Security, QoS, MAC Notification, LACP, Access Profile Table (Таблица профилей доступа), System Log Servers (Серверы системного журнала), PAE Access Entity, Layer 3 IP Networking.

Security Management (управление безопасностью) – содержит опции, позволяющие настроить Security IP, User Accounts (Учетные записи пользователей), Access Authentication Control (TACACS), Secure Sockets Layer (SSL), Secure Shell (SSH) и SNMP V3.

Monitoring (Мониторинг) – содержит окна, касающиеся мониторинга коммутатора, относящиеся к Port Utilization (Использование порта), CPU Utilization (Использование CPU), Packets (Статистика по пакетам), Errors Size (Статистика по количеству ошибок), MAC Address (MAC-адрес), IGMP Snooping Group, IGMP Snooping Forwarding, VLAN Status (Статус VLAN), Router Port (Порт маршрутизатора), Port Access Control (Управление доступом на основе портов) и Layer 3 Feature (Функционал L3).

Maintenance (Обслуживание) – содержит опции, позволяющие настроить и просмотреть информацию по технической эксплуатации коммутатора, включая TFTP Services (Сервисы TFTP), Switch History (Архив коммутатора), Ping Test , Save Changes (Сохранение изменений), Reboot Services (Сервисы перезапуска коммутатора), Logout (Выход из системы).

Single IP Management (Управление через единый IP-адрес) – содержит опции, позволяющие задать настройки Single IP Management (Управление через единый IP-адрес), включая SIM Settings (Настройки SIM), Topology (Топология), Firmware/Configuration downloads (Загрузка программного обеспечения / конфигурационного файла).

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

Раздел 6 - Настройка Коммутатора

Информация о Коммутаторе
IP-адрес
Дополнительные настройки
Конфигурирование портов
Описание портов
Зеркалирование портов
Агрегирование каналов
Настройка портов LACP
MAC-оповещение (MAC Notification)
IGMP
Алгоритм покрывающего дерева
Forward Filtering
VLANs
Управление трафиком
Безопасность на основе портов (Port Security)
QoS
Серверы системного журнала (System Log Servers)
Настройки SNTP
Таблица профилей доступа (Access Profile Table)
Port Access Entity
Связка IP и MAC-адресов (IP-Mac Binding)
Ограничение диапазона IP Multicast

Информация о Коммутаторе

Ниже описано, как можно изменить некоторые из основных настроек коммутатора, такие как IP-адрес, имя пользователя, пароль для управления доступом к настройкам привилегий, а также как сохранить настройки и перегрузить Коммутатор. Кликните по **Switch Information** в меню **Configuration.**

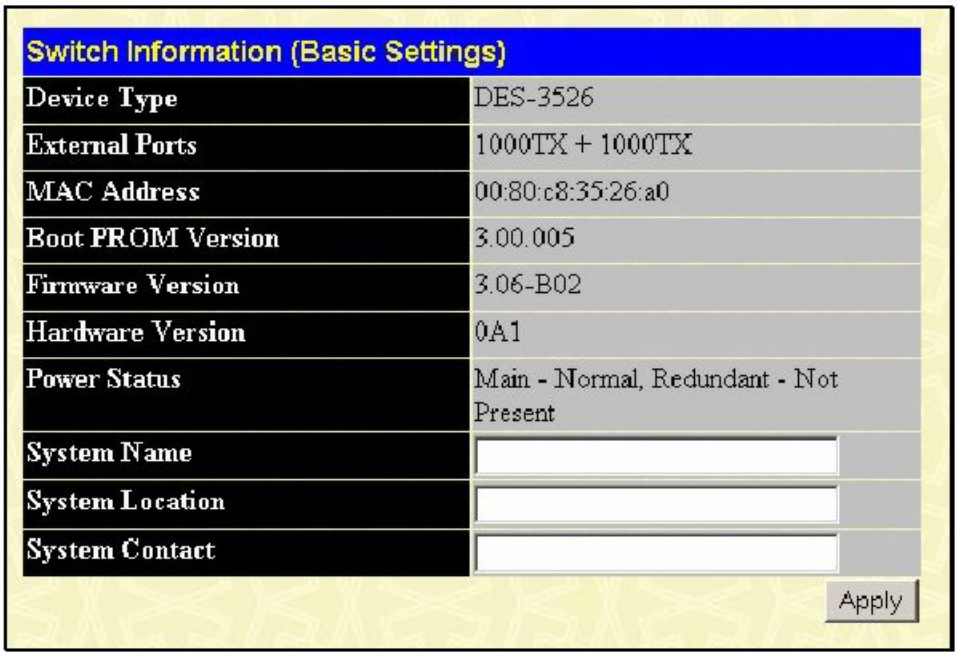


Рисунок 6-1. Окно Switch Information (Basic Settings)

Окно **Switch Information (Basic Settings)** содержит MAC-адрес коммутатора (прошивается на заводе и не изменяется), версию Boot PROM (загрузчик), версию Firmware (программного обеспечения), версию Hardware (аппаратного обеспечения). Эта информация полезна для обновления версии PROM и программного обеспечения, а также для получения информации о MAC-адресе Коммутатора, что может пригодиться для работы с другими опциями.

Пользователь также может для удобства ввести информацию о названии устройства (System Name), его месте расположения (System Location) и контактную информацию (System Contact).

IP-адрес

Первоначально до подключения коммутатора к Ethernet его IP-адрес может быть установлен с помощью интерфейса командной строки. Если IP-адрес ещё не изменён, следует обратиться к руководству по работе с командной строкой для DES-3526 или вернуться к изучению раздела 4 данного руководства.

Для изменения IP-адреса через Web-интерфейс, нужно зайти в меню **IP Address**, расположенное в папке **Configuration**.

Чтобы настроить IP-адрес Коммутатора:

Откройте папку **Configuration** и кликните по линку **IP Address**. В окне **IP Address Settings** отобразятся текущие IP-настройки Коммутатора, как это показано ниже.

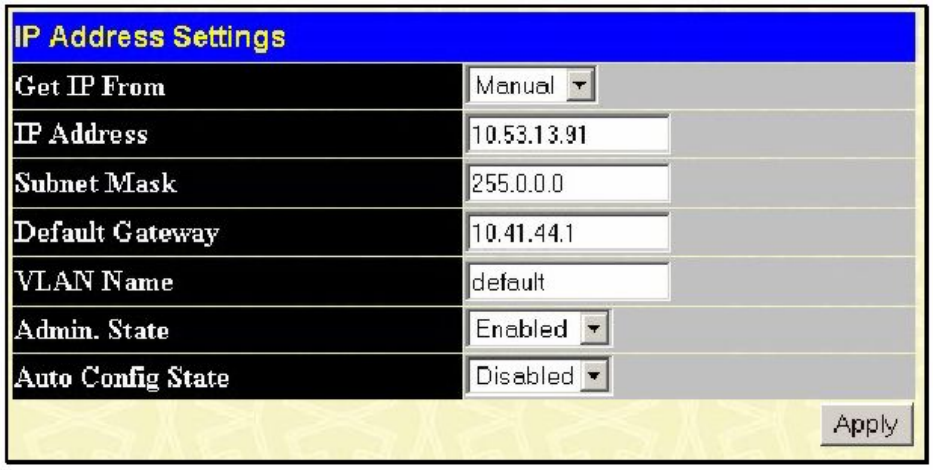


Рисунок 6-2. Окно IP Address Settings

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 шлюза по умолчанию. Если Коммутатор будет управляться через подсеть, в которой он находится, можно оставить адрес по умолчанию (0.0.0.0).
4. Если ни один VLAN пока не был сконфигурирован на Коммутаторе, можно использовать имя VLAN по умолчанию - *Default*. Если VLAN были предварительно установлены на Коммутаторе, необходимо установить ID VLAN (VID), который указывает на порт, соединённый с управляющей станцией, которая разрешает доступ к Коммутатору. Коммутатор позволит управлять доступом со станций с таким же VID, который указан здесь.

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

Чтобы задать настройки IP-адреса, маски подсети, адреса шлюза по умолчанию с помощью протоколов BOOTP или DHCP, в поле **Get IP From** следует выбрать соответственно *BOOTP* или *DHCP*. Так указывается, каким образом Коммутатор будет получать IP-адрес при следующей перезагрузке.

Примечание: Если выбрано *AutoConfig*, в поле **Get IP From** автоматически установится значение *DHCP*.

Настройки IP-адреса:

Параметр	Описание
BOOTP	При включении Коммутатор будет посылать широковещательный BOOTP-запрос. При этом IP-адрес, маска подсети, шлюз по умолчанию 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, шлюз по умолчанию 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 которого управляющей станции будет позволено управлять 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 протоколами 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 устройство сможет управляться 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.

Расширенные настройки

Окно **Switch Information (Advanced Settings)** содержит опции для настройки основных функций Коммутатора. Для работы с окном **Advanced Settings** кликните по соответствующей ссылке в папке **Configuration**.

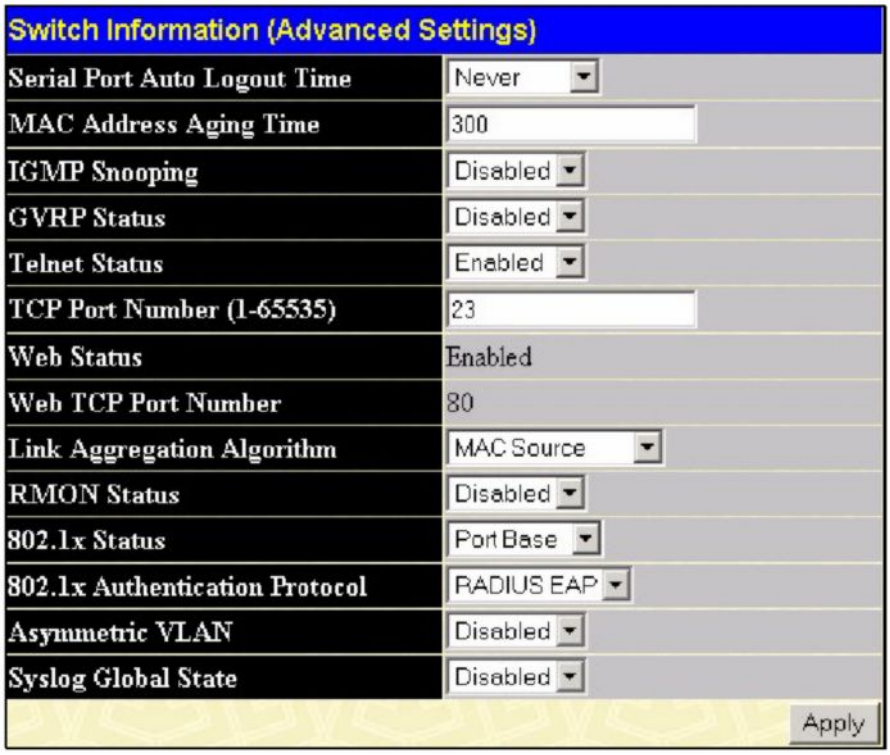


Рисунок 6-3. Окно Switch Information (Advanced Settings)

Параметр	Описание
Serial Port Auto Logout Time	Устанавливается время автоматического выхода из интерфейса консоли. Если в течение определённого промежутка времени пользователь не работал, он автоматически отключается. Можно выбрать значения: *2 Minutes, 5Minutes, 10 Minutes, 15 Minutes* или *Never*. Значение по умолчанию *10 minutes*.
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	Для того чтобы включить IGMP Snooping следует выбрать *Enable*. По умолчанию этот параметр отключён. IGMP Snooping применяется для того, чтобы рабочие станции, не запросившие групповой многоадресный трафик, не получали его. Конфигурация IGMP Snooping для отдельных VLAN производится в окне **IGMP Snooping** папки **IGMP**.
GVRP Status	Используется для выбора/отмены использования протокола GVRP на Коммутаторе.
Telnet Status	По умолчанию опция Telnet включена. Если требуется запретить настройку устройства через Telnet, следует выбрать значение *Disable*.
TCP Port Number (1-65535)	Номер TCP-порта. TCP-порты нумеруются от 1 до 65535. TCP- порт протокола Telnet - 23.
Web Status	Управление через Web-интерфейс по умолчанию включено (*Enable)*. Выключение данной опции приведет к потере возможности настройки Коммутатора через Web-интерфейс.
Web TCP Port Number	Номер TCP-порта, закрепленный за Web-интерфейсом управления Коммутатора (порт 80).
Link Aggregation Algorithm	Алгоритм, который Коммутатор использует для уравновешивания загрузки портов, входящих в группу агрегированных каналов связи. Можно выбрать *MAC Source, MAC Destination, MACSrc & Dest, IP Source, IP Destination* или

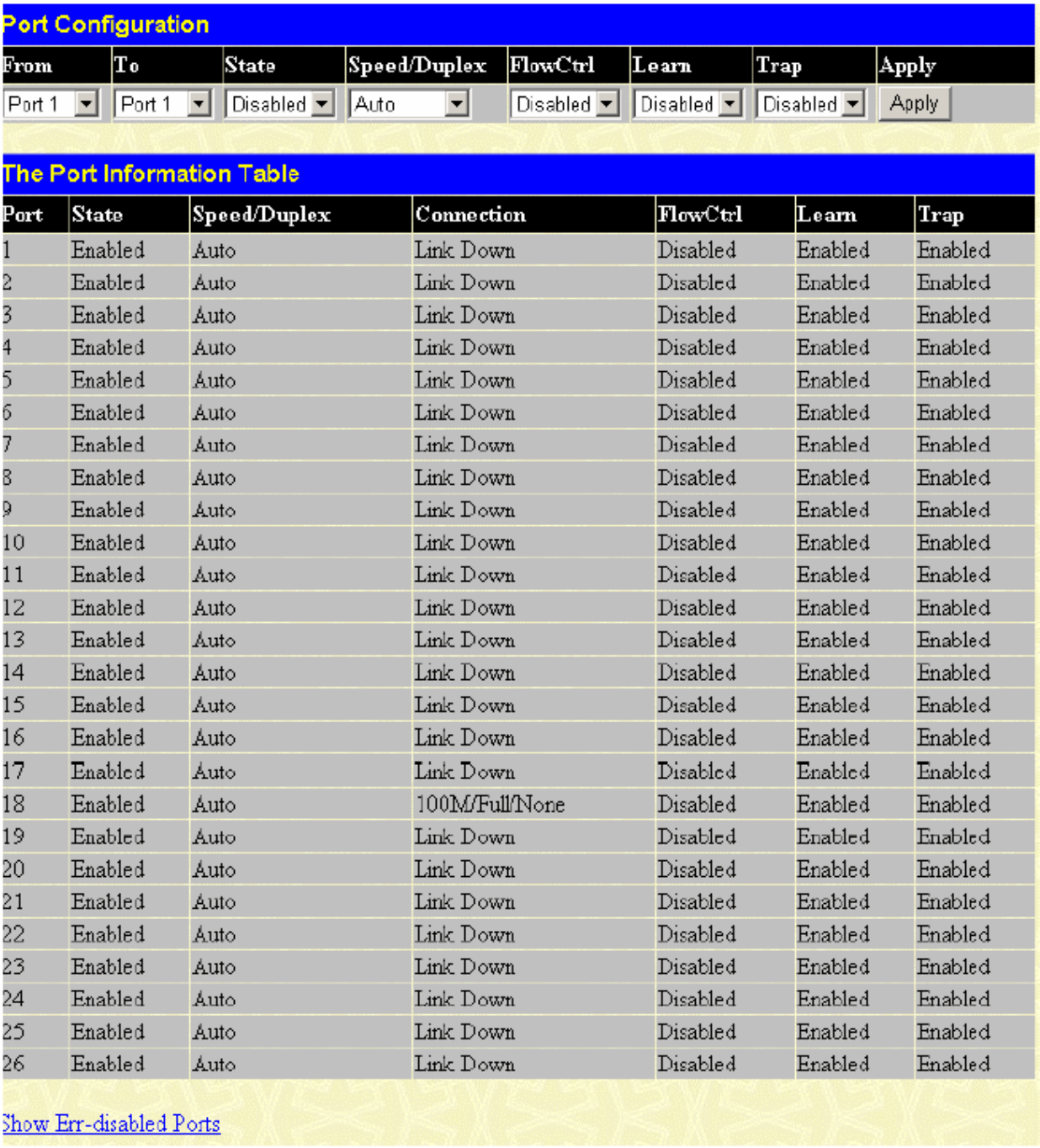
	IP Src & Dest. (Подробно значение данных параметров описано в главе «Агрегирование каналов» данного руководства.)
RMON Status	Эта опция позволяет включить/отключить удалённый мониторинг Коммутатора.
802.1x Status	Здесь возможно настроить опцию 802.1x Коммутатора на основе портов и MAC-адресов (По умолчанию она выключена: значение *Disable)*. Подробно эта тема рассмотрена в главе Port Access Entity. Аутентификация 802.1x на основе портов определяет инициализацию только на основе номера порта, а только затем переходит к другим параметрам аутентификации. Аутентификация 802.1x на основе MAC-адресов определяет инициализацию на основе MAC-адреса и номера порта, а только затем переходит к другим параметрам аутентификации.
802.1x Authentication Protocol	Меню позволяет выбрать значения между *radius eap* и *radius pap* для 802.1x протокола Коммутатора. Значение по умолчанию *radius eap*.
Asymmetric VLAN	Здесь включаются/отключаются ассиметричные VLAN на Коммутаторе. Значение по умолчанию *Disabled*.
Syslog Global State	Включает/отключает Syslog State (системный журнал). По умолчанию *Disabled*.

Для применения настроек кликните **Apply**.

Примечание: Когда ассиметричные VLAN не выбраны, пользователь должен изменить на Коммутаторе настройки VLAN на установленные по умолчанию.

Настройка портов

Эта глава содержит информацию по индивидуальной настройке различных атрибутов и свойств для физических портов. Кликните по **Port Configurations** меню, в результате появится следующее окно:



Port Configuration

From	To	State	Speed/Duplex	FlowCtrl	Learn	Trap	Apply
Port 1	Port 1	Disabled	Auto	Disabled	Disabled	Disabled	Apply

The Port Information Table

Port	State	Speed/Duplex	Connection	FlowCtrl	Learn	Trap
1	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
2	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
3	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
4	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
5	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
6	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
7	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
8	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
9	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
10	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
11	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
12	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
13	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
14	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
15	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
16	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
17	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
18	Enabled	Auto	100M/Full/None	Disabled	Enabled	Enabled
19	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
20	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
21	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
22	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
23	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
24	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
25	Enabled	Auto	Link Down	Disabled	Enabled	Enabled
26	Enabled	Auto	Link Down	Disabled	Enabled	Enabled

Show Err-disabled Ports

Рисунок 6-4. Окно Port Configuration

Для настройки портов Коммутатора необходимо:

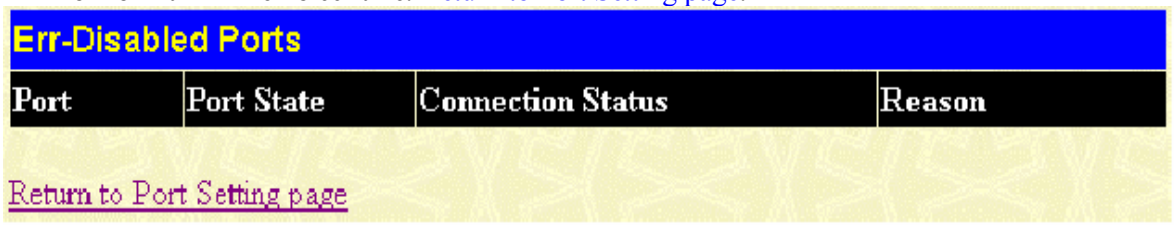
1. Выбрать порт или диапазон портов, используя выпадающие меню **From…To…**.
2. Другие выпадающие меню используются для конфигурирования следующих параметров:

Параметр	Описание
State	Поле используется для включения/выключения портов или группы портов.
Speed/Duplex	Поле используется для установки дуплексного/полудуплексного режима порта. *Auto* означает автоматическое согласование скорости устройствами между 10 и 100 Мбит/с в дуплексном или полудуплексном режиме. *Auto* позволяет порту автоматически устанавливать оптимальные настройки соединения. Значения могут быть: *Auto, 10M/Half, 10M/Full, 100M/Half* и *100M/Full*. Автоматическая установка настроек возможна только при значении *Auto*.

Flow Control	Показывает схему управления потоком, используемую для различных конфигураций порта. Порты, настроенные для работы в дуплексном режиме, используют управление потоком 802.3x. Порты, настроенные для работы в полудуплексном режиме, используют управление потоком с помощью метода «обратного давления». Порты с настройкой Auto автоматически выбирают нужную схему управления потоком. По умолчанию, задано значение *Disabled*.
Learn	Можно включить/отключить изучение MAC-адресов на выбранном порте. Значение *Enable* означает, что MAC-адрес источника автоматически попадет в таблицу MAC-адресов. Когда в данном поле выбрано значение *Disabled*, необходимо вводить MAC-адреса в таблицу MAC-адресов вручную. Иногда это делается с целью обеспечения безопасности. Информация о занесении MAC-адресов в таблицу представлена в главе Forwarding/Filtering. Значение по умолчанию *Disabled*.
Trap	Это поле позволяет включить/выключить отправку trap-сообщений на Коммутаторе.

Для применения настроек кликните **Apply**.

Для получения детальной информации о выключенных портах кликните по ссылке Show Err-disabled Ports в показанном выше окне **Port Configuration**. Окно **Err-Disabled Ports** содержит список отключенных портов, их статус и причину выключения порта. Для завершения работы с данным окном кликните по ссылке: Return to Port Setting page.



Описание портов

DES-3526 позволяет пользователю задать описание портов Коммутатора. Чтобы назначить определенному порту соответствующее описание, следует кликнуть по **Port Description** в меню **Configuration**:

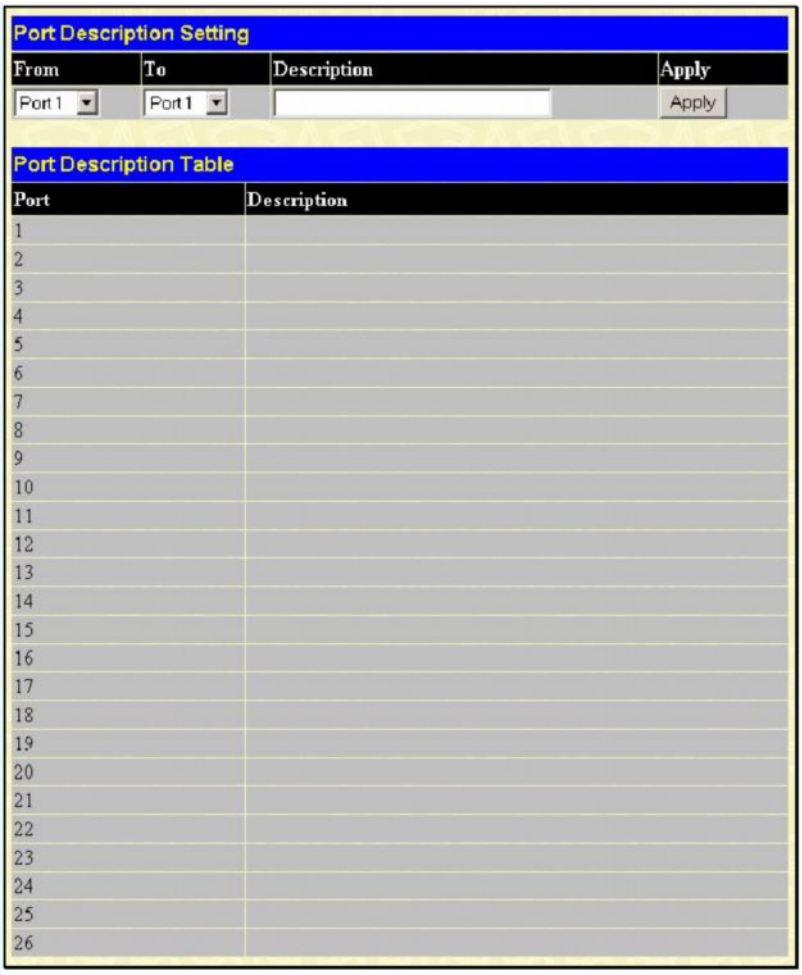


Рисунок 6-5. Окно «Port Description Setting»

Для выбора порта или группы портов используются выпадающие меню **From** и **To**, затем можно ввести описание выбранных портов. Кликните **Apply** для применения настроек в окне **Port Description Table**.

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.

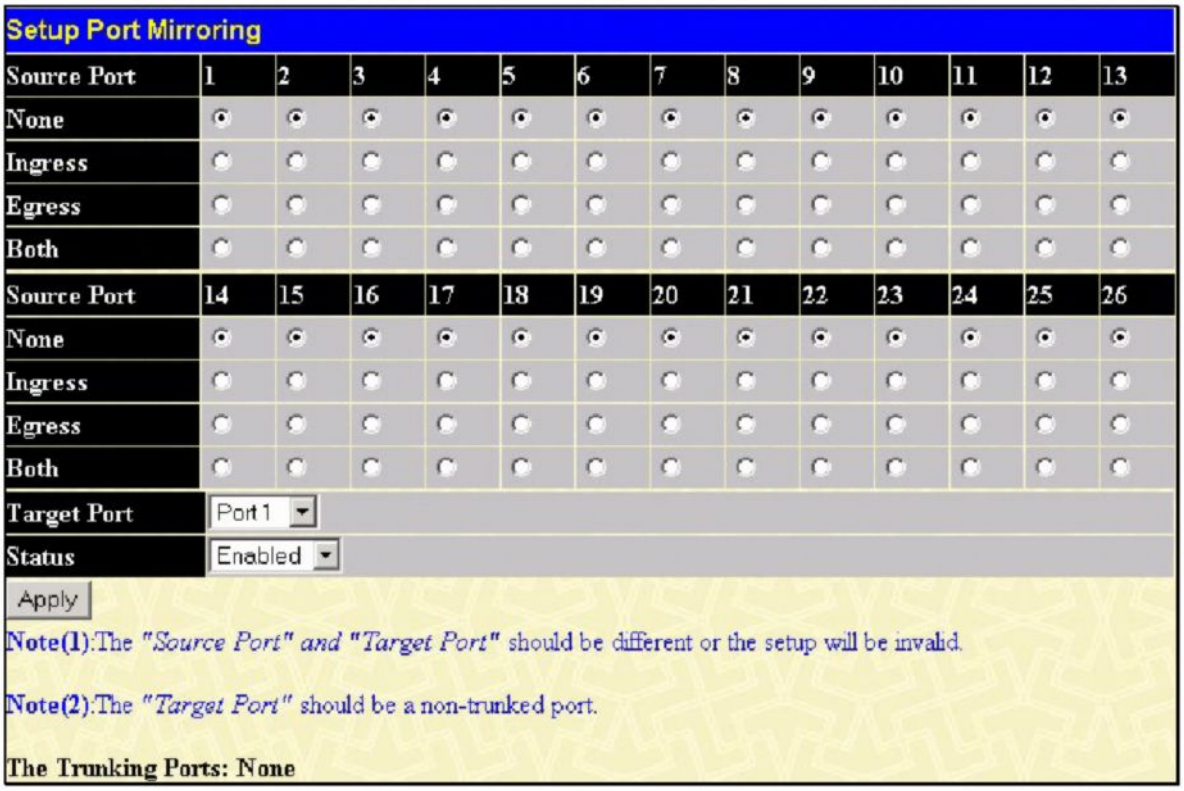


Рисунок 6-6. окно «Setup Port Mirroring»

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 100Мбит – порт на 10Мбит – порт, 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.

Агрегирование каналов

Понятие группы агрегированных каналов

Группа агрегированных каналов связи (Port trunk groups) используется для объединения портов в одну высокоскоростную магистраль. DES-3526 поддерживает до шести групп агрегированных каналов связи с количеством портов от 2 до 8 на группу. Таким образом, может быть достигнута потенциальная скорость передачи 8000Мбит/с

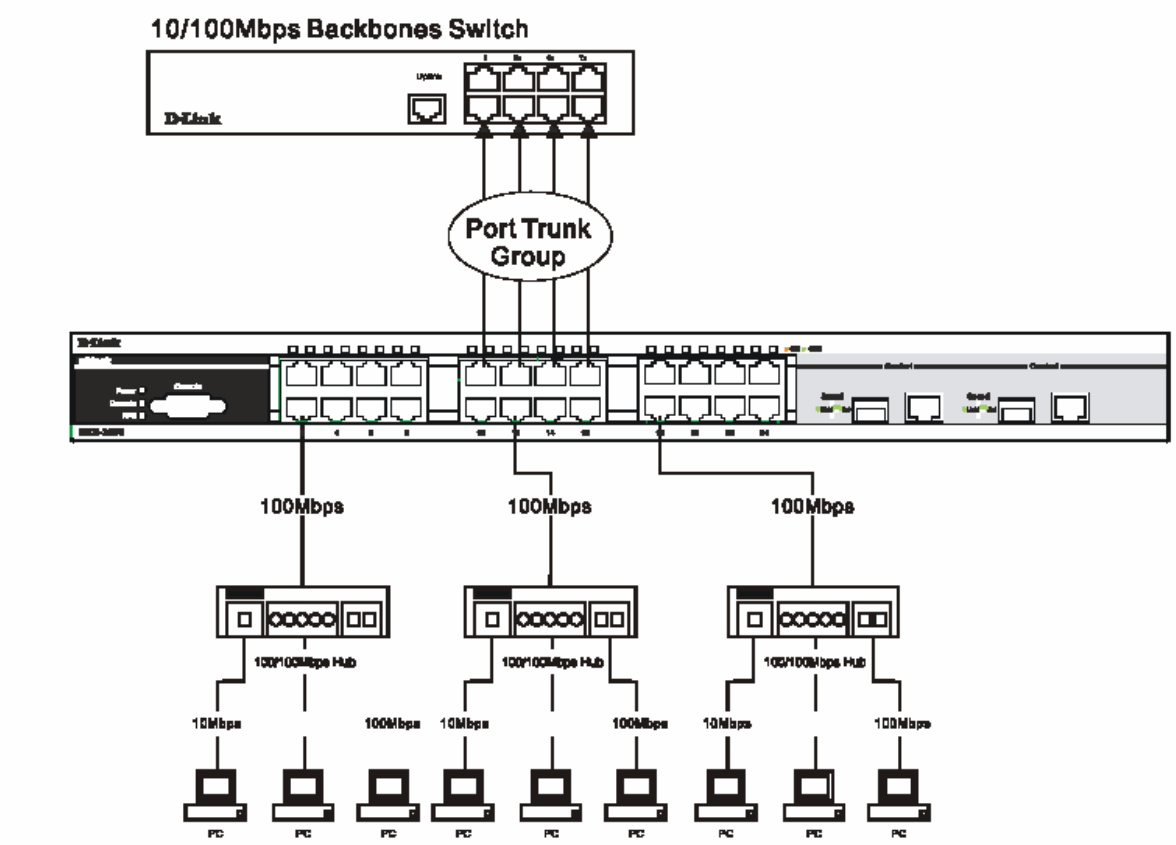


Рисунок 6-7. Пример группы агрегированных каналов связи

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.

Предупреждение: 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 групы.
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.

Для настройки агрегирования портов кликните по **Link Aggregation** в папке **Configuration**, в результате откроется следующее окно:

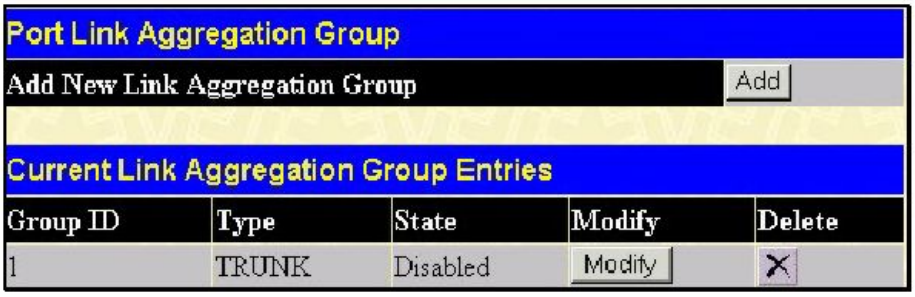


Рисунок 6-8. Окно Port Link Aggregation Group

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.

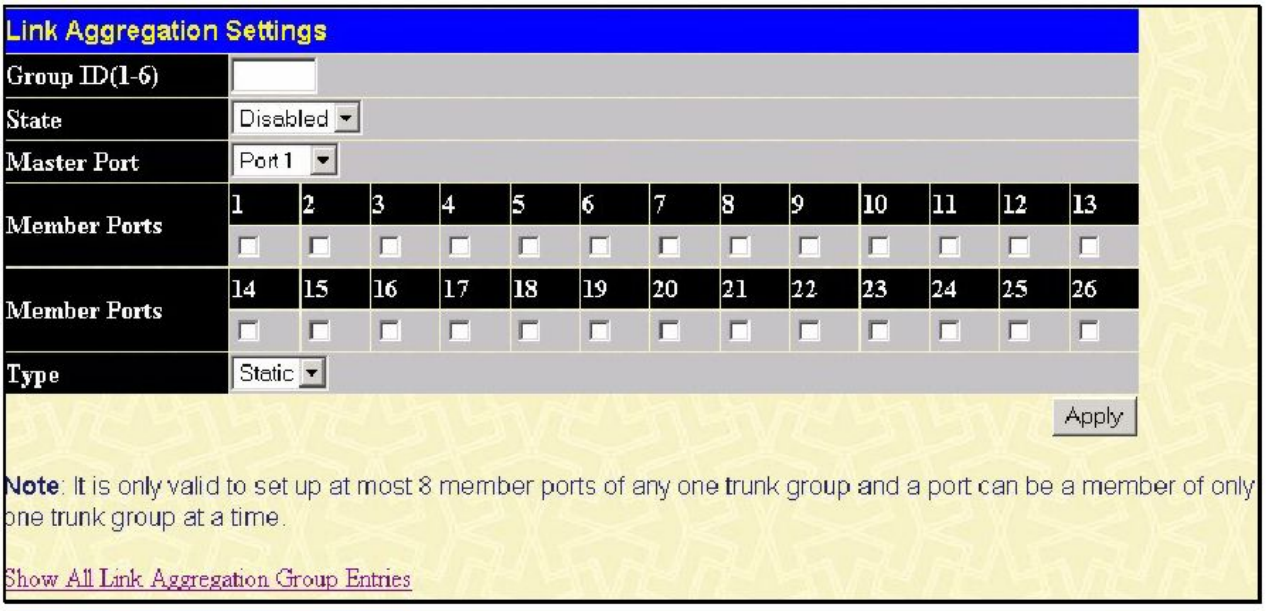


Рисунок 6-9. Окно Link Aggregation Settings - добавление

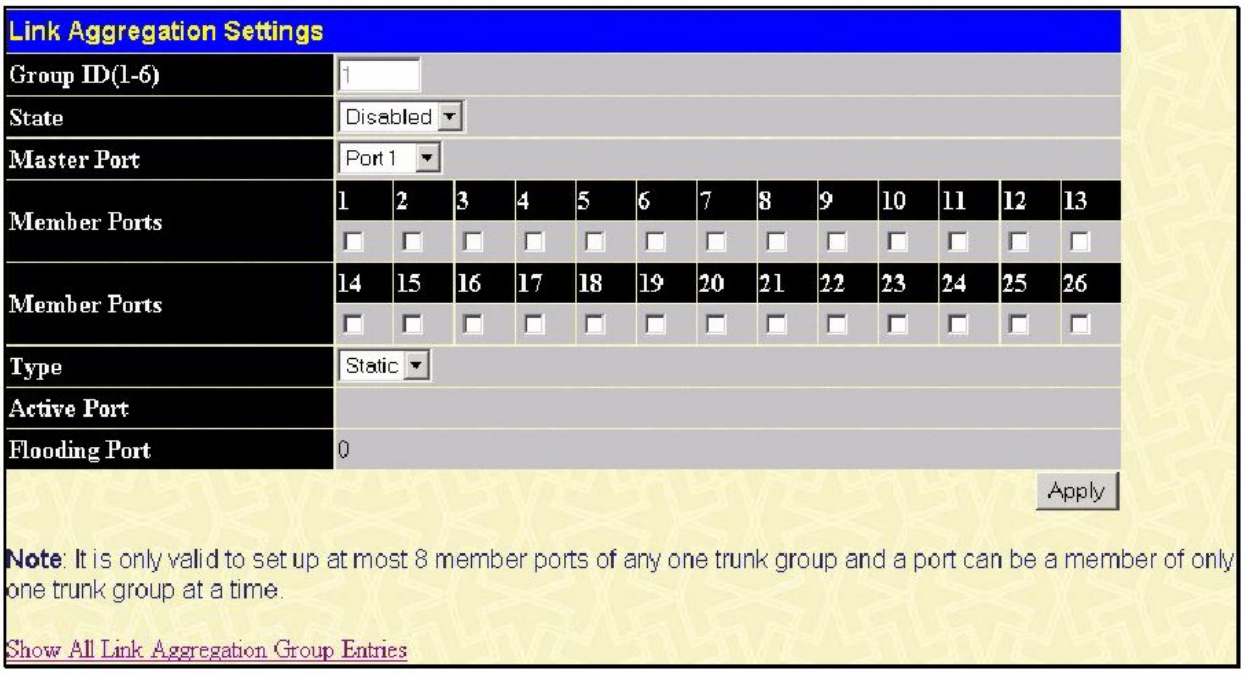


Рисунок 6-10. Окно Link Aggregation Settings - редактирование

Значения параметров, изменяемых пользователем:

Параметр	Описание
Group ID	Выбирается ID группы от 1 до 6
State	Группы агрегированных каналов связи могут быть включены (Enabled) или выкючены (Disabled). Используется при диагностике, для быстрого отключения устройств с интенсивной полосой пропускания или для создания резервной копии группы, которая не находится под автоматическим контролем.
Master Port	Используя выпадающее меню, установите главный порт группы,.
Member Ports	Позволяет выбрать членов группы агрегированных каналов. В группу может входить до восьми портов.
Flooding Port	В группе агрегированных каналов связи необходимо выделить один порт для широковещательной рассылки и нераспознанных адресаций.
Active Port	Отображается порт, который в настоящее время пересылает данные.
Type	В этом поле можно выбрать *Static* или *LACP* (Link Aggregation Control Protocol). Использование протокола *LACP* позволяет организовать автоматическое распределение связей в группе агрегированных каналов связи.

После установки параметров следует кликнуть Apply, чтобы настройки вступили в силу. Успешно созданная группа будет отображаться в таблице **Current Link Aggregation Group Entries**, показанной на рисунке 6-8.

Настройки портов LACP

Окно **LACP Port Setting** используется в сочетании с окном **Link Aggregation** для создания на Коммутаторе группы агрегированных каналов связи. Используя следующее окно, пользователь может установить, какие порты будут активными или пассивными при обработке и посылке контрольных LACP-фреймов.

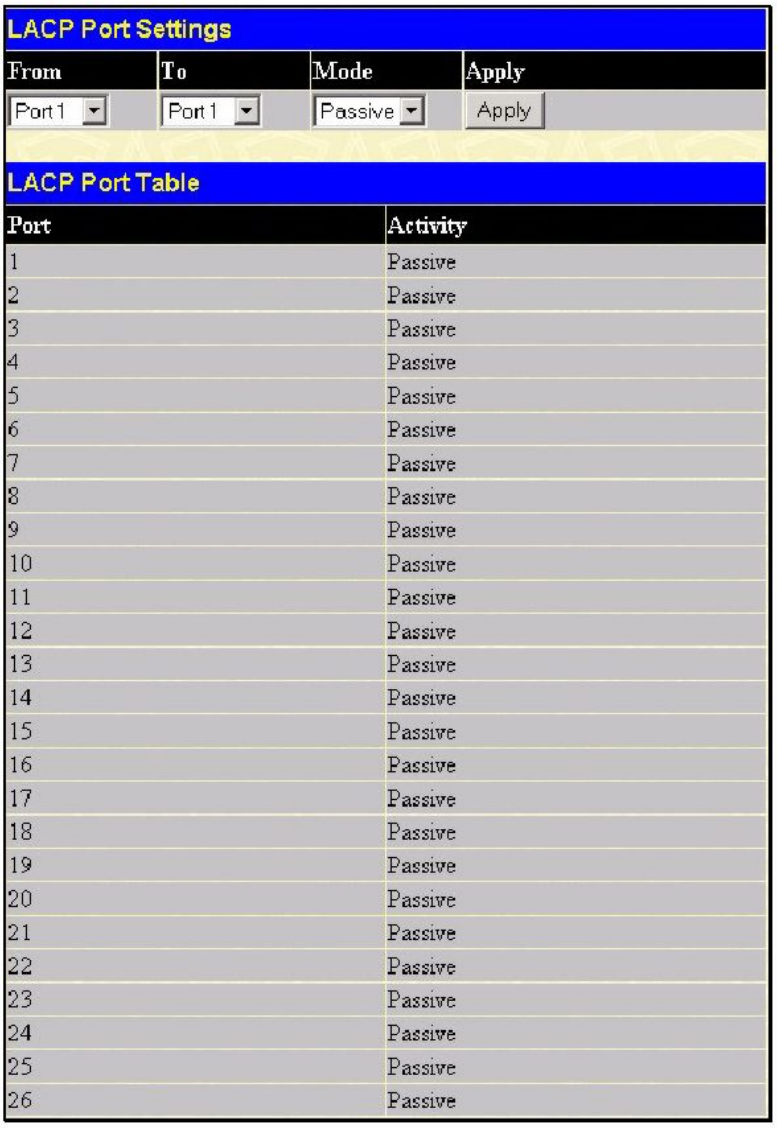


Рисунок 6- 11. Окно LACP Port Settings

Пользователь может установить следующие параметры:

Параметр	Описание
From/To	Необходимо задать диапазон портов.
Mode	Данное поле позволяет настроить режим работы LACP-порта *Active* – активные LACP-порты, которые способны обрабатывать и посылать контрольные LACP-фреймы. Это позволяет соответствующим LACP-устройствам осуществлять согласование и при необходимости динамически изменять группу агрегированных каналов. Для того чтобы использовать возможность вносить изменения в группу портов – добавлять или удалять порты из группы, по крайней мере, на одном из устройств должен быть установлен активный LACP–порт. При этом оба устройства должны поддерживать протокол LACP. *Passive* - Пассивные LACP-порты не могут посылать контрольные LACP-фреймы. Для того чтобы использовать возможность вносить изменения в группу портов – добавлять или удалять порты из группы, по крайней мере, на одном из устройств должен быть установлен активный LACP–порт (см. выше).

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

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** и кликнуть по линку **MAC Notification Global Settings.**

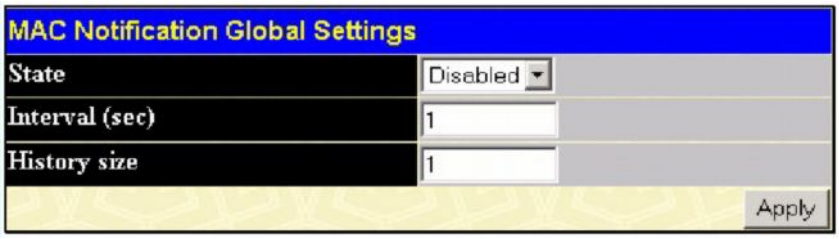


Рисунок 6- 12. Окно MAC Notification Global Settings

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, надо кликнуть по **Port Settings** в папке **MAC Notification**. После чего откроется следующее окно:

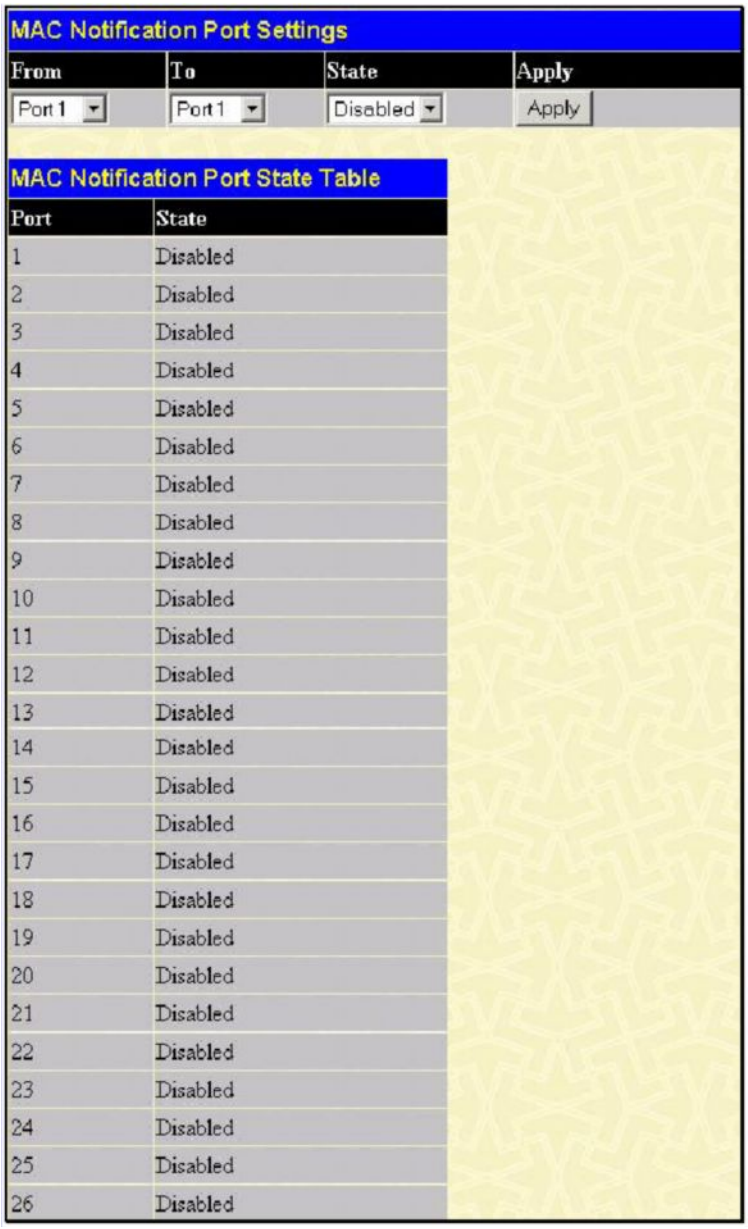


Рисунок 6- 13. Окно MAC Notification Port Settings

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.

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 широковещательной рассылки на основе IGMP-сообщений, проходящих через коммутатор. Коммутатор отслеживает IGMP – сообщения и прекращает посылать широковещательные пакеты, когда больше нет хостов, запрашивающих продолжение рассылки.

IGMP Snooping

Окно **Current IGMP Snooping Group Entries** используется для просмотра настроек **IGMP Snooping**. Для изменения настроек надо кликнуть по кнопке **Modify,** соответствующей определенному VLAN ID.

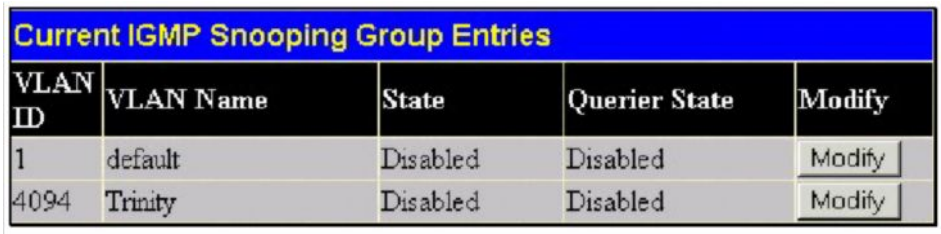


Рисунок 6- 14. Окно Current IGMP Snooping Group Entries

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

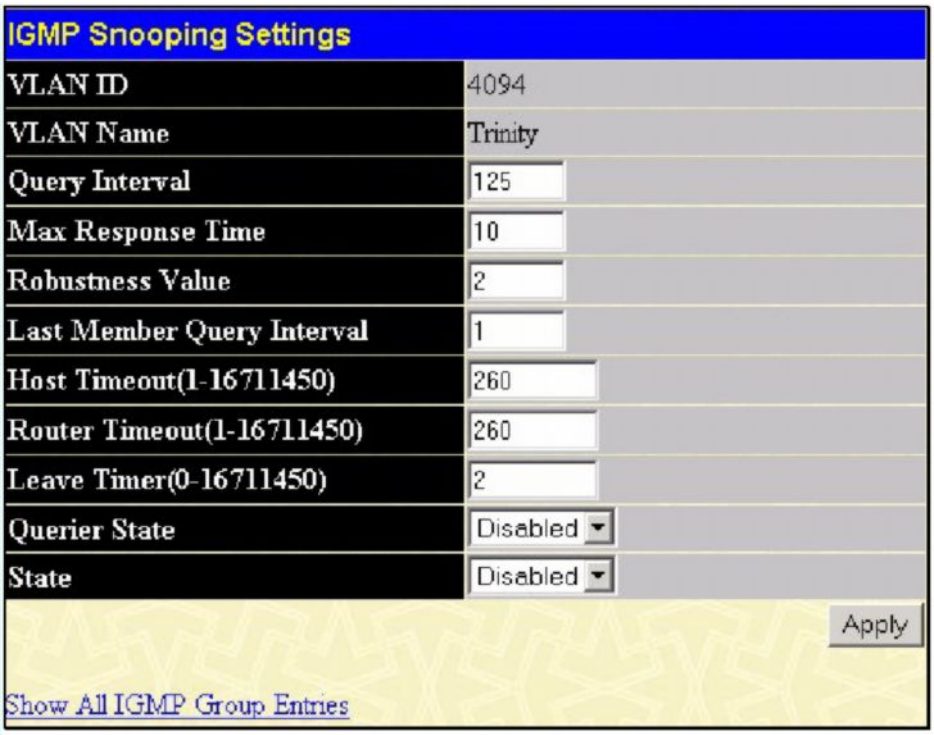


Рисунок 6- 15. Окно IGMP Snooping Settings

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*.
Route Timeout	Максимальное время хранения маршрута в таблице адресов (в секундах). Значение по умолчанию 260.
Leave Timer	Это максимальный временной интервал в секундах между получением коммутатором сообщения Leave от клиента и исключением клиента из группы.
Querier State	Значение *Enabled* – для включения IGMP-запросов, *Disabled* – для отключения. Значение по умолчанию – *Disabled*.
State	Значение *Enabled* – для применения IGMP snopping. Значение по умолчанию – *Disabled.*

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

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.

Для открытия окна **Current Static Router Ports Entries** (показано ниже) следует открыть папку **IGMP**, кликнуть по линку **Static Router Ports Entry.**

Рисунок 6- 16. Окно Current Static Router Ports 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:

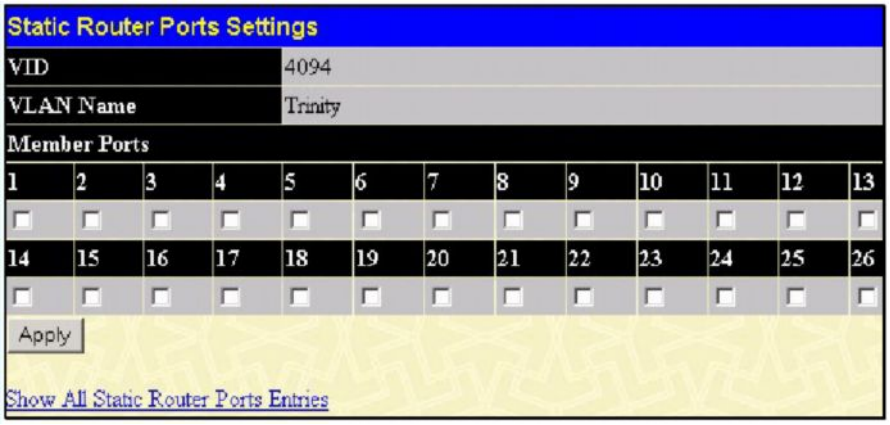


Рисунок 6- 17. Окно Static Router Ports Settings

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**, надо кликнуть по линку Show All Static Router Port Entries.

Запрещенные порты для подключения маршрутизатора

Окно **Forbidden Router Ports Entry** позволяет пользователям задать порт или группу портов, которые принадлежат определенной VLAN и которым запрещено получать информацию или быть подключенными к многоадресным маршрутизаторам. Для работы со следующим окном кликните **Configuration > IGMP > Forbidden Router Ports Entry**.

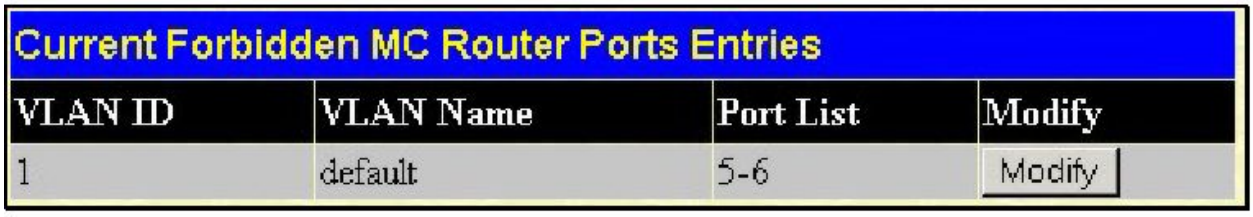


Рисунок 6- 18. Окно Current Forbidden MC Router Ports Entries

Для изменения настроек запрещенных портов для подключения маршрутизатора в определенной VLAN кликните по соответствующей кнопке **Modify**, что приведет к отображению следующего окна.

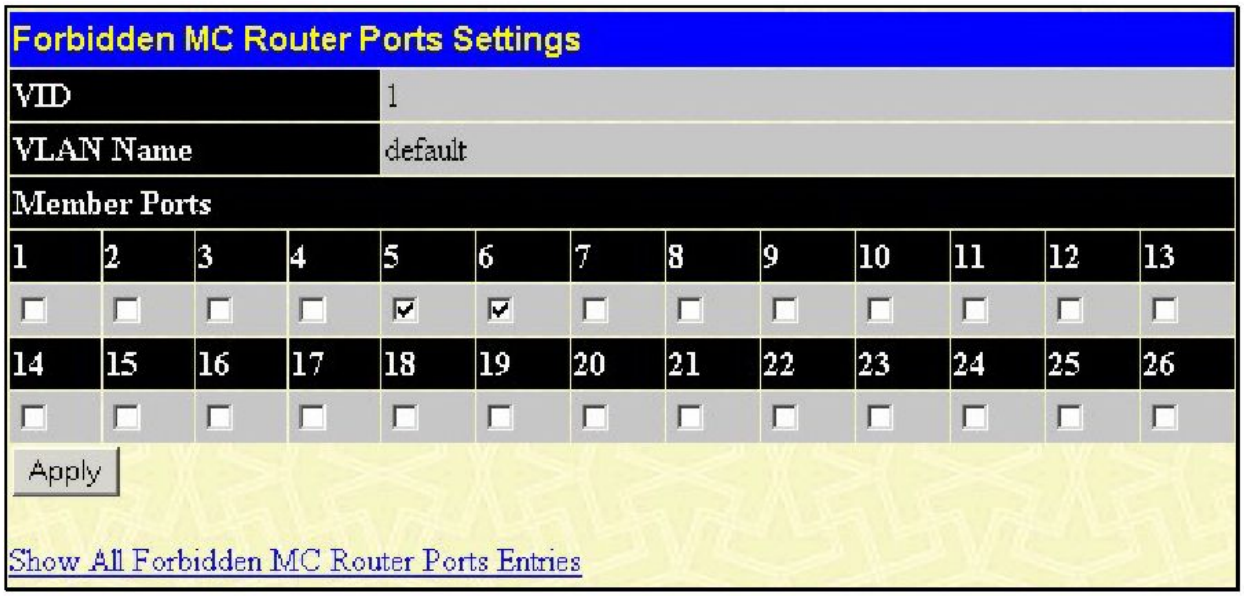


Рисунок 6- 19. Окно Forbidden MC Router Ports Settings

Чтобы добавить определенные порты в список запрещенных портов для подключения маршрутизатора, поставьте галочки в соответствующих полях, а затем кликните по **Apply**. Установленные надлежащим образом запрещенные порты для подключения маршрутизатора отобразятся в окне **Current Forbidden MC Router Ports Entries** под заголовком **Port List**.

Многоадресная VLAN IGMP

Использование функции IGMP snooping позволяет ограничить многоадресный трафик таким образом, что многоадресную рассылку получают только те интерфейсы, которые на нее подписаны. Коммутатор 2-го уровня отслеживает трафик IGMP-пакетов между многоадресным маршрутизатором и хостами для того, чтобы изучить и занести в таблицу многоадресные группы и относящиеся к ним порты. Таблица многоадресной рассылки ведется для каждой многоадресной группы. Она содержит записи, которые включают многоадресные группы и относящиеся к ним порты. Хост посылает запрос на вступление в группу (IGMP Join Group) и запрос на выход из группы многоадресной рассылки (Leave Group). Также коммутатор периодически посылает запросы многоадресному маршрутизатору с целью обновления информации в таблице многоадресных групп.

IGMP snooping находит широкое применение в сетях предприятий и сетях кампуса, обеспечивая необходимую полосу пропускания коммутации. Однако, использование IGMP snooping в сетях провайдеров для предоставления пользователям сервисов многоадресной рассылки, при которых каждый пользователь находится в своей VLAN, является проблематичным из-за особенностей взаимодействия коммутатора с поддержкой IGMP-snooping и многоадресного маршрутизатора. Ведь в этом случае возникает проблема передачи многоадресного трафика пользователям, находящимся в различных VLAN.

В DES-3526 эта проблема решается путем возможности создать для многоадресной рассылки область сети (многоадресную VLAN), совместно используемую различными VLAN. В результате каждый порт находится в своей VLAN, а для специально для многоадресной рассылки будет использоваться специальная VLAN, в которую входят все порты. Каждый пользователь может подписаться на многоадресную рассылку (Join Group) или оставить группу многоадресной рассылки (Leave Group). Пользователи, которые не подписаны на многоадресную рассылку, не будут ее получать.

Другими словами, коммутатор использует специальную многоадресную VLAN, таблица MAC-адресов которой представляет таблицу многоадресной рассылки. Изменение таблицы MAC-адресов производится на основании получения от хостов запроса на вступление в группу (IGMP Join Group) или запроса на выход из группы многоадресной рассылки (Leave Group).

Для создания многоадресной VLAN на Коммутаторе необходимо кликнуть **Configuration > IGMP > IGMP Multicast VLAN.** В результате откроется следующее окно:

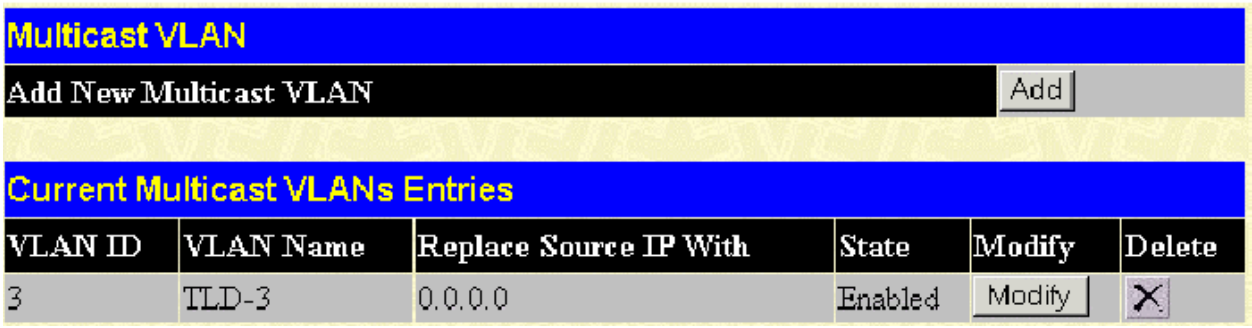


Рисунок 6- 20. Окно Multicast VLAN и таблица Current Multicast VLANs Entries

Для создания новой многоадресной VLAN следует кликнуть по кнопке **Add** в окне, представленном выше.

Рисунок 6- 21. Окно Multicast VLAN (добавить)

Можно установить следующие параметры:

Параметр	Описание
VID	ID (идентификатор) созданного VLAN. Пользователь может выбрать номер от 1 до 4094. Можно сконфигурировать до 3-х многоадресных VLAN.
VLAN Name	Имя созданной многоадресной VLAN. Имя многоадресной VLAN может быть длиной до 32 символов. Можно сконфигурировать до 3-х многоадресных VLAN.
Replace Source IP With	Введите IP-адрес, который нужно указывать в качестве IP-адреса источника.
State	Данное поле позволяет включить или выключить многоадресную VLAN, используя выпадающее меню.
Source Port	В этом поле задается порт коммутатора, назначенный портом-источником для многоадресного трафика. Многоадресный трафик будет приходить на этот порт, а затем пересылаться на порты данной VLAN. Стоит отметить, что порт-источник не должен входить в члены создаваемой многоадресной

	VLAN, указываемые в седующем поле.
Member Port	Порт или ряд портов для добавления в многоадресную VLAN. На эти порты будет передаваться многоадресный трафик с порта-источника. Необходимо помнить, что порт-источник не может совпадать с этими портами.

Кликните **Apply** для создания многоадресной VLAN.
Для того чтобы изменить настройки уже существующей многоадресной VLAN, необходимо кликнуть по кнопке **Modify** в окне **Current Multicast VLANs Entries Table**, после чего откроется следующее окно:

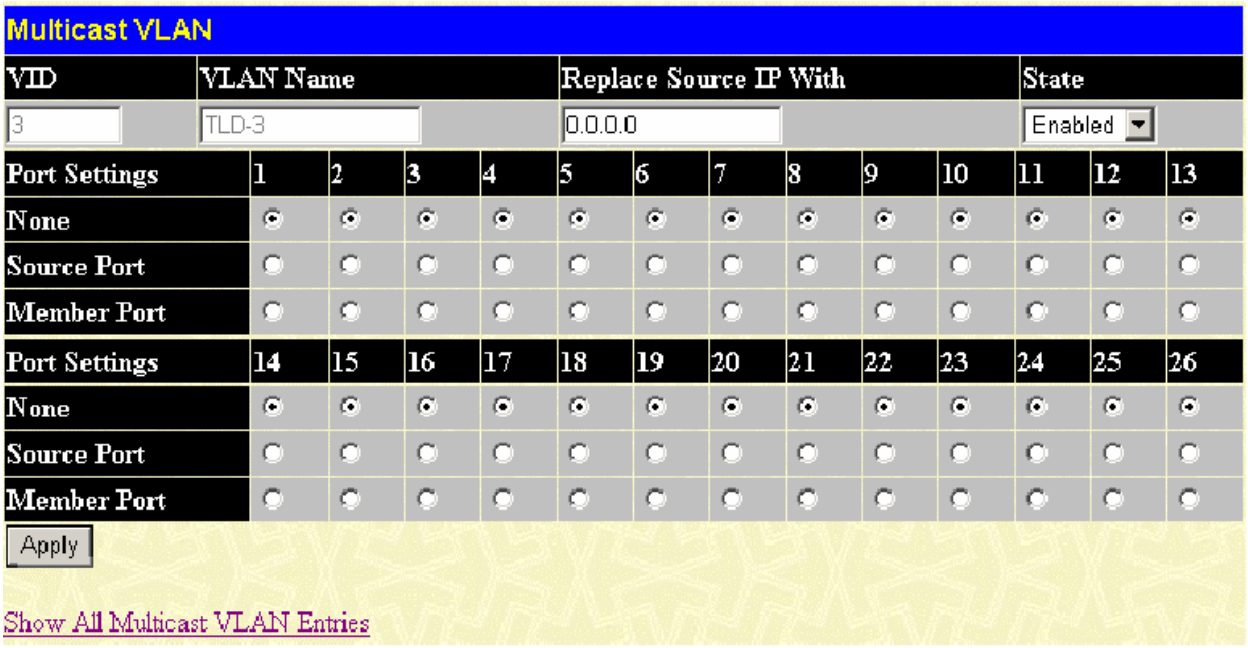


Рисунок 6- 22. Окно Multicast VLAN

Можно изменить следующие параметры:

Параметр	Описание
VID	ID (идентификатор) созданного VLAN. Пользователь может выбрать номер от 1 до 4094. Можно сконфигурировать до 3-х многоадресных VLAN.
VLAN Name	Имя созданной многоадресной VLAN. Имя многоадресной VLAN может быть длиной до 32 символов. Можно сконфигурировать до 3-х многоадресных VLAN.
Replace Source IP With	Введите IP-адрес, который нужно указывать в качестве IP-адреса источника.
State	Здесь можно включить или отключить VLAN, используя выпадающее меню.
Source Port	В этом поле задается порт коммутатора, назначенный портом-источником для многоадресного трафика. Многоадресный трафик будет приходить на этот порт, а затем пересылаться на порты данной VLAN. Стоит отметить, что порт-источник не должен входить в члены создаваемой многоадресной VLAN, указываемые в седующем поле.
Member Port	Порт или ряд портов для добавления в многоадресную VLAN. На эти порты будет передаваться многоадресный трафик с порта-источника. Необходимо помнить, что порт-источник не может совпадать с этими портами.

Затем необходимо кликнуть **Apply** для принятия изменений.

Примечание: Если на коммутаторе настроена и включена многоадресная VLAN, то последующие настройки IGMP Snooping не будут приняты во внимание, т.к. многоадресная VLAN IGMP Snooping обладает приоритетом.

Алгоритм покрывающего дерева

Коммутатор поддерживает три версии протокола покрывающего дерева (Spanning Tree): 802.1d STP, 802.1w Rapid STP и 802.1s MSTP. Протокол 802.1s, в отличие от 802.1d STP и 802.1w Rapid STP MSTP, появился относительно 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.

802.1s MSTP

Multiple Spanning Tree Protocol (MSTP) – стандарт, принятый IEEE, который позволяет объединить несколько VLAN в единое покрывающее дерево, обеспечивая множественные связи внутри сети. Использование MSTP позволяет распределить нагрузку в сети, а также обеспечивает резервирование маршрутов при выходе из строя одного из маршрутов, обеспечивая высокую степень сходимости. Фреймы, циркулирующие по таким VLAN, быстро обрабатываются и передаются с помощью одного из протоколов (STP, RSTP или MSTP).

Протокол покрывающего дерева также добавляет в BDPU-пакеты теги с тем, чтобы принимающие устройства могли распознать маршрут, область spanning tree и VLAN. Идентификатор MSTI ID позволяет классифицировать эти маршруты. MSTP позволяет объединить несколько отдельных покрывающих деревьев в общее внешнее покрывающее дерево (CIST). CIST автоматически распознаёт области MSTP, их максимальный размер и служит своего рода виртуальным мостом между отдельными покрывающими деревьями. Следовательно, фреймы различных VLAN будут следовать различными маршрутами в пределах установленных областей сети, при этом осуществляется простая и быстрая обработка фреймов независимо от административных ошибок в определенных VLAN и соответствующих им покрывающих деревьях.

Для каждого Коммутатора, использующего протокол MSTP, необходимо задать соответствующие настройки, включающие следующие три атрибута:

1. Конфигурационное имя задаётся цифробуквенной строкой не более 32 символов (вводится в поле **Configuration Name**, в окне **STP Bridge Global Settings**).
2. Номер ревизии конфигурации (здесь называется Revision Level и находится в окне **STP Bridge Global Settings**).
3. Таблица на 4096 элементов (здесь называется VID List, находится в окне **MST Configuration Table**), которая будет идентифицировать каждую из 4096 возможных VLAN, поддерживаемых коммутатором.

Для использования MSTP-функции Коммутатора неоходимо выполнить следующие три шага:

1. Задать на Коммутаторе настройки MSTP (находятся в окне **STP Bridge Global Settings** в поле **STP Version**).
2. Необходимо задать приоритет данного покрывающего дерева (здесь называется **Priority**, задается в окне **MSTConfiguration Table**, когда конфигурируются настройки MSTI ID).
3. VLAN, которые будут предоставлены для общего доступа, должны быть добавлены в MSTP Instance ID (здесь называется VID List в окне **MST Configuration Table**, настраивается, когда конфигурируются настройки MSTI ID).

802.1w Rapid Spanning Tree

В Коммутаторе используются три версии протокола Spaning Tree: Multiple Spanning Tree Protocol (MSTP), определённый как стандарт IEEE 802.1s; Rapid Spanning Tree Protocol (RSTP), определённый как IEEE 802.1w, и версия совместимая с IEEE 802.1d STP. Протокол RSTP совместим с протоколом IEEE 802.1d, однако, приэтом 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 в протоколах STP, MSTP, RSTP

Основные различия между этими тремя 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). Протоколы MSTP и RSTP используют 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 6-1 показано сравнение изменения состояия портов для трёх протоколов.

Все три 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.

802.1d MSTP	802.1w RSTP	802.1d STP	Пересылка	Изучение
Отказ (Discarding)	Отказ (Discarding)	Отключен (Disabled)	Нет	Нет
Отказ (Discarding)	Отказ (Discarding)	Блокировка (Blocking)	Нет	Нет
Отказ (Discarding)	Отказ (Discarding)	Прослушивание (Listening)	Нет	Нет
Изучение (Learning)	Изучение (Learning)	Изучение (Learning)	Нет	Да
Продвижение пакетов (Forwarding)	Продвижение пакетов (Forwarding)	Продвижение пакетов (Forwarding)	Да	Да

Таблица 6-1. 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/MSTP все порты, работающие в дуплексном режиме, являются P2P-портами, если обратное не было задано вручную.

Совместимость 802.1d/802.1w/802.1s

MSTP или RSTP позволяют 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 MSTP и RSTP, способных 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.

Глобальные настройки STP-моста

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

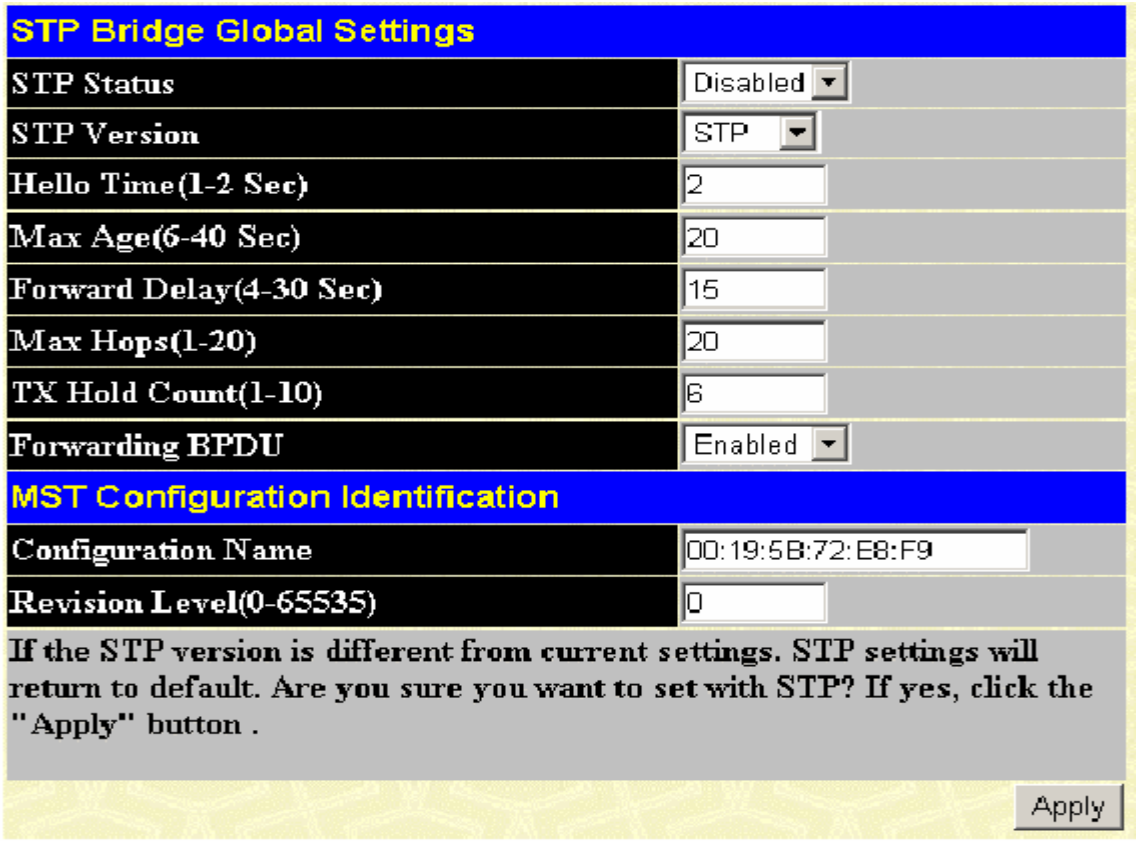


Рисунок 6- 23. Окно STP Bridge Global Settings – STP

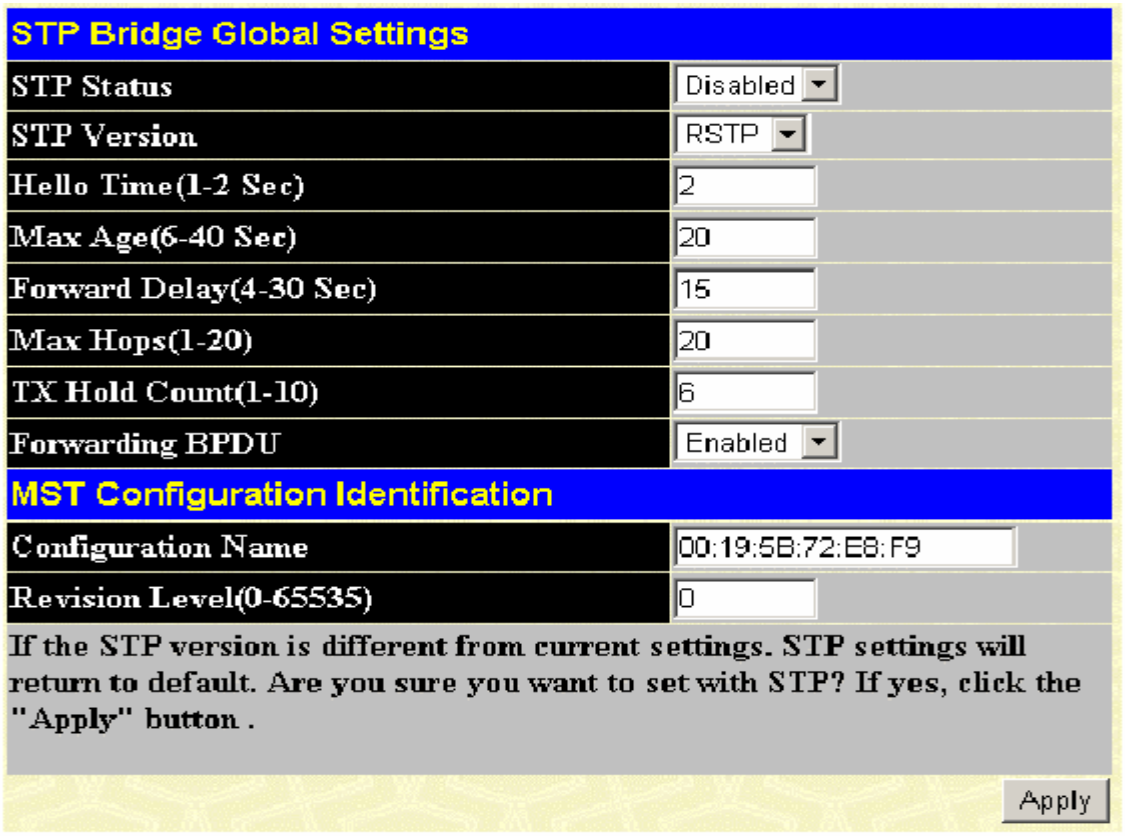


Рисунок 6- 24. Окно STP Bridge Global Settings - RSTP (по умолчанию)

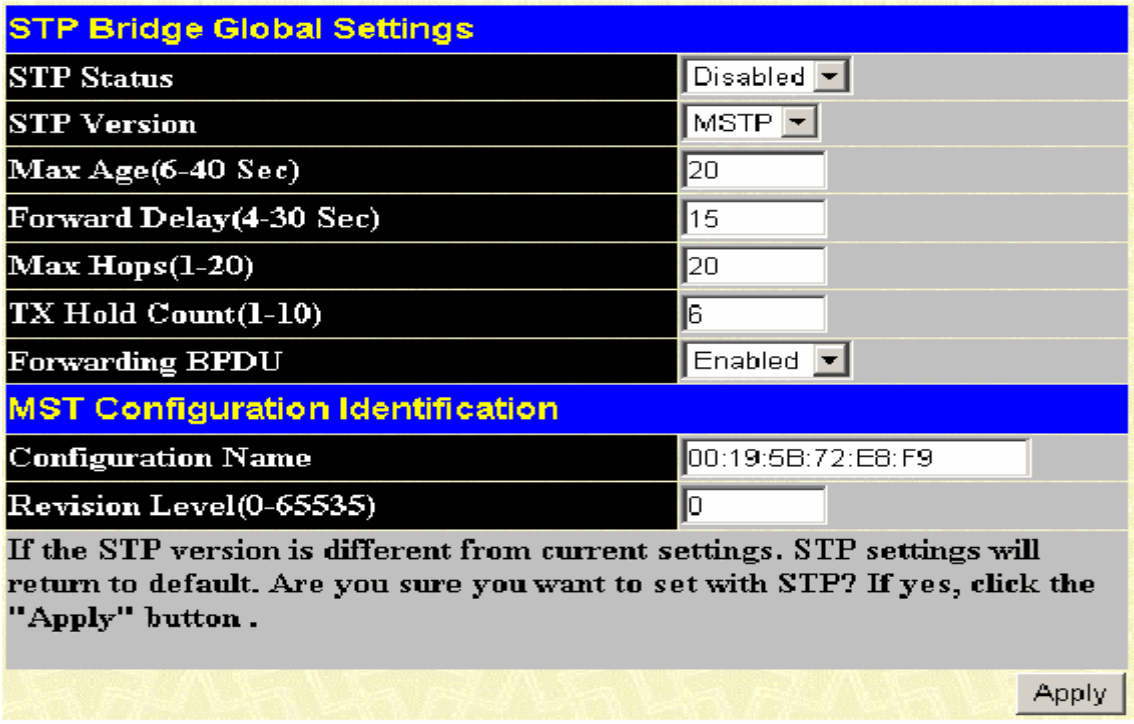


Рисунок 6- 25. Окно STP Bridge Global Settings - MSTP

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)

Можно установить следующие параметры:

Параметр	Описание
STP Status	В выпадающем меню можно включить/выключить функцию STP на коммутаторе. Значение по умолчанию *Disabled* (выключено).
STP Version	Выпадающее меню позволяет выбрать версию STP, которая будет использоваться. Возможны следующие значения: *STP* - Spanning Tree Protocol (STP) *RST*P - Rapid Spanning Tree Protocol (RSTP) *MSTP* - Multiple Spanning Tree Protocol (MSTP)
Hello Time	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. Это поле доступно только при настройке STP или RSTP. Для MSTP этот параметр задается на уровне портов. Детальное описание настроек MSTP приведено в главе, посвященной настройкам порта MST.
Max Age	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.
Forward Delay	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	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.
TX Hold Count	Используется для установки максимального количества Hello-пакетов, передаваемыз 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*.
MST Configuration Identification	
Configuration Name	Это поле позволяет ввести цифробуквенную строку до 32 символов для идентификации MSTP-области Коммутатора. Этот параметр, наряду с

	параметром Revision Level, позволяет идентифицировать MSTP-область. Если значение поля не задано, то значением по умолчанию будет MAC-адрес устройства. Это поле доступно только тогда, когда на Коммутаторе глобально задано использование протокола MSTP.
Revision Level	Можно установить значение от 0 до 65535 для идентификации MSTP-области. Это значение наряду с предыдущим полем идентифицирует MSTP-область. Значение по умолчанию - 0. Это поле доступно только тогда, когда на Коммутаторе глобально задано использование протокола MSTP.

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

Таблица конфигурации MST

Опции, предоставляемые окном **Current MST Configuration Identification,** позволяют пользователю конфигурировать копию MSTI на коммутаторе. Эти настройки будут уникально идентифицировать несколько копий spanning tree, установленные на Коммутаторе. Первоначально Коммутатор обладает 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 **Current MST Configuration Identification**, кликните **Configuration > Spanning Tree > MST Configuration Table**.

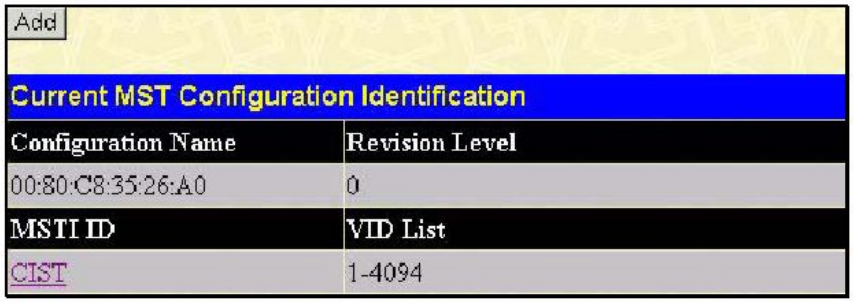


Рисунок 6- 26. Окно Current MST Configuration Identification

Окно, представленное выше, содержит следующую информацию:

Параметр	Описание
Configuration Name	Этот параметр, наряду с параметром Revision Level, позволяет идентифицировать MSTP-область. Если значение поля не задано, то значением по умолчанию будет MAC-адрес устройства. Это поле также может быть задано в окне STP Bridge Global Settings.
Revision Level	Значение данного поля, наряду с Configuration Name, идентифицирует MSTP-область, настроенную на Коммутаторе. Данный параметр также может быть установлен в окне STP Bridge Global Settings.
MSTI ID	Это поле показывает список MSTI ID Коммутатора. В этом списке всегда будет присутствовать CIST MSTI, который не может быть удалён.
VID List	Это поле показывает список VLAN ID, принадлежащих определенному MSTI.

Кликните по **Add** для того, чтобы открыть следующее окно:

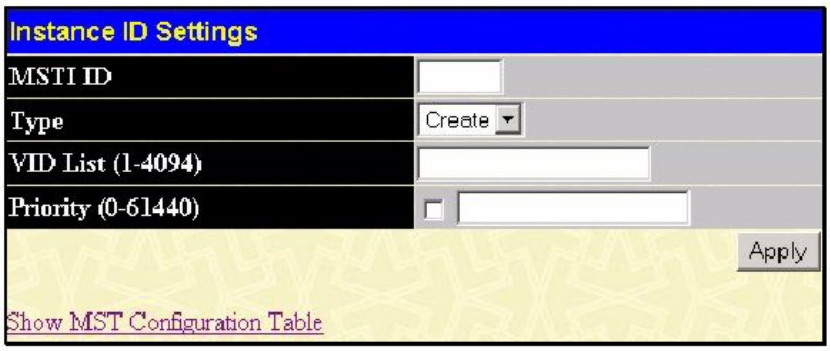


Рисунок 6- 27. Окно Instance ID Settings window – добавить

Параметр	Описание
MSTI ID	Допускается выбор значения от 1 до 15 для установки нового MSTI на Коммутаторе.
Type	Значение Create означает, что создаётся новый MSTI.
VID List (1-4094)	Это поле используется для определения VID, используемых для настроенных на Коммутаторе VLAN. Диапазон значений VID, доступных на коммутаторе, - от 1 до 4094.
Priority (0-61440)	Выбирается значение от 0 до 61440 для задания приоритета MSTI при продвижении пакетов. Чем меньше значение, тем выше приоритет. Это значение должно быть кратно 4094.

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

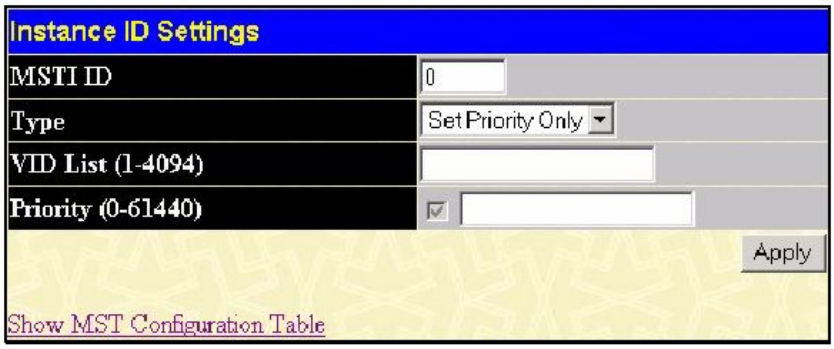


Рисунок 6- 28. Окно Instance ID Settings – модификация CIST

Пользователь может сконфигурировать следующие параметры CIST:

Параметр	Описание
MSTI ID	Значение MSTI ID равно 0 и не может быть изменено.
Type	Тип конфигурации. Поле используется только для задания приоритета CIST. Все остальные параметры не доступны для изменения.
VID List (1-4094)	Это поле используется для определения диапазона VID для VLAN, сконфигурированных на Коммутаторе. Диапазон значений от 1 до 4094. При

	настройке CIST это поле не доступно.
Priority (0-61440)	Выбирается значение от 0 до 61440 для задания приоритета MSTI при пересылке пакетов. Чем ниже значение, тем выше приоритет. Это значение должно быть кратно 4094.

Для применения настроек следует кликнуть по **Apply.**
Для установки параметров MSTI следует кликнуть по соответствующему MSTI ID, откроется следующее окно:

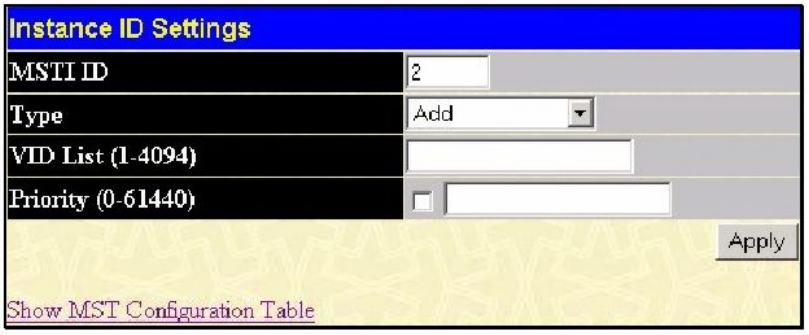


Рисунок 6- 29. Окно Instance ID Settings – модификация

Пользователь может сконфигурировать следующие параметры MSTI на Коммутаторе:

Параметр	Описание
MSTI ID	Отображает MSTI ID, предварительно установленный пользователем.
Type	Этот параметр позволяет пользователю выбрать способ изменения настроек MSTI. Пользователь может сделать следующий выбор: *Add* – для добавления VID в MSDI ID. В этом случае будет доступно поле VID List. *Remove* – для удаления VID из MSDI ID. В этом случае будет доступно поле VID List. *Delete* – для удаления данного MSDI ID. *Set Priority Only* – для установки приоритета MDSI ID. Это поле используется вместе с полем Priority.
VID List (1-4094)	Это поле используется для определения диапазона VID для VLAN, сконфигурированных на Коммутаторе. Диапазон значений от 1 до 4094. Это поле доступно только, когда значение поля **Type** *Add* или *Remove*.
Priority (0-61440)	Выбирается значение от 0 до 61440 для задания приоритета MSTI при продвижении пакетов. Чем ниже значение, тем выше приоритет. Это значение должно быть кратно 4094. Данное поле используется только, когда значение поля **Type** установлено *Set Priority Only.*

Для применения настроек следует кликнуть **Apply**.

Настройки MSTI

Данное окно отображает текущие настройки MSTI и может быть использовано дня обновления конфигурации порта для MSTI ID. При возникновении петли функция MSTI использует приоритет порта для выбора интерфейса, переведенного в состояние продвижения пакетов. Интерфейсы, через которые должна осуществляться передача в первую очередь, должны обладать более высшим приоритетом. В том случае, когда приоритеты нескольких интерфейсов одинаковы, функция MSTP выбирает из таблицы MAC-адресов интерфейс с наименьшим MAC-адресом, а остальные интерфейсы при этом будут заблокированы. Стоит помнить, что чем меньше значение приоритета, тем выше приоритет при выборе интерфейса для продвижения пакета.

Для работы со следующим окном необходимо кликнуть **Configuration > Spanning Tree > MSTP Settings**:

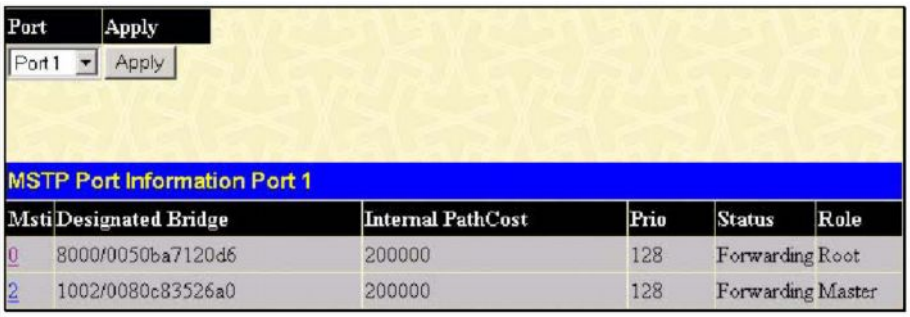


Рисунок 6- 30. Окно MSTP Port Information

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

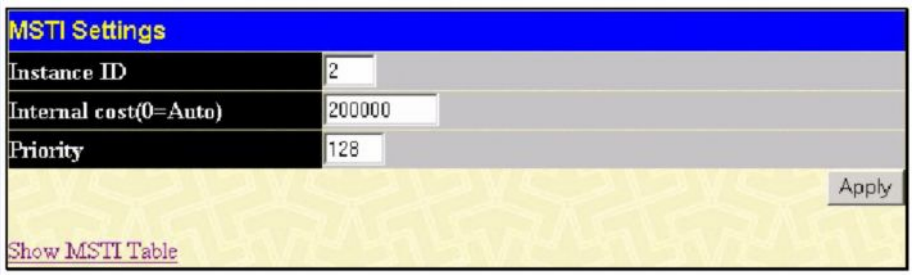


Рисунок 6- 31. Окно MSTI Settings

Параметр	Описание
Instance ID	Отображает идентификатор ID настраиваемой копии MSTI. Нулевое значение данного поля означает, что выбрано CIST (значение по умолчанию).
Internal cost (0=Auto)	Этот параметр представляет относительную стоимость передачи пакетов на определённые порты, принадлежащие той же копии STP. Значение по умолчанию 0 (авто). Возможны два варианта: • 0 (авто) – устанавливает самый быстрый и оптимальный маршрут. Определяет передачу со скоростью среды интерфейса. • Значение от *1* до *2000000* – позволяет выбрать наилучший маршрут при возникновении петли. Чем ниже данное значение, тем выше скорость передачи.
Priority	Это поле позволяет задать значение от *0* до *240* для настройки приоритета порта. Интерфейс, через который данные будут передаваться первыми, обладает высшим приоритетом. Чем меньше значение данного параметра, тем выше приоритет.

Для принятия изменений необходимо кликнуть по **Apply**.

Настройки копии STP

Следующее окно отображает MSTI, в настоящий момент настроенные на Коммутаторе. Для просмотра следующей таблицы кликните **Configuration > Spanning Tree > STP Instance Settings**:

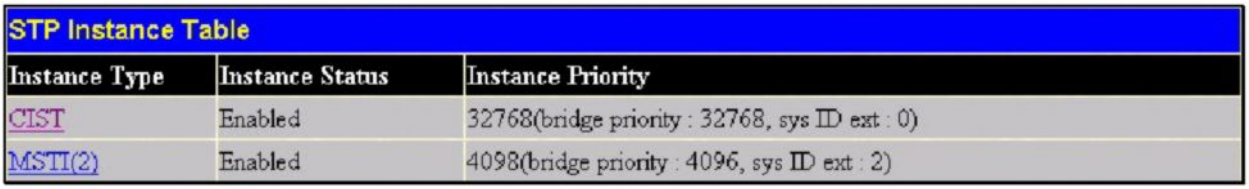


Рисунок 6- 32. Окно STP Instance Table

Здесь отображена следующая информация:

Параметр	Описание
Instance Type	Отображает все MSTI, представленные в текущей конфигурации Коммутатора.
Instance Status	Отображает текущий статус MSTI ID.
Instance Priority	Отображает приоритет MSTI ID. Наименьший приоритет будет у корневого моста.

Для принятия настроек необходимо кликнуть **Apply**.

Для получения более подробной информации по конкретной копии STP, необходимо кликнуть по соответствующей ссылке в столбце Instance Type. В результате отобразится показанное ниже окно, доступное только для чтения.

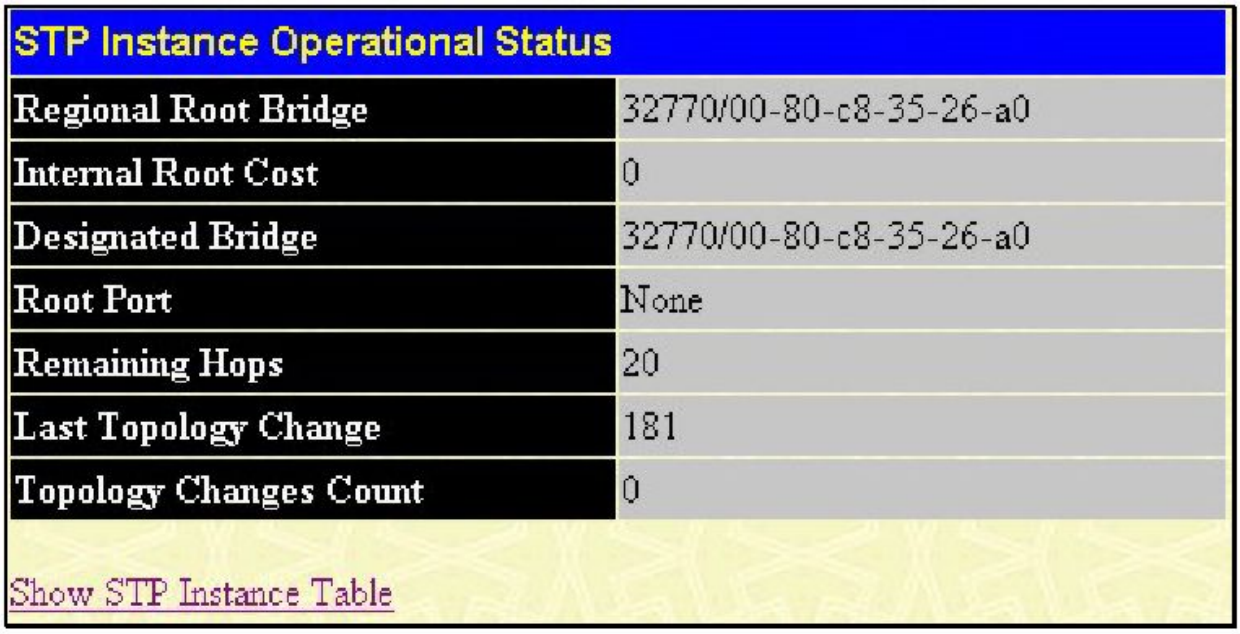


Рисунок 6- 33. Окно STP Instance Operational Status

Информация о портах MSTP

Задать настройки STP можно, не только глобально, но и на основе портов. Для просмотра следующего окна необходимо кликнуть **Configuration > Spanning Tree > MST Port Information**:

STP Port Settings

From	To	External Cost (0=Auto)	Hello Time	Migrate	Edge	Restricted Role	Restricted TCN	P2P	Forward BPDU	State
Port 1	Port 1	0		Yes	False	False	False	Auto	False	Enabled

Apply

MSTP Port Information Table

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

Рисунок 6- 34. Окно STP Port Settings

В дополнение к установкам параметров Spanning Tree, использующимся на уровне коммутаторов, коммутатор позволяет конфигурацию групп портов. Каждая группа портов будет обладать своим Spanning Tree, со своими конфигурационными настройками. STP группа будет использовать параметры, заданные глобально на уровне коммутатора, а также приоритет порта и стоимость порта. Покрывающее дерево группы STP работает так же, как покрывающее дерево на уровне коммутаторов, но понятие корневого моста замещается понятием корневого порта. Корневой порт – это порт группы, который выбирается на основе приоритета и стоимости порта и служит для подключения группы к сети. Избыточные связи блокируются точно так же, как и на уровне коммутаторов.

На уровне коммутаторов STP блокирует избыточные связи между коммутаторами (и аналогичными сетевыми устройствами). На уровне портов STP блокирует избыточные связи внутри STP-группы. Целесообразно определять STP-группы в соотвтетсвии с группами портов VLAN.

Примечание: если требуется включить опцию продвижения BPDU-пакетов на основе портов, следует сделать следующие настройки: 1. Опцию STP необходимо глобально отключить. 2. Опция продвижения BPDU-пакетов должна быть глобально включена. Эти параметры заданы по умолчанию и могут быть настроены в меню **STP Bridge Global Settings**, рассмотренном ранее.

Можно задать следующие настройки STP-порта:

Параметр	Описание
From/To	Позволяют задать диапазон портов.
External Cost	Этот параметр определяет относительную стоимость продвижения паетов пакетов к списку определённых портов. Стоимость порта может вычисляться автоматически или задана определённым значением. Значение по умолчанию 0 (авто). *0 (авто)* – автоматически устанавливает оптимальную скорость пересылки пакетов на порт(ы). Значения стоимости порта по умолчанию: для 100Мбит/с порта=200000; для Gigabit порта=20000 *Значение от 1 до 200000000* – определяет внешнюю стоимость. Чем меньше значение, тем выше приоритет порта и больше вероятность того, что именно он будет выбран для продвижения пакетов.
Hello Time	Интервал между передачами конфигурационных сообщений корневым портом на другие устройства в LAN. Пользователь может выблать значение от 1 до 2 секунд. Значение по умолчанию 2 секунды. Это поле доступно только, когда на Коммутаторе выбран протокол MSTP.
Migration	При установке значения «yes» порты будут посылать BPDU-пакеты на другие мосты, запрашивая информацию об их настройках STP. Если коммутатор сконфигурирован под RSTP, порт может мигрировать от 802.1d STP до 802.1w RSTP. Если Коммутатор настроен на использование протокола MSTP, порт может автоматически выбирать сове состояние между 802.1d STP и 802.1s MSTP. RSTP и MSTP поддерживают совместимость со стандартом STP, однако, преимущества RSTP и MSTP не реализуются на порту при соединении 802.1d с 802.1w или 802.1s.
Edge	Выбор значения *True* в данном поле определяет порт как пограничный. Пограничный порт подключен к сегменту сети, на котором невозможно образование петли. Пограничный порт не должен принимать BPDU-пакеты. Если был принят BPDU-пакет, это приведёт к автоматической потере статуса пограничного порта. Выбор значения *False* означает, что порт не является пограничным портом.
Restricted Role	Этот параметр может принимать два значения: True и False. При выборе значения TRUE этот порт не будет корневым портом для CIST или других MSTI, даже если он будет обладать наименьшим приоритетом. Таким образом, порт становится альтернативным портом, который будет выбираться всегда после корневого порта. По умолчанию этот параметр установлен как FALSE. Выбор True может привести к потере связности покрывающего дерева. Это позволяет избежать влияния внешних мостов на

	активную топология покрывающего дерева, поскольку данные мосты не находятся под управлением сетевого администратора.
Restricted Tcn	Возможно два значения этого поля: True и False. При выборе значения TRUE полученные с этого порта уведомления (topology change notifications и topology change) не будут распространяться на другие порты. Этот параметр установлен в значение FALSE, по умолчанию. При установленной опции False может временно теряться связность из-за некорректных пакетов изменения топологии (topology change), полученных с клиентских портов.
P2P	Значение *True* в данном поле означает, что данный порт является портом point-to-point (P2P)-портом. P2P-порты похожи на пограничные порты, однако P2P-порты обязательно должны работать в режиме полного дуплекса. Так же как и пограничные порты, P2P-порты переходят в состояние продвижения пакетов быстрее, обеспечивая преимущество протокола RSTP. Значение False означает, что порт не является P2P-портом. Значение *Auto* позволяет порту быть со статусом P2P всегда, когда возможно и оперировать так, как если бы значение P2P-статуса было *True*. Если порт по каким-либо причинам не может поддерживать этот статус (например, если порт был принудительно поставлен в режим полу-дуплекса), порт будет оперировать так, как если бы значение P2P-статуса было *False*. Значение по умолчанию для данного параметра *Auto*.
Forward BPDU	Значение True позволит пересылку BPDU-пакетов с сетевых устройств на заданные порты. Для этого опция STP должна быть глобально отключена, а продвижение BPDU-пакетов глобально разрешено (более подробная информация приведена в главе **STP Bridge Global Settings**). Значение по умолчанию *False:* в этом случае BPDU-пакеты не будут пересылаться, даже если опция STP отключена.
State	Позволяет включить/отключить STP для выбранной группы портов. Значение по умолчанию *Enabled* (включено).

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

Функция Loopback Detection

Эта функция позволяет временно отключить порт Коммутатора, когда пакет CTP (Configuration Testing Protocol) вернулся на Коммутатор. Когда Коммутатор обнаружит получение CTP-пакетов, отправленных с его порта или VLAN, то это означает образование петли в сети. При этом Коммутатор автоматически заблокирует данный порт или VLAN и отправит предупреждение администратору. По истечении Loopback Detection Recover Time состояние порта изменится на discarding (отказ). Функция Loopback Detection может использоваться на определенном диапазоне портов. Пользователь может включить или выключить эту функцию, используя выпадающее меню.

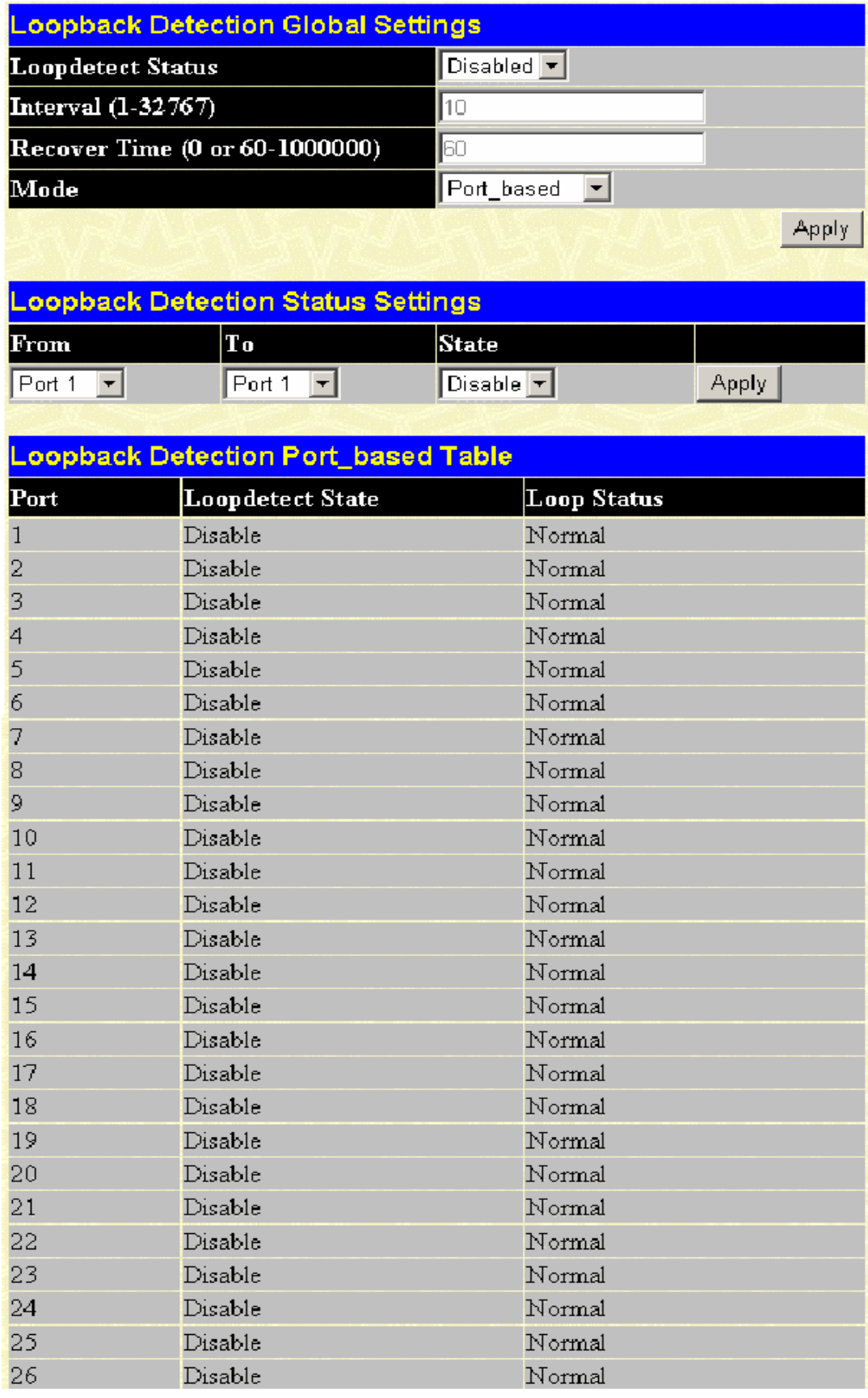


Рисунок 6- 35. Окно LoopBack Detection Global Settings

Параметр	Описание
Loopback Detection Global Settings	
Loopback Detection Status	Это поле содержит выпадающее меню для глобального включения / выключения функции Loopback Detection на Коммутаторе. По умолчанию, значение *Disabled* (выключено).
Interval (1-32767)	Используя выпадающее меню, задайте временной интервал (в секундах), через который удаленное устройств будет передавать CTP-пакеты для обнаружения петель. Значение по умолчанию равно 10, но может быть изменено в интервале от 1 до 32767.
Recover Time (0 или 60 – 1000000)	Временной интервал (в секундах), используемый механизмом автовосстановления для принятия решения, как долго будет действовать Loopback. Допустимый диапазон значений от 60 до 1000000. Также специально предусмотрено значение «0», которое выключает механизм автовосстановления. По умолчанию, значение равно 60.
Mode	Доступны два режима работы функции LoopBack Detection: *Port_based* (на основе портов), *VLAN_based* (на основе VLAN). В режиме *Port_based* порт будет отключен в течение всего времени действия петли. В режиме *vlan-based*, порт не будет обрабатывать пакеты, предназначенные для VLAN, в которой возникла петля.
Loopback Detection Status Settings	
From/To	Позволяет задать диапазон портов.
State	Данное поле позволяет с помощью выпадающего меню включить / выключить функцию Loopback Detection для выбранной группы портов. По умолчанию значение *Disabled* (выключено).

Для принятия изменений кликните по кнопке **Apply**.

Продвижение и фильтрация пакетов (папка Forwarding Filtering)

Продвижение пакетов на заданный Unicast-адрес (Unicast Forwarding)

Папка **Forwarding Filtering** открывается из меню **Configuration,** далее следует кликнуть по ссылке **Unicast Forwarding,** в результате откроется окно **Setup Static Unicast Forwarding Table**.

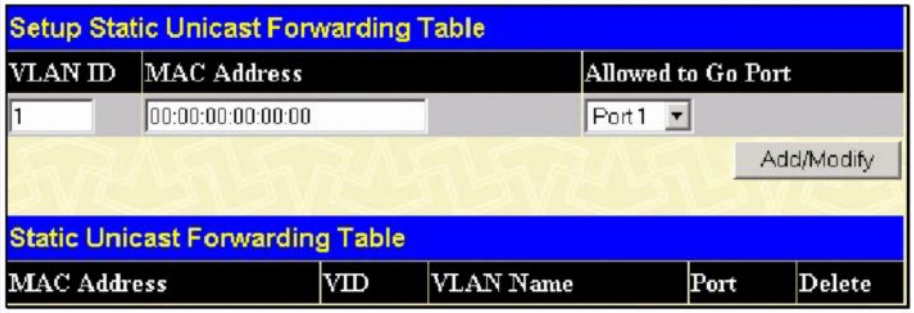


Рисунок 6- 36. Окно Setup Static Unicast Forwarding Table

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 **Static 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- 37. Окно Static 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- 38. 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:

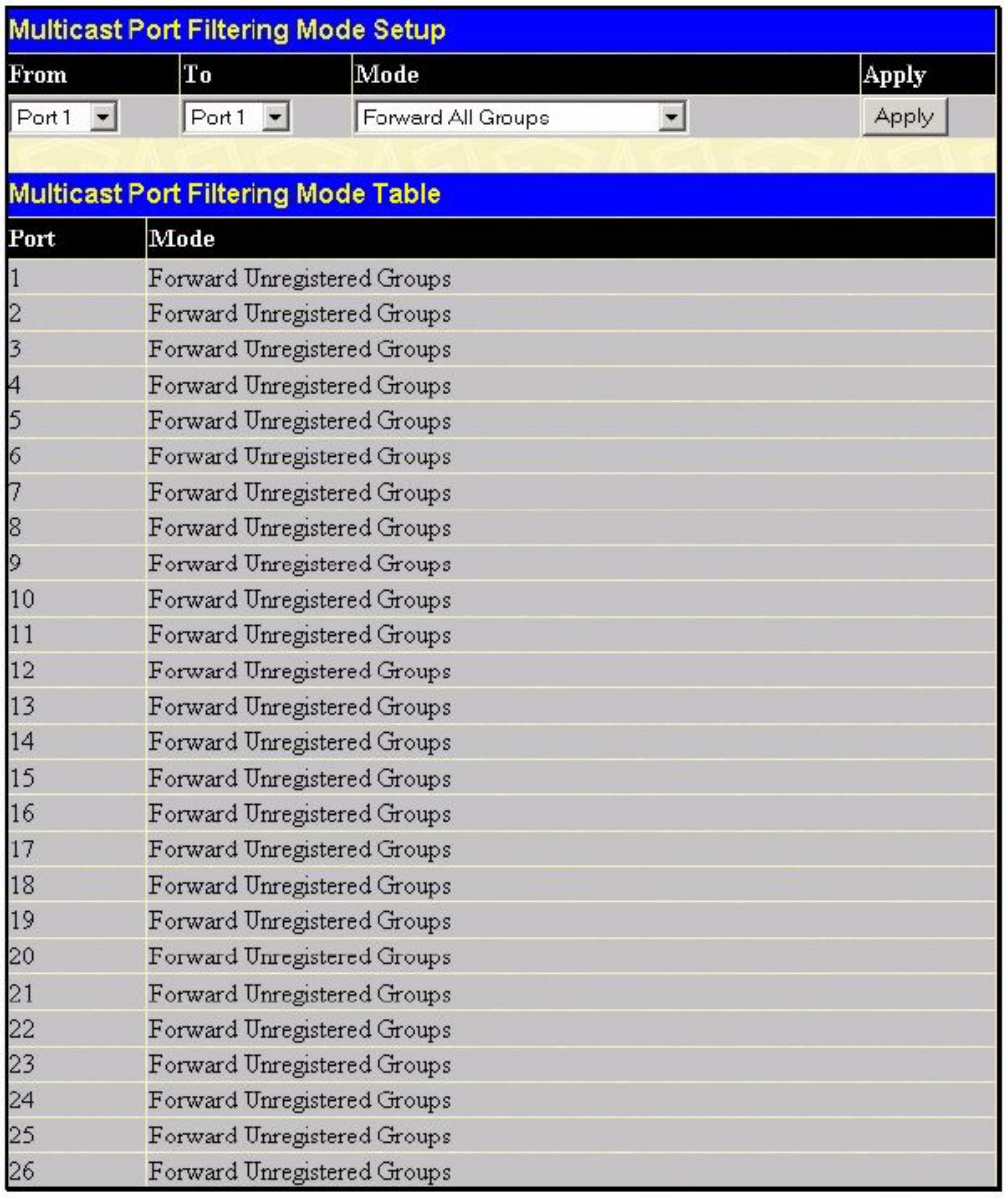


Рисунок 6- 39. Окно Multicast Port Filtering Mode Setup

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 All Groups* – Выбор данной опции приведет к тому, что Коммутатор будет передавать многоадресный пакет на все многоадресные группы, которым принадлежат определённые выше порты. • *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**.

Виртуальные локальные сети (VLAN)

Понятие приоритета IEEE 802.1p

Назначение приоритетов опеделяется стандартом IEEE 802.1p и предназначено для управления трафиком в сети, где могут одновременно передаваться различные типы данных. Эта функция обеспечивает надлежащую работу приложений, чувствительных к задержкам, поскольку при работе, например, с видеоконференцией даже небольшие задержки передачи данных могут существенно повлиять на качество.

Сетевые устройства, поддерживающие стандарт IEEE 802.1p, обладают способностью распознавать уровень приоритета пакетов данных. Кроме того, эти устройства спопособны также назначать уровни приоритета пакетов, добавляя к ним соответствующие теги (метки). Приоритет определяет степень срочности передачи пакета, а также задает номер очереди.

Значение приоритета может быть от 0 до 7: 0 обозначает наименьший приоритет, 7 – наивысший. Приоритет 7 обычно присваивается данным приложений, чувствительных к задержкам (например, видео- и аудио- приложения) или же при передаче данных пользователей, оплативших соответствующую услугу по передаче их данных с наивысшим приоритетом.

Коммутатор позволяет настроить, каким образом тегированные пакеты данных далее будут обрабатываться в сети. Гибкая система очередей приоритетов в каждом конкретном случае позволяет задать оптимальные настройки. Существуют случаи, когда предпочтительнее, чтобы два или более пакетов с различными приоритетами были поставлены в одну очередь. Однако обычно рекомендуется очередь с наивысшим приоритетом Queue 1 полностью выделять для данных с приоритетом 7. Пакеты, не получившие никакого приоритета, помещаются в Queue 0, и таким образом, получают наименьший приоритет доставки.

Используемый алгоритм обработки приоритетов weighted round robin (взвешенный круговой режим или WRR) определяет, в какой последовательности будут опустошаться очереди пакетов. При очистке очередей соблюдается соотношение 4:1, т.е. если очередь наивысших приоритетов Queue 1 освобождается от 4-х пакетов, то очередь Queue 0 – от одного.

Стоит помнить, что настройки очередей и приоритетов устанавливаются на Коммутаторе для всех портов, и это будет влиять на все устройства, подключенные к Коммутатору. Система установки приоритетов и очередей будет особенно эффективна в том случае, если другие коммутаторы на сети также поддерживают данную функцию.

Описание 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 котором была инициирована широковещательная рассылка.

Замечания по реализации функции VLAN в коммутаторах серии DES-3500

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-3500 поддерживает два вида VLAN: VLAN IEEE 802.1Q s 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.

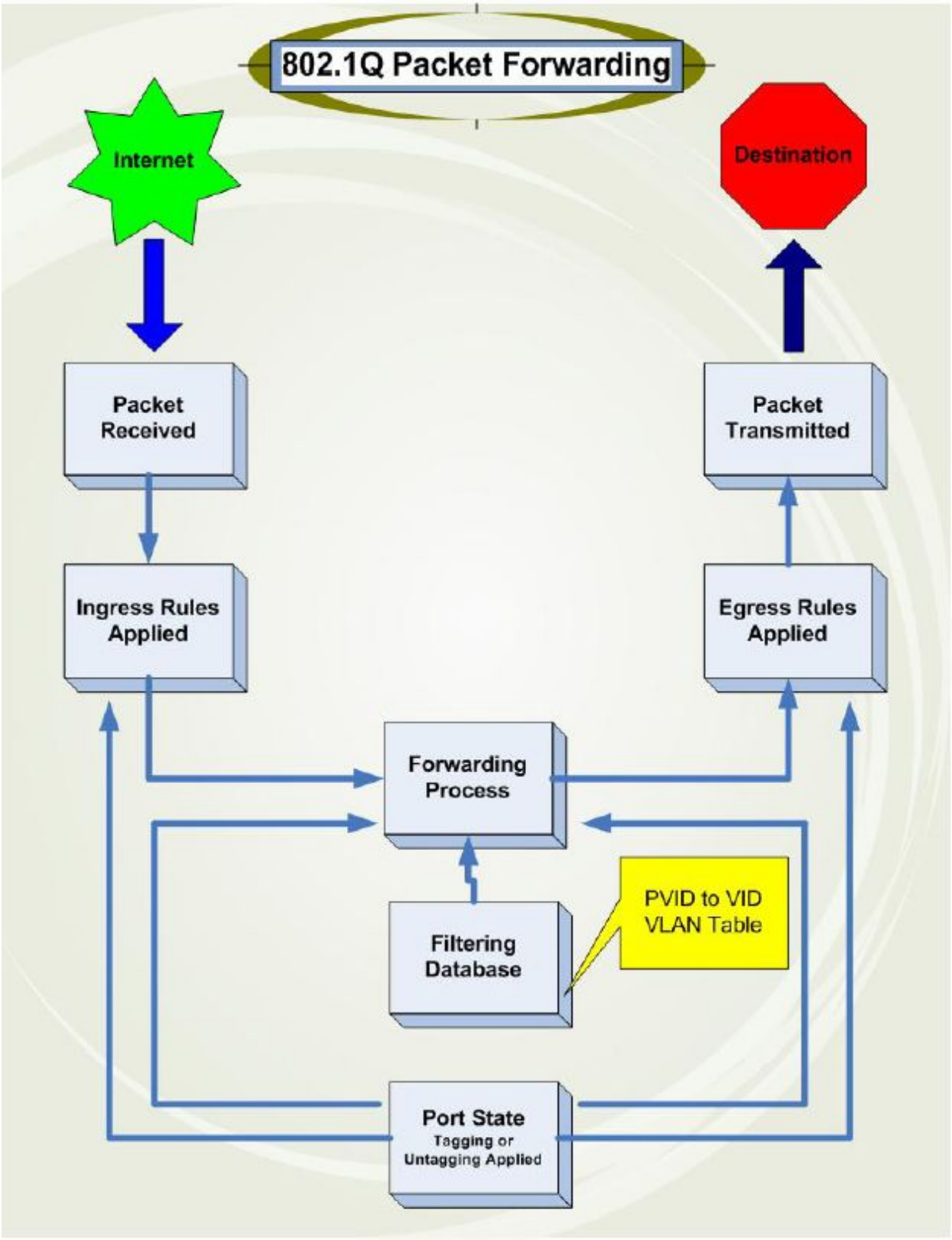


Рисунок 6- 40. Продвижение пакетов согласно IEEE 802.1Q

Теги 802.1Q VLAN

На рисунке 6.41 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.

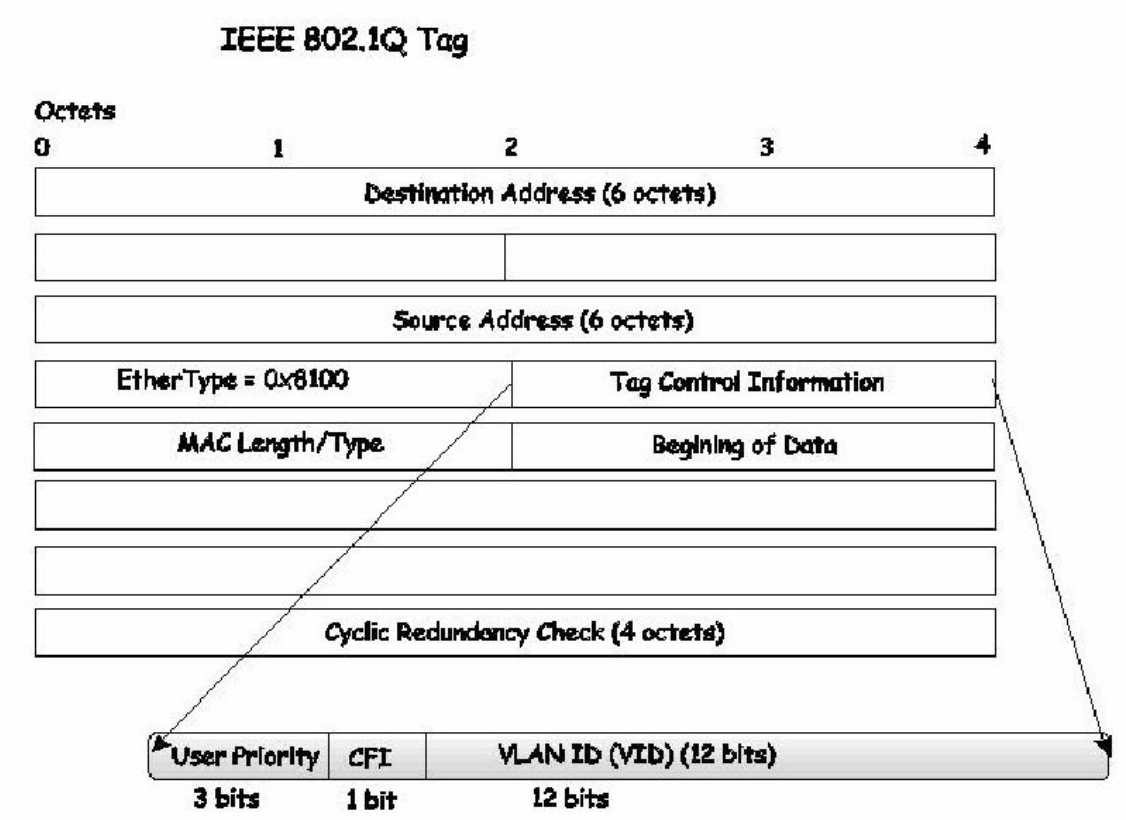


Рисунок 6- 41. Тег IEEE 802.1Q

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).

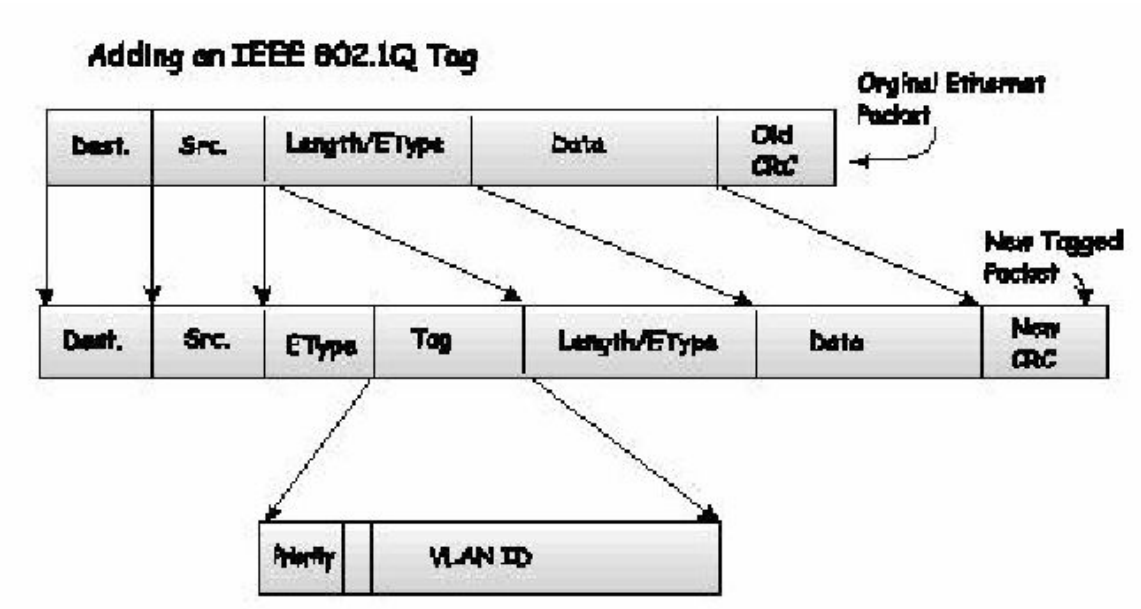


Рисунок 6- 42. Добавление IEEE 802.1Q тега

Идентификатор порта VLAN ID

Пакеты с тегами 802.1Q могут быть переданы от одного устройства, поддерживающего 802.1Q, к другому. К сожалению, не все устройства поддерживают 802.1Q.

До появления VLAN 802.1Q, находили широкое применение Port-Based VLAN (на основе портов) и MAC-Based VLAN (на основе MAC-адресов). Эти VLAN при продвижении пакетов используют идентификатор Port VLAN ID (PVID). При этом порт, на который пришел пакет, дополняет в этот пакет PVID, а затем пересылает его на соответствующий порт, указанный в таблице Коммутатора. Если PVID порта, который принял пакет, отличается от PVID порта, который передал пакет, Коммутатор отбросит пакет.

Для Коммутатора различные PVID означают различные VLAN (помните, что различные VLAN не могут взаимодействовать без внешнего маршрутизатора). Таким образом, идентификация VLAN на основе PVID не позволяет создавать VLAN, выходящие за пределы одного коммутатора или стека.

Каждому физическому порту Коммутатора назначен свой PVID. Порты 802.1Q также в пределах Коммутатора используют PVID. По умолчанию все порты Коммутатора добавлены в VLAN по умолчанию с PVID, равным 1. Нетегированные пакеты получают PVID порта, на который они были получены. Решения о продвижении пакетов принимаются на основе PVID. Тегирование пакеты пересылаются на основе информации, содержащейся в теге VID. Тегированные пакеты также обладают PVID, но PVID не используется для принятия решения о продвижении пакета.

Коммутаторы, поддерживающие 802.1Q VLAN, ведут таблицу соответствия PVID Коммутатора и VID сети. Коммутатор сравнивает VID передаваемого пакета с VID порта, передающего пакет. Если эти два идентификатора VID различны, то Коммутатор отбрасывает пакет. Использование PVID для нетегированных пакетов и VID для тегированных пакетов обеспечивает совместную работу в одной сети как устройств с поддержкой 802.1Q VLAN, так и без нее.

Порту коммутатора может быть назначен только один PVID, в то время как максимальное количество VID, назначенных порту коммутатора, ограничивается лишь размером памяти коммутатора, выделенной для хранения таблицы VLAN.

Поскольку в сети могут также присутствовать устройства, не поддерживающие 802.1Q VLAN, кажды порт устройства, поддерживающего 802.1Q VLAN, должен до передачи пакетов принять решение о необходимости тегирования. Так, если передающий порт соединён с устройством, не поддерживающим 802.1Q VLAN, пакет должен быть нетегированным. Если же передающий порт соединён с устройством, поддерживающим 802.1Q VLAN, пакет будет тегированным.

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 6- 2. Пример VLAN – назначение портов различным отделам

Port-based VLAN (на основе портов)

VLAN на основе портов ограничивают входящий и исходящий трафик на портах коммутатора. Таким образом, все устройства, соединённые с портом коммутатора, являются членами VLAN, к которому относится данный порт.

В VLAN на основе портов сетевым адаптерам нет необходимости в распознавании тегов 802.1Q в заголовках пакетов. Адаптеры посылают и принимают обычные Ethernet-пакеты. Если адрес назначения пакета лежит в том же самом сегменте, взаимодействие происходит по обычным Ethernet-протоколам. Если адресом назначения пакета является другй порт коммутатора, то принимается решение на основании настроек VLAN о дальнейшей передаче пакета.

Сегментация VLAN

Возьмём для примера пакет, переданный устройством, подключенным к порту 1 (Port 1), который является членом VLAN 2. Далее Коммутатор определяет, является ли порт назначения (Port 10) членом VLAN 2 (т.е. 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 на Port 10. Этот пример наглядно иллюстрирует сегментацию VLAN.

Асимметричные VLAN

Коммутаторы серии xStack DES-3500 позволяют создавать и настраивать асимметричные VLAN. Использование асимметричных VLAN позволяет устройстваим передать пакет в одной VLAN, а получить его в другой VLAN. Настройка асимметричных VLAN состоит из следующих действий: 1) включение функции VLAN, 2) создание VLAN и настройка GVRP. Ниже приводится пример.

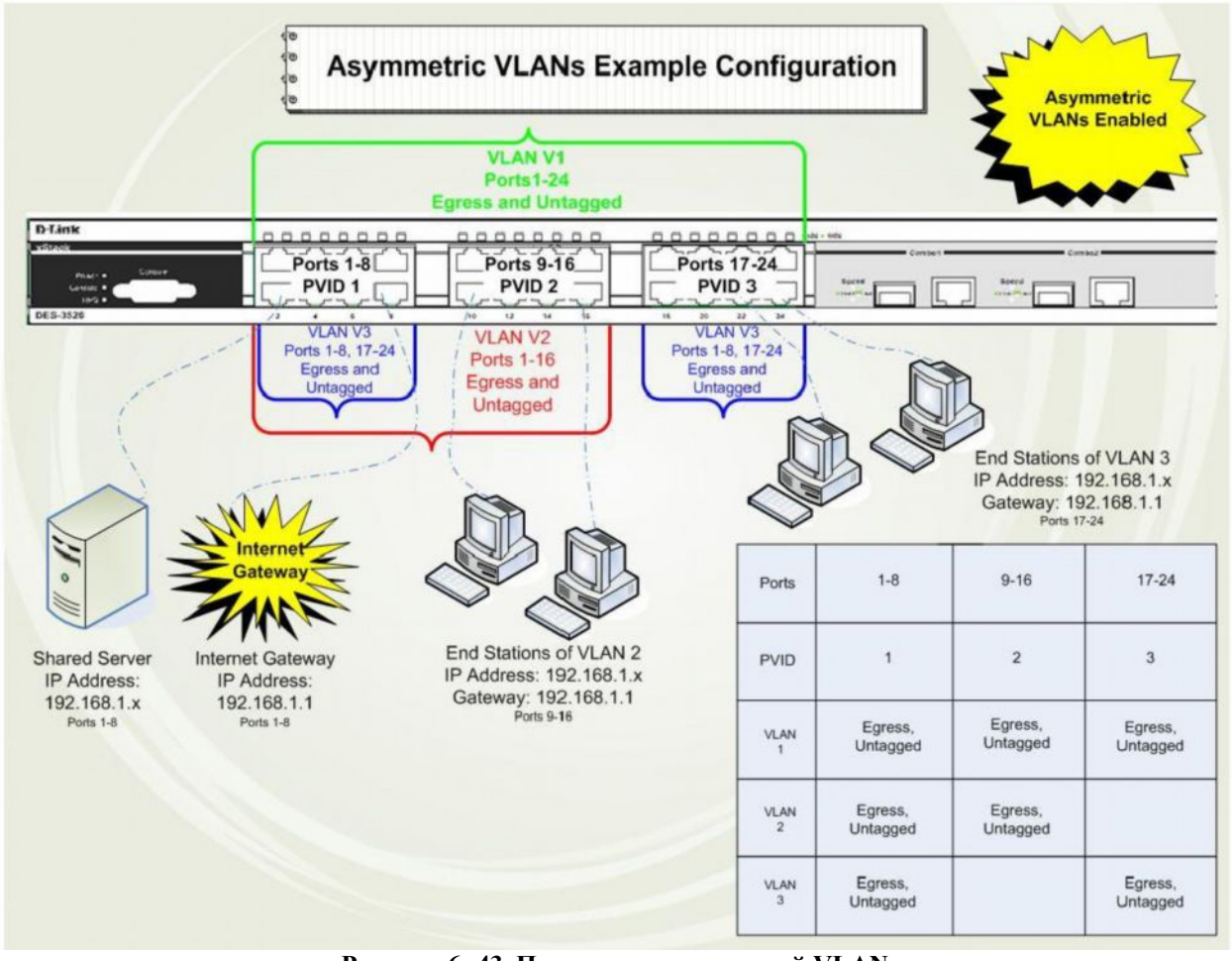


Рисунок 6- 43. Пример асимметричной VLAN

Рассмотрим настройку асимметричной VLAN более подробно:

1. Включите функцию асимметричной VLAN в окне **Advanced Settings**, доступном из папки **Configuration**.
2. Задайте настройки VLAN. В приведенном примере порты 1-8 используются для подключения устройств, совместно используемых пользователями. Например, серверы и принтеры для совместного использования. Следовательно, эту группу портов необходимо включить во все VLAN. Так, в VLAN V2 добавлены порты 1-8 (общие порты VLAN), а также другие порты, принадлежащие только этой VLAN (порты 9-16). Аналогично в VLAN V3 добавлены порты 1-8 (общие порты), а также ряд портов, принадлежащих только этой VLAN(17-24). В результате настроены две VLAN, часть портов которых совпадает, а часть - нет.
3. Задайте настройки PVID с помощью функции GVRP, доступной в папке VLANs. Неободимо задать совместно используемым портам PVID 1, а другим портам PVID 2 и PVID 3 соответственно. Теперь пользователь сможет использовать совместные устройства (им присвоен PVID 1), а также две небольшие подсети VLAN (обозначены как PVID 2 и PVID 3). Настройка асимметричной VLAN успешно завершена.

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.

Примечание: Для того чтобы использовать VLAN-сегментацию в сочетании с группой агрегированных каналов, сначала необходимо задать настройки групп(ы) агрегированных каналов, а лишь затем настройки VLAN. Если требуется изменить группировку в группах агрегированных каналов, при этом VLAN уже настроены, переконфигурировать VLAN не нужно: достаточно только изменить настройки групп агрегированных каналов. Настройки VLAN автоматически изменятся с изменением настроек групп агрегированных каналов.

Статическая запись VLAN

Для открытия следующего окна необходимо открыть папку **Configuration**, далее открыть папку **VLAN** и кликнуть по ссылке **Static VLAN Entry:**

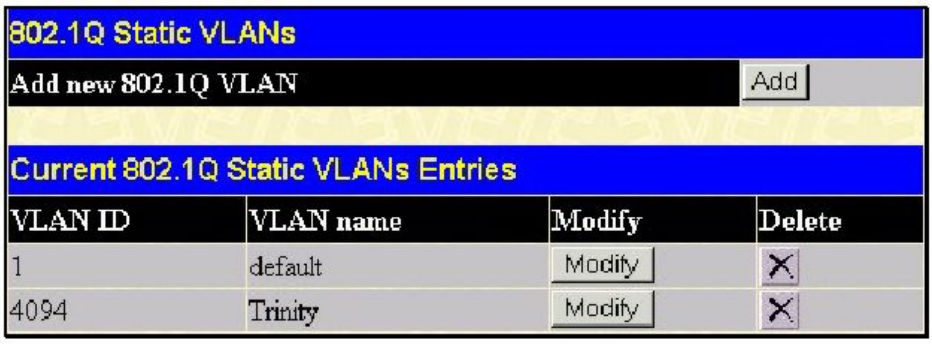


Рисунок 6- 44. Окно Current 802.1Q Static VLANs Entries

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 нового 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 номера новой VLAN. Описание параметров представлено ниже в таблице:

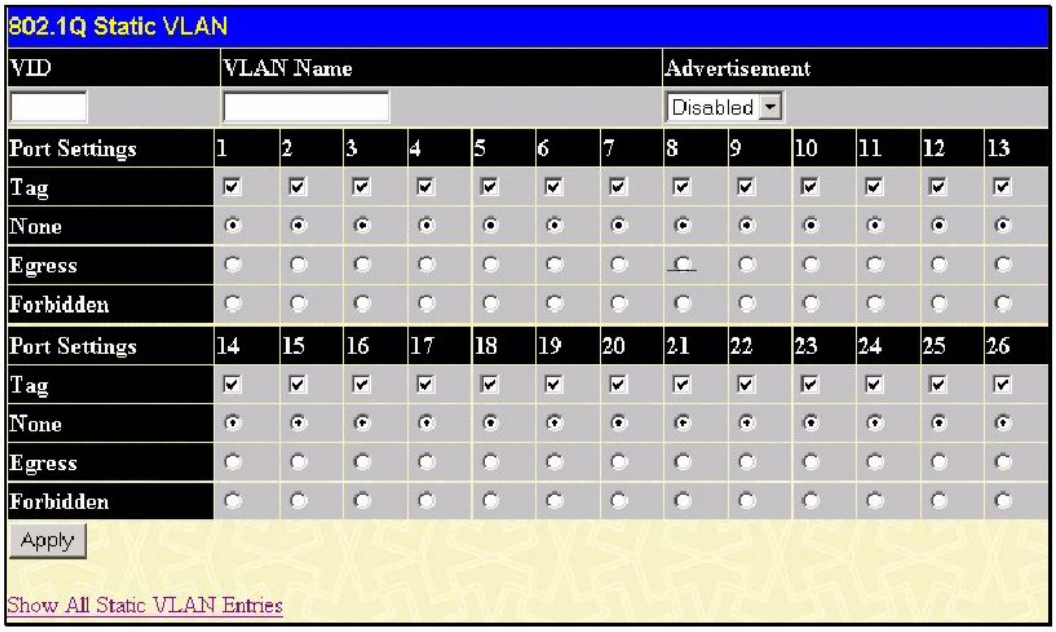


Рисунок 6- 45. Окно 802.1Q Static VLAN - добавить

Для возвращения в окно **Current 802.1Q Static VLANs Entries** 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.

Примечание: Коммутатор поддерживает до 255 статических VLAN.

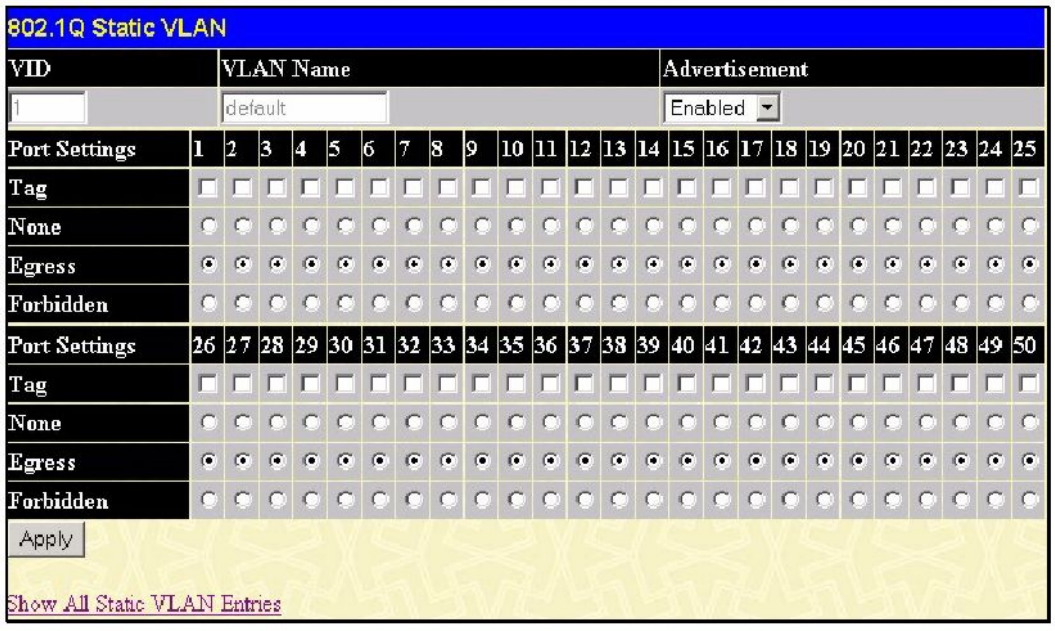


Рисунок 6- 46. Окно 802.1Q Static VLAN window – изменить

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**.
Advertisement	При выборе этой функции Коммутатор сможет посылать GVRP-пакеты на внешние устройства, уведомляя их о том, что они могут присоединяться к существующей VLAN.
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.
Forbidden	Используется для определения портов, которые не являются членами VLAN и которым запрещено динамически становиться членом VLAN.

Для применения настроек следует кликнуть **Apply**.

Настройки GVRP

В меню **Configuration** откройте папку **VLANs** и кликните по **GVRP Setting.**

Окно **802.1Q Port Settings** показано ниже. Данное окно 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:

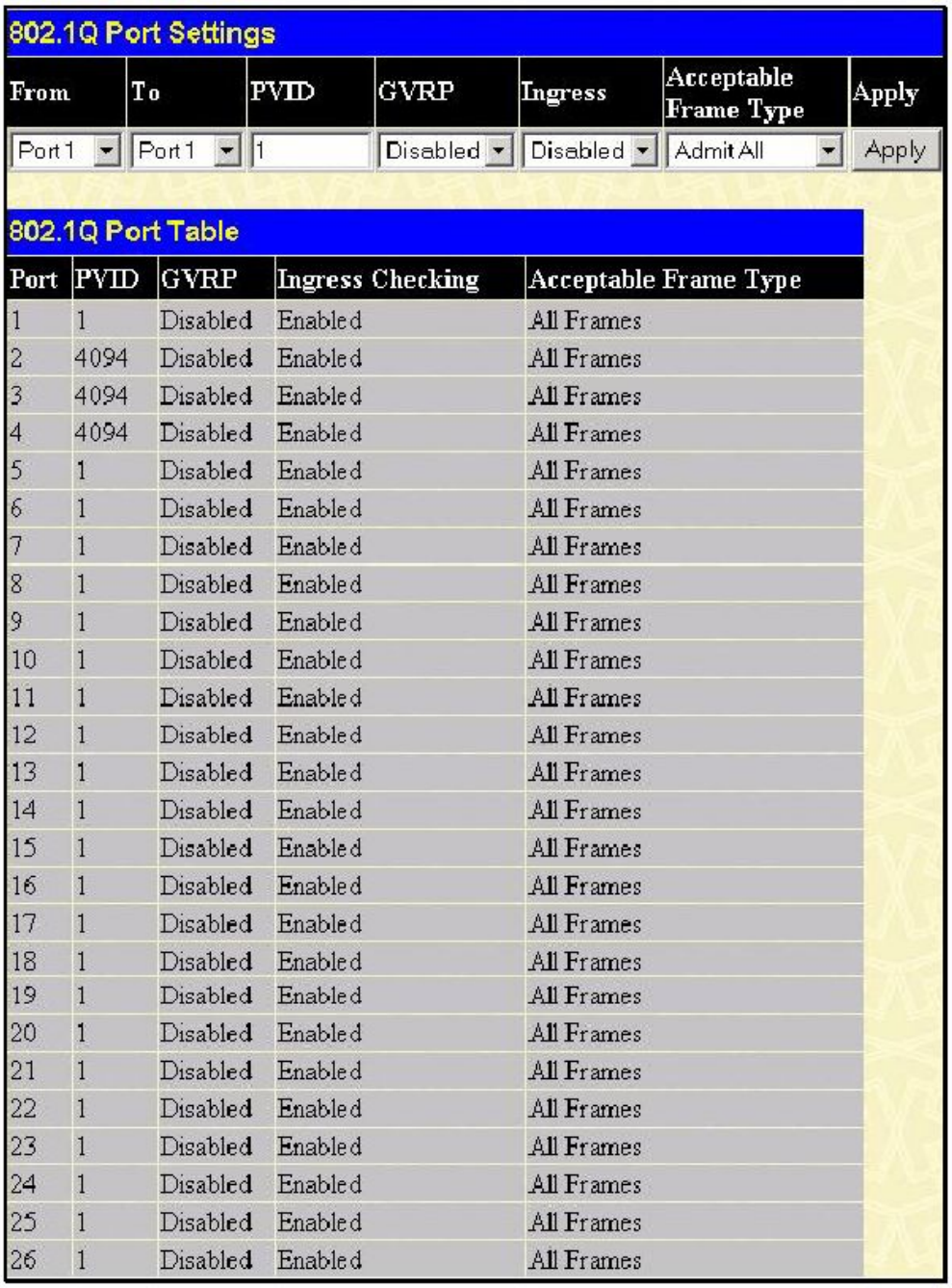


Рисунок 6- 47. Окно 802.1Q Port Settings

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.**
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.
GVRP	Включение опции Group VLAN Registration Protocol (GVRP) динамически позволяет порту динамически становиться членом VLAN. По умолчанию эта опция отключена.
Ingress	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.
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**.

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 ниже 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. 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** окна **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.

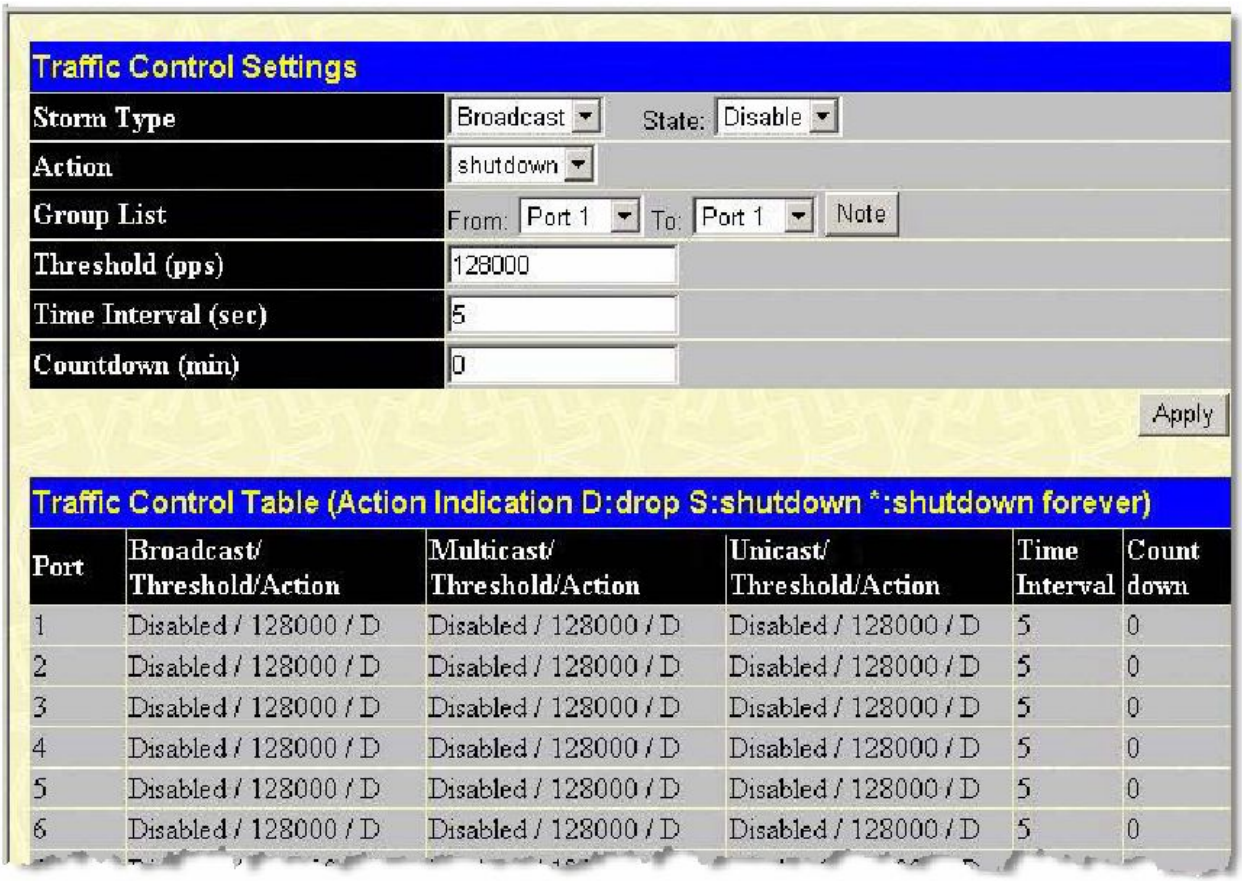


Рисунок 6- 48. Окно Traffic Control Setting

Окно **Traffic Control Setting** используется для включения/выключения опции управления широковещательным штормом и настройки порогов широковещательных и многоадресных штормов, а также DLF (Destination Look Up Failure). Параметры контроля трафика применимы к отдельным модулям Коммутаторам. Для работы с показанным выше окном необходимо кликнуть **Configuration > VLANs > Traffic Control**.

Пользователь может настроить следующие параметры:

Параметр	Описание
Trap Setting	
Traffic Control 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
Storm Type	Выберите тип шторма, для которого будет применяться функция управления. Доступны значения: Broadcast (для управления широковещательным штормом), Multicast (для управления многоадресным штормом) или Unicast (для управления одноадресным штормом). После выбора типа шторма ниже в том же окне доступно выпадающее меню, позволяющее включить (*Enable*) или выключить (*Disable*) опцию управления этим видом шторма.
Action	Данное поле позволяет выбрать метод управления трафиком. Доступны следующие опции: *shutdown* – Для обнаружения пакетного шторма будет использоваться программный механизм управления трафиком. При обнаружении шторма порт будет закрыт для всех пакетов, кроме STP BPDU-пакетов, используемых для функционирования покрывающего дерева коммутатора. Если по истечении времени countdown пакетный шторм продолжается, порт переходит в режим Shutdown Forever и не будет работать, пока пользователь не введет вручную команду **config ports enable** или по истечении 5 мин режим Shutdown Forever сменится режимом Auto- Recovery. При выборе данной опции необходимо особенное внимание уделить настройке временного интервала. *drop* – Для обнаружения пакетного шторма будет использоваться аппаратный механизм управления трафиком. При этом пакетный шторм будет определяться аппаратным обеспечением коммутатора на основании превышения заданного порога, и пакеты пудут отбрасываться до тех пор, пока шторм не прекратится.
Group List	Укажажите группу портов, которые моут быть включены вручную после перехода в состояние Shutdown.
Threshold	Данное поле задает максимальное количество пакетов в секунду, при котором будет запущена функция управления трафиком. Данный параметр может принимать значение 0-255000. При этом по умолчанию задано 128000.
Time Interval	Это поле позволяет задать временной интервал, через который микросхема коммутатора будет предоставлять данные по количеству многоадресных и широковещательных пакетов для надлежащей работы функции управления трафиком. Эти данные будут опередеяющим фактором при принятии решения о том, что число входящих пакетов превысило пороговую величину. Этот интервал может принимать значения от 5 до 30 с (по умолчанию 5 с).
Count Down	Таймер Count Down позволяет определить время в минутах, в течение которого Коммутатор не будет закрывать порт, на котором обнаружен пакетный шторм. Этот параметр имеет значение только для портов, настроенных со значением **Shutdown** в поле **Action,** т.е. при использовании программной функции управления трафика. Допустимые значения в данном поле 0, 5-30 с. По умолчанию задано 0, что означет, что порт никогда не будет переходить в состояние shutdown.

Примечание: Порты, находящиеся в режиме Shutdown forever, получат статус Discarding в концепции Spanning Tree, и BPDU-пакеты будут отправляться на CPU Коммутатора.

Примечание: Порты, находящиеся в режиме Shutdown Forever, будут показаны как порты, соединение с которыми отсутствует (link down) во всех окнах для настройки до тех пор, пока пользователь не включит эти порты вручную или по истечении 5 минут режим Shutdown Forever перейдет в режим Auto-Recovery (автоматическое восстановление).

Примечание: При настройке функции управления трафиком помните, что при выборе опции ***shutdown*** Коммутатор будет рассматривать Group List как отдельные порты. При выборе же в поле Action опции ***drop*** Коммутатор будет рассматривать Group list как группу портов. (Например, 1 будет означать порты с 1 по 8, 2 - порты 9-16 и т.д.)

На Коммутаторе доступны следующие группы портов при выборе опции drop в поле **Action**:
Group 1 – включает порты 1-8.
Group 2 – включает порты 9-16.
Group 3 – включает порты 17-24.
Group 4 – включает порты 9-16 (для DES-3550) и порт 25 Gigabit Ethernet (для DES-3526).
Group 5 – включает порты 33-40 (DES-3550) и порт 26 Gigabit Ethernet (DES-3526).
Group 6 – включает порты 41-48 (только для DES-3550).
Group 7 – включает порт 49 Gigabit Ethernet (только для DES-3550).
Group 8 - включает порт 50 Gigabit Ethernet (только для DES-3550).

Port Security (Безопасность на урове 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.

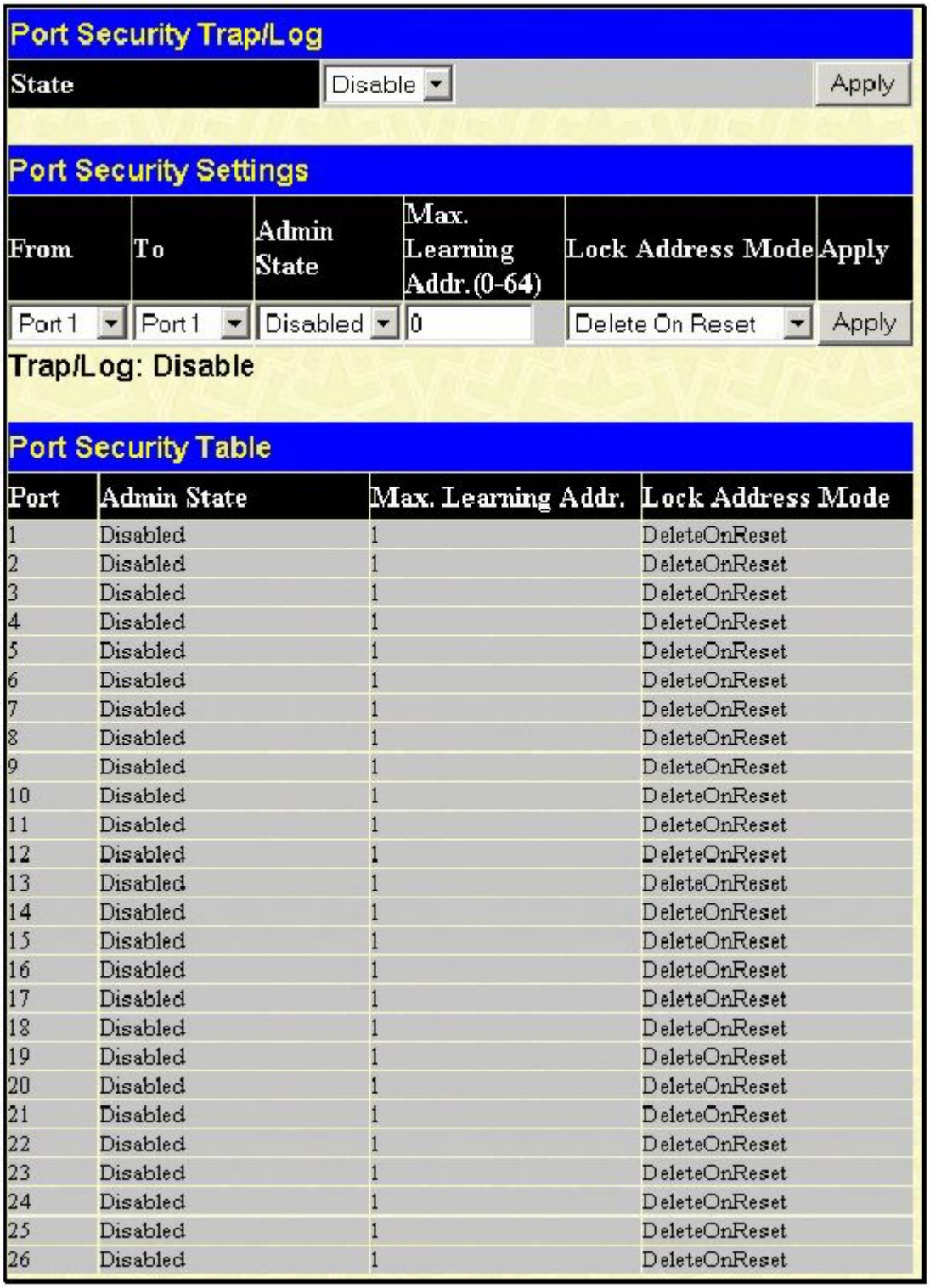


Рисунок 6- 49. Окно Port Security Settings

Могут быть установлены следующие параметры:

Параметр	Описание
Port Security Trap/Log	
State	Данное выпадающее меню позволяет включить (enable) или выключить (disable) отправку сообщений (trap) в журнал коммутатора или на SNMP-менеджер.
Port Security Settings	
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. (0-64)	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.

Для принятия настроек надо кликнуть **Apply**.

QoS

Для обеспечения надлежащего качества обслуживания(QoS) коммутаторы серии DES-3500 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-3500.

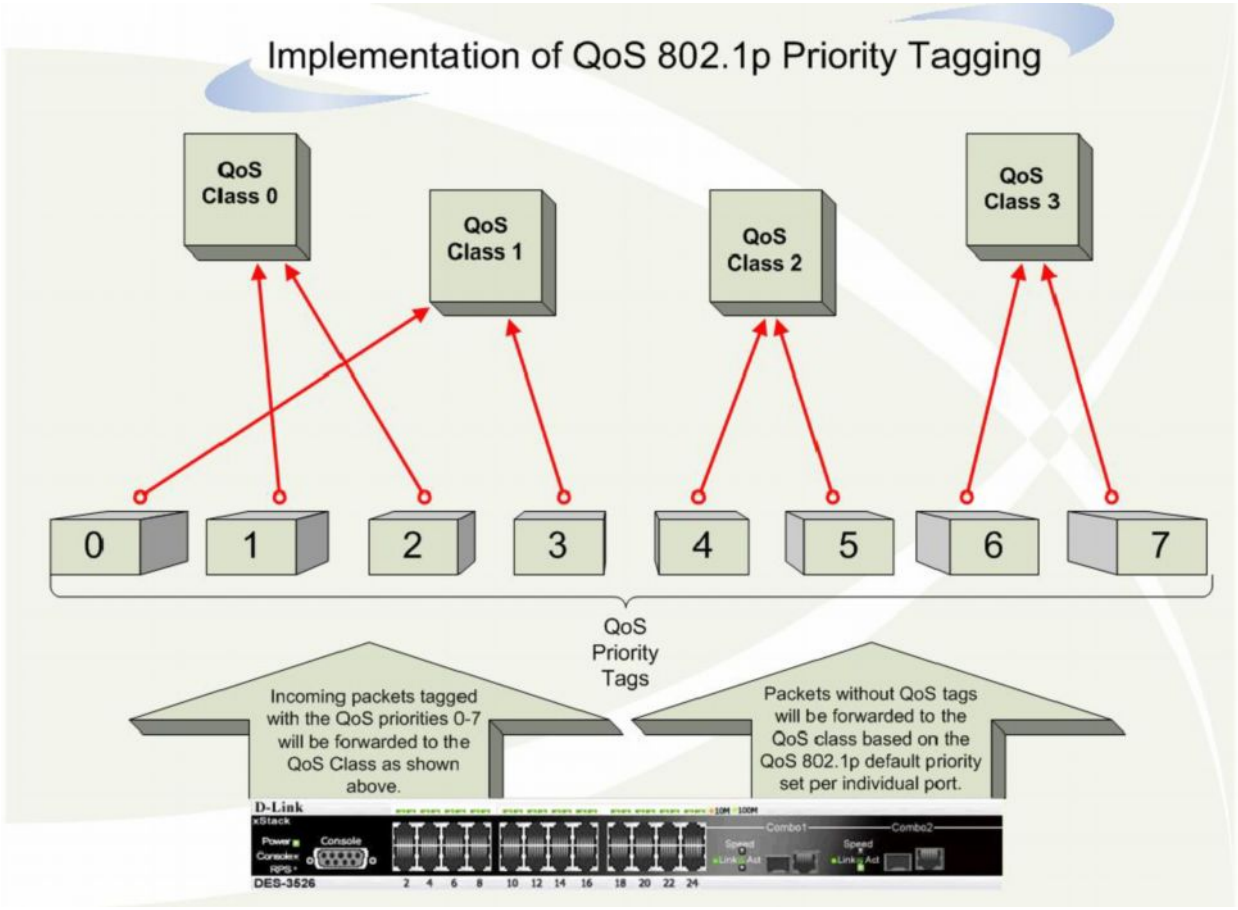


Рисунок 6- 50. Распределение очередей QoS на Коммутаторе

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 видео-данных обеспечивают оптимальное использование полосы пропускания, доступной для видео-конференции.

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-3500 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 кликните по **Port Bandwidth** в папке **Configuration:**

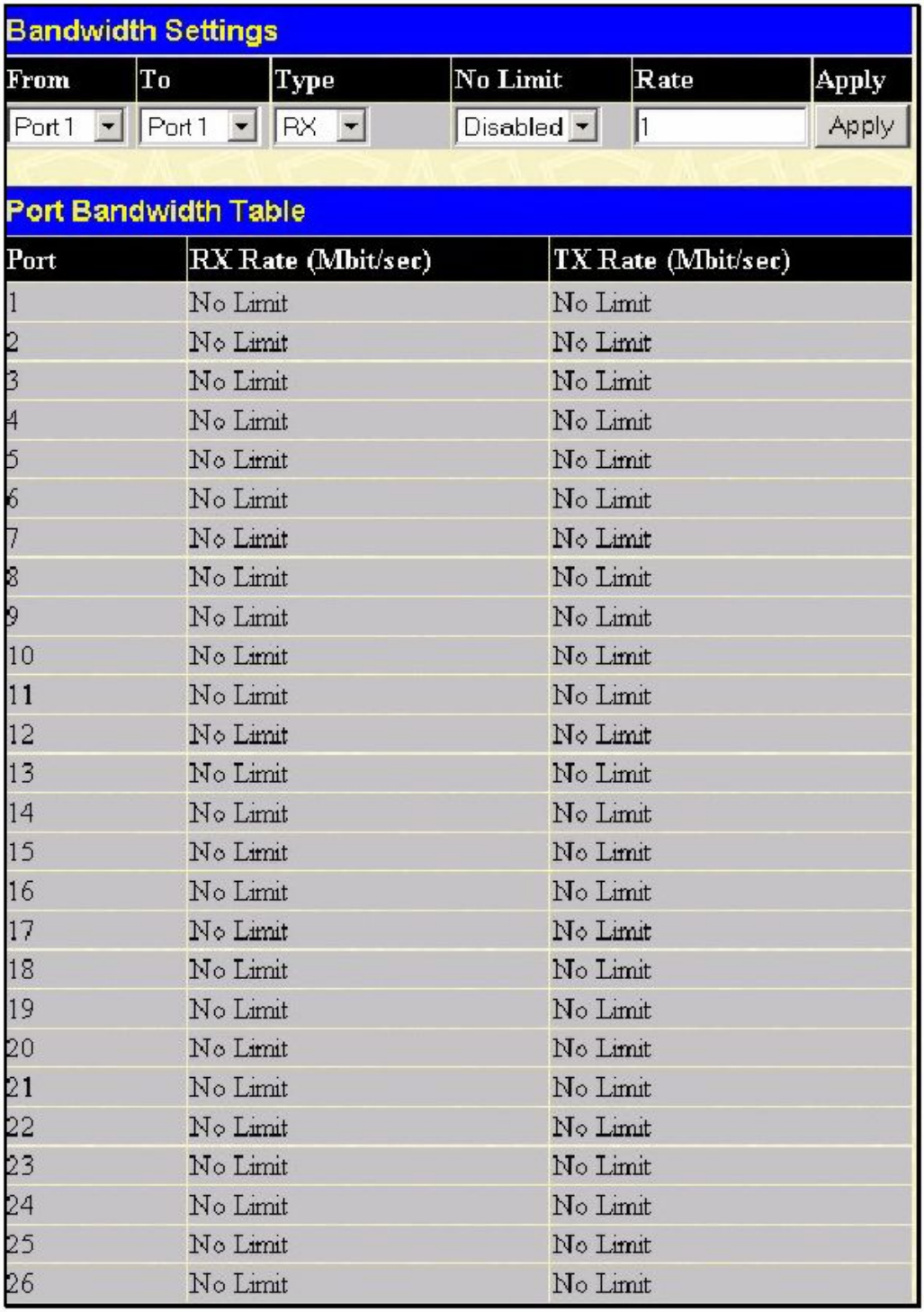


Рисунок 6- 51. Окно Bandwidth Settings

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 *Enable*.
Rate	Данное поле позволяет ввести максимальную скорость в Мбит/с для выбранных портов.

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

Работа по расписанию

Изменение расписания аппаратных очередей Коммутатора позволяет настроить QoS 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 **QoS** в папке **Configuration** и кликните по **QoS Output Scheduling**.

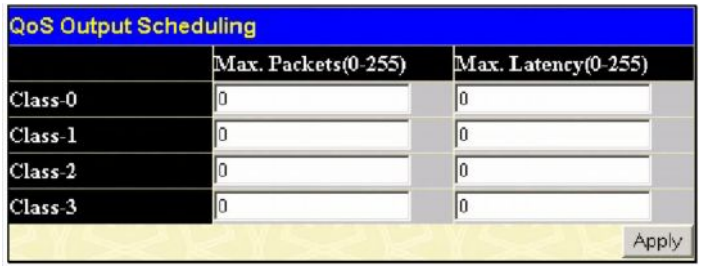


Рисунок 6- 52. Окно QoS Output Scheduling

Следующие параметы доступны для настройки:

Параметр	Описание
Max. Packets (0-255)	Определяет максимальное количество пакетов в аппаратной очереди, которое может быть передано до того, как начнут обрабатываться пакеты из очереди низшего приоритета. Диапазон значений в данном поле от 0 до 255.
Max. Latency (0-255)	Определяет максимальное время обработки пакетов для аппаратной очереди до того, как начнут обрабатываться пакеты из очереди низшего приоритета. Диапазон значений от 0 до 255. Это значение, умноженное на 16 мс, показывает максимальное время, отведённое очереди на передачу пакетов. Например, значение 3 означает 3x16=48мс. Очередь будет передавать пакеты до тех пор, пора не истечёт это время.

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

Примечание: Здесь параметры назначаются для очередей с номерами от 0 до 7: эти номера представляют теги приоритета, определенные стандартом IEEE 802.1p. Не путайте, пожалуйста, эти настройки с номерами портов.

Приоритет 802.1p по умолчанию

Коммутатор позволяет назначить каждому порту приоритет по умолчанию 802.1p. Для просмотра окна, показанного правее, следует открыть папку **Configuration**, затем открыть папку **QoS** и кликнуть по **802.1p Default Priority**. Данное окно позволяет задать приоритет 802.1p по умолчанию для любого передающего порта Коммутатора. Приоритеты нумеруются от 0 – низший приоритет до 7 – наивысший приоритет. Для применения выполненных настроек следует кликнуть по **Apply**.

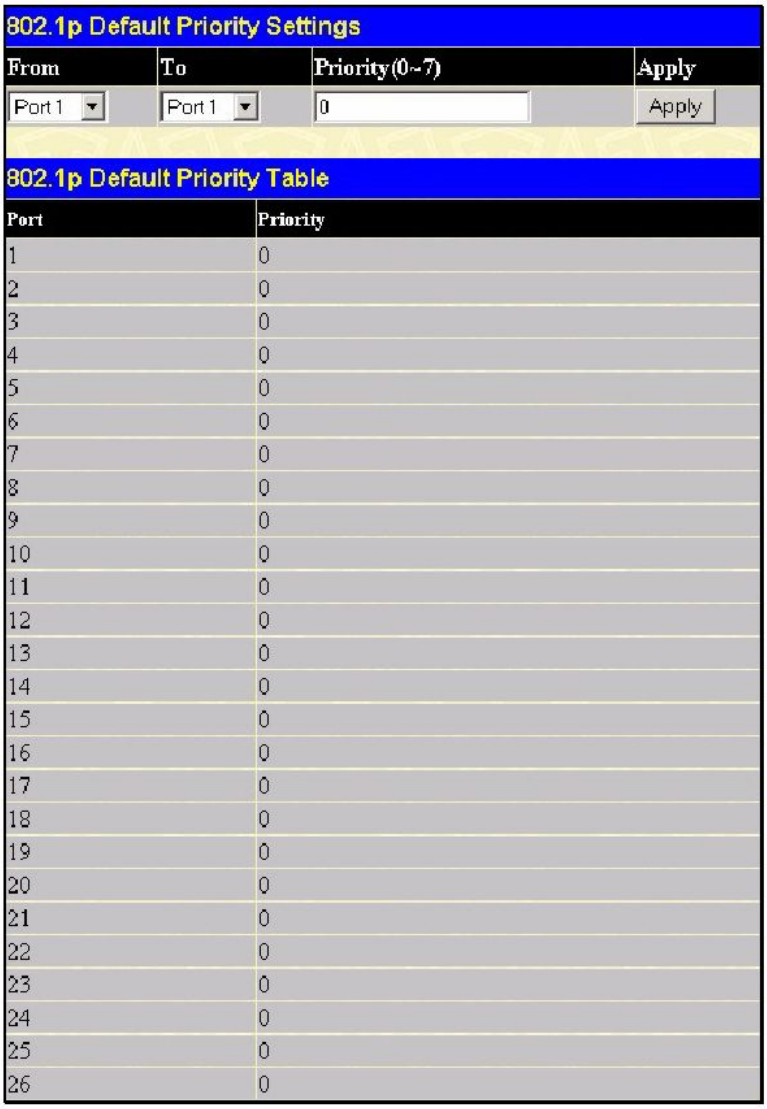


Рисунок 6- 53. Окно 802.1p Default Priority Settings

Приоритет пользователя 802.1p

Коммутатор серии DES-3500 поддерживают назначение приоритета пользователя приоритетам 802.1p. Для работы со следующим окном необходимо открыть в папке **Configuration** папку **QoS**, а затем кликнуть по **802.1p User Priority.** Назначив приоритет групп портов Коммутатора, можно назначить также приоритетам 802.1p соответствующий Class. Для принятия настроек следует кликнуть по **Apply**.

Рисунок 6- 54. Окно QoS Class of Traffic

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.

Для работы с окном, представленным ниже, следует в папке **Configuration** открыть папку **QoS** и кликнуть по **Traffic Segmentation.**

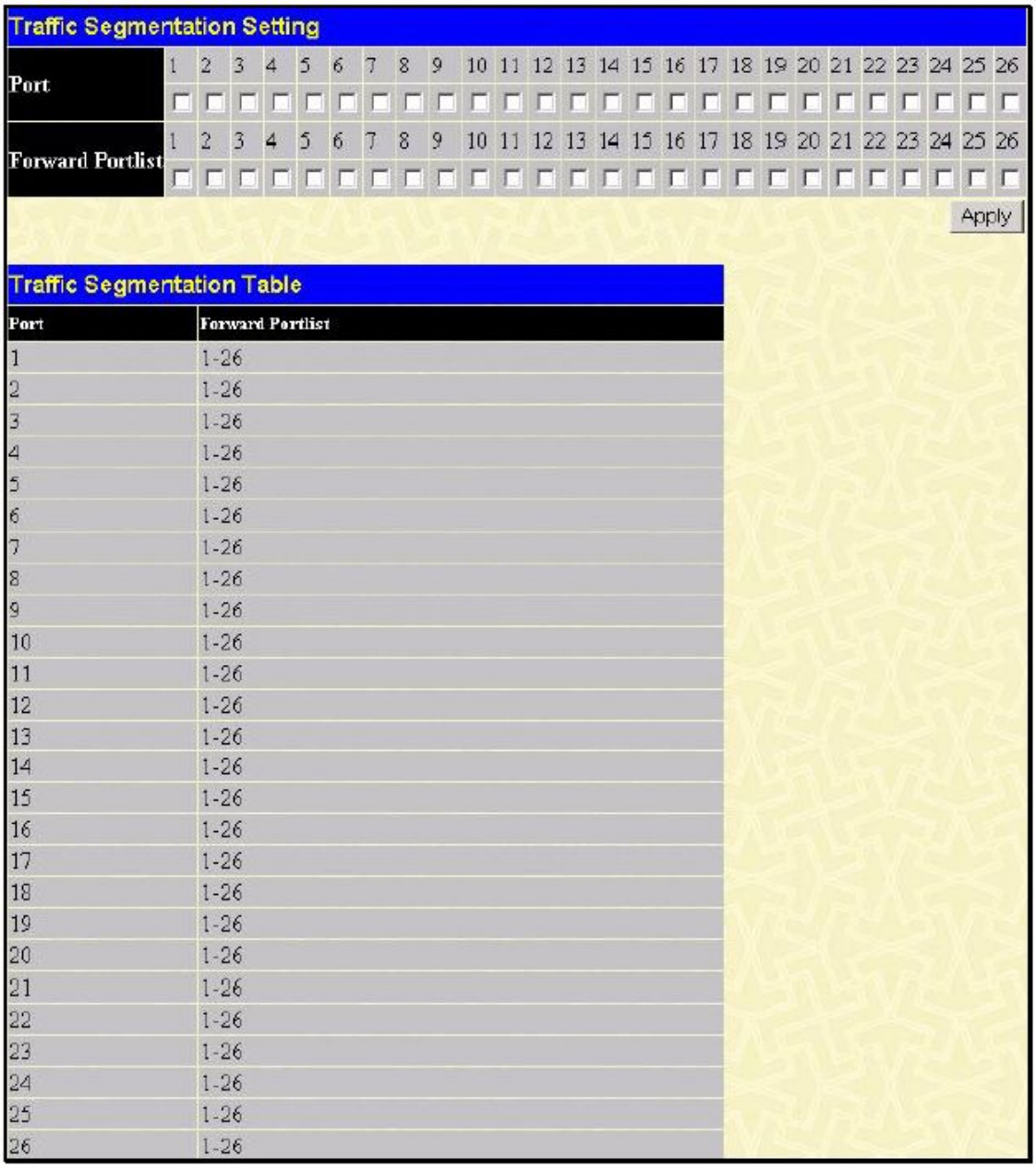


Рисунок 6- 55. Окно Traffic Segmentation Setting

Эта страница позволяет задать комбинацию передающего порта и принимающих портов Коммутатора. Для настройки доступны следующие параметры:

Параметр	Описание
Port	Отметьтьте галочкой соответствующие порты.
Forward Portlist	Отметьте порты Коммутатора, которые смогут взаимодействовать с портами указанными в предыдущем поле.

Кликните по кнопке **Apply, чтобы** добавить комбинацию принимающих и передающих портов в **Traffic Segmentation Table** (таблицу сегментации трафика Коммутатора).

Задание уровня проблемы для отправки сигнала предупреждения

Коммутаторы серии DES-3500 позволяют задать уровень проблемы для отправки сигналов предупреждений. Сообщения предупреждения могут заноситься в системный журнал и/или отправляться в виде SNMP-сигналов (trap). Уровень проблемы, при котором отправляется сигнал предупреждения, может варьироваться. Для его настройки используется меню **System Severity Settings**. Текущие настройки показаны в том же окне.

Примечание: В Приложении C к данному Руководству приводится подробная информация о возможных вариантах записей системного журнала.

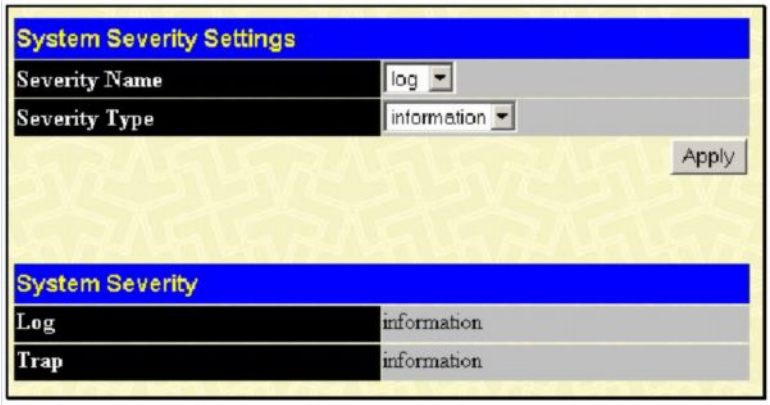


Рисунок 6- 56. System Severity Settings

Для конфигурации параметров, описанных ниже, используется выпадающее меню.

Параметр	Описание
Severity Name	С помощью выпадающего меню выберите, какой вид предупреждения будет использоваться. Значение *log* используется для записи сообщений в системный журнал. Значение *trap* используется для посылки SNMP-сообщений (Trap). Значение *all* – для записи в системный журнал и посылки SNMP-сообщений (Trap).
Severity Type	Определяется, при каком уровне проблемы будут передаваться сигналы предупреждения. Значение *critical* – определяет передачу сигналов предупреждения только при возникновении критических проблем. Значение *warning* – определяет передачу сигналов предупреждения при возникновении критических проблем, а также для предостережения от их возникновения. При значении *information* – определяет передачу сигналов предупреждения при любых событиях на Коммутаторе.

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

Системный журнал

Коммутатор позволяет задать до четырех серверов, на которые будут отправляться системные сообщения. Для работы с окном System Log Servers необходимо кликнуть по **System Log Server** в папке **Configuration**.

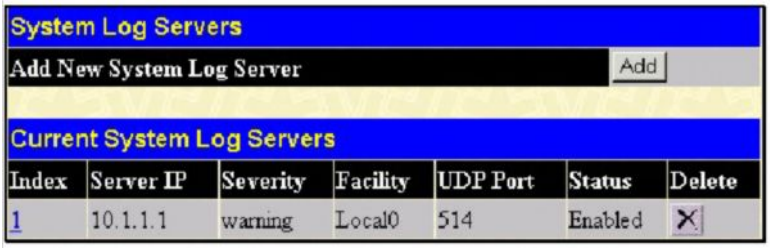


Рисунок 6- 57. Окно System Log Servers

Параметры, которые необходимо ввести в окне **System Log Server** при редактировании настроек и для добавления новых серверов**,** одинаковы. Описание этих параметров представлено в таблице ниже.

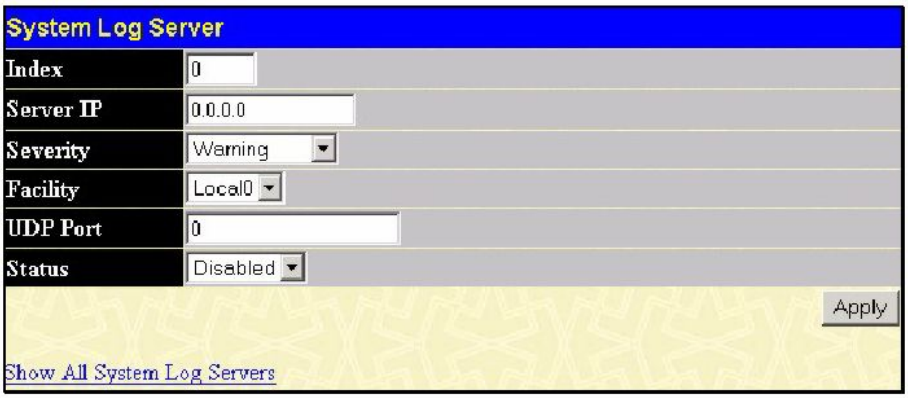


Рисунок 6- 58. Окно System Log Server – добавить

Параметр	Описание
Index	Номер (1-4) сервера, на котором расположен системный журнал (Syslog-сервер).
Server IP	IP-адрес Syslog-сервера.
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: 0- сообщения ядра 1- сообщения пользовательского уровня 2- почтовая система 3- системные демоны 4- сообщения безопасности/авторизации 5- сообщения, генерируемые внутри системы подсистемой syslog line printer

	7- подсистема сетевых новостей 8- подсистема UUCP 9- демон часов 10- сообщения безопасности/авторизации 11- FTP-демон 12- подсистема NTP 13- Аудит журнала регистрации 14- Предупреждение журнала регистрации 15- демон часов **16- локальное использование 0(local0)** **17- локальное использование 1(local1)** **18- локальное использование 2(local2)** **19- локальное использование 3(local3)** **20- локальное использование 4(local4)** **21- локальное использование 5(local5)** **22- локальное использование 6(local6)** **23-локальное использование 7(local7)**
UDP Port (514 or 6000-65535)	В данном поле указывается номер UDP-порта, использующегося для отправки системных сообщений. Значение по умолчанию 0.
Status	Данное поле используется для включения *(Enabled)* или выключения *(Disabled)* соответствующего сервера.

Для применения настроек System Log Server необходимо кликнуть по **Apply**. Для удаления записи из окна **System Log Server** следует кликнуть по соответствующей ***X*** под надписью Delete. Чтобы вернуться в окно **Current System Log Servers,** кликните по Show All System Log Servers.

Настройки SNTP

Настройка времени

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

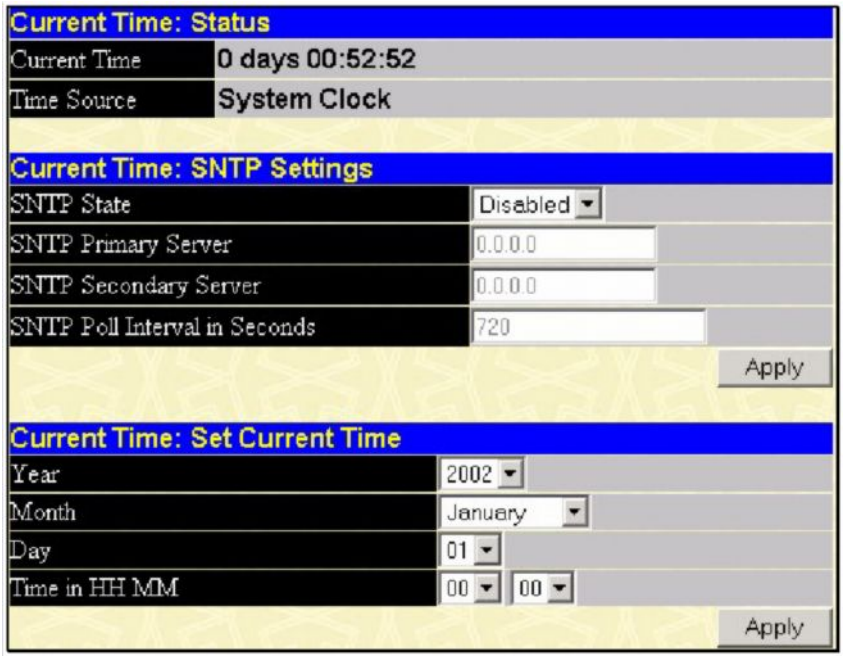


Рисунок 6- 59. Окно Current Time: Status

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

Параметр	Описание
Current Time: Status	
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**

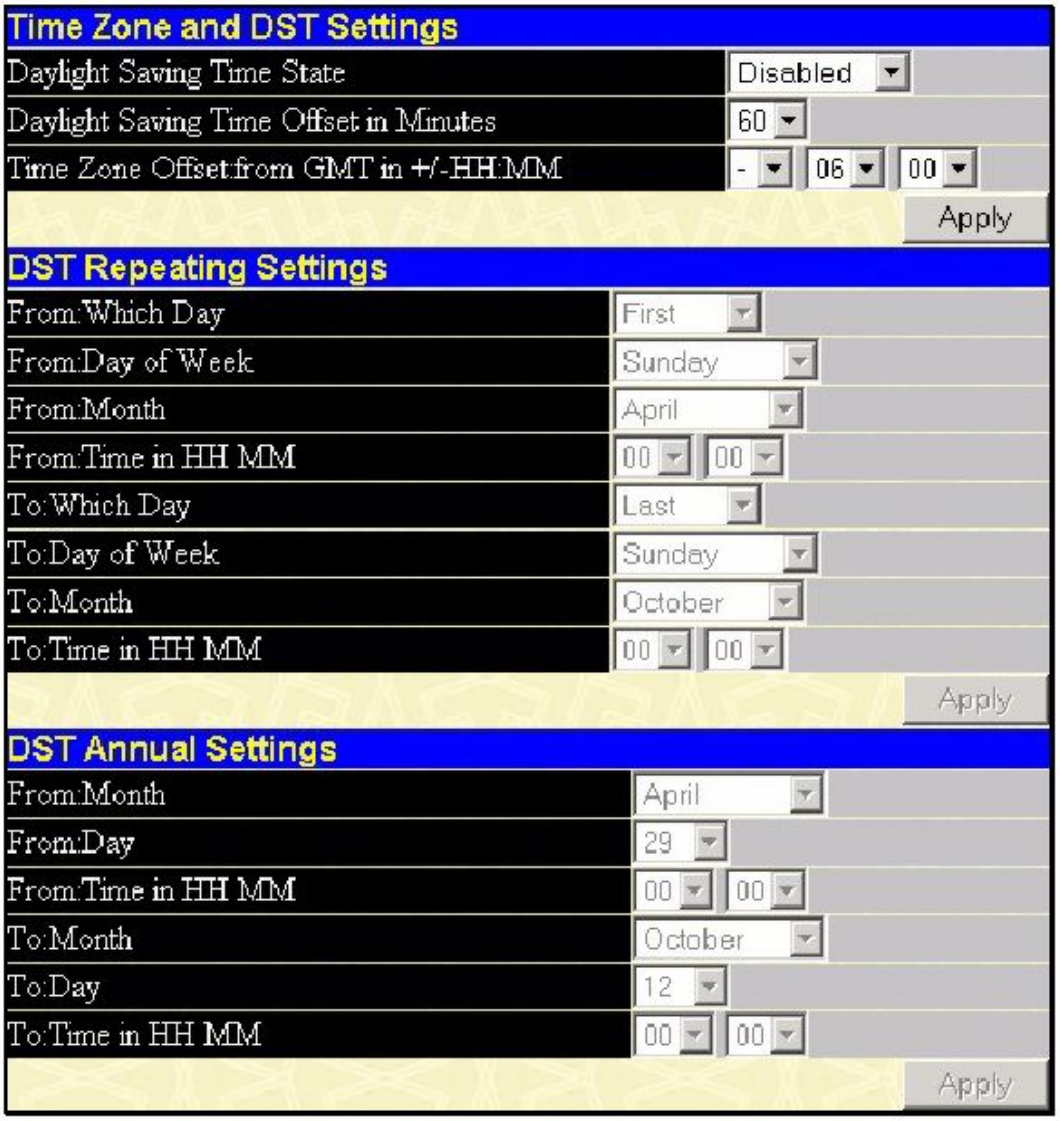


Рисунок 6- 60. Окно Time Zone and DST Settings

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**.

Таблица профилей доступа

Настройка таблицы профилей доступа

Профили доступа позволяют задать критерии для принятия решения о продвижении или отрасывании пакетов, основываясь на информации, содержащейся в заголовке пакетов.

Примечание: Начиная с версии программного обеспечения 3, был изменен механизм обработки профилей доступа. Существуют некоторые ограничения в использовании профилей доступа на Коммутаторе. Для получения более подробной информации по изменениям и ограничениям в использовании профилей доступа обратитесь к разделу, касающемуся списков управления доступом (ACL), в Руководстве по использованию интерфейса командной строки CLI.

Создание профиля доступа, по большому счету, 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.

Для просмотра текущей конфигурации профилей доступа Коммутатора откройте папку **Configuration** и кликните по ссылке **Access Profile Table.** В результате откроется окно, представленное ниже:

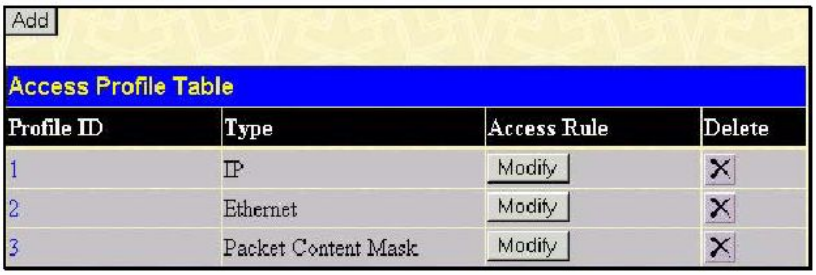


Рисунок 6- 61. Окно Access Profile Table

Для добавления записи в **Access Profile Table** следует кликнуть по кнопке **Add,** в результате чего откроется окно **Access Profile Configuration,** показанное ниже. На Коммутаторе предусмотрено три окна **Access Profile Configuration**: одно для настройки профиля Ethernet (на основе MAC-адресов), одно для настройки профиля на основе IP-адресов и одно для настройки профиля на основе маски содержимого пакета. Переключение между тремя выпадающими окнами **Access Profile Configuration** осуществляется с помощью выпадающего меню. Ниже показано окно **Access Profile Configuration**, предназначенное для настройки профиля Ethernet.

Примечание: Коммутатор поддерживает создание до 9 профилей доступа, диапазон идентификаторов которых от 1 до 255. ID профиля помимо уникальной идентификации профиля служит своего рода приоритетом в случаях, когда правила одного профиля вступают в противоречие с правилами другого профиля. Для получения более подробной информации, пожалуйста, обратитесь к главе, касающейся команд для списков управления доступом (ACL), в Руководстве по использованию интерфейса командной строки CLI.

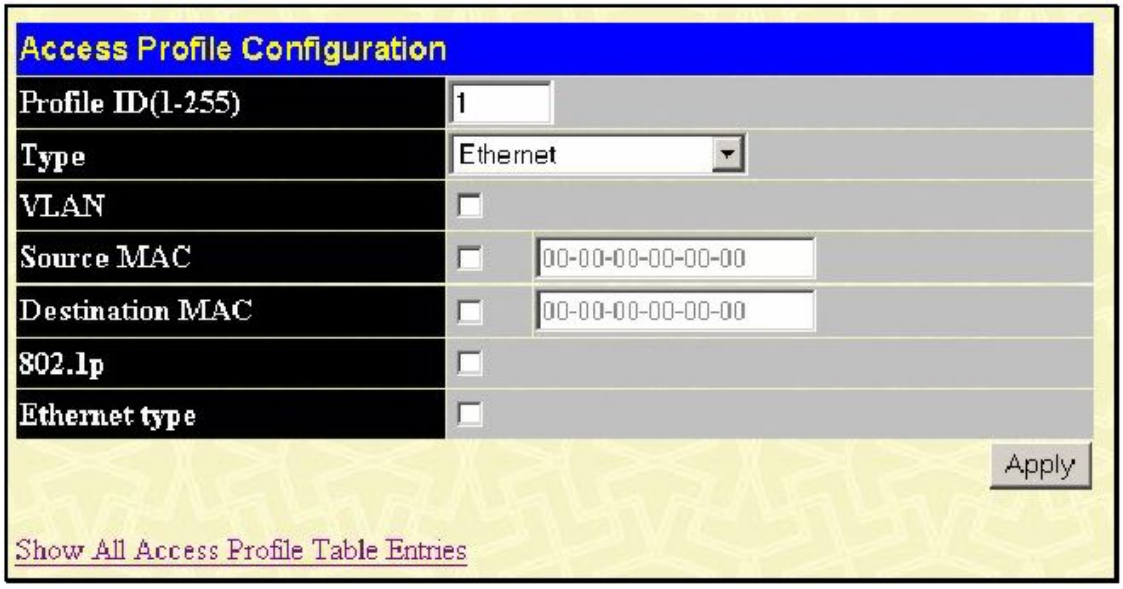


Рисунок 6- 62. Окно Access Profile Configuration (Ethernet)

При выборе в поле Type значения Ethernet могут быть настроены следующие параметры:

Параметр	Описание
Profile ID (1-255)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Идентификатор профиля также используется в качестве приоритета профиля. Причем чем ниже этот идентификатор, тем выше приоритет. Учет приоритета профиля позволяет разрешить конфликт между правилами доступа различных профилей. Значение этого поля может быть от 1 до 255, однако, как отмечалось ранее, количество создаваемых профилей ограничивается 9 профилями.

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. 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 будет проверять значение поля Ethernet type в каждом заголовке пакетов.

Ниже представлено окно **Access Profile Configuration** для настройки профилей на основе IP-адресов.

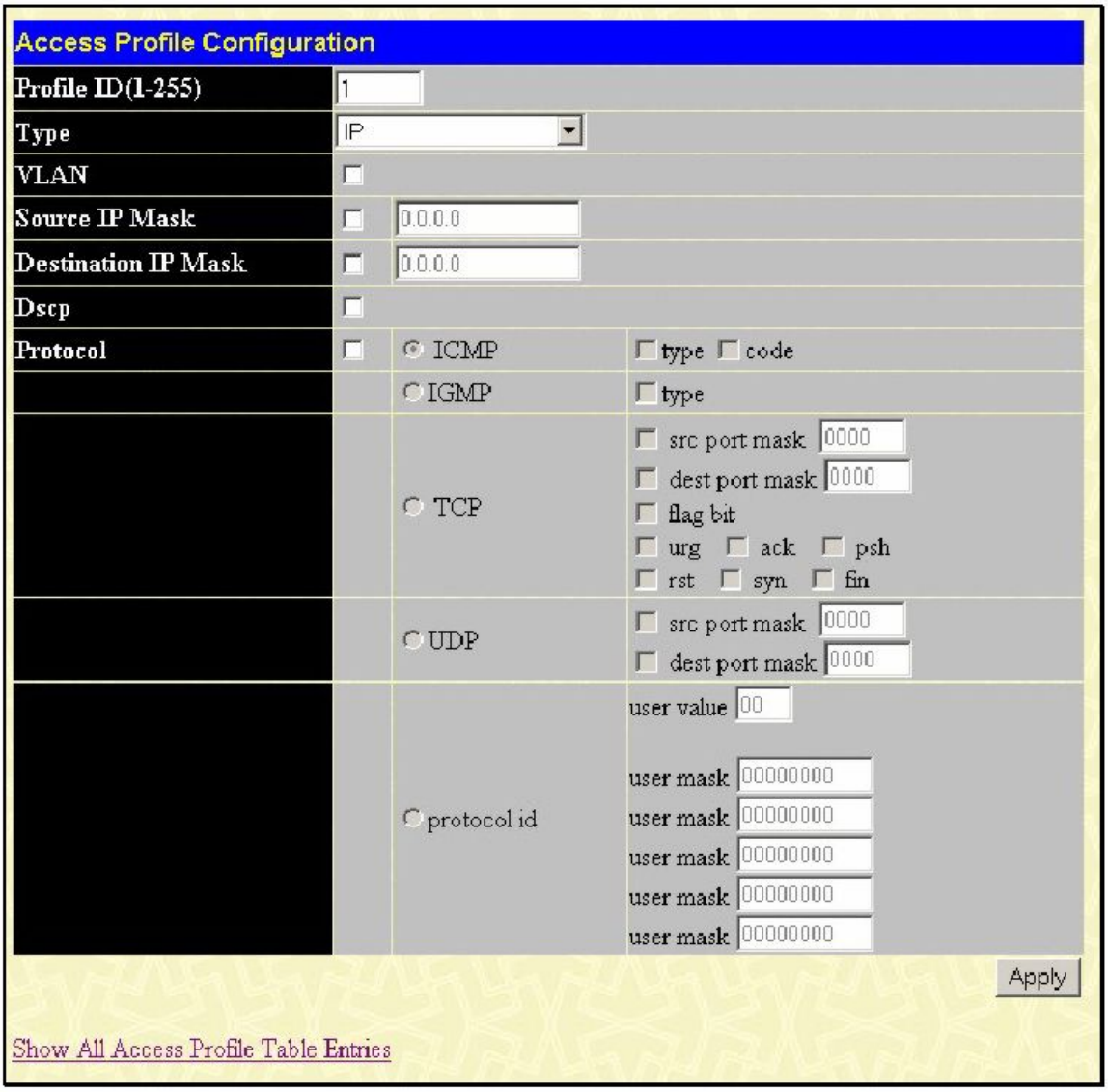


Рисунок 6- 63. Окно Access Profile Configuration (IP)

При выборе в поле Type значения IP могут быть настроены следующие параметры:

Параметр	Описание
Profile ID (1-255)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Идентификатор профиля также используется в качестве приоритета профиля. Причем чем ниже этот идентификатор, тем выше приоритет. Учет приоритета профиля позволяет разрешить конфликт между правилами доступа различных профилей. Значение этого поля может быть от 1 до 255, однако, как отмечалось ранее, количество создаваемых профилей ограничивается 9 профилями.
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. Именно этот вариант и будет

	рассмотрен в данной таблице. • 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 р 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* – идентификатор протокола, используемый для маски в заголовке

	пакета. Можно задать до 5 масок 4-го уровня для портов назначения в шестнадцатиричной форме (0x0-0xffffffff).

Ниже представлено окно **Access Profile Configuration** для настройки профилей на основе маски содержимого пакетов.

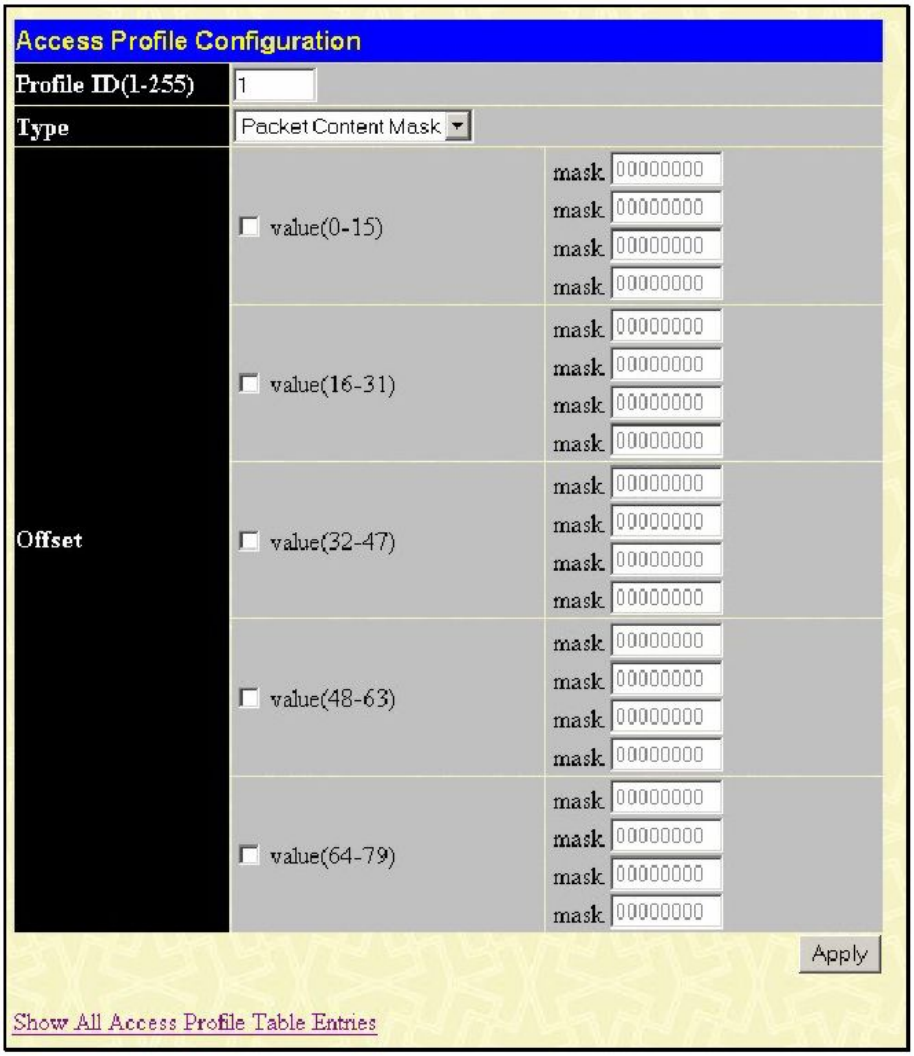


Рисунок 6- 64. Окно Access Profile Configuration window (Packet Content Mask)

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 (1-255)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Значение этого поля может быть от 1 до 255.
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. Именно этот вариант и будет рассмотрен в данной таблице.
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.

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

Чтобы установить правило для созданного ранее профиля доступа необходимо следующее:

В папке **Configuration** кликните по ссылке **Access Profile Table**, после чего откроется окно **Access Profile Table**. Под заголовком **Access Rule** кликните по кнопке **Modify,** после чего откроется следующее окно:

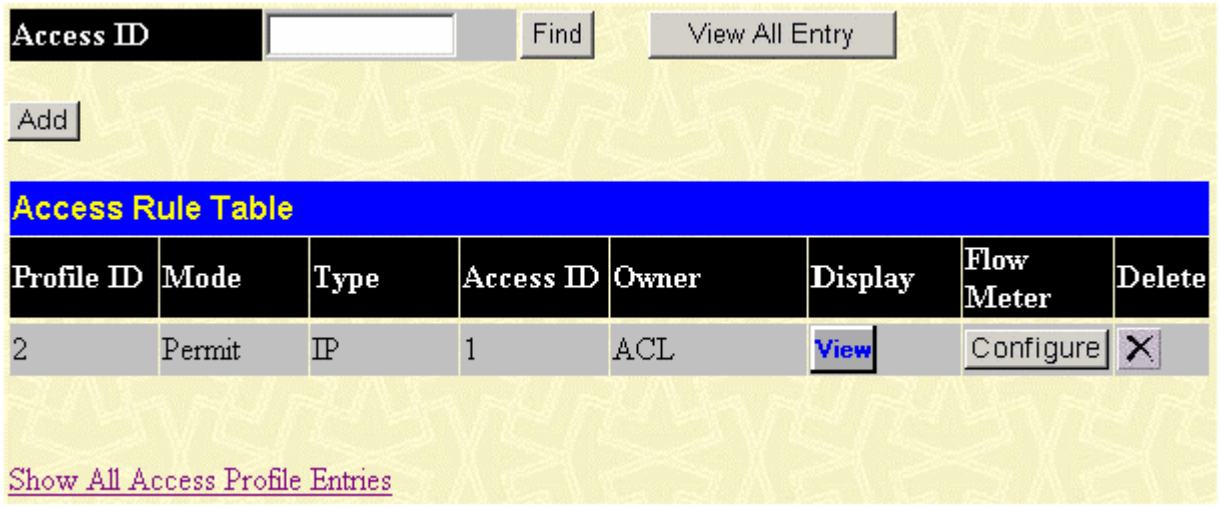


Рисунок 6- 65. Окно Access Rule Table

Для быстрого поиска настроек конкретного профиля доступа в верхней части экрана предусмотрен ввод ID. После ввода соответствующего значения и клика по кнопке **Find** настройки будут отображены. Пользователь может также отобразить все профили доступа, кликнув по кнопке **View All Entry**.

Чтобы создать новое правило для определенного профиля доступа, кликните по кнопке **Add**. Откроется новое окно. Для удаления ранее созданного правила необходимо кликнуть по соответствующей кнопке ***X.***

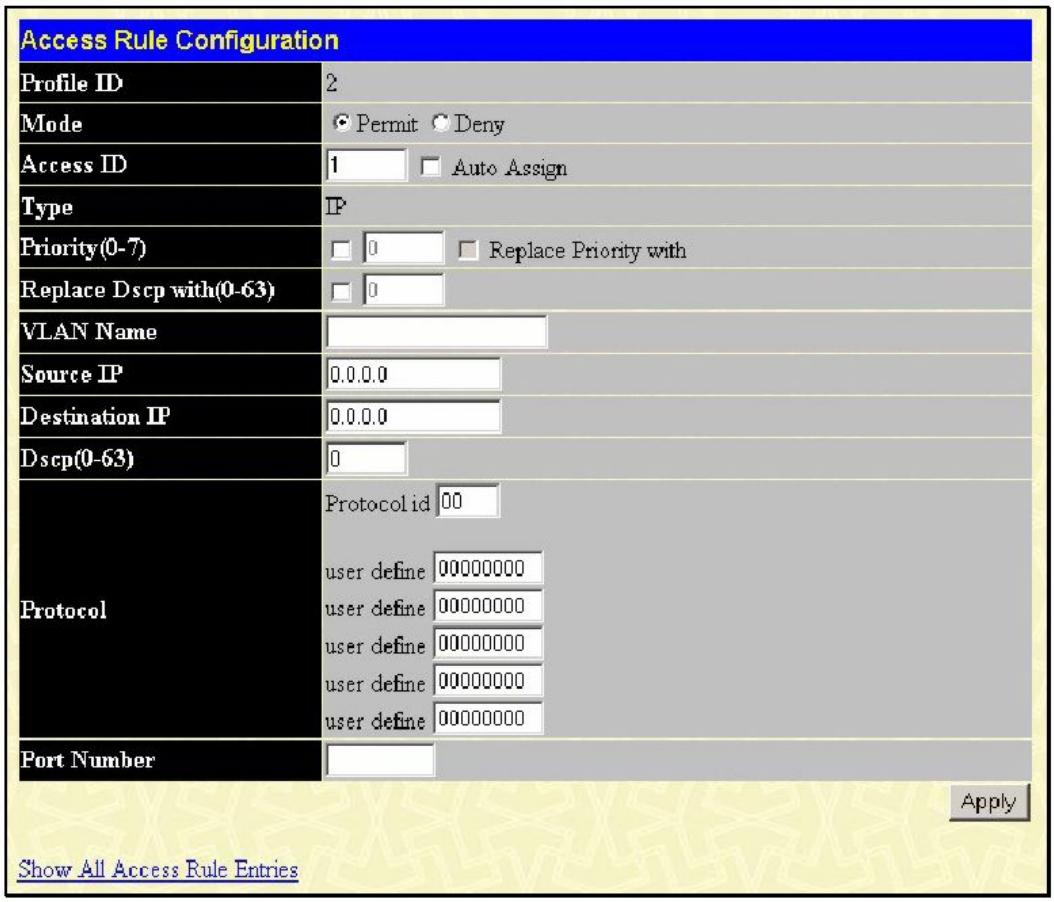


Рисунок 6- 66. Окно Access Rule Configuration (IP)

В этом окне пользователь может задать следующие параметры:

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 (1-65535)	Здесь следует ввести уникальный идентификационный номер. В данном поле могут быть установлены значения от 1 до 65 535. **Auto Assign** – выбор данной опции означает, что Коммутатор будет автоматически назначать идентифкатор доступа.
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.
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. *Replace Priority with* – поставьте галочку в данном поле, если необходимо заменить приоритет 802.1p, установленный по умолчанию, на значение поля **Priority (0-7)** перед отправкой пакетов, соответствующих заданному критерию, в очередь CoS. В противном случае пакеты будут со своим первоначальным 802.1p приоритетом. Для получения более подробной информации об очередях приоритетов, очередях CoS и распределении приоритетов 802.1p, следует обратиться к разделу QoS данного руководства.
Replace DSCP (0-63)	Данное поле позволяет ввести значение от 0 до 63, на которое будет заменяться исходное значение DSCP в пакетах, соответствующих выбранным критериям.
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.
Protocol	Данное поле дает возможность изменить протокол, используемый таблицей правил доступа, в зависимости от протокола, используемого для таблицы профилей доступа.
Port Number	Введите в данном поле номер(а) порта, к которому (-ым) будет применено правило.

Для просмотра правильно настроенного ранее правила, кликните по кнопке View в Access Rule Table, в результате появится следующее окно:

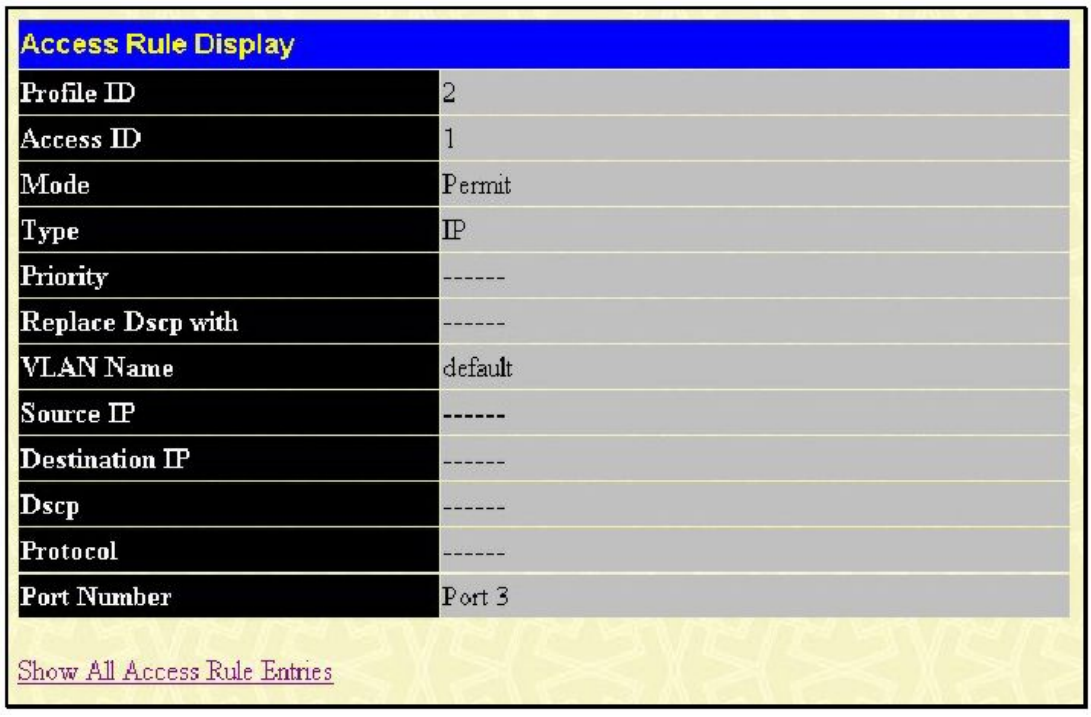


Рисунок 6- 67. Окно Access Rule Display (IP)

Кликните по кнопке Configure в показанном выше окне **Access Rule Table**. В результате откроется окно **ACL Meters Setting**, позволяющее ограничить полосу пропускания для входящего трафика. Когда пользователь создает ACL-правило для фильтрации пакетов, может быть создано также относящееся к данному ACL правило, ограничивающее трафик. При этом шаг настройки полосы пропускания для портов Fast Ethernet равен 1000Кбит/с, а для портов Gogabit Ethernet 8000Кбит/с. Имейте в виду, что не для всех правил ACL можно задать соответствующие правила, ограничивающие полосу пропускания.

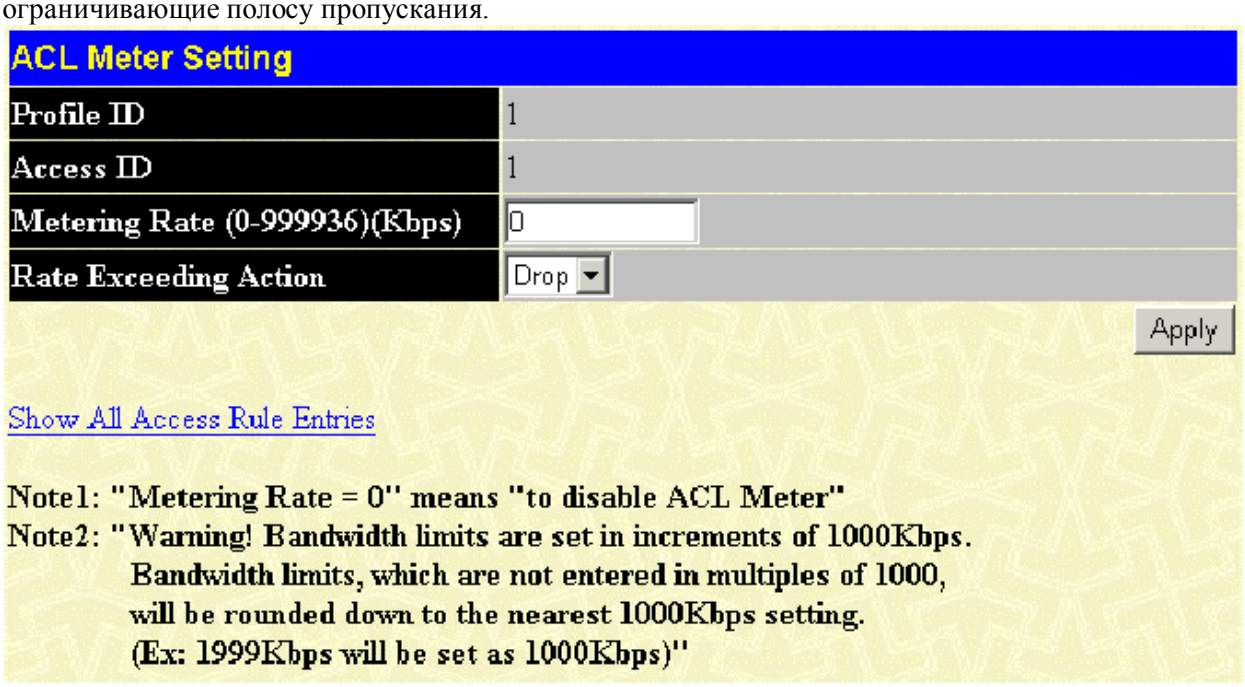


Рисунок 6- 68. Окно ACL Meter Setting (Настройка)

Для настройки правил доступа для профилей доступа на основе *Ethernet* откройте **Access Profile Table** и кликните по кнопке **Modify.** Откроется следующее окно:

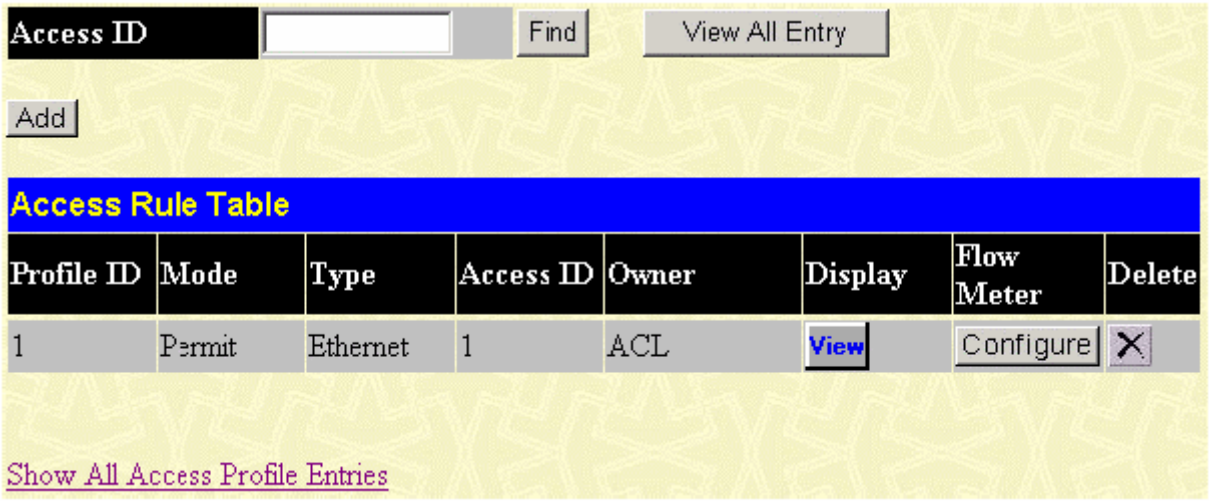


Рисунок 6- 69. Окно Access Rule Table (Ethernet)

Для быстрого поиска настроек конкретного профиля доступа в верхней части экрана предусмотрен ввод ID. После ввода соответствующего значения и клика по кнопке **Find** настройки будут отображены. Пользователь может также отобразить все профили доступа, кликнув по кнопке **View All Entry**.

Чтобы создать новое правило для определенного профиля доступа, кликните по кнопке **Add**. Откроется новое окно. Для удаления ранее созданного правила необходимо кликнуть по соответствующей кнопке ***X.***

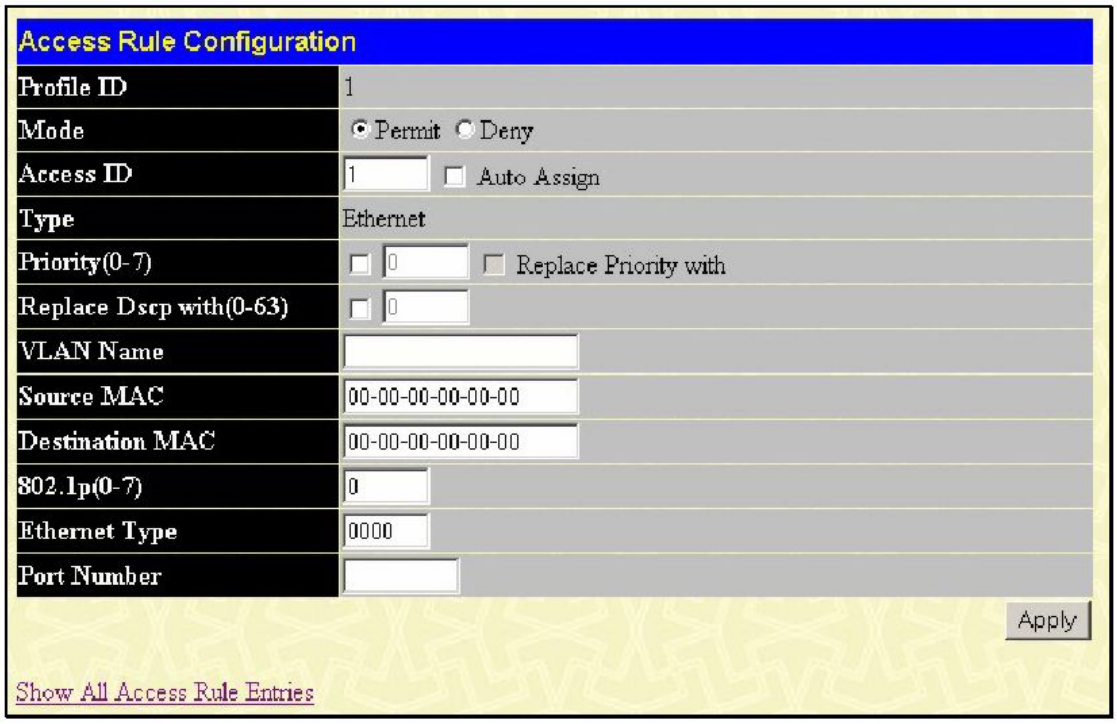


Рисунок 6- 70. Окно Access Rule Configuration (Ethernet)

Для настройки правила доступа для профиля доступа на основе Ethernet необходимо задать следующие параметры:

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 (1-65535)	Здесь следует ввести уникальный идентификационный номер. В данном поле могут быть установлены значения от 1 до 65 535. **Auto Assign** – выбор данной опции означает, что Коммутатор будет автоматически назначать идентифкатор доступа.
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.
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. *Replace Priority with* – поставьте галочку в данном поле, если необходимо заменить приоритет 802.1p, установленный по умолчанию, на значение

	поля **Priority (0-7)** перед отправкой пакетов, соответствующих заданному критерию, в очередь CoS. В противном случае пакеты будут со своим первоначальным 802.1p приоритетом. Для получения более подробной информации об очередях приоритетов, очередях CoS и распределении приоритетов 802.1p, следует обратиться к разделу QoS данного руководства.
Replace DSCP (0-63)	Данное поле позволяет ввести значение от 0 до 63, на которое будет заменяться исходное значение DSCP в пакетах, соответствующих выбранным критериям.
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.
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.
Protocol	Данное поле дает возможность изменить протокол, используемый таблицей правил доступа, в зависимости от протокола, используемого для таблицы профилей доступа.
Port Number	Введите в данном поле номер (а) порта, к которому (-ым) будет применено правило.

Для просмотра правильно настроенного ранее правила, кликните по кнопке View в Access Rule Table, в результате появится следующее окно:

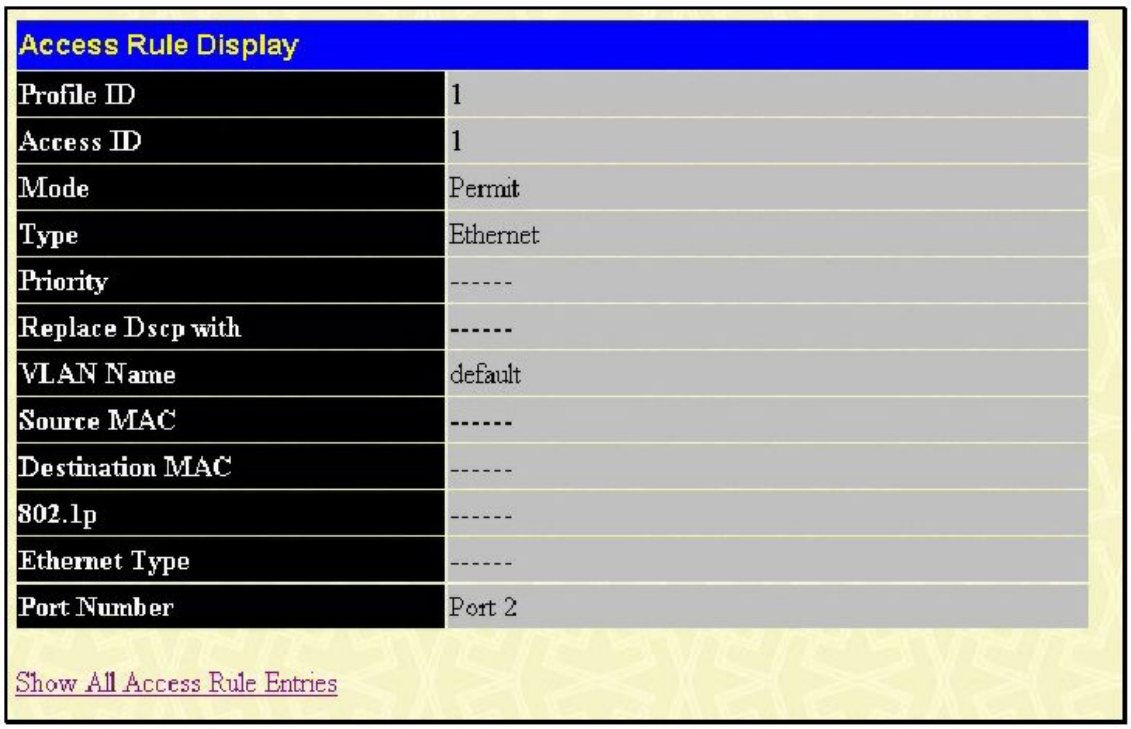


Рисунок 6- 71. Окно Access Rule Display (Ethernet)

Для настройки правил доступа (Access Rule) для профилей доступа на основе *Packet Content Mask* откройте окно **Access Profile Table** и кликните по кнопке **Modify.** Откроется следующее окно:

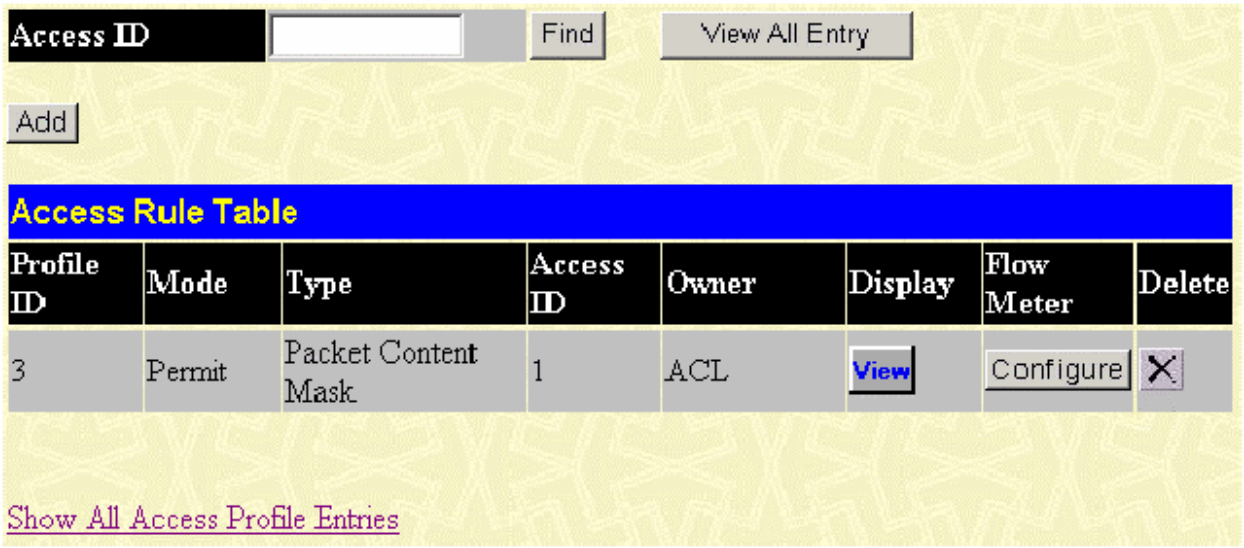


Рисунок 6- 72. Окно Access Rule Table (Packet Content Mask)

Для быстрого поиска настроек конкретного профиля доступа в верхней части экрана предусмотрен ввод ID. После ввода соответствующего значения и клика по кнопке **Find** настройки будут отображены. Пользователь может также отобразить все профили доступа, кликнув по кнопке **View All Entry**.

Чтобы создать новое правило для определенного профиля доступа, кликните по кнопке **Add**.Чтобы создать новое правило доступа необходимо кликнуть по кнопке **Add** в окне **Access Rule Table**, откроется окно **Access Rule Configuration:**

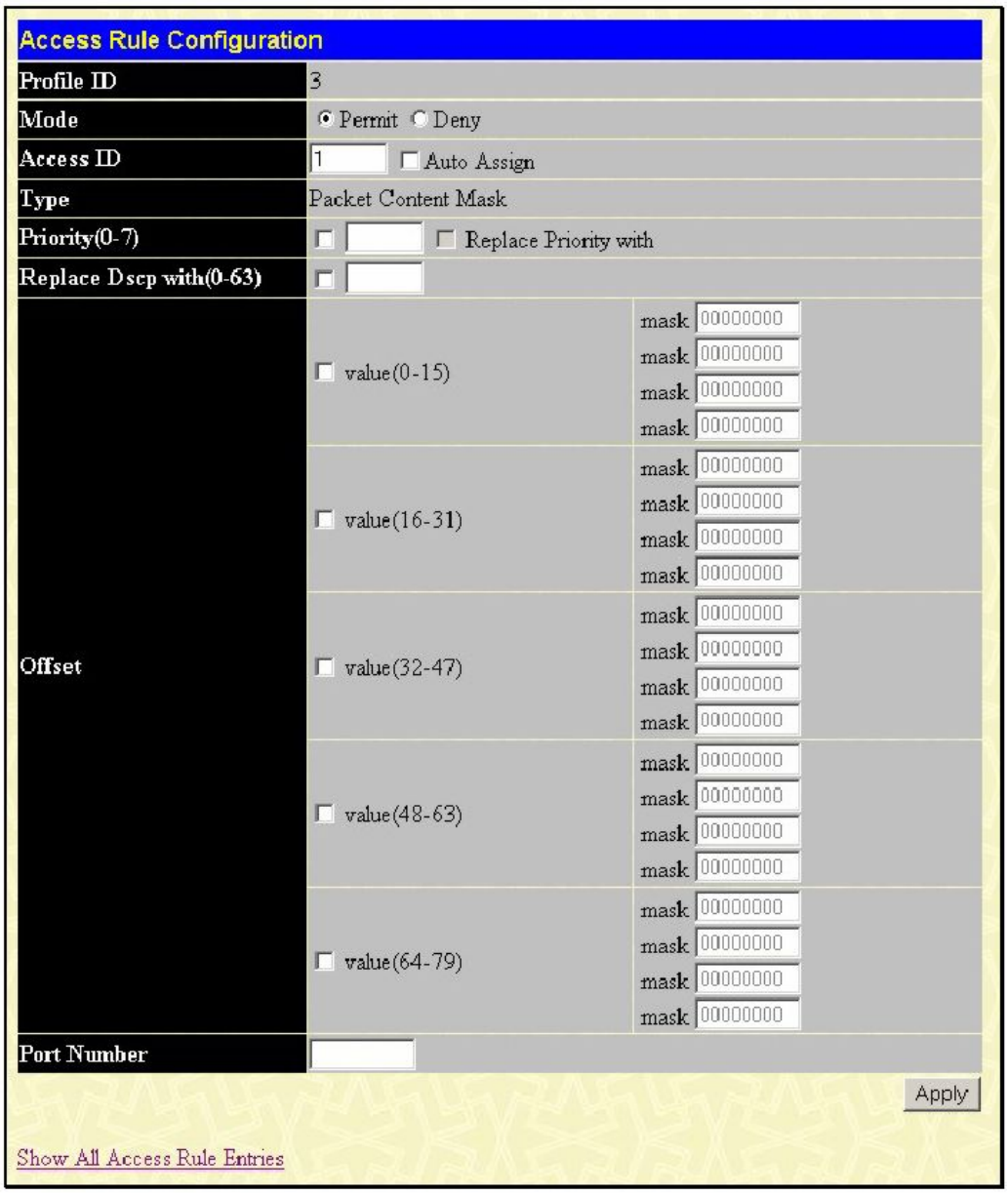


Рисунок 6- 73. Окно Access Rule Configuration (Packet Content Mask)

Для настройки правила доступа для профиля доступа на основе Packet Content Mask необходимо задать следующие параметры:

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 65 535. **Auto Assign** – выбор данной опции означает, что Коммутатор будет автоматически назначать идентифкатор доступа.
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.
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. *Replace Priority with* – поставьте галочку в данном поле, если необходимо заменить приоритет 802.1p, установленный по умолчанию, на значение поля **Priority (0-7)** перед отправкой пакетов, соответствующих заданному критерию, в очередь CoS. В противном случае пакеты будут со своим первоначальным 802.1p приоритетом. Для получения более подробной информации об очередях приоритетов, очередях CoS и распределении приоритетов 802.1p, следует обратиться к разделу QoS данного руководства.
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 Number	Введите в данном поле номер (а) порта, к которому (-ым) будет применено правило.

Для просмотра правильно настроенного ранее правила, кликните по кнопке 

в Access Rule Table, в результате появится следующее окно:

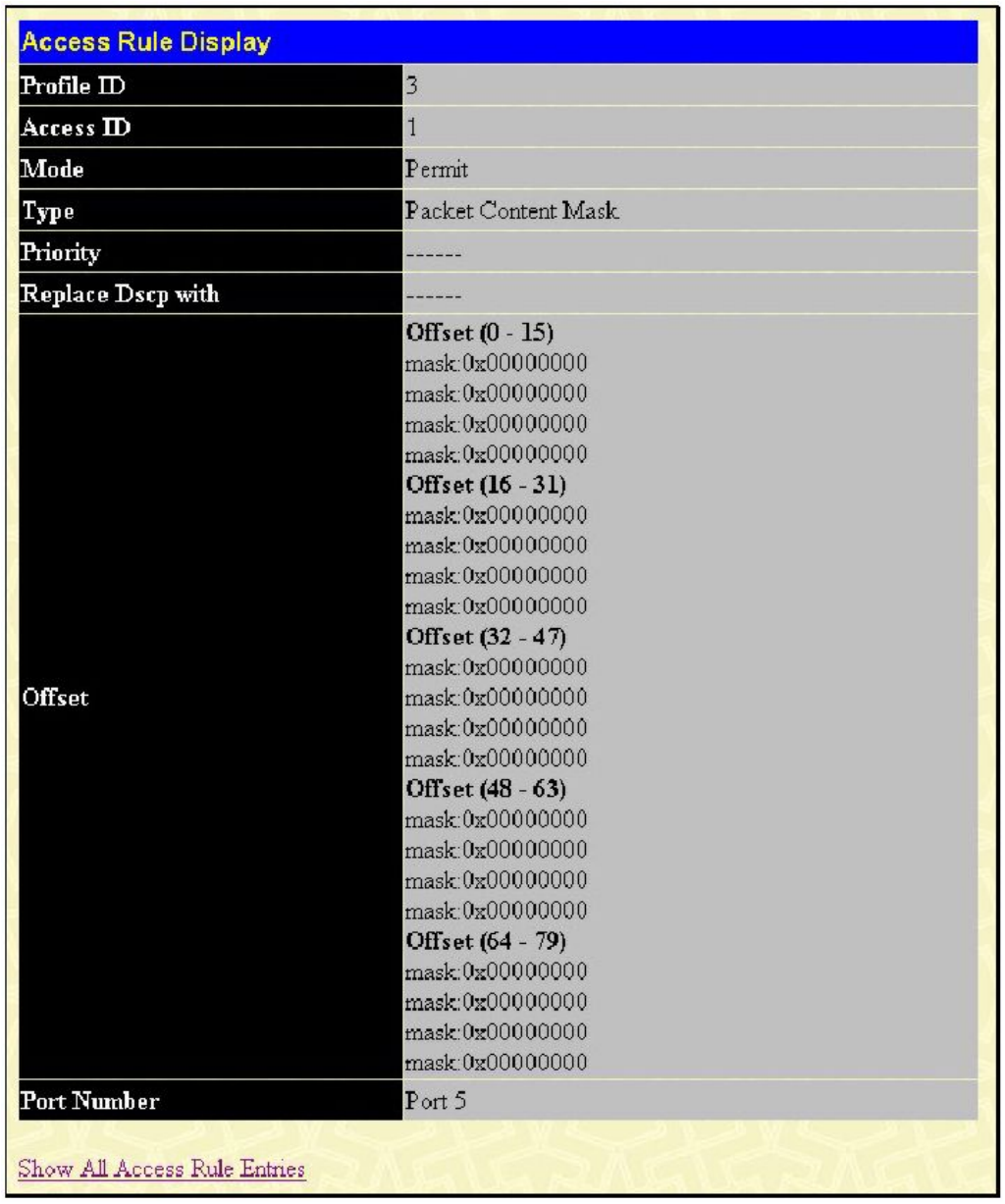


Рисунок 6- 74. Окно Access Rule Display (Packet Content)

CPU Interface Filtering

Коммутаторы серии xStack DES-3500 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 подзволяет 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.

Таблица профилей CPU Interface Filtering

Кликните по **Configuration** > **CPU Interface Filtering,** чтобы отобразить записи Таблицы профилей доступа CPU, созданные на Коммутаторе. Для просмотра настроек каждого профиля кликните по сслыке соответствующего идентификатора **Profile ID**.

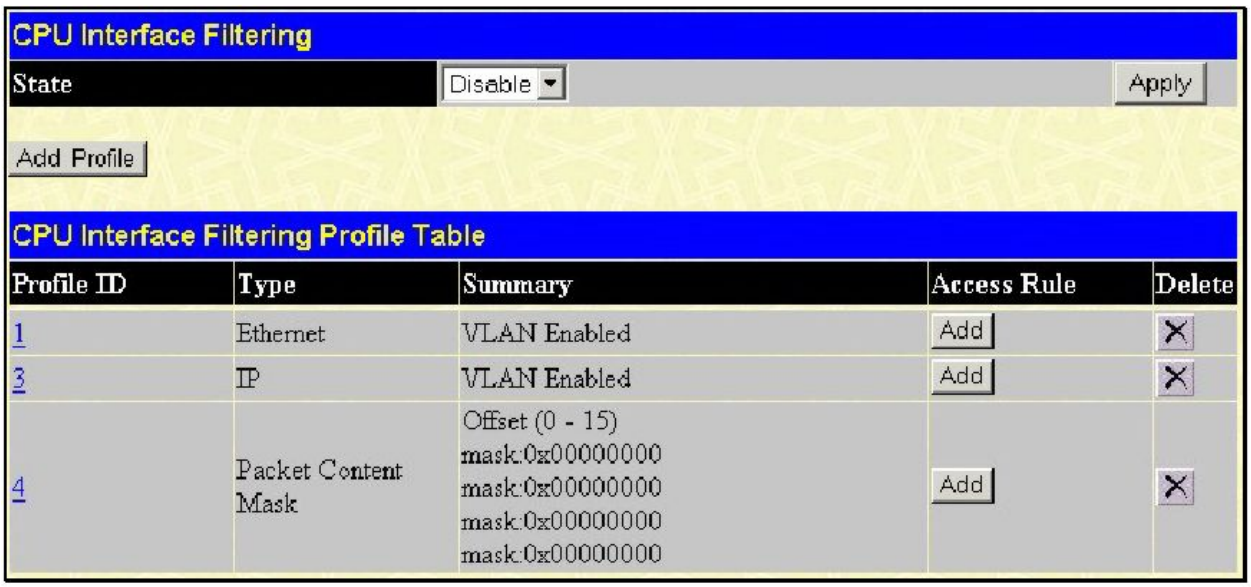


Рисунок 6- 75. Окно CPU Interface Filtering

Чтобы добавить запись в **CPU Interface Filtering Profile Table**, кликните по кнопке **Add**. В результате откроется окно **CPU Interface Filtering Profile Configuration**, показанное ниже. Доступно три 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 тремя 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**.

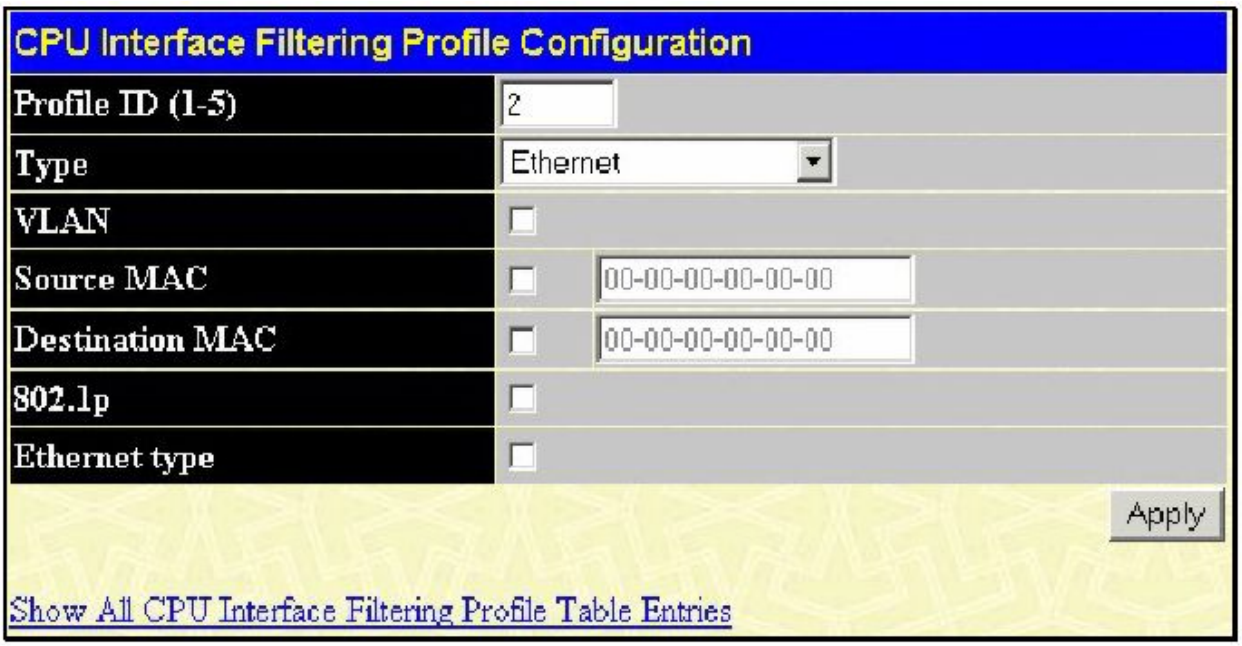


Рисунок 6- 76. Окно CPU Interface Filtering Profile Configuration (Ethernet)

В данном окне доступны для настройки следующие параметры:

Profile ID (1-5)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Значение этого поля может быть от 1 до 5.
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.
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 будет проверять значение поля Ethernet type в каждом заголовке пакетов.

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

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

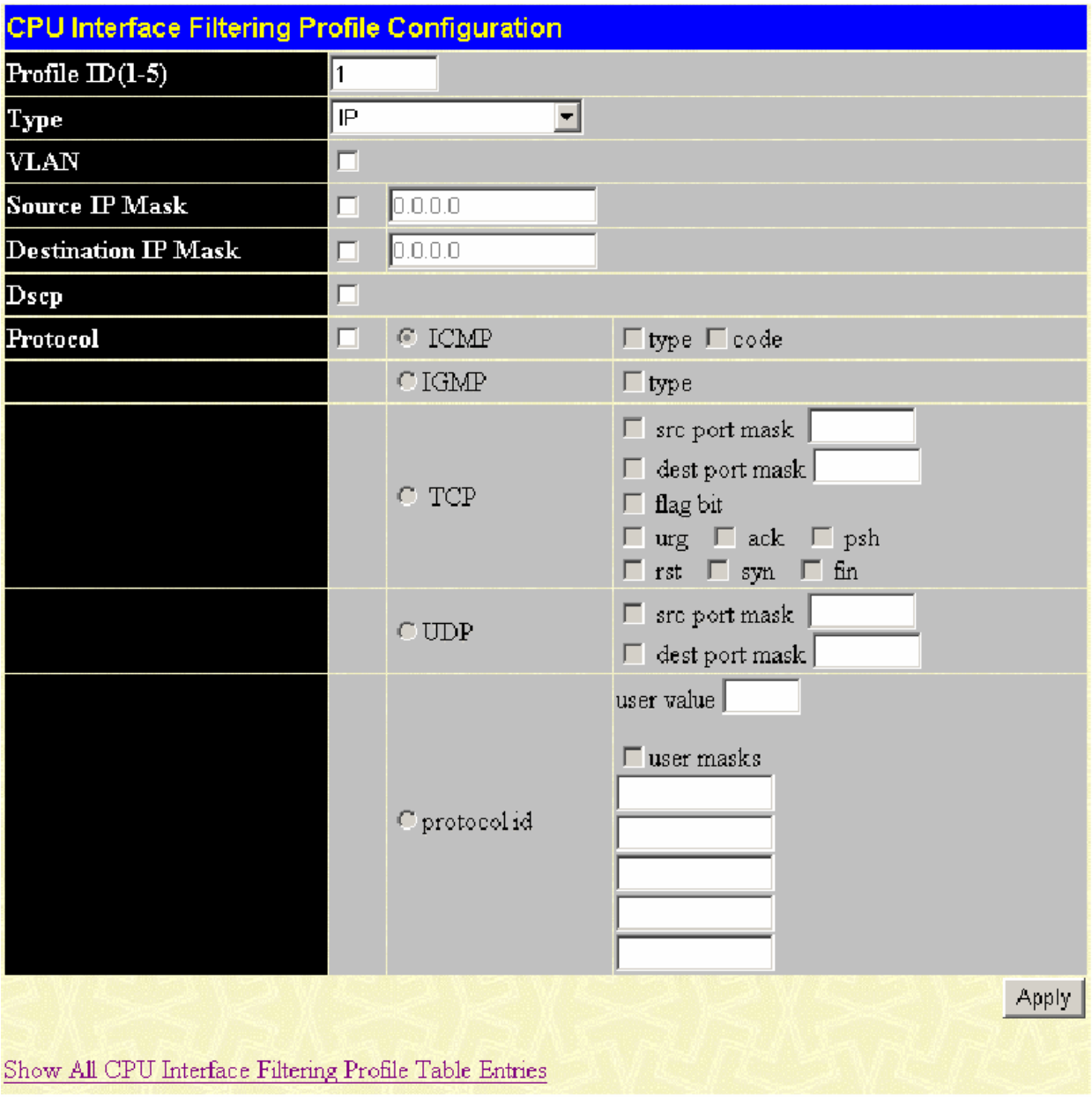


Рисунок 6- 77. Окно CPU Interface Filtering Profile Configuration (IP)

Здесь для настройки доступны следующие поля:

Параметр	Описание
Profile ID (1-5)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Значение этого поля может быть от 1 до 5.
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. Именно этот вариант и будет рассмотрен в данной таблице. • 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 (0x0-0xffffffff).

Кликните по **Apply** для принятия настроек Коммутатора.

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

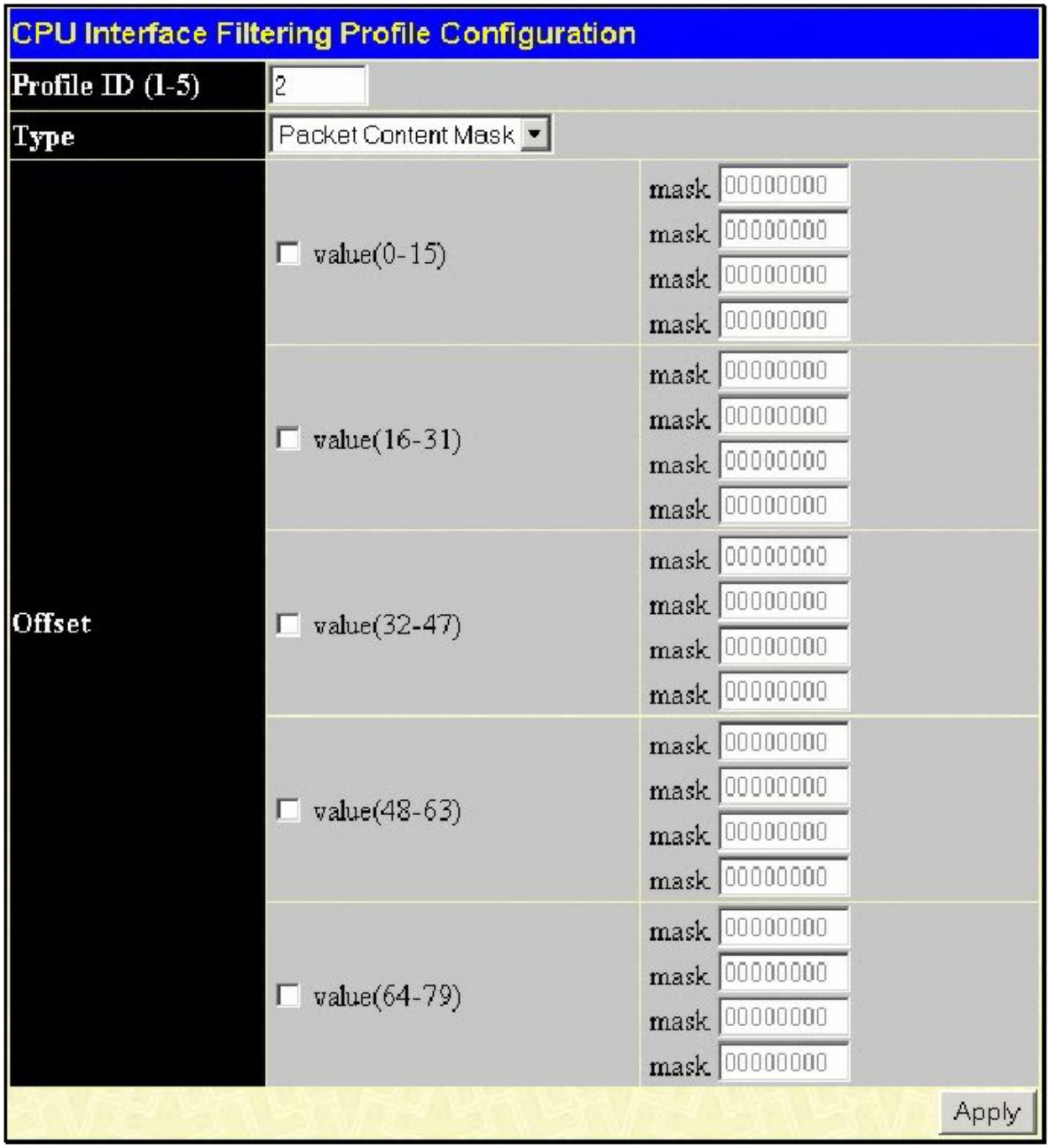


Рисунок 6- 78. Окно CPU Interface Filtering Profile Configuration (Packet Content Mask)

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 (1-5)	В этом поле необходимо ввести уникальный идентификационный номер профиля. Значение этого поля может быть от 1 до 5.
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. Именно этот вариант и будет рассмотрен в данной таблице.
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.

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

Для настройки правила для созданного предварительно профиля доступа CPU:
В папке **Configuraion кликните по CPU Interface Filtering,** чтобы открыть окно **CPU Interface Filtering Profile Table**. Это окно позволяет добавить правило для ранее созданного профиля доступа CPU путем нажатия на кнопку **Add Rule** для настройки профиля на основе **Ethernet**, на основе **IP**-адреса или содержимого маски пакета (**Packet Content Mask)**.

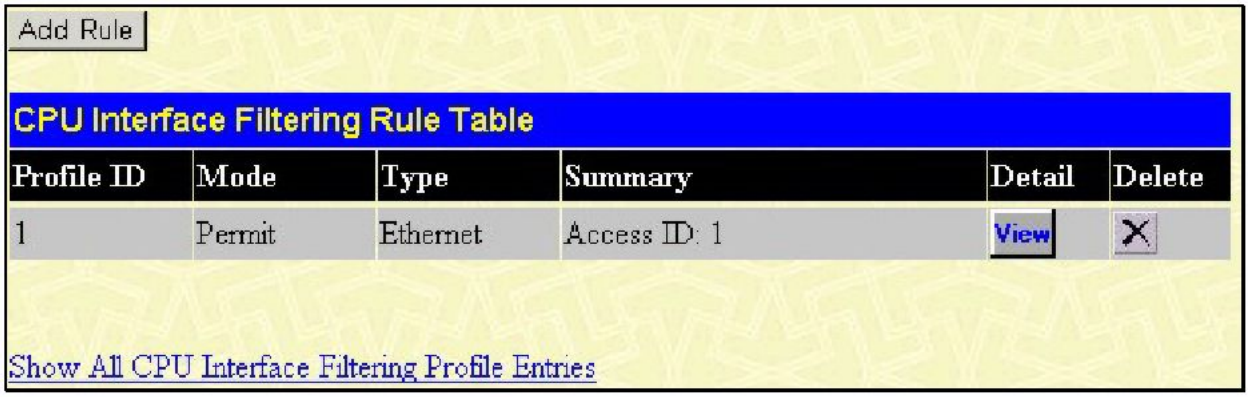


Рисунок 6- 79. CPU Interface Filtering Rule Table

Кликните по кнопке **Add Rule,** чтобы добавить новое правило в окне **CPU Interface Filtering Rule Table**. Появившееся окно позволит настроить соответствующие правила.

Для изменения правила, предварительно созданного в окне CPU Access Profile Rule:
Пользователь может изменить ранее созданное правило в этом окне, нажав на соответствующую кнопку **Modify**.

Рисунок 6- 80. Окно CPU Interface Filtering

В результате откроется окно **CPU Interface Filtering Rule Table**. Кликните по кнопке View для просмотра ранее созданного правила или по кнопке для удаления соответствующего правила. Ниже приведено окно для настройки правиладля профиля доступа на основе Ethernet.

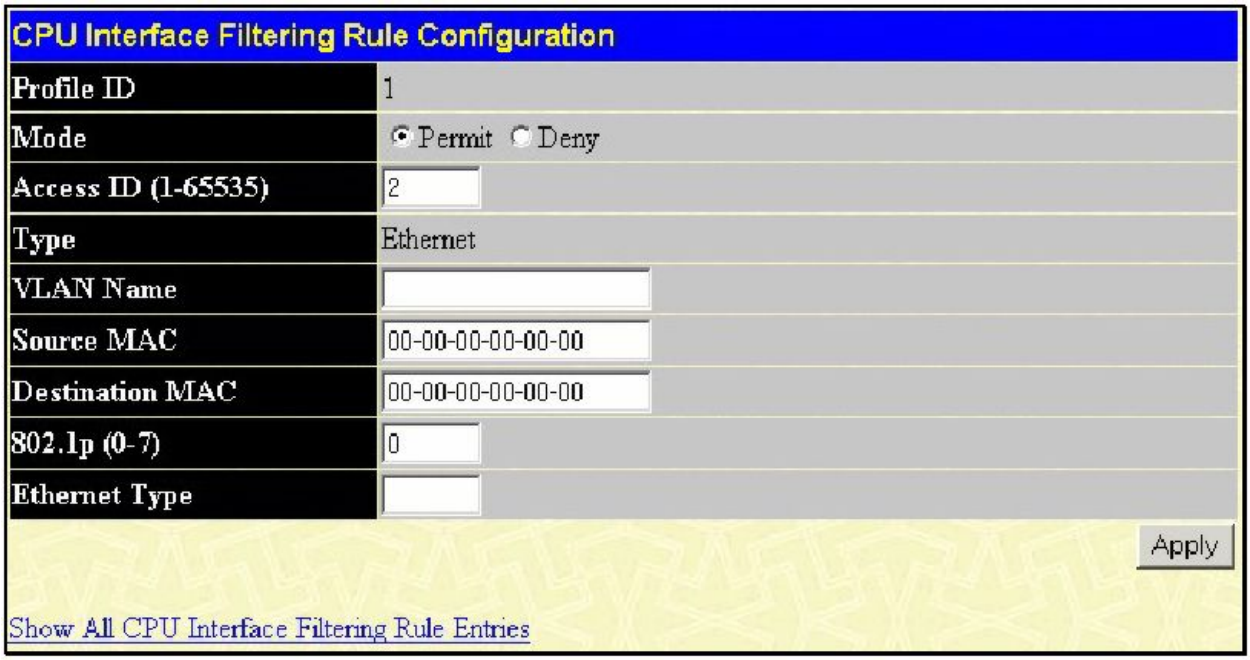


Рисунок 6- 81. Окно CPU Interface filtering rule Configuration (Ethernet)

Для настройки правила доступа к CPU для профиля доступа на основе Ethernet необходимо задать следующие параметры:

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 (1-65535)	Здесь следует ввести уникальный идентификационный номер. В данном поле могут быть установлены значения от 1 до 65 535.

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.
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 шестнадцатиричном 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 0-9999.

Для просмотра ранее созданного правила кликните по кнопке View в окне **CPU Interface Filtering Rule Table.** В результате появится следующее окно:

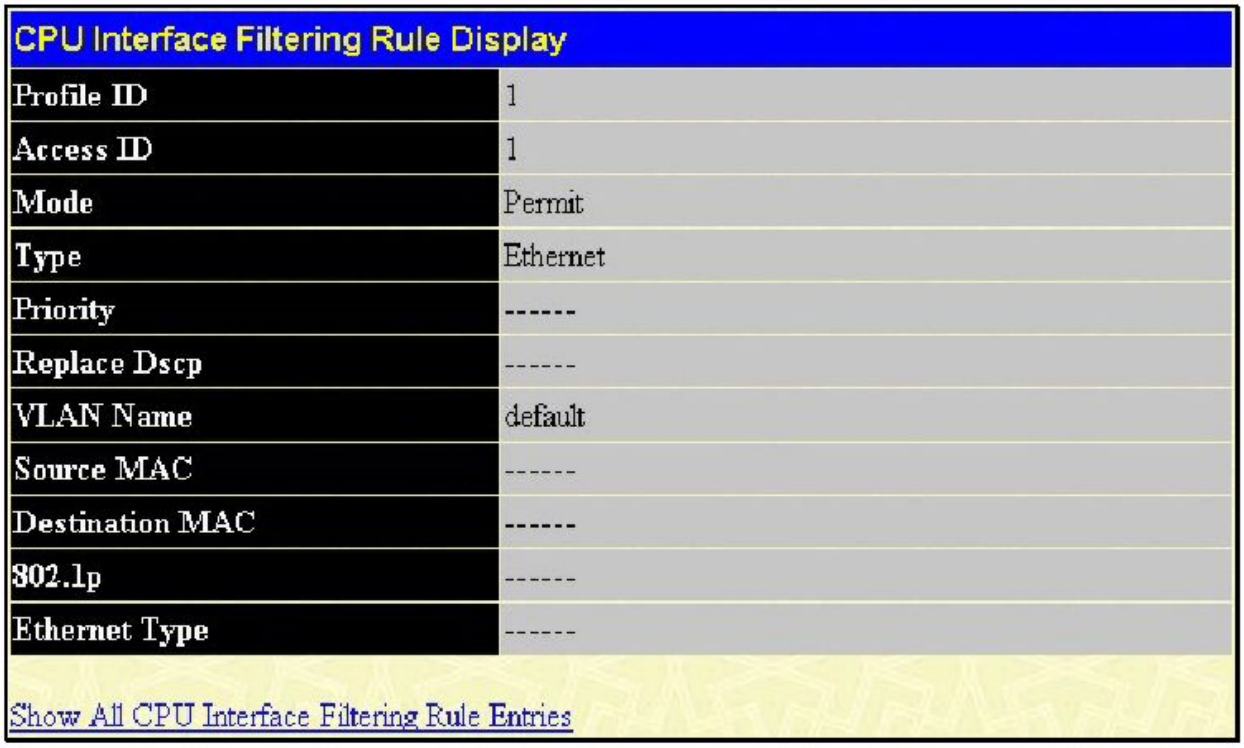


Рисунок 6- 82. Окно CPU Interface Filtering Rule Display (Ethernet)

Ниже показано окно **CPU Interface Filtering Rule Configuration** для профиля доступа на основе IP.

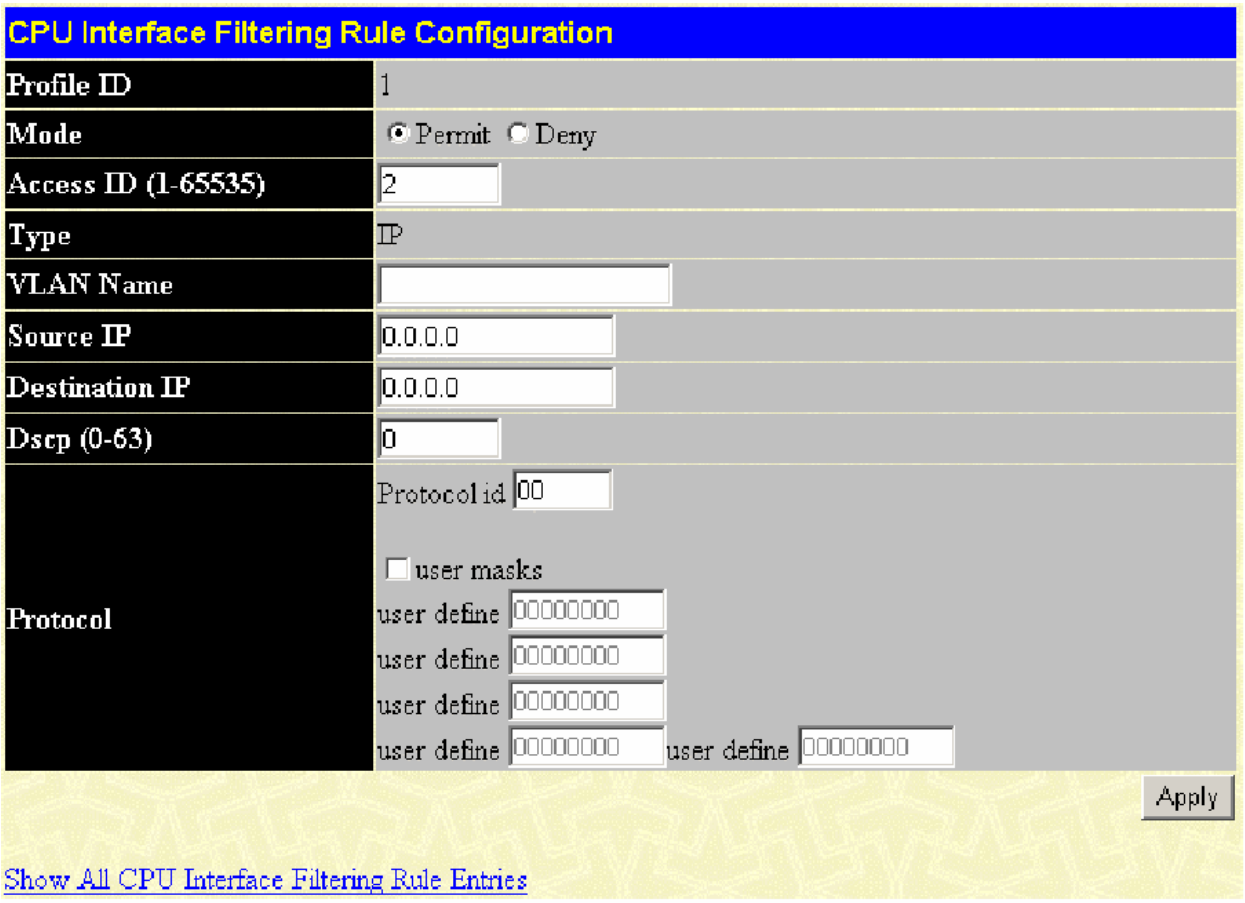


Рисунок 6- 83. Окно CPU Interface Filtering Rule Configuration (IP)

В этом окне пользователь может задать следующие параметры:

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 (1-65535)	Здесь следует ввести уникальный идентификационный номер. В данном поле могут быть установлены значения от 1 до 65 535. **Auto Assign** – выбор данной опции означает, что Коммутатор будет автоматически назначать идентфкатор доступа.
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.
Protocol	Это поле позволяет модифицировать протокол, используемый для настройки **CPU Interface Filtering Rule Table,** в зависимоти от выбранного пользователем значения в поле **CPU Interface Filtering Profile Table**.

Для просмотра корректно настроенного ранее правила кликните по кнопке View в окне **CPU Interface Filtering Rule Table.** В результате появится следующее окно:

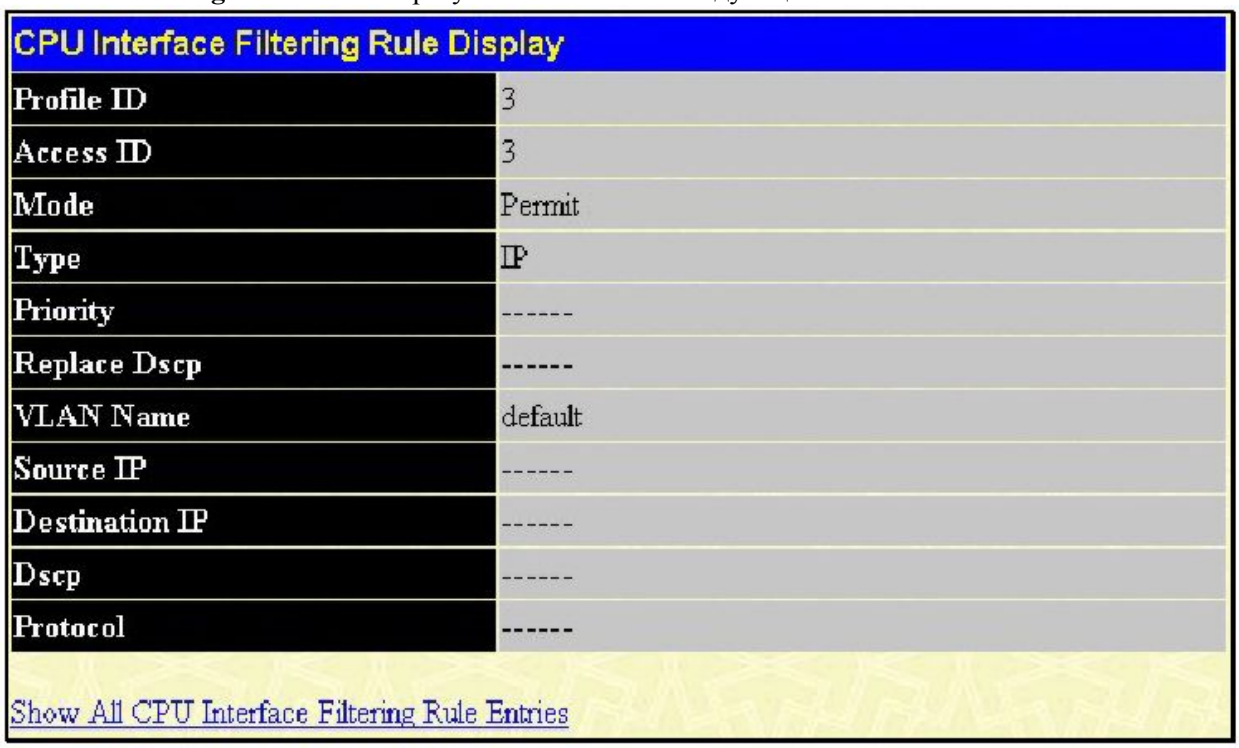


Рисунок 6- 84. Окно CPU Interface Filtering Rule Display (IP)

Ниже приведено окно **CPU Interface Filtering Rule Configuration** при выборе в поле **Type** значения **Packet Content**.

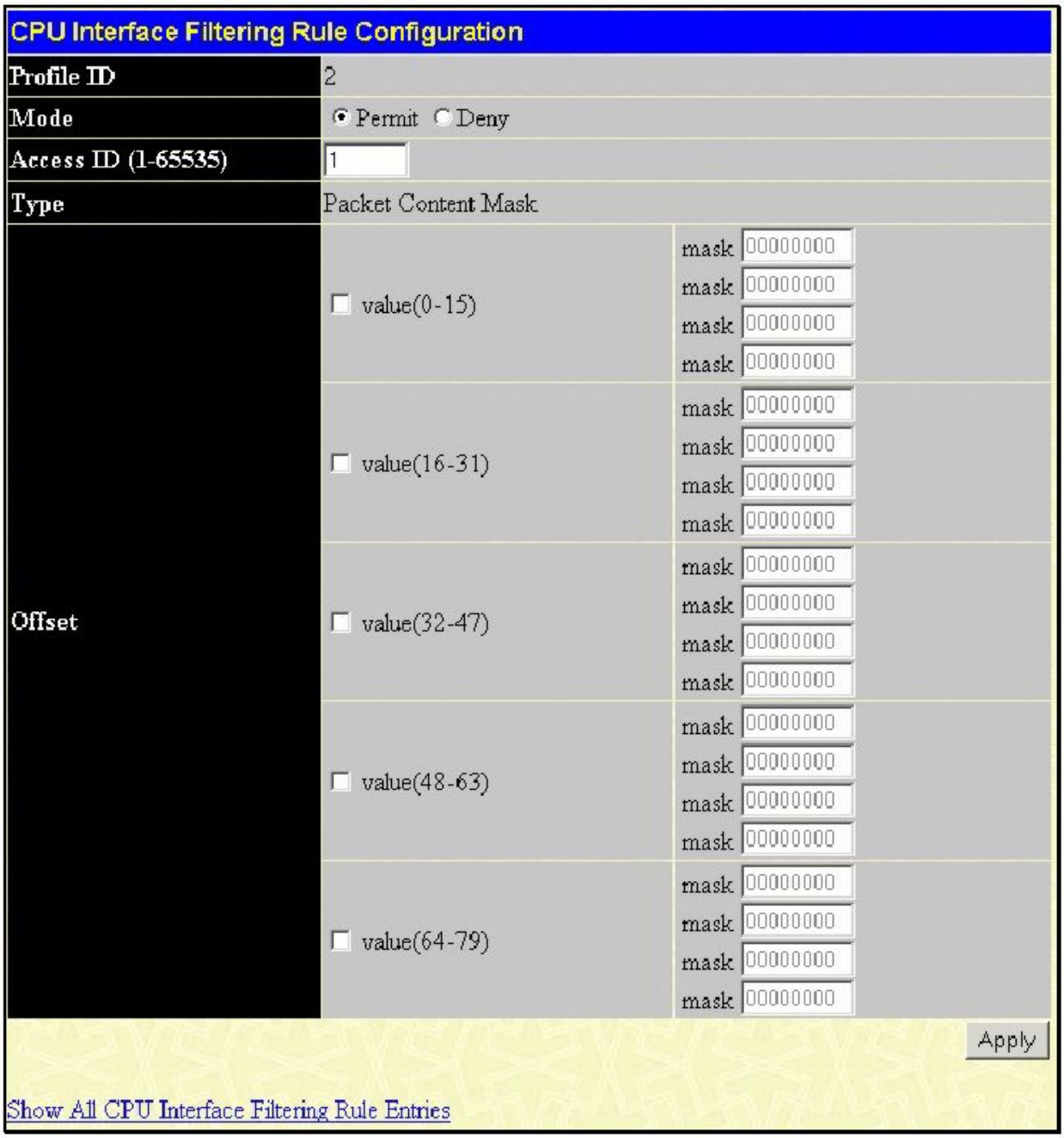


Рисунок 6- 85. Окно CPU Interface Filtering Rule Configuration (Packet Content Mask)

Для настройки правила доступа к CPU для профиля доступа на основе Packet Content Mask необходимо задать следующие параметры:

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 65 535.
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.

Для просмотра настроек успешно созданного ранее правила кликните по кнопке 

в окне **Access Rule Table.** В результате появится следующее окно:

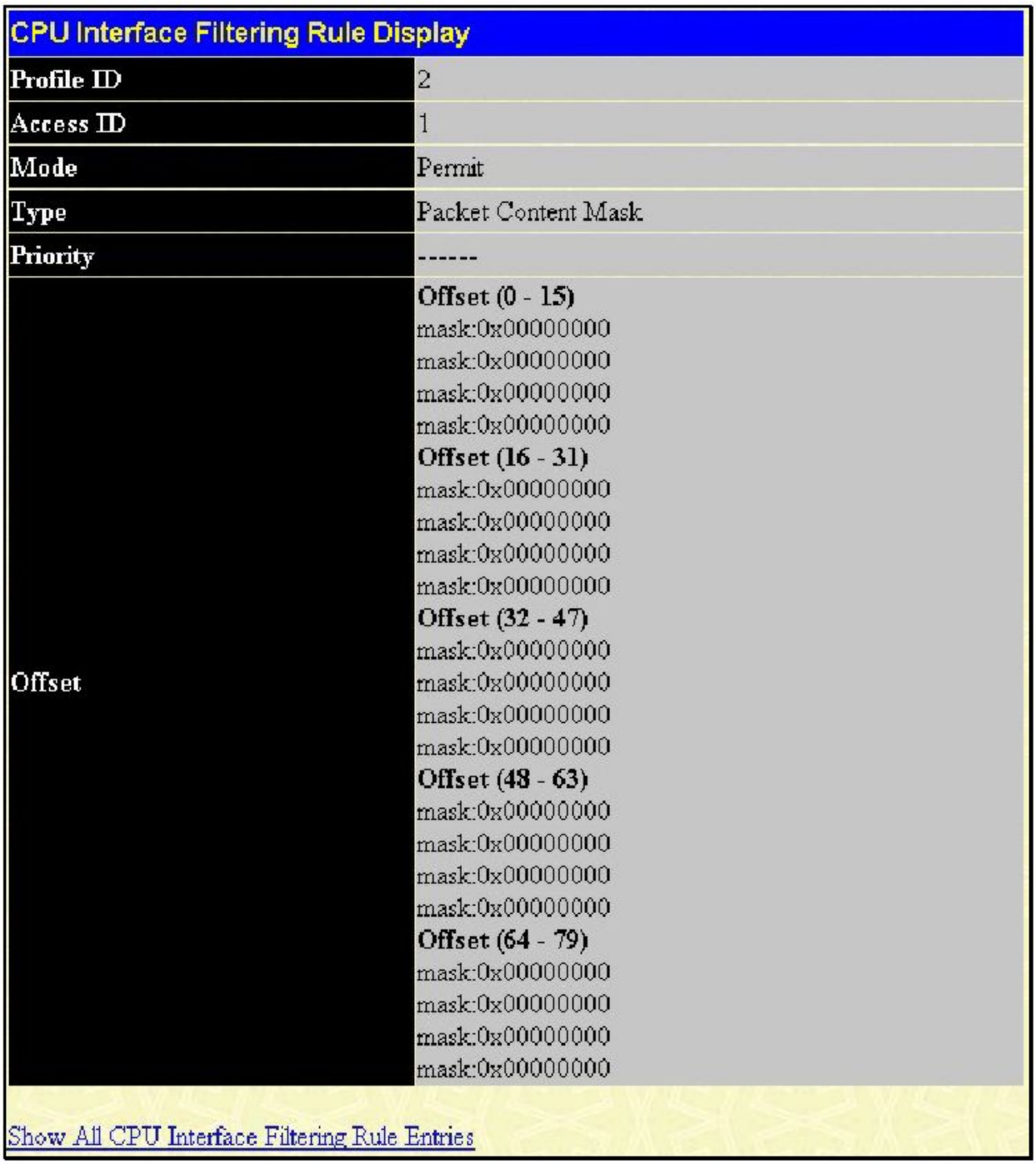


Рисунок 6- 86. Окно CPU Interface Filtering Rule Display (Packet Contenet Mask)

Port Access Entity (802.1X)
Аутентификация 802.1x на основе портов и MAC-адресов

Стандарт IEEE 802.1x обеспечивает безопасность при авторизации и аутентификации пользователей для получения доступа к различным проводным и беспроводным устройствам локальной сети, используя модель доступа 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.

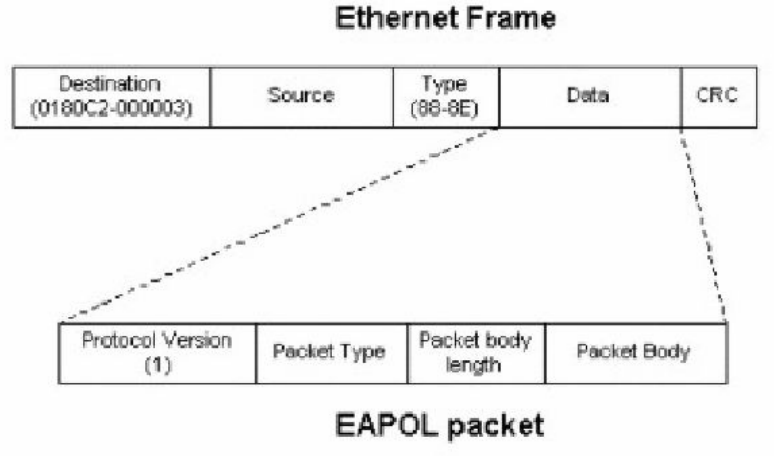


Рисунок 6.87 – Структура пакета EAPOL

При использовании данного метода неавторизованным устройствам будет запрещено подключение к локальной сети через пользовательский порт, поскольку до прохождения авторизации могут передаваться лишь пакеты протокола EAPOL. Управление доступом согласно протоколу 802.1x подразумевает наличие трех основных компонентов, а именно: клиента, аутентифкатора и сервера аутентификации.

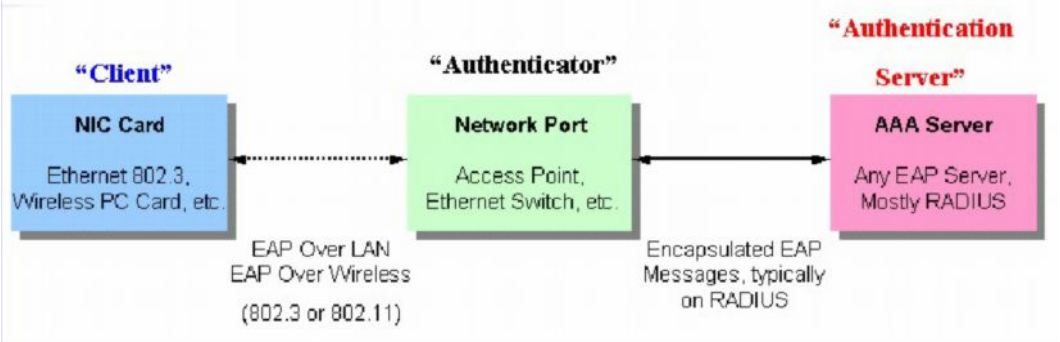


Рисунок 6.88 – Три функции протокола 802.1x

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.

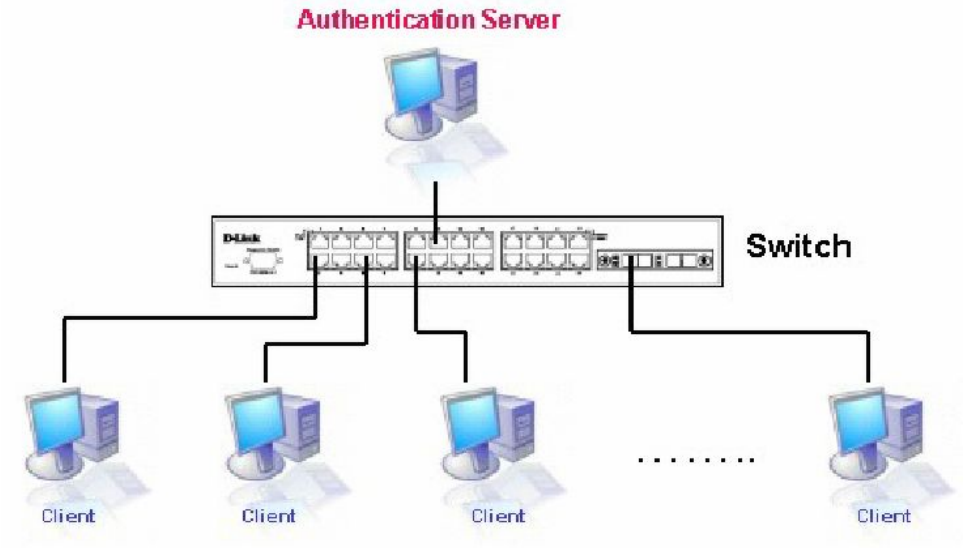


Рисунок 6.89 – Сервер аутентификации

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 (**Configuration ⇨ Switch Information ⇨Advanced Settings ⇨ 802.1x Status).**
2. Настроить 802.1x на портах **(Port Access Entity ⇨ PAE System Control ⇨ Port Capability ⇨Capability).**
3. Настроить параметры RADIUS-сервера на Коммутаторе **(Port Access Entity ⇨ RADIUS Server ⇨ Authentic RADIUS Server).**

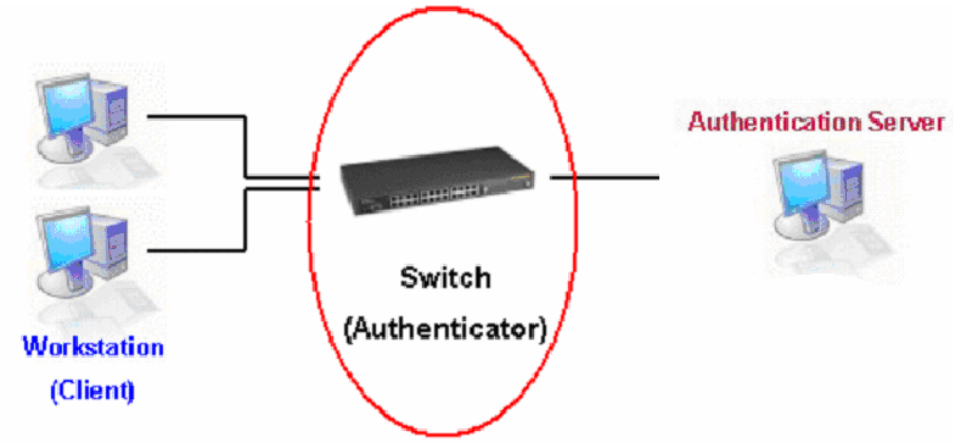


Рисунок 6.90 – Аутентификатор

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.

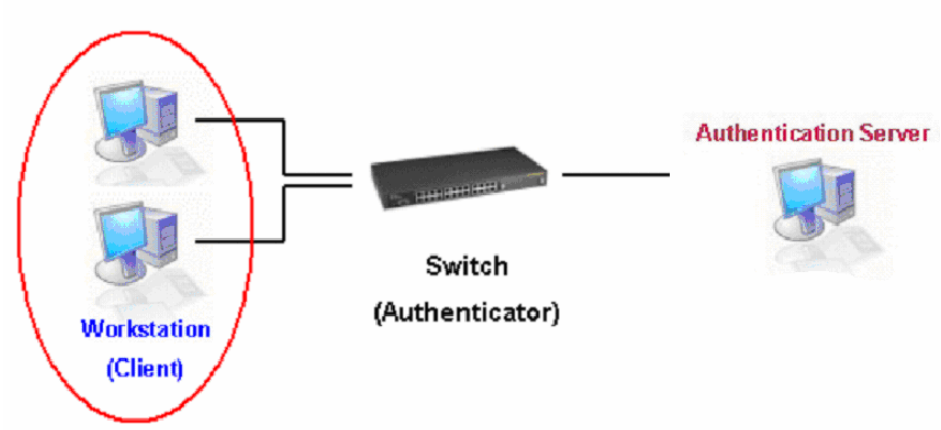


Рисунок 6.91 - Клиент

Процесс аутентификации

Балгодаря 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. 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.

Аутентификация на основе портов

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).

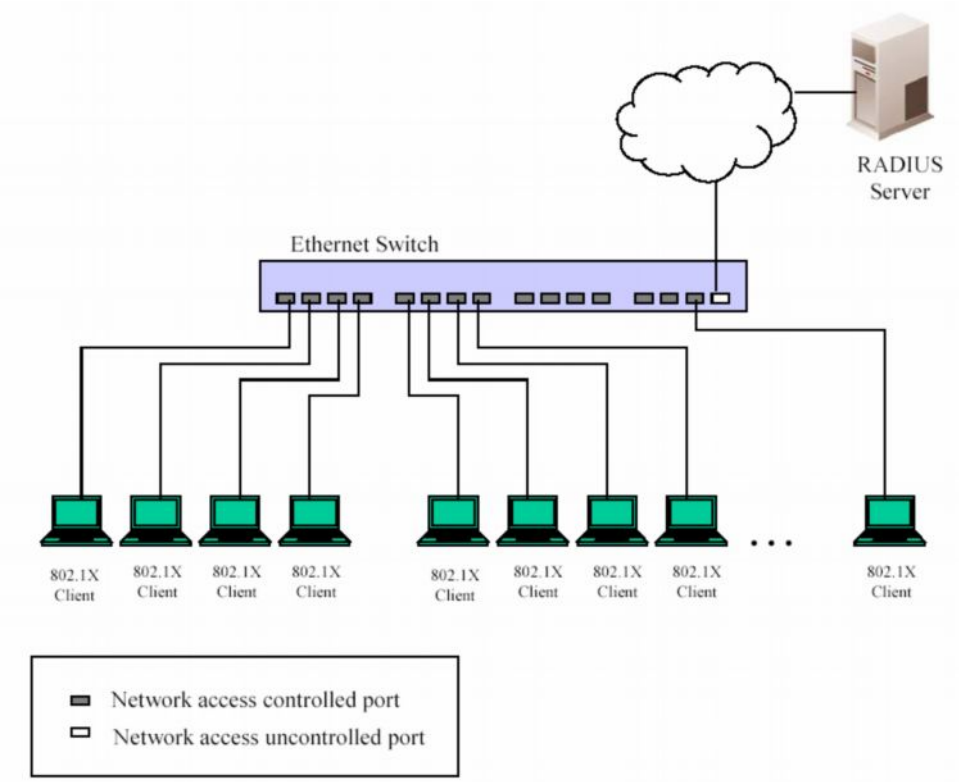


Рисунок 6- 92. Пример типичной конфигурации Port-Based (на основе портов)

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

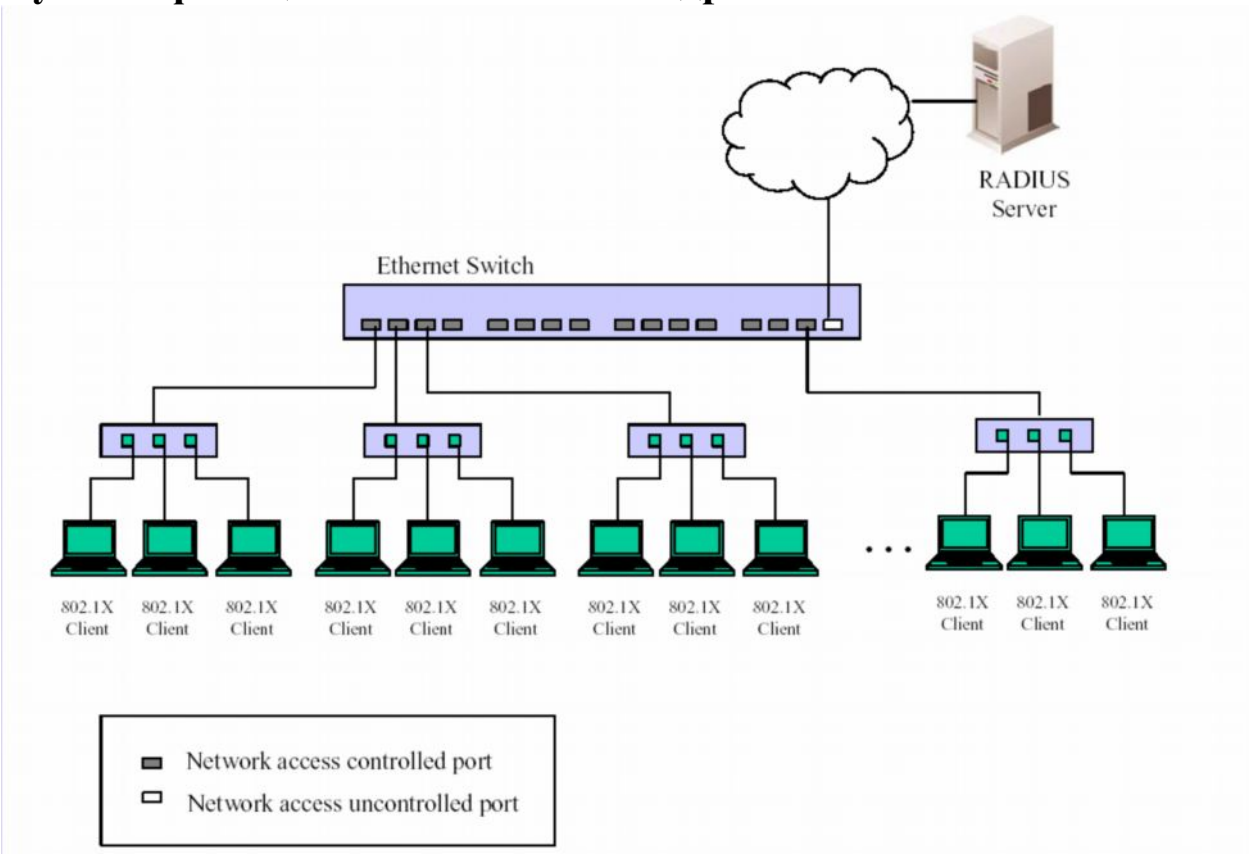
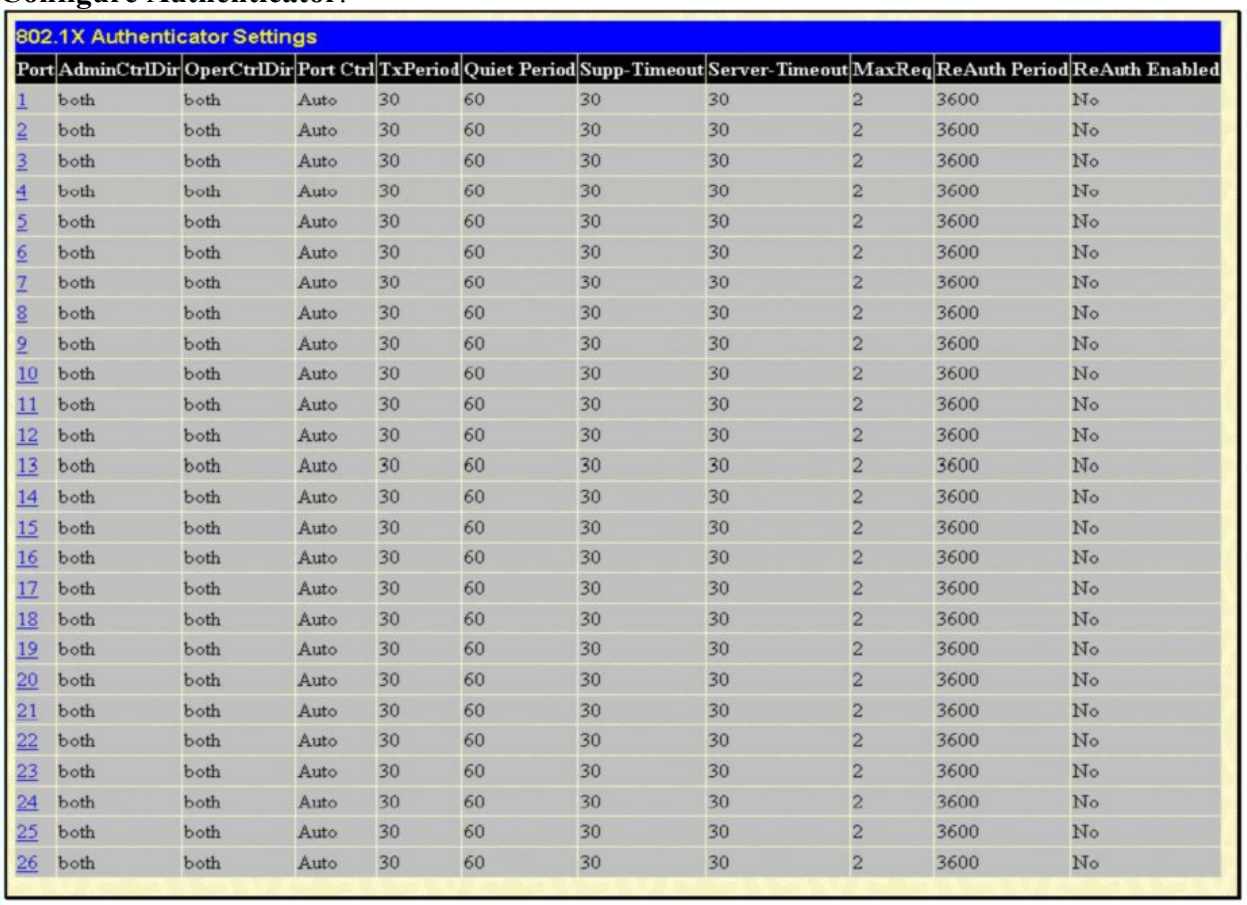


Рисунок 6- 93. Пример типичной конфигурации MAC-Based (на основе MAC-адресов)

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.

Настройка аутентификатора

Для задания настроек аутентификатора 802.1X следует кликнуть **PAE Access Entity** > **Configure Authenticator**:



802.1X Authenticator Settings

Port	AdminCtrlDir	OperCtrlDir	Port Ctrl	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	both	Auto	30	60	30	30	2	3600	No
2	both	both	Auto	30	60	30	30	2	3600	No
3	both	both	Auto	30	60	30	30	2	3600	No
4	both	both	Auto	30	60	30	30	2	3600	No
5	both	both	Auto	30	60	30	30	2	3600	No
6	both	both	Auto	30	60	30	30	2	3600	No
7	both	both	Auto	30	60	30	30	2	3600	No
8	both	both	Auto	30	60	30	30	2	3600	No
9	both	both	Auto	30	60	30	30	2	3600	No
10	both	both	Auto	30	60	30	30	2	3600	No
11	both	both	Auto	30	60	30	30	2	3600	No
12	both	both	Auto	30	60	30	30	2	3600	No
13	both	both	Auto	30	60	30	30	2	3600	No
14	both	both	Auto	30	60	30	30	2	3600	No
15	both	both	Auto	30	60	30	30	2	3600	No
16	both	both	Auto	30	60	30	30	2	3600	No
17	both	both	Auto	30	60	30	30	2	3600	No
18	both	both	Auto	30	60	30	30	2	3600	No
19	both	both	Auto	30	60	30	30	2	3600	No
20	both	both	Auto	30	60	30	30	2	3600	No
21	both	both	Auto	30	60	30	30	2	3600	No
22	both	both	Auto	30	60	30	30	2	3600	No
23	both	both	Auto	30	60	30	30	2	3600	No
24	both	both	Auto	30	60	30	30	2	3600	No
25	both	both	Auto	30	60	30	30	2	3600	No
26	both	both	Auto	30	60	30	30	2	3600	No

Рисунок 6- 94. Окно 802.1X Authenticator Settings

Для задани настроек каждого порта следует кликнуть по гиперссылке номера порта под заголовком Port, после чего откроется следующее окно:

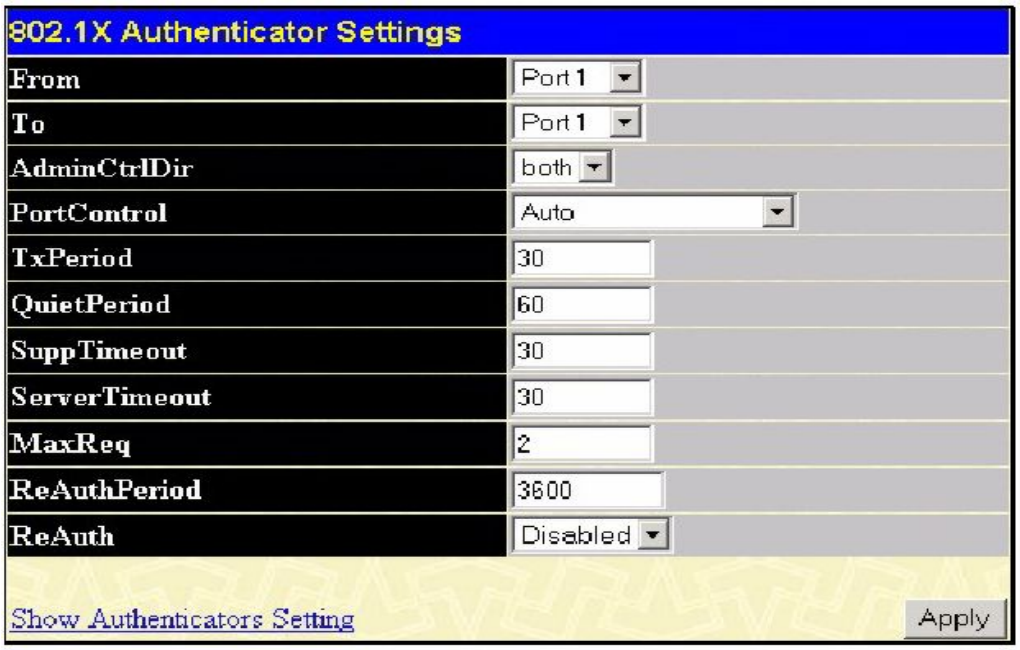


Рисунок 6- 95. Окно 802.1X Authenticator Settings (Изменить)

Данное окно позволяет пользователю осуществить следующие настройки:

Параметр	Описание
From [ ] To [ ]	Данные выпадающие меню позволяют ввести порт (или порты) для настройки.
AdmCtrlDir	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*.

Для принятия настроек следует кликнуть по **Apply**. Для просмотра настроек аутентификации 802.1X следует обратиться к окну **802.1X Authenticator Settings**.

Система управления PAE

Ниже рассматриваются окна, содержащие опции, позволяющие отобразить и изменить настройки 802.1x для портов.

Port Capability

Для работы со следующим окном кликните **Port Access Entity > PAE System Control > Port Capability:**

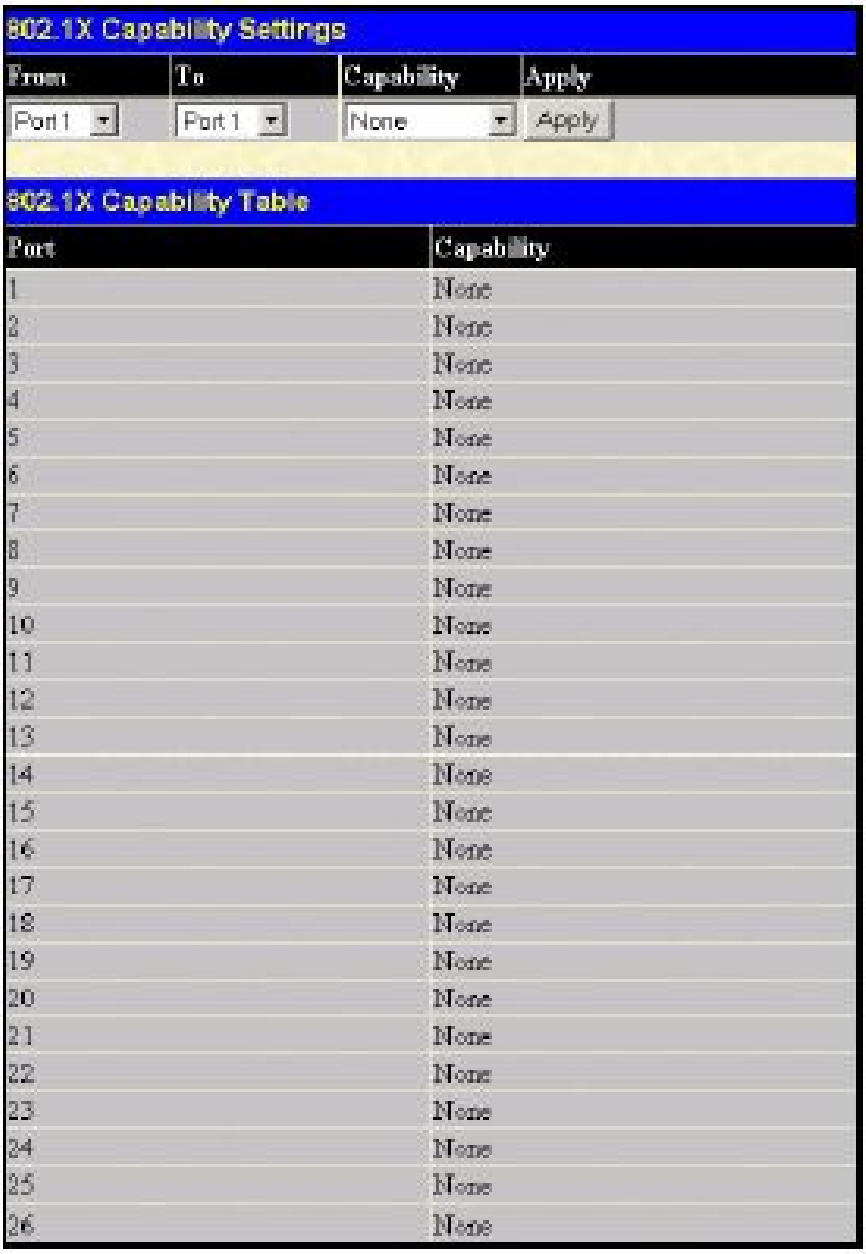


Рисунок 6- 96. Окно 802.1x Capability Settings

Для настройки на Коммутаторе аутентификации 802.1x на основе портов выберите с помощью полей **From** и **To** нужные порты для настройки. Затем включите данную опцию для определенных портов, выбрав значение *Authenticator* в выпадающем меню под заголовком **Capability**. Для принятия настроек следует кликнуть по **Apply**.
Здесь доступны для настройки следующие поля:

Параметр	Описание
From and To	Выберите порты для настройки 802.1x.
Capability	В данном поле доступны для выбора следующие опции: *Authenticator* – при выборе данной опции пользователь получит доступ к сети только после завершения процесса аутентификации 802.1x. *None* – выбор данной опции позволяет выключить аутентификацию 802.1x для указанных портов.

Инициализация портов при аутентификации 802.1x на основе портов

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

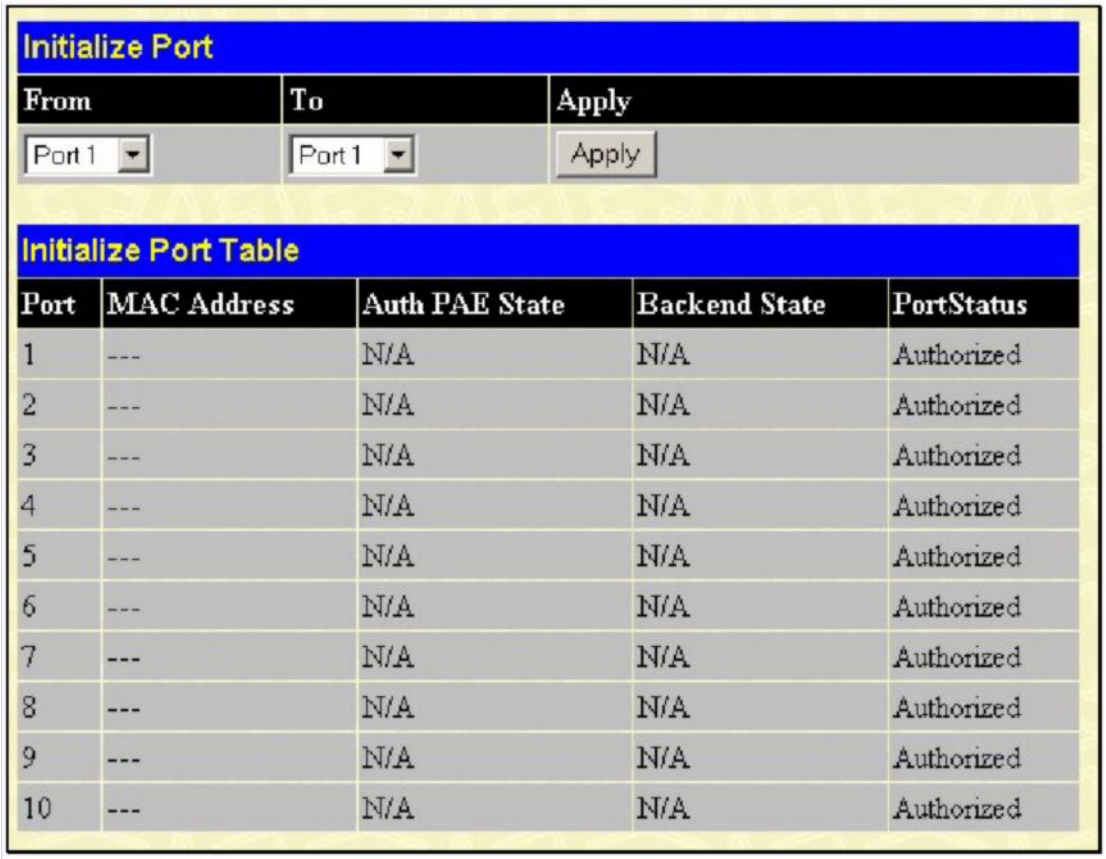


Рисунок 6- 97. Окно Initialize Port

Это окно позволяет инициализировать порт или группу портов. В нижней части окна в **Initialize Port Table** отображаются текущие статусы порта(ов).

В данном окне отображается следующая информация:

Параметр	Описание
From and To	Выбираются порты для инициализации.
Port	Это поле, доступное только для чтения, содержит номер порта Коммутатора.
MAC Address	MAC-адрес Коммутатора, относящийся к соответствующему порту.

Auth PAE State	В поле **Auth PAE State** будет отображаться одно из следующих значений: *Initialize, Disconnected,Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth* и *N/A*.
Backend State	В поле **Backend Authentication State** будет отображаться одно из следующих значений: *Request, Response,Success, Fail, Timeout, Idle, Initializ,* и *N/A*.
Port Status	Статус контролируемого порта может быть *Authorized, Unauthorize,* или *N/A*.

Инициализация портов для 802.1x на основе MAC-адресов

Для инициализации портов 802.1x на основе MAC-адресов сначала необходимо выбрать опцию «802.1x by MAC address» в окне **Advanced Settings**. Для работы со следующим окном кликните по **Configuration > Port Access Entity > PAE System Control > Initialize Port(s):**

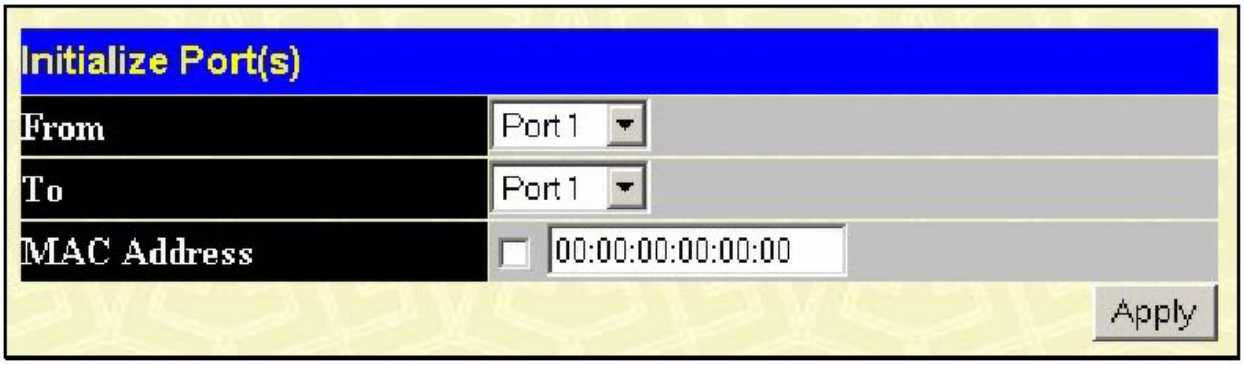


Рисунок 6- 98. Окно Initialize Port(s) (MAC based 802.1x)

Для инициализации портов сначала необходимо выбрать диапазон портов в выпадающих меню **From** и **To**. Далее пользователь должен задать MAC-адрес для инициализации, введя его значение в поле MAC Address и поставив галочку в соответствующем поле. Для начала инициализации кликните по **Apply**.

Примечание: Перед инициализацией портов необходимо глобально установить опцию 802.1X в папке **Configuration** в окне **Switch Information (Advanced Settings).** До включения опции 802.1X информация не может отображаться в таблице Initialize Ports Table.

Повторная аутентификация портов для 802.1x на основе портов

Данное окно позволяет осуществить повторную аутентификацию порта или группы портов. Для этого необходимо задать диапазон портов, используя выпадающие меню **From** и **To,** а затем кликнуть по **Apply**. После этого в таблице Reauthenticate Port отображаются текущие состояния повторно аутентифицирующихся порта(ов).

Кликните **Configuration > Port Access Entity > PAE System Control > Reauthenticate Port(s),** чтобы открыть окно **Reauthenticate Port(s):**

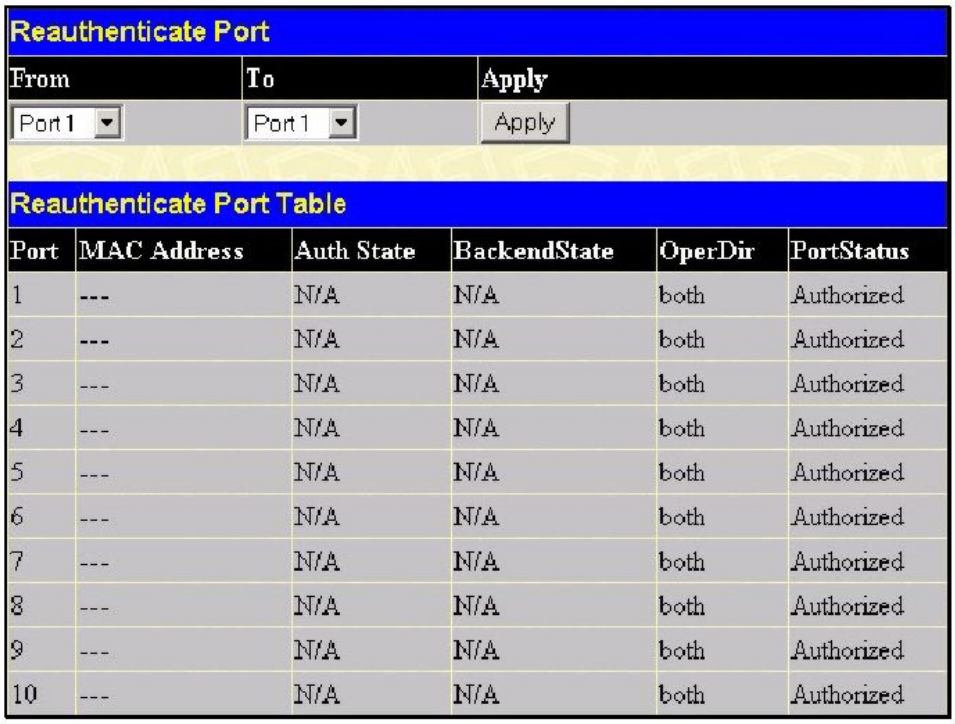


Рисунок 6- 99. Окно Reauthenticate Port

Данное окно отображает следующую информацию:

Параметр	Описание
Port	Данное поле отображает номер повторно аутентифицирующегося порта.
MAC Address	Отображает MAC-адрес Коммутатора, к которому относится порт.
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*.
OpenDir	Данное поле позволяет задать нарпавление контролируемого трафика и может принимать значения *both* (для контроля входящего и исходящего трафика) и *in* (для контроля входящего трафика).
PortStatus	Статус контролируемого порта может быть *Authorized, Unauthorized,* или *N/A*.

RADIUS-сервер

Поддержка аутентификации RADIUS позволяет осуществлять централизованное управление учетными записями пользователей, а также обеспечить защиту от хакерских атак. Для открытия окна **RADIUS Server Authentication Setting**, представленного ниже, следует кликнуть **Port Access Entity > RADIUS Server > Authentic Radius Server:**

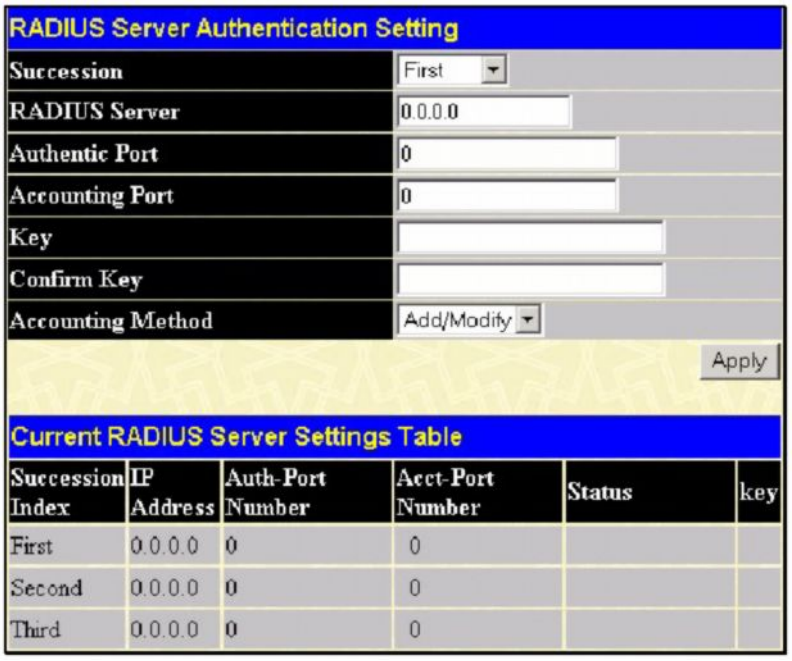


Рисунок 6- 100. Окно RADIUS Server Authentication Setting

Данное окно отображает следующую информацию:

Параметр	Описание
Succession	В этом поле выбирается необходимый RADIUS-сервер: *First, Second* или *Third.*
RADIUS Server	Установите IP-адрес RADIUS-сервера.
Authentic Port	Введите UDP-порт сервера(ов) аутентификации RADIUS. Порт по умолчанию *1812*.
Accounting Port	Введите UDP-порт учетной записи RADIUS-сервера(ов). Порт по умолчанию *1813*.
Key	Устанавливается тот же ключ, что и на RADIUS-сервере.
Confirm Key	Подтверждение ключа, введенного в предыдущем поле.
Accounting Method	Позволяет добавить, изменить или удалить (*Add/Modify* или *Delete)* настройки RADIUS-сервера.

Guest VLAN

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.

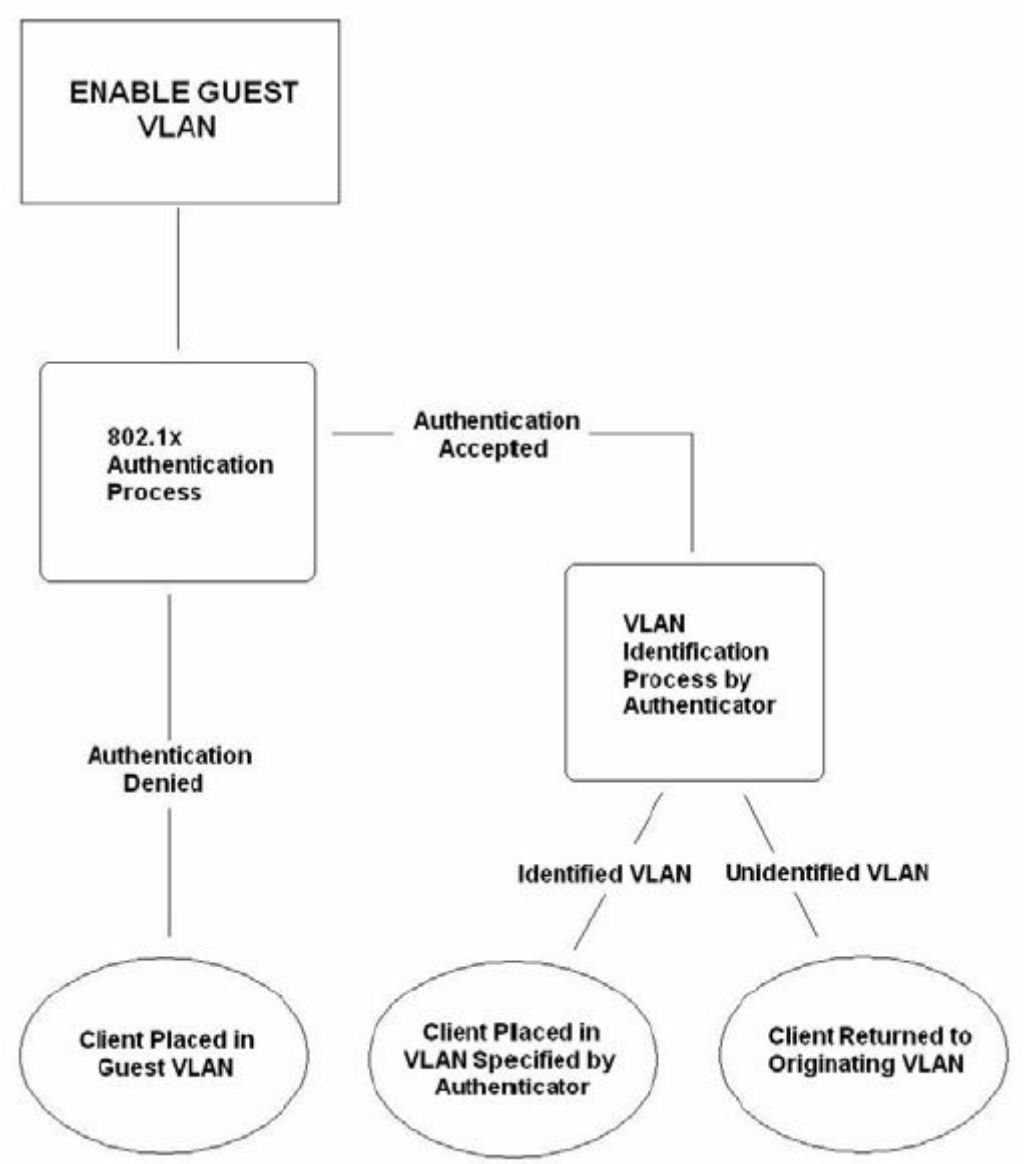


Рисунок 6- 101 Процесс аутентификации Guest VLAN

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

IP-MAC Binding (Связка IP-MAC)

Коммутатор на уровне IP использует IP-адрес, состоящий из четырех байт. На уровне Ethernet-канала используется шестибайтный MAC-адрес. Связка этих адресов позволяет осуществлять передачу данных между уровнями. Основной задачей функции IP-MAC Binding является ограничения доступа неавторизованных пользователей. Только авторизованные клиенты, связки IP- и MAC- адресов которых занесены в заранее созданную базу данных, могут получить доступ к порту Коммутатора. Если неавторизованный пользователь попытается получить доступ к порту с установленной функцией IP-MAC Binding, система заблокирует доступ, отбрасывая пакеты соответствующего пользователя. Максимальное количество записей в базе данных IP-MAC Binding зависит от используемого чипа (в частности, поддерживаемого размера таблицы ARP) и размера памяти устройства. Для коммутаторов серии DES-3500 xStack максимальное количество записей IP-MAC Binding равно 512. Авторизованные пользователи могут быть настроены вручную с помощью команд интерфейса командной строки CLI или Web-интерфейса. Данная функция поддерживается на основе портов, т.е. она может быть включена или выключена для каждого порта.

Режим ACL

Для ряда специальных случаев, возникающих для IP-MAC binding, Коммутаторы поддерживают режим ACL для IP-MAC Binding. При включении данной опции в окне **IP-MAC Binding Port** Коммутатор создаст две записи в таблице профилей доступа, как показано ниже. Эти записи могут быть созданы, если на Коммутаторе доступно, как минимум, два идентификатора профилей доступа. Если это условие не соблюдено, то при включении опции ACL Mode, появится сообщение об ошибке. При включении функции ACL Mode Коммутатор будет принимать IP-пакеты только от записей, представленных в окне IP-MAC Binding Setting. Все другие пакеты будут отброшены.

Для просмотра отдельных настроек, относящихся к этим двум записям, необходимо кликнуть по соответствующим гиперссылкам Profile ID. В результате появятся следующие окна:

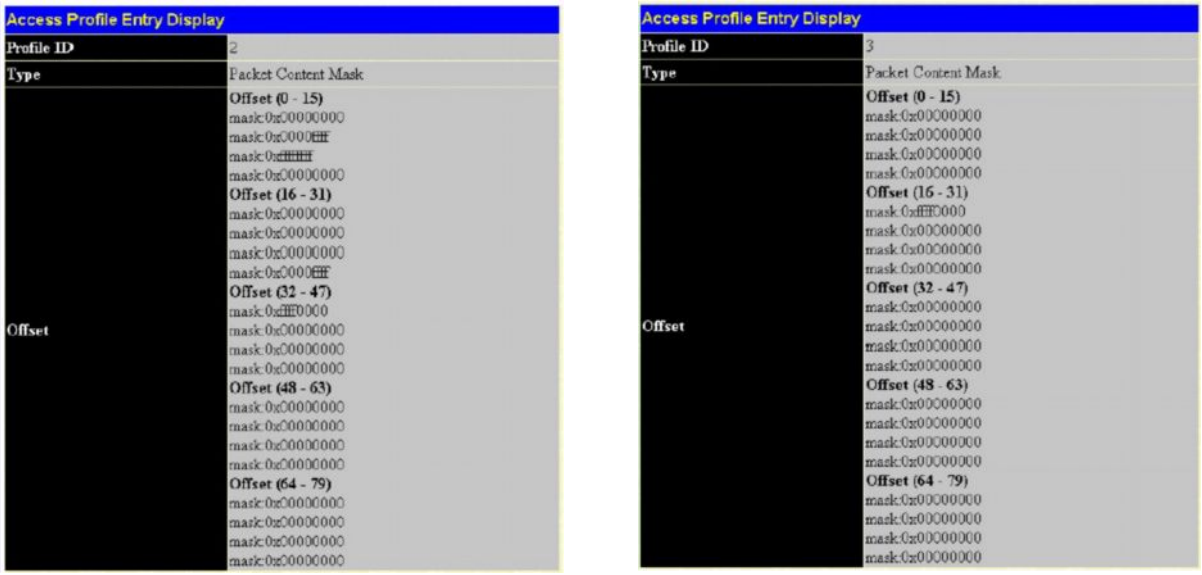


Рисунок 6- 103. Окно Access Profile Entry Display для IP-MAC Binding в режиме ACL

Эти две записи не могут быть изменены и удалены с помощью окна **Access Profile Table**, и любые попытки сделать это приведут к появлению предупреждающего сообщения:

Рисунок 6- 104. Предупреждающее сообщение IP-MAC (режим ACL)

Пользователь может удалить эти две записи, выключив опцию **ACL Mode** в окне **IP-MAC Binding Port**.

Аналогичные правила могут быть созданы также для других портов Коммутатора. Для просмотра настроек ACL-правила в режиме ACL кликните по соответствующей кнопке **Modify** в окне **Access Profile Table**, после чего появится показанное ниже окно **Access Rule Table**. Помните, что опция **Flow Meter** доступна для настройки только в том случае, если в поле Owner указано ACL.

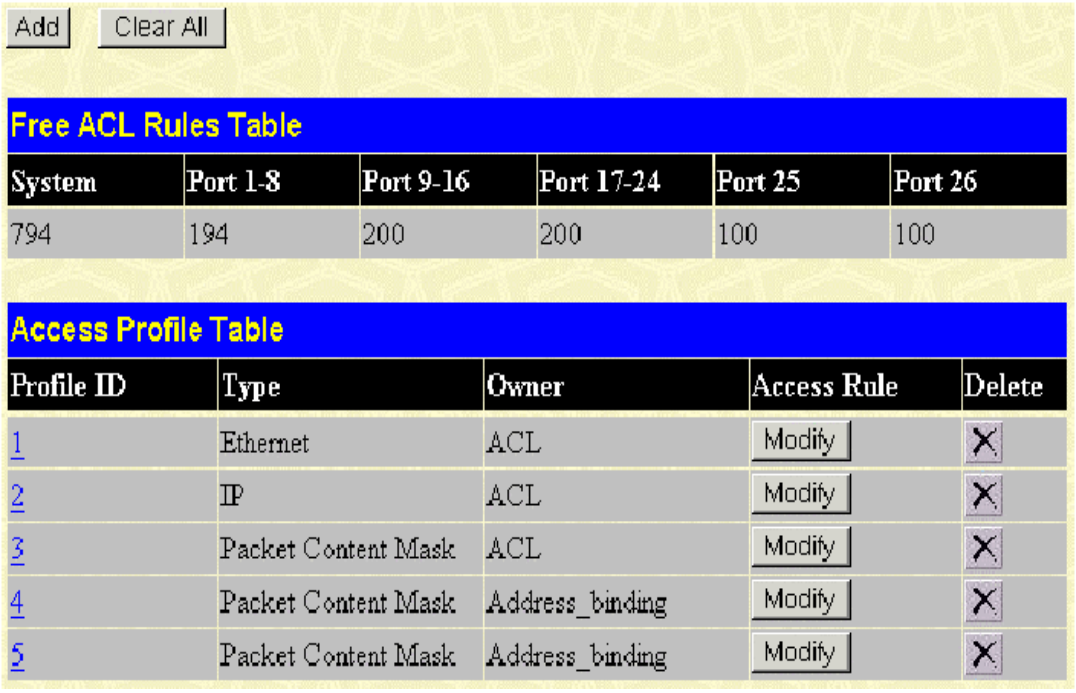


Рисунок 6- 105. Таблица профилей доступа для правила IP-MAC Binding

ПРИМЕЧАНИЕ: При настройке режима ACL функции IP-MAC binding, пожалуйста, обратите особое внимание на настроенные ранее ACL. Поскольку записи режима ACL занимают два первых доступных профиля и ID профилей указывают на приоритет ACL, то записи режима ACL могут получить приоритет, по сравнению с другими записями ACL. Это может привести к тому, что некоторые параметры ACL, заданные пользователем, не будут работать. Более подробная информация по настройкам ACL доступна в разделе “Настройка профиля доступа” этой главы.

ПРИМЕЧАНИЕ: Пользователь не может именить, удалить или добавить ACL-правила в записи профилей доступа режима ACL. Любая попытка выполнить это приведет к ошибке настройки и появлению показанного выше окна.

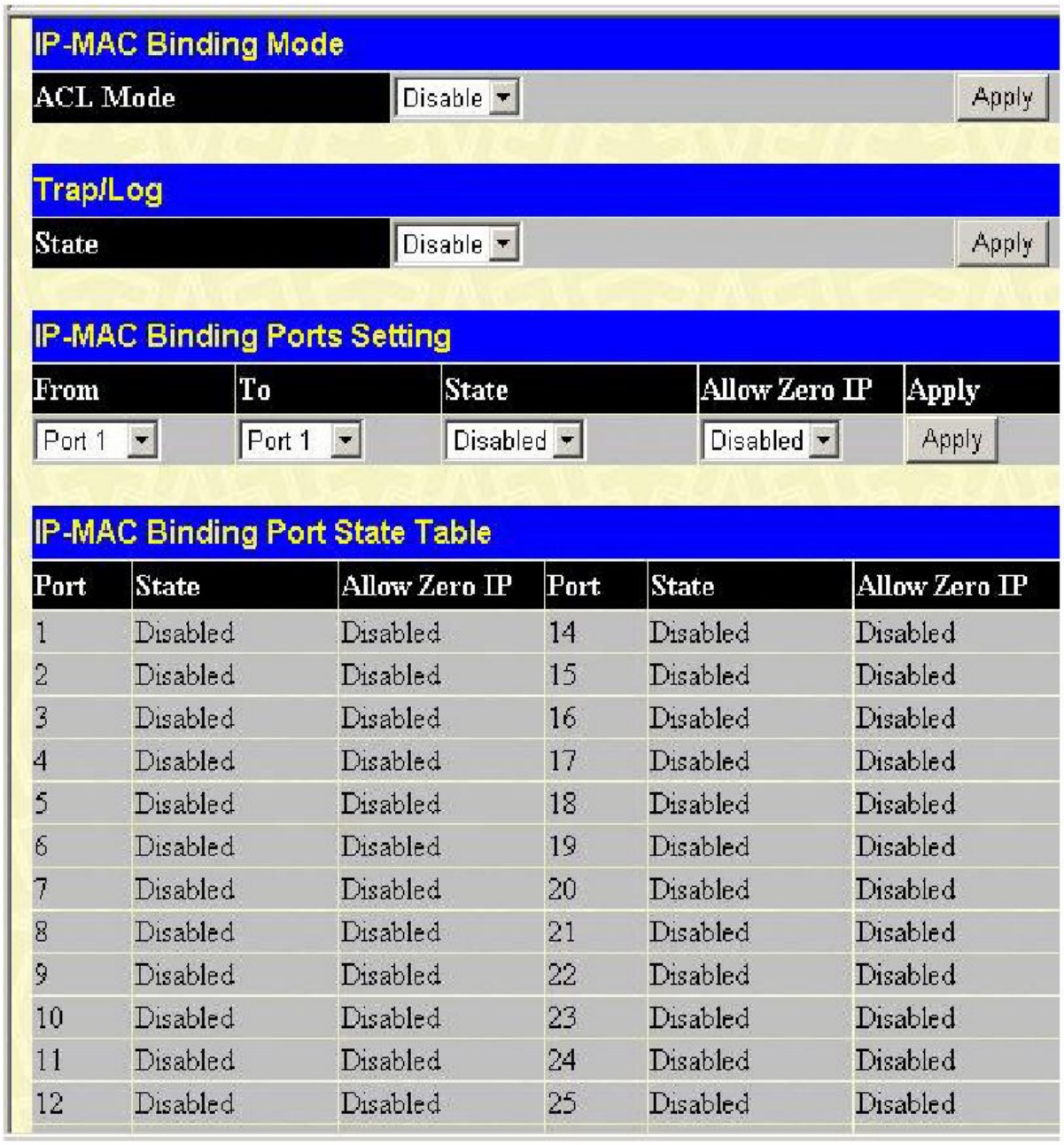
ПРИМЕЧАНИЕ: При закрузке конфигурационного файла на Коммутатор внимательно отнеситесь к загружаемым при этом настройкам ACL, в том числе профилям доступа режма ACL. Это поможет избежать многих проблем.

Пользователь может просмотреть настройки для каждого порта, кликнув по соответствующей данному порту кнопке **View** под заголовком **Display**. Эти записи не могут быть изменены или удалены, а также нельзя добавить новые правила. Тем не менее, в этих окнах представлена необходимая пользователю информация при настройке другх профилей. Кликните по кнопке **Next** для перехода к следующей странице правил. Также пользователю доступен быстрый поиск по **Access ID** путем ввода этого ID в соответствующее поле и клика по **Find**.

Рисунок 6- 106 Окно Access Rule Table для правила IP-MAC Binding (Изменить)

Настройка IP-MAC Binding для портов

Для включения или выключения функции IP-MAC Binding на определенных портах используется окно **IP-MAC Binding Ports Setting.** Для этого необходимо в меню **Configuration Menu** открыть папку **IP-MAC Binding** и кликнуть по **IP-MAC Binding Port**. Данное окно позволяет выбрать порт или диапазон портов с помощью полей **From…To**. Включение или выключение статуса IP-MAC Binding порта осуществляется в поле **State**. Включение (Enable) или выключение (Disable) опции нулевого IP-адреса осуществляется с помощью поля **Allow Zero IP**. Пользователь может также вкючить режим ACL для IP-MAC Binding, что создаст записи профилей доступа на Коммутаторе, как говорилось ранее. Кликните по **Apply** для сохранения выполненных настроек.



Port	State	Allow Zero IP	Port	State	Allow Zero IP
1	Disabled	Disabled	14	Disabled	Disabled
2	Disabled	Disabled	15	Disabled	Disabled
3	Disabled	Disabled	16	Disabled	Disabled
4	Disabled	Disabled	17	Disabled	Disabled
5	Disabled	Disabled	18	Disabled	Disabled
6	Disabled	Disabled	19	Disabled	Disabled
7	Disabled	Disabled	20	Disabled	Disabled
8	Disabled	Disabled	21	Disabled	Disabled
9	Disabled	Disabled	22	Disabled	Disabled
10	Disabled	Disabled	23	Disabled	Disabled
11	Disabled	Disabled	24	Disabled	Disabled
12	Disabled	Disabled	25	Disabled	Disabled

Рисунок 6- 107. Окно IP-MAC Binding Ports

Таблица IP-MAC Binding

Представленное ниже окно **IP-MAC Binding Setting** позволяет создать записи IP-MAC Binding. Для работы с этим окном необходимо в меню **Configuration,** в папке **IP-MAC Binding** кликнуть по **IP-MAC Binding Table.** В соответствующих полях необходимо

ввести IP- и MAC-адреса авторизованных пользователей и кликнуть по кнопке **Add**. Чтобы изменить IP- или MAC-адрес для какого-либо порта, следует в соответствующих полях сделать необходимые изменения и кликнуть по **Modify**. Для быстрого поиска записи IP-MAC Binding следует ввести нужные IP- и MAC-адреса, затем нажать **Find**. Для удаления записи необходимо кликнуть по соответствующей кнопке **Delete**. Чтобы удалить все записи из таблицы, кликните по кнопке **Delete All**.

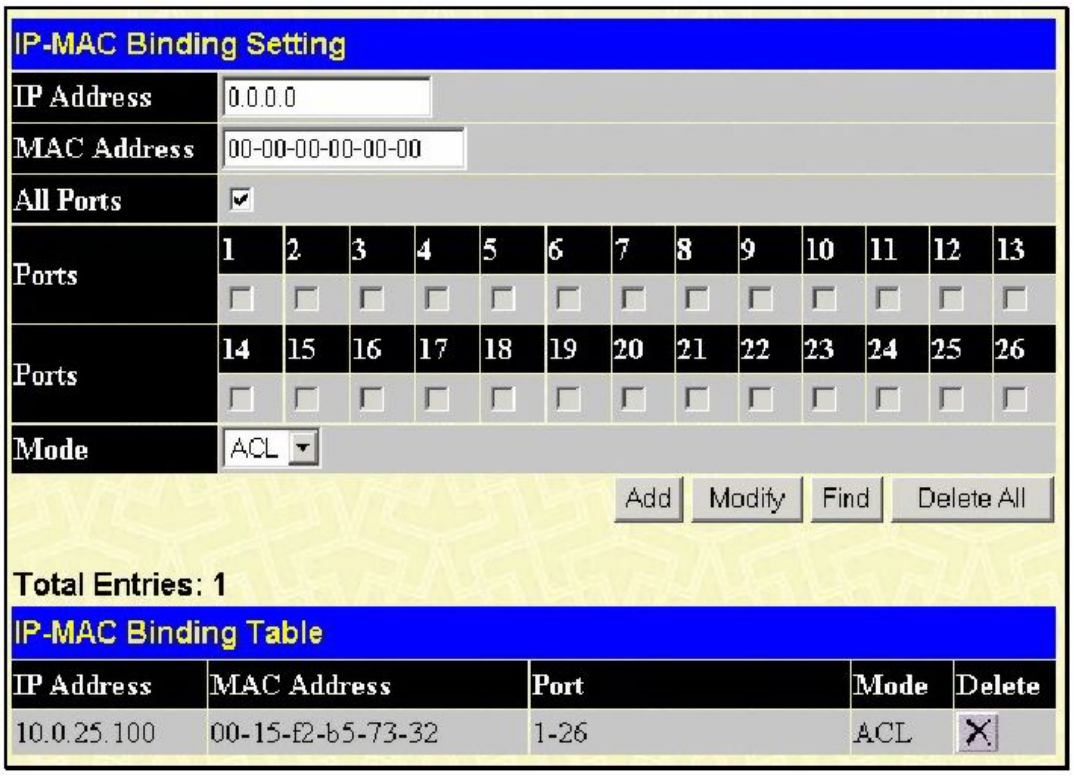


Рисунок 6- 108. Окно IP-MAC Binding Table

Для настройки и изменения доступны следующие поля:

Параметр	Описание
IP Address	Введите IP-адрес, который будет связан с MAC-адресом, представленным ниже
MAC Address	Введите MAC-адрес, который будет связан с IP-адресом, представленным выше.
All Ports	Для настройки IP-MAC Binding (IP-адрес+MAC-адрес) для всех портов Коммутатора, поставьте галочку в данном поле.
Ports	Выберите порты Коммутатора, для которых задается настройка IP-MAC Binding (IP-адрес+MAC-адрес)
Mode	Данное выпадающее меню позволяет пользователю выбрать режим работы функции IP-MAC Binding. На выбор доступны следующие опции: *ARP* – Выбор данной опции задает нормальный режим работы IP-Mac Binding, позволяющий создавать связки IP- и MAC-адреса. *ACL* – Выбор данной опции означает, что будут разрешены только пакеты от источника, IP- и MAC-адреса которого удовлетворяют связке IP-MAC Binding. Остальные пакеты будут отброшены Коммутатором. Этот режим может использоваться только в том случае, если режим ACL был включен в окне IP-MAC Binding Ports, описанном ранее.

Блокировка из-за несоответствия связки IP-MAC

Для просмотра неавторизованных устройств, которые были заблокированы из-за несоответствия связки IP-MAC, следует открыть окно **IP-MAC Binding Blocked**, представленное ниже. Для того чтобы открыть это окно**,** необходимо в меню **Configuration,** в папке **IP-MAC Blocked** кликнуть по **IP-MAC Binding Blocked.**

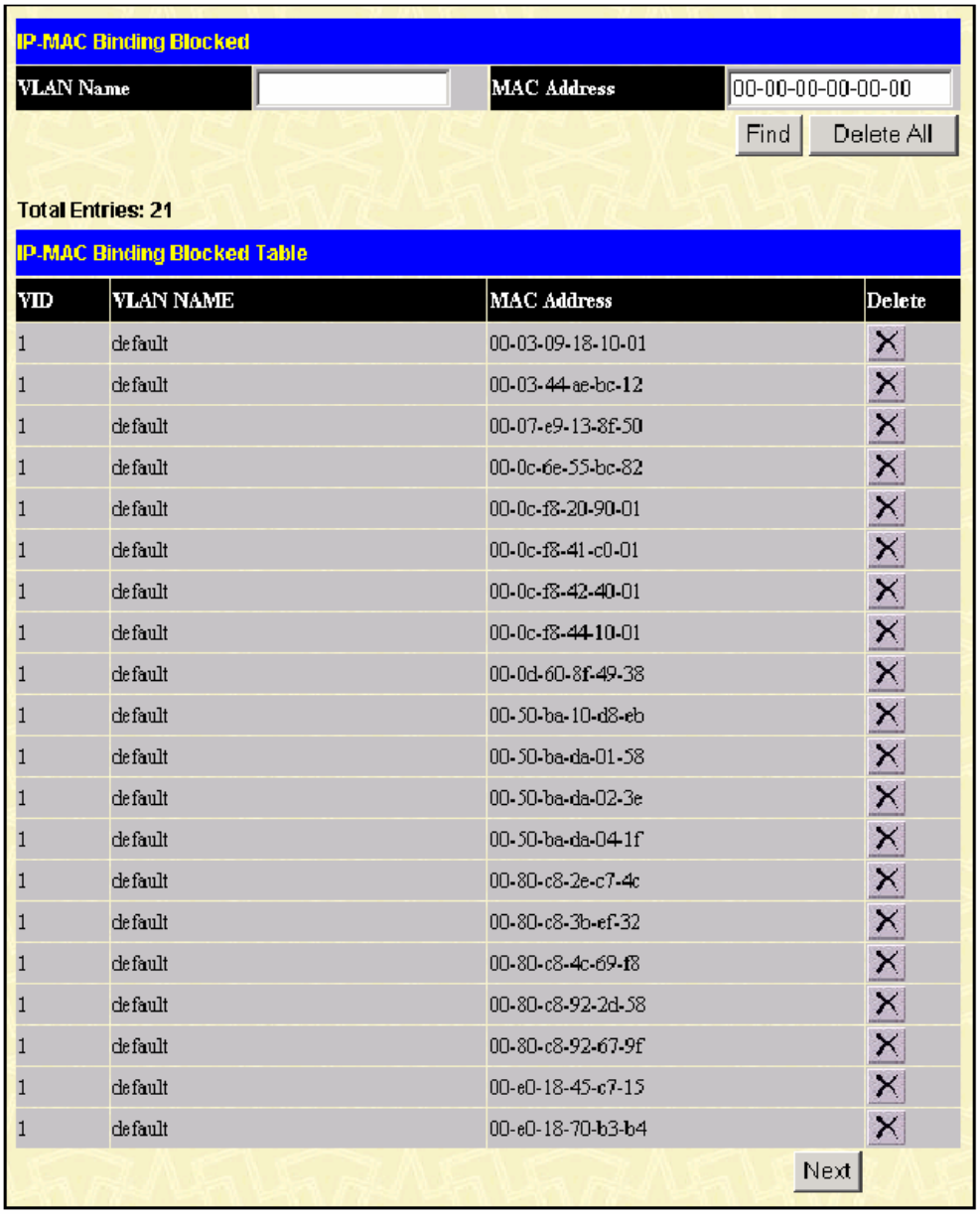


Рисунок 6- 109. Окно IP-MAC Binding Blocked

Для быстрого поиска неавторизованного устройства, заблокированного из-за несоответствия связки IP-MAC, следует ввести имя **VLAN** и MAC-адрес в соответствующих полях, а затем кликнуть по кнопке **Find**. Для удаления записи необходимо кликнуть по соответствующей кнопке под заголовком **Delete**. Для удаления всех записей в таблице **IP-MAC Binding Blocked Table** кликните по кнопке **Detete All**.

Настройки ограничения диапазона IP-адресов многоадресной рассылки

Окно **Limited IP Multicast Range** позволяет пользователю определить, какие многоадресные сообщения будут приняты на определённый порт коммутатора. Таким образом, эта функция

ограничивает количество принятых сообщений и количество многоадресных групп на Коммутаторе. Пользователь может задать IP-адрес или диапазон IP-адресов, с которых будет разрешен (Permit) или зарещен (Deny) приём многоадресных сообщений на определенные порты Коммутатора.

Настройка профиля ограничения диапазона IP-адресов многоадресной расылки

Для начала создайте профиль IP-адреса многоадресной рассылки, кликнув по **Configuration** > **Limited IP Multicast Range.** В результате откроется окно **Limited IP Multicast Range Profile Settings,** показанное ниже. Затем задайте диапазон IP-адресов многоадресной рассылки в профиле, введя макимальный и минимальный IP-адреса диапазона в поля **From Multicast IP** и **To Multicast IP** соответственно.

Кликните по кнопке Apply для принятия выполненных настроек. Новый профиль диапазона IP-адресов многоадресной рассылки отобразится в окне **The Port Information Table**. Чтобы удалить существующий профиль из списка **The Port Information Table**, кликните по соответствующей кнопке под заголовком "**Delete**".

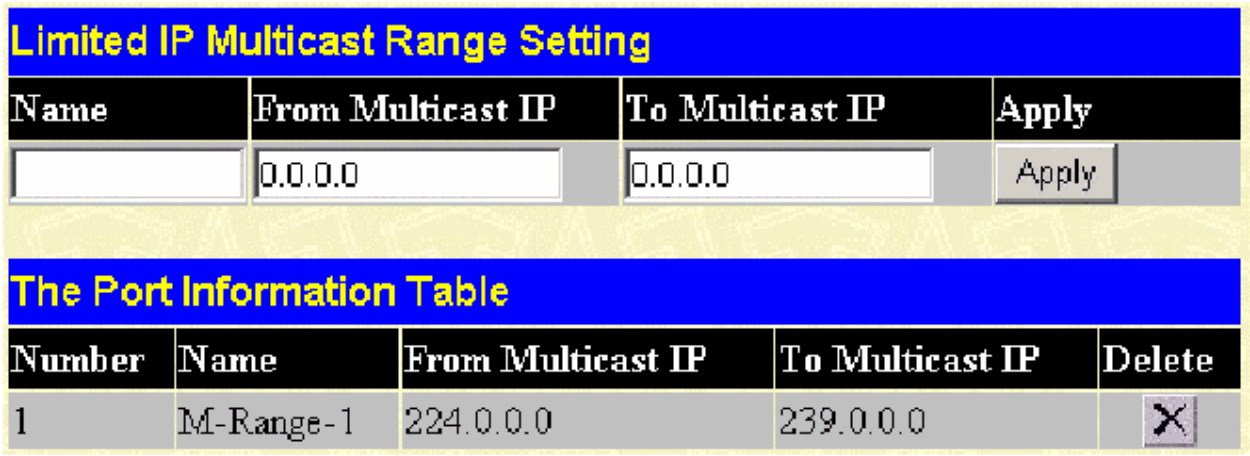


Рисунок 6- 110. Окно Limited Multicast Range Setting

Параметр	Описание
Name	Введите название профиля
From Multicast IP	Введите младший IP-адрес многоадресной рассылки.
To Multicast IP	Введите старший IP-адрес многоадресной рассылки.

Настройка статуса ограниченного диапазона IP-адресов многоадресной рассылки

После создания профилей диапазонов IP-адресов многоадресной рассылки можно начать настройку функции фильтрации адресов многоадресной рассылки для определнного порта или диапазона портов, используя окно **Limited IP Multicast Range Status,** показанное ниже. Для работы с этим окном кликните по **Configuration** > **Limited IP Multicast Range.**

Limited IP Multicast Range Status

From	To	State	Access	Apply
Port 1	Port 1	Disabled	Permit	Apply

The Port Information Table

Port	State	Access
1	Disabled	Deny
2	Disabled	Deny
3	Disabled	Deny
4	Disabled	Deny
5	Disabled	Deny
6	Disabled	Deny
7	Disabled	Deny
8	Disabled	Deny
9	Disabled	Deny
10	Disabled	Deny
11	Disabled	Deny
12	Disabled	Deny
13	Disabled	Deny
14	Disabled	Deny
15	Disabled	Deny
16	Disabled	Deny
17	Disabled	Deny
18	Disabled	Deny
19	Disabled	Deny
20	Disabled	Deny
21	Disabled	Deny
22	Disabled	Deny
23	Disabled	Deny
24	Disabled	Deny
25	Disabled	Deny
26	Disabled	Deny

Рисунок 6- 111 Окно Limited Multicast Range Status

Параметр	Описание
From…To	С помощью данных выпадающих меню задайте диапазон портов.
State	Поле **State** позволяет включить (*Enabled)* или выключить (*Disabled)* настройки для заданного порта или группы портов.
Access	В этом поле доступны следующие опции: *Permit* (по умолчанию) и *Deny*. Выбор опции *Permit* означает, что будет разрешена передача пакетов, IP-адрес источника которых совпадает с указанным в профиле. Выбор опции *Deny* означает, что будет запрещена передача пакетов, IP-адрес источника которых совпадает с указанным в профиле.

Для принятия настроек кликните по **Apply**.

Настройка ограниченного диапазона IP-адресов многоадресной рассылки

Чтобы задать порт или диапазон портов многоадресной рассылки, кликните по **Configuration** > **Limited IP Multicast Range.** В результате откроется окно **Limited IP Multicast Range,** показанное ниже.

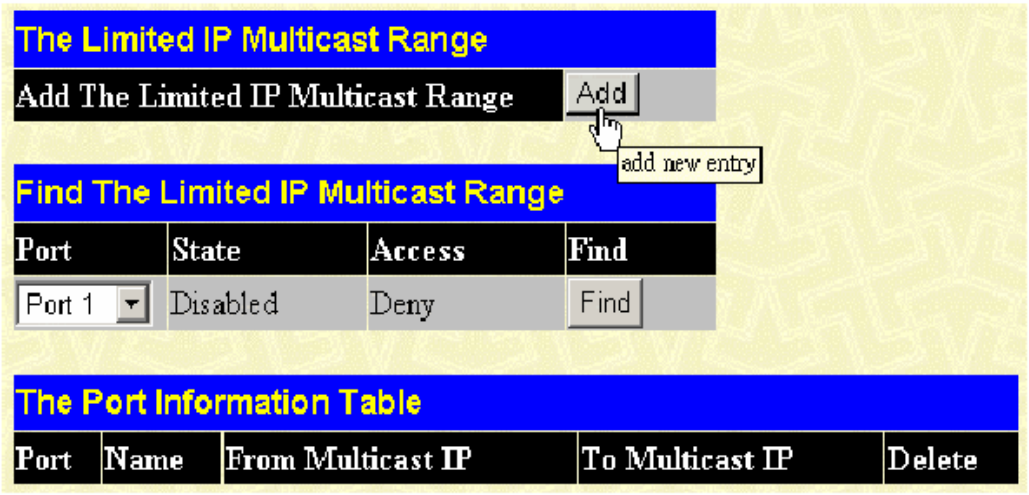


Рисунок 6- 112 Окно Limited IP Multicast Range

Затем кликните по кнопке **Add,** в результате чего откроется следующее окно **Limited IP Multicast Range Setting**. С помощью выпадающих меню **From** и **To укажите нужные порты** и введите имя профиля, созданное ранее в окне **Limited IP Multicast Range Profile Settings**, в поле **Name of Multicast Range**. Затем кликните по кнопке **Apply,** чтобы выполненные настройки вступили в силу.

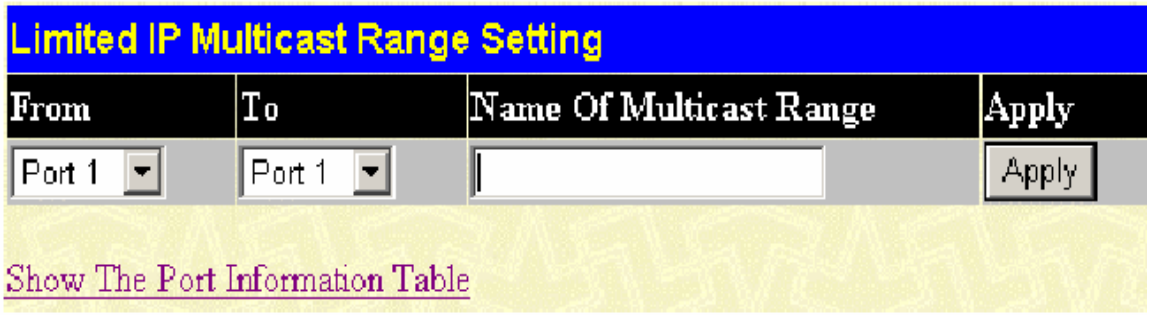
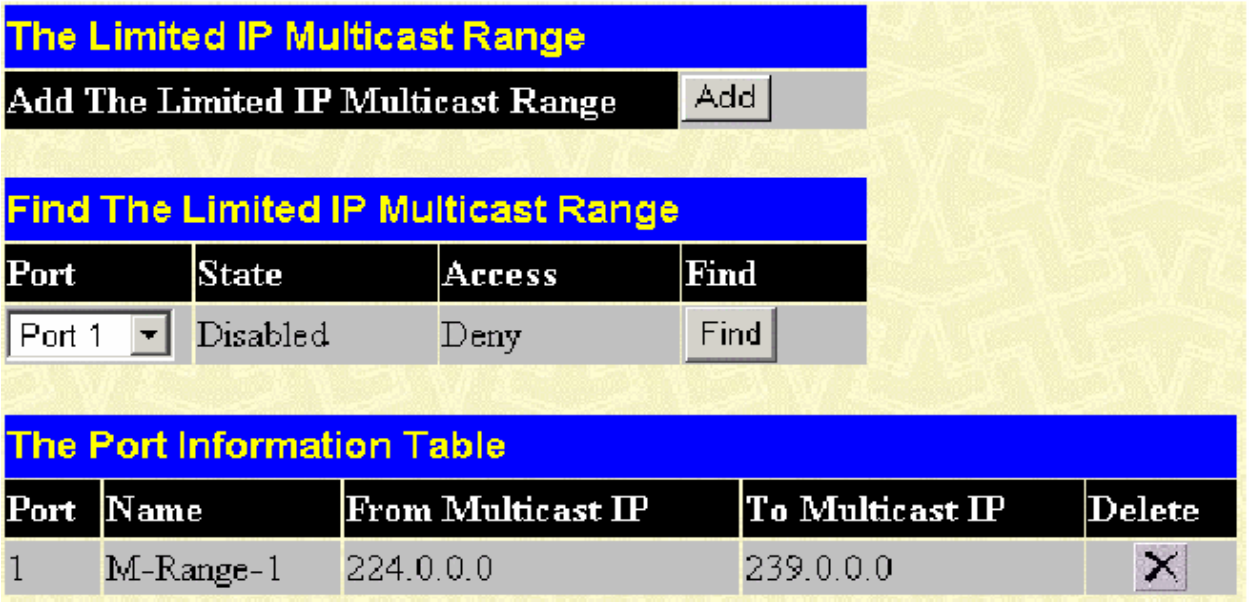


Рисунок 6- 113 Окно Limited Multicast Range Setting (Добавить)

Окно **Limited IP Multicast Range** отображает диапазон IP-адресов многоадресной рассылки для каждого порта. С помощью выпадающего меню **Port** выберите нужный номер порта и кликните по

кнопке **Find**, детализированная информация появится в окне **The Port Information Table**. Чтобы удалить текущие настройки, кликните по соответствующей кнопке под заголовком “Delete”.



Построение IP-сетей 3 уровня
Статическая таблица ARP

Address Resolution Protocol (ARP) – TCP/IP-протокол, который позволяет осуществлять преобразование IP-адресов в физические адреса (MAC-адреса). Статическая таблица ARP дает возможности сетевым администраторам для работы (просмотр, изменение, удаление) с ARP-информацией, касающейся определённых устройств.

Введенные в ARP-таблицу статические записи позволяют осуществлять трансляцию IP-адресов в MAC-адреса.

Для работы с окном **Static ARP Table** откройте папку **Configuration**, затем откройте папку **Layer 3 IP Networking** и кликните по **Static ARP Table**.

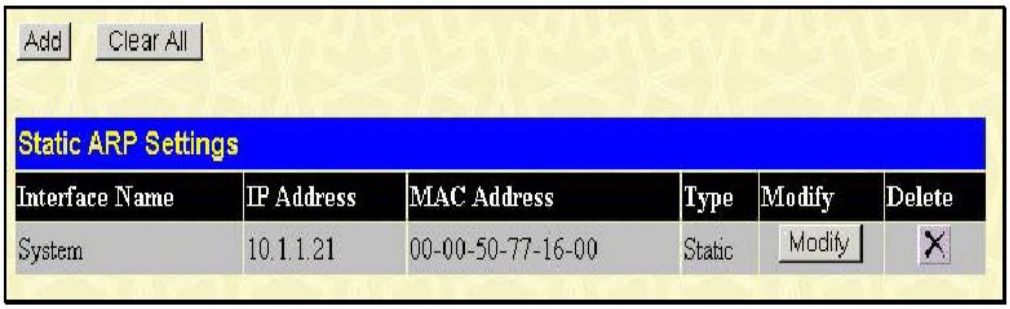


Рисунок 6- 114. Окно Static ARP Settings

Для добавления новой записи следует кликнуть по кнопке **Add**, показанной в следующем окне конфигурации:

Рисунок 6- 115. Окно Static ARP Table – добавление новой записи.

Для изменения записи следует кликнуть по кнопке **Modify**, в результате появится следующее окно для настройки.

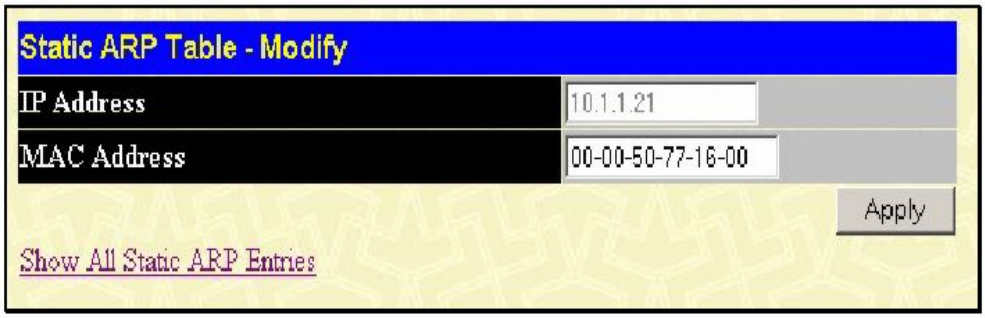


Рисунок 6- 116. Окно Static ARP Table - изменить

Могут быть установлены следующие поля:

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

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

Примечание: Коммутатор поддерживает до 255 статических ARP-записей.

DHCP/BOOTP Relay

Параметр Relay Hops Count Limit (Лимит количества шагов) позволяет задать максимальное число шагов (hop, маршрутизаторов) при отправке DHCP/BOOTP-сообщений. Если значение данного счетчика становится больше, чем лимит счётчика, то пакет отбрасывается. Диапазон значений от *1* до *16* шагов, значение по умолчанию равно *4*. Параметр Relay Time Threshold задает максимальное время (в секундах), в течение которого Коммутатор будет ждать до продвижения BOOTREQUEST-пакета. Если значение данного поля пакета меньше, чем этот порог, то пакет будет отброшен. Диапазон значений данного поля может быть от 0 до *65 536* секунд, значение по умолчанию *0*.

Глобальная настройка DHCP / BOOTP Relay на Коммутаторе

Для работы с окном **DHCP/BOOTP Relay Global Settings** кликните **Configuration** > **Layer 3 Networking >DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Global Settings**:

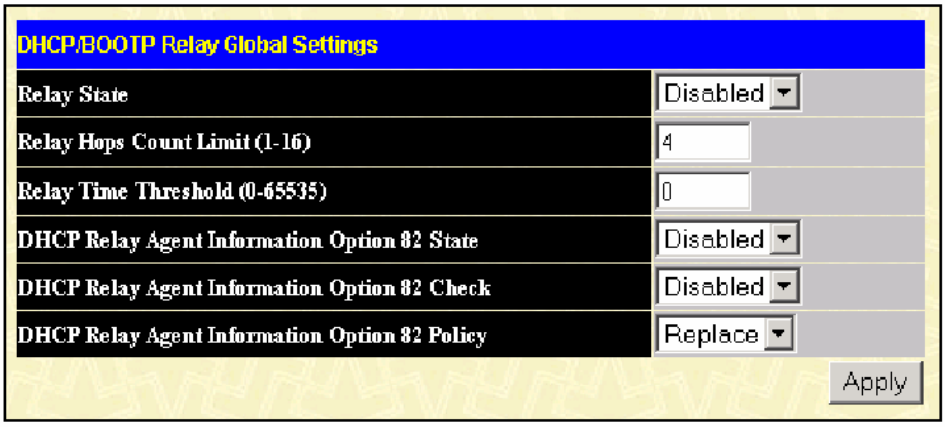


Рисунок 6- 117. Окно DHCP/ BOOTP Relay Global Settings

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.

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

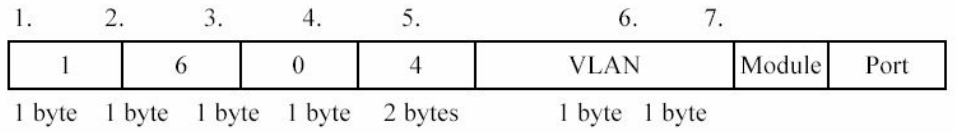
Примечание: Если коммутатор получает от DHCP-клиента пакет, содержащий поле option-82, и функция **DHCP Agent Information Option 82 Check** включена, то коммутатор отбросит пакет. Однако возможность настроить клиента с полем option 82 существует. В случае необходимо выключить функцию **DHCP Agent Information 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-3500 xStack

Команда **config dhcp_relay option_82** позволяет настроить option-82 агента перенаправления запросов DHCP на коммутаторе. Форматы circuit ID sub-option и remote ID sub-option следующие:

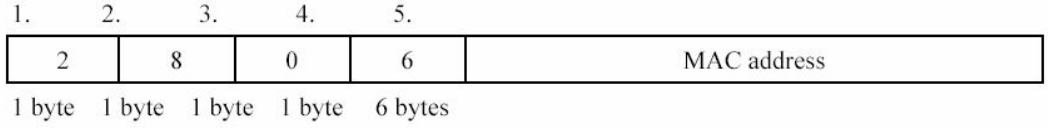
Примечание: В circuit ID sub-option автономного коммутатора значение поля Module всегда равно нулю.

Формат Circuit ID sub-option:



а. Тип Sub-option
б. Длина
в. Тип Circuit ID
г. VLAN: исходящий VLAN ID пакета DHCP-клиента.
д. Module: для автономного коммутатора это поле всегда равно 0; для стекируемого коммутатора – это Unit ID.
е. Port: номер исходящего порта для пакета DHCP-клиента, нумерация портов начинается с 1.

Формат Remote ID sub-option:



1. Тип Sub-option
2. Длина
3. тип Remote ID
4. длина
5. MAC-адрес: MAC-адрес Коммутатора.

Рисунок 6- 118. Форматы Circuit ID sub-option и Remote ID Sub-option

Настройки интерфейса DHCP/BOOTP

DHCP/ BOOTP Relay Interface Settings позволяет пользователю настроить IP-адрес сервера для передачи DHCP/ BOOTP-информации на Коммутатор. Используя следующее окно, пользователь может ввести предварительно сконфигурированный IP-интерфейс, который будет напрямую соединяться с DHCP/BOOTP-сервером. Выполненные надлежащим образом настройки отобразятся в окне **BOOTP Relay Table** после того, как пользователь кликнет по кнопке **Add** под заголовком **Apply.** Пользователь может добавить до четырёх IP-адресов серверов на один IP-интерфейс Коммутатора. Записи могут быть удалены путём нажатия по соответствующей кнопке . Для включения и настройки **DHCP/BOOTP Relay Global Settings** на Коммутаторе следует кликнуть **Configuration** > **Layer 3 Networking > DHCP/BOOTP Relay** > **DHCP/BOOTP Relay Interface Settings**:

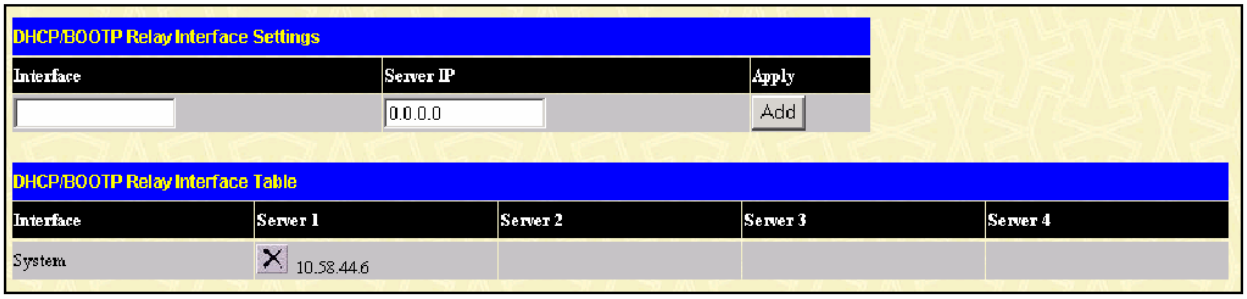


Рисунок 6-92. Окно DHCP/BOOTP Relay Interface Settings и DHCP/BOOTP Relay Interface Table

Могут быть сконфигурированы или просмотрены следующие параметры:

Параметр	Описание
Interface	IP-интерфейс Коммутатора, к которому напрямую будет подключен Сервер.
Server IP	Введите IP-адрес DHCP/BOOTP-сервера. Для одного интерфейса можно задать до четырёх IP-адресов серверов.

Раздел 7 - Управление

Задание безопаных IP-адресов
Учётные записи пользователей
Управление аутентификацией доступа (TACACS)
Secure Sockets Layer (SSL)
Secure Shell (SSH)
SNMP-менеджер

Данный раздел поможет пользователю в настройке функций безопасности Коммутатора. Коммутатор оснащен такими функциями безопасности, как TACACS, управление безопаностью IP-адресов, SSL и SNMP. Все эти функции будут подробно рассмотрены в этом разделе.

Задание безопасных IP-адресов

В папке **Management** кликните по **Security IP**, после чего появится следующее окно:

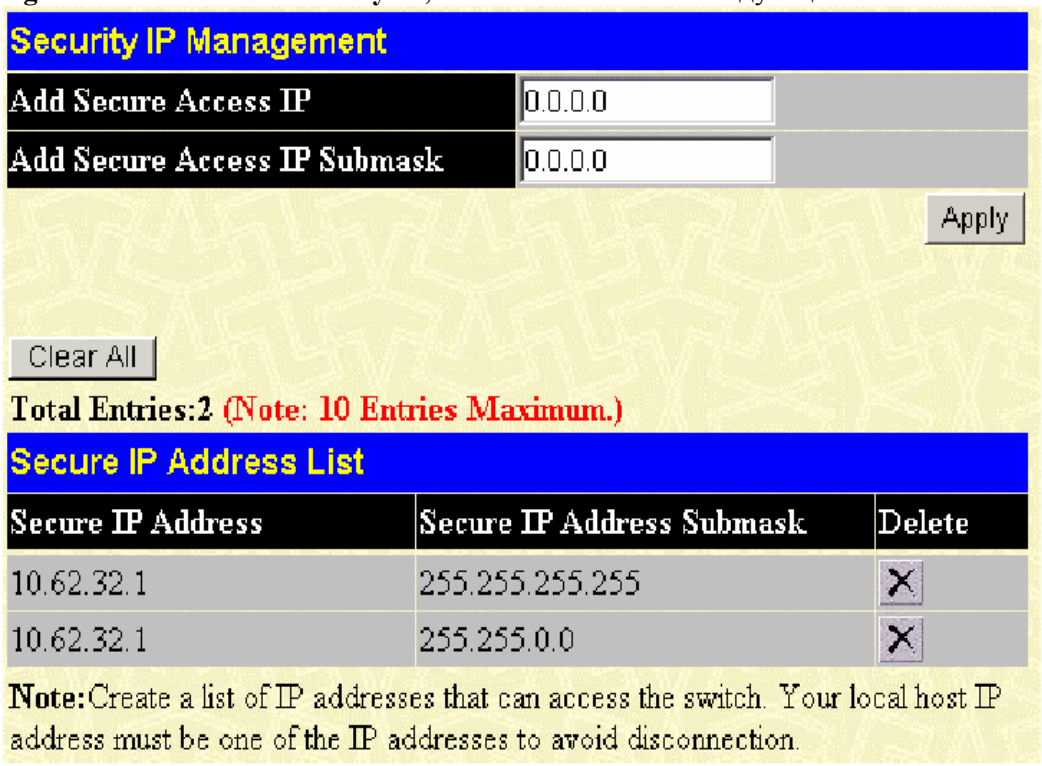
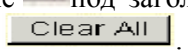


Рисунок 7.1 – Окно Security IP Management

Окно Security IP Management позволяет разрешить настройки Коммутатора с удаленных станций. В данном окне существует возможность ввести IP-адреса станций управления, и только с этих станций будет доступно управление с помощью Web-интерфейса или через Telnet. Введите IP-адрес или IP Submask и нажмите кнопку **Apply** для применения настроек**.**

Для удаления записи кликните по соответствующей кнопке  под заголовком Delete. Для удаления всех записей безопасных IP-адресов кликние по кнопке  .

Учетные записи пользователей

Окно **User Account Management** позволяет осуществлять управление привилегиями пользователя. Для просмотра существующих учетных записей пользователей откройте папку

Security Management и кликните по **User Accounts.** В результате откроется окно **User Account Management**, показанное ниже.

Рисунок 7.2 – Окно User Account Management

Для добавления нового пользователя, кликните по кнопке **Add**. Для изменения или удаления существующей учетной записи пользователя кликните по кнопке **Modify** напротив соответствующей записи.

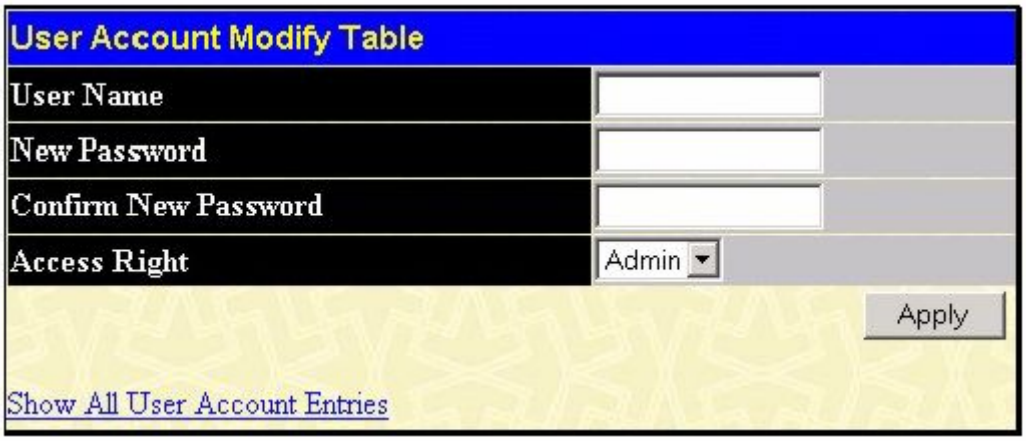


Рисунок 7.3 – Окно User Accounts Modify Table – Add

Для добавления нового пользователя введите имя пользователя **User Name** и новый пароль **New Password**, затем в поле **Confirm New Password** повторно введите указанный пароль для подтверждения. Выберите уровень привилегий (*Admin*, *Operator* или *User*) в выпадающем меню поля **Access Right**.

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

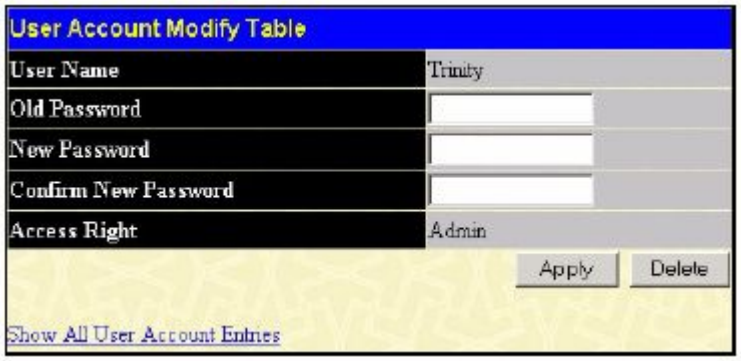


Рисунок 7.4 – Окно User Account Modify Table - Изменить

Изменение или удаление учетной записи существующего пользователя доступно в окне **User Account Modify Table**. Для удаления учетной записи пользователя кликните по кнопке **Delete.** Для изменения пароля введите его в поле New Password и повторите ввод в поле Confirm New Password. Уровень привилегий (*Admin, Operator* или *User)* можно посмотреть в поле **Access Right**.

Привилегии пользователей «Admin», «Operator» и «User»

Существует три уровня привилегий: *Admin* (Администратор), *Operator* (Оператор) и *User* (Пользователь). Настройки, доступные пользователям с привилегией *Admin,* далеко не всегда доступны пользователям с привилегией *User*. Следующая таблица иллюстрирует основные различия в уровнях привилегий *Admin, Operator* и *User:*

Функции управления	Admin	Operator	User
Мониторинг сети	Да	Да	Только чтение
Настройка Community String и станций для отправки сообщений Trap	Да	Да	Только чтение
Обновление программного обеспечения и конфигурационных файлов	Да	Только чтение	Только чтение
Системные утилиты	Да	Нет	Нет
Сброс к заводским настройкам	Да	Нет	Нет
Создание/ настройка/ удаление учетных записей пользователей	Да	Нет	Нет
Просмотр учетных записей пользователей	Да	Нет	Нет

Таблица 7.1 – Привилегии *Admin, Operator* и *User*

После создания учетной записи пользователя с уровнем привилегий Admin, убедитесь, что изменения сохранены. Для этого откройте папку **Maintenance** и кликните по кнопке **Save Configuration.**

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

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 кликните **Security Management ⇨ Access Authentication Control ⇨ Policy & Parameters**:

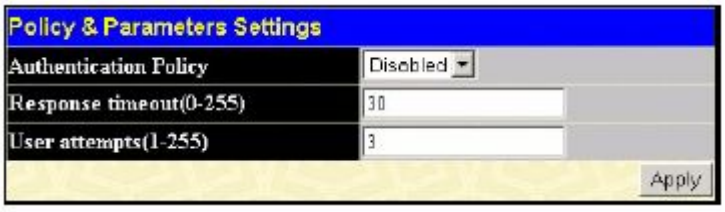


Рисунок 7.5 – Окно «Policy&Parameters Settings»

В этом окне доступны для настройки следующие параметры:

Параметры	Описание
Authentification Policy	Данное выпадающее меню позволяет включить (Enabled) и выключить (Disabled) политике аутентификации на Коммутаторе.
Response Timeout (0 –	Данное поле позволяет задать время ожидания от пользователя информации аутентификации. Доступны значения от 0 до 255 секунд. По умолчанию

255)	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**, чтобы измененные настройки вступили в силу.

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 просмотра данного окна нажмите:
Security Management ⇨ Access Authentication Control ⇨ Application Authentication Settings

Рисунок 7.6 – Окно Application's Authentication Settings

Для настройки доступны следующие параметры:

Параметры	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**, чтобы новые настройки вступили в силу.

Настройка группы 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 Management ⇨ Access Authentication Control ⇨ Authentication Server Group**:

Рисунок 7.7 – Окно Authentication Server Group Settings

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 7.8 – Окно Add a Server Host to Server Group (tacacs)

Для добавления в список сервера аутентификации введите IP-адрес в поле IP Address, выберите протокол, связанный с IP-адресом группы серверов аутентификации, и кликните по **Add to Group**. Для того чтобы добавить новую пользовательскую группу серверов которая кликните по кнопке **Add**, после чего появится следующее окно для настроек.

Рисунок 7.9 – Окно Authen 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(в данном случае, Trinity), заданное пользователем, появится в окне **Authentication Server Group Settings**, которое представлено ниже.

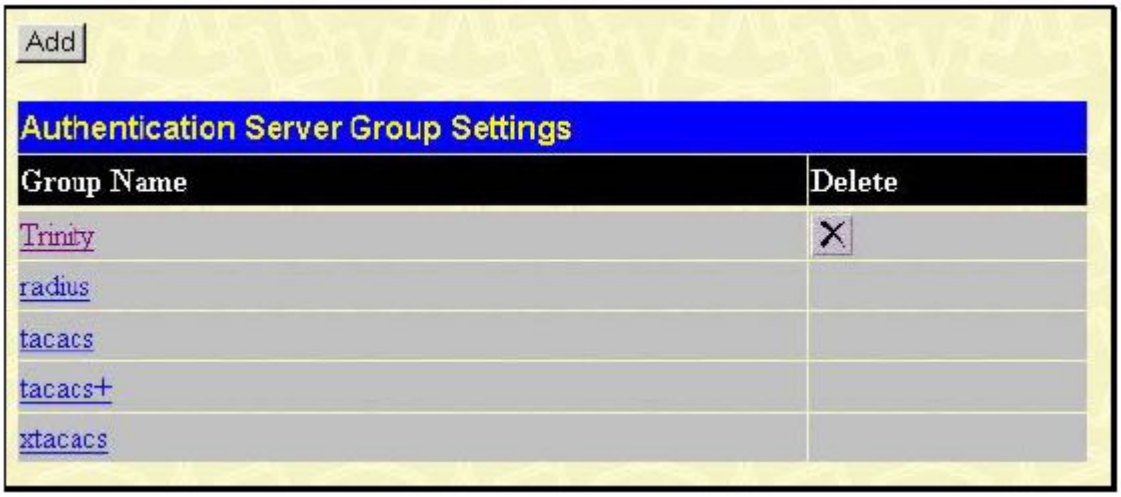


Рисунок 7.10 – Окно Authentication Server Group Settings

Настройки новой группы, как и других групп, могут быть изменены путем нажатия на гиперссылку имени группы. Кроме того, в отличие от других групп, группа, определенная пользователем, может содержать любую комбинацию протоколов, используемых серверами в данной группе (Например, tacacs – xtacacs –tacacs+).

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. Т.е. нельзя добавить сервер аутентификации, работающий на основе протокола TACACS, в группу серверов аутентификации XTACACS.

Серверы аутентификации

Данное окно отображает определенные пользователем серверы аутентификации ***Authentication Server Hosts*** для TACACS/XTACACS/TACACS+/RADIUS протоколов безопасности. Когда пользователь пытается получить доступ к коммутатору по 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 Management ⇨ Access Authentication Control ⇨ Authentication Server Host**:

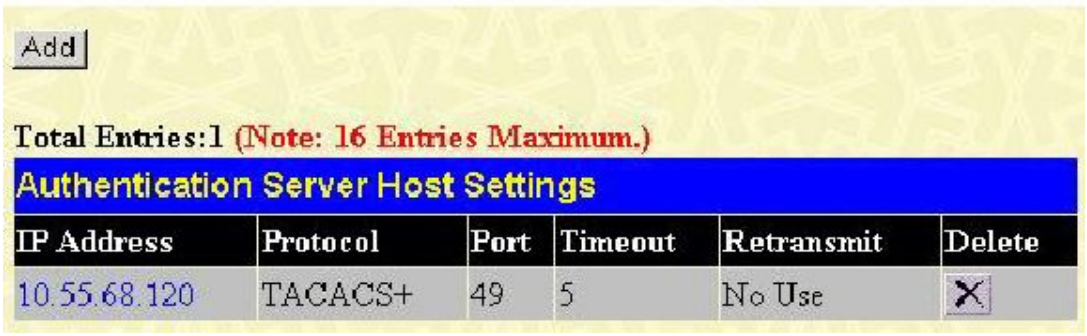


Рисунок 7.11 – Окно Authentication Server Host Settings

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

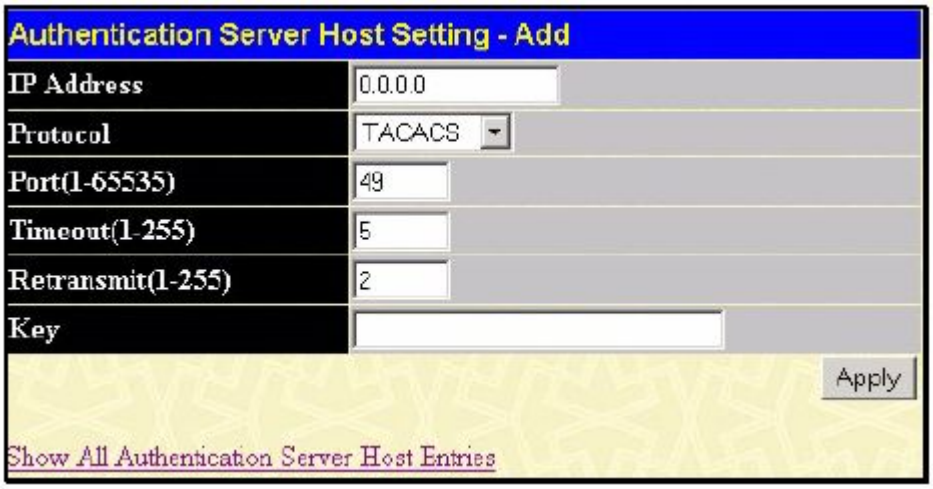


Рисунок 7.12 - Окно Authentication Server Host Settings – Add

Для нового сервера аутентификации доступны для настройки следующие параметры:

Параметр	Описание
IP Address	IP-адрес внешнего сервера аутентификации, который предполагаетсфя 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	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 новый 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.

Списки методов регистрации (Login Metod Lists)

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 Management ⇨ Access Authentication Control ⇨ Login Method Lists**:

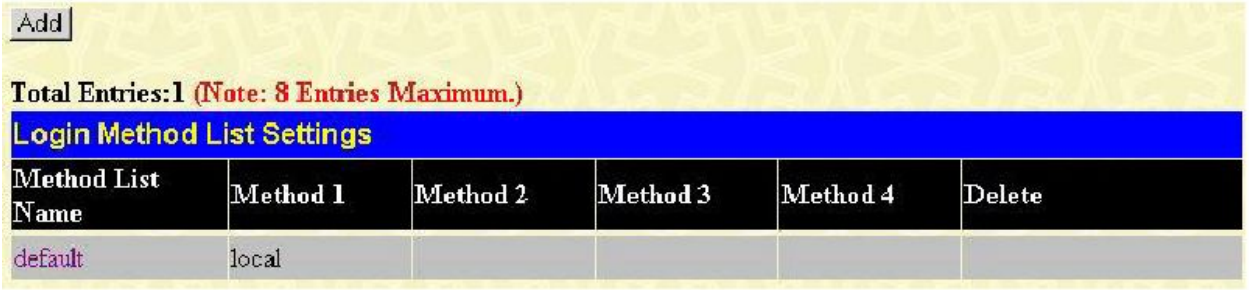


Рисунок 7.13 – Окно Login Method Lists Settings

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 ***X*** 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:

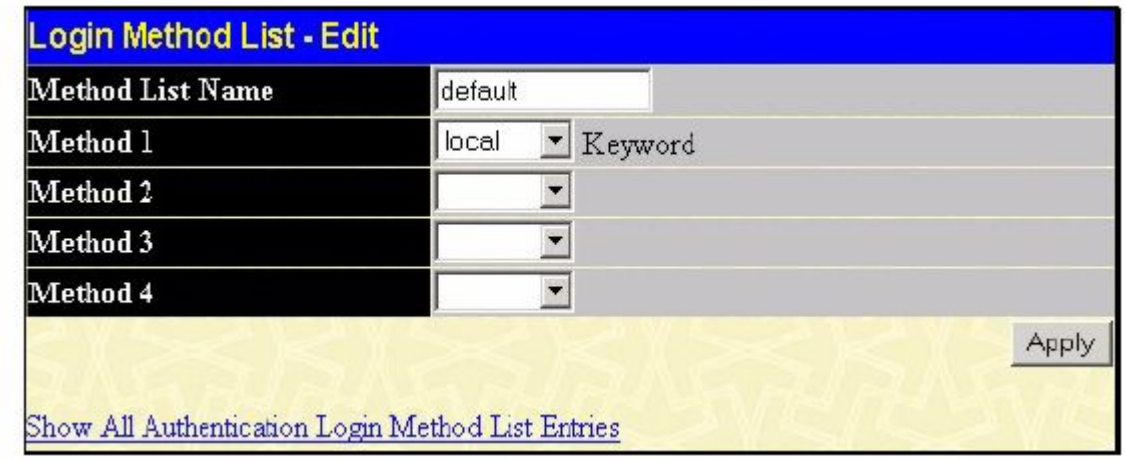


Рисунок 7.14 – Окно Login Method List – Edit (по умолчанию)

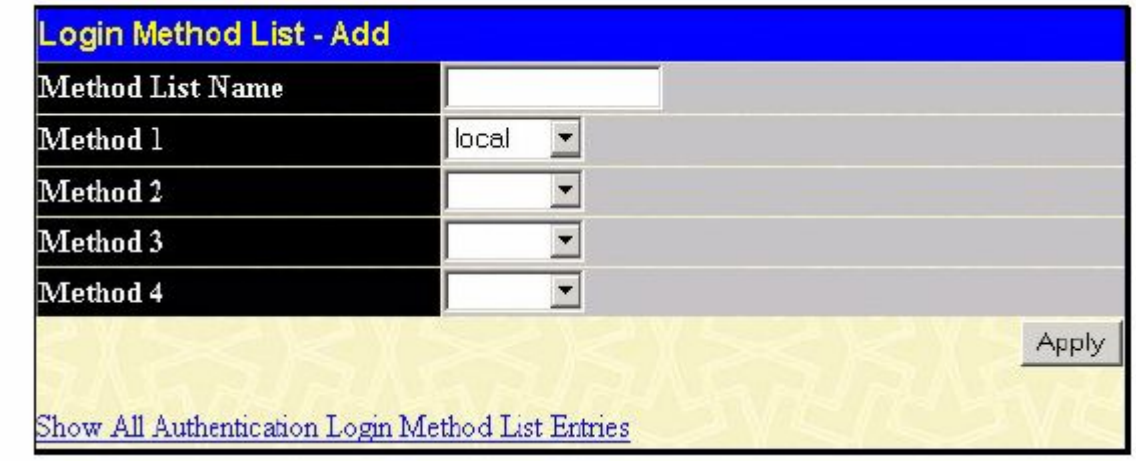


Рисунок 7.15 – Окно Login Method List – Add

Для задания списка методов регитрации 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 Management ⇨ Access Authentication Control ⇨ Enable Method Lists**:

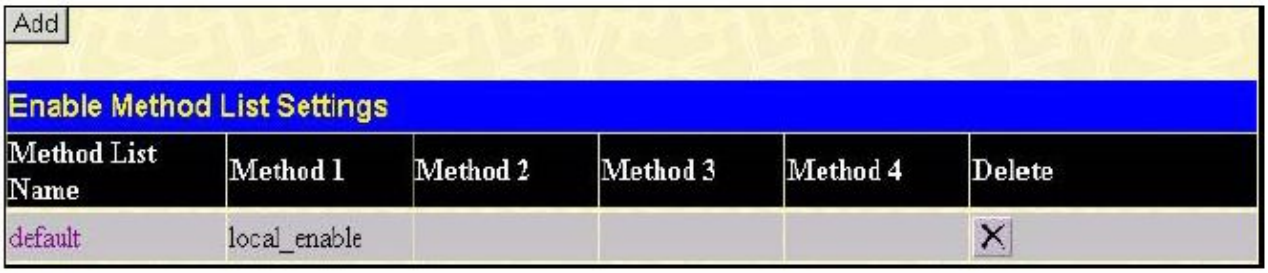


Рисунок 7.16 – Окно «Enable Method List Settings»

Для удаления списка Enable Method List, созданного пользователем, нажмите ***X*** 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:

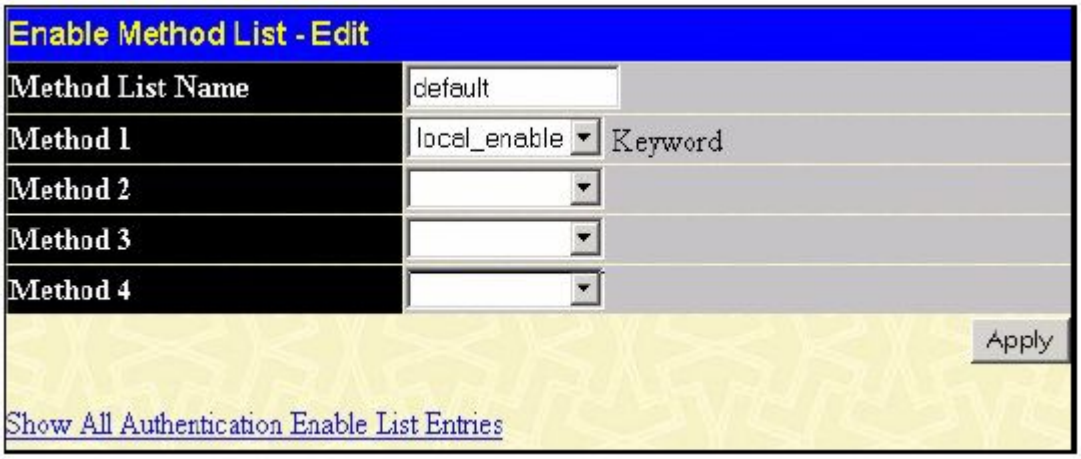


Рисунок 7.17 – Окно Enable Method List - Edit

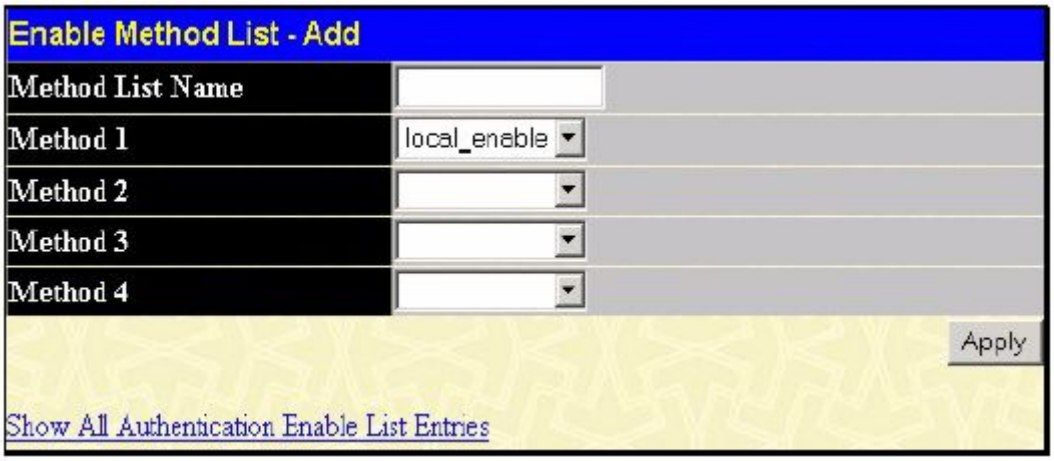


Рисунок 7.18 – Окно Enable Method List - Add

Данное окно позволяет задать следующие параметры:

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.

Локальный пароль

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 просмотра следующего окна, нажмите **Security Management ⇨ Access Authentication Control ⇨ Local Enable Password**:

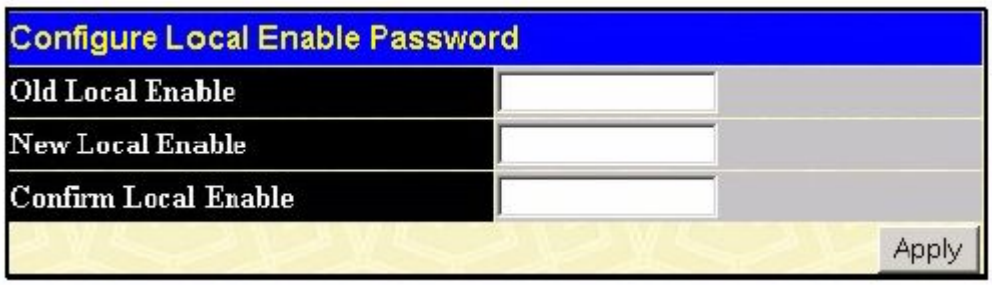


Рисунок 7.19 – Окно Configure Local Enable Password

Для установки локального пароля необходимо настроить следующие параметры и кликнуть по **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 (Включение привилегий уровня Администратора)

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. Для работы со следующеим окном нажмите **Security Management ⇨ Access Authentication Control ⇨ Enable Admin**:

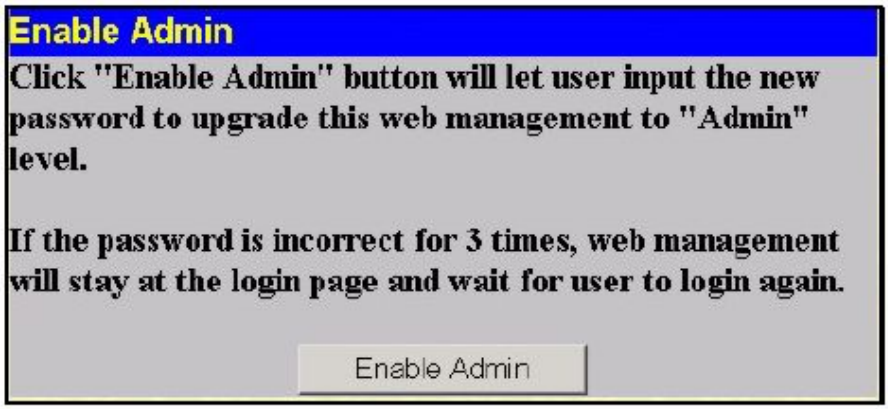


Рисунок 7.20 – Окно Enable Admin

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 7.21 – Диалоговое окно Enter Network Password

Secure Socket Layer (SSL)

Secure Sockets Layer (SSL) – протокол, который обеспечивает безопасное взаимодействие между хостом и клиентом с помощью использованию 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 TFPT-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. Для работы с показанным ниже окном кликните **Configuration >Secure Socket Layer (SSL) > Download Certificate:**

Рисунок 7.22 – Окно Download Certificate

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

Параметр	Описание
Certificate Type	Выберите тип загружаемого сертификата, который относится к серверу ответственный за подачу сертификата. В данной реализации это поле может содержать только значение *local*
Server IP	Введите IP-адрес TFPT-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).

Настройка 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, http://10.90.90.90). В противном случае будет возникать ошибка и отказ в доступе при авторизации.

Для работы со следующим окном кликните **Configuration > Secure Socket Layer (SSL) > Configuration:**

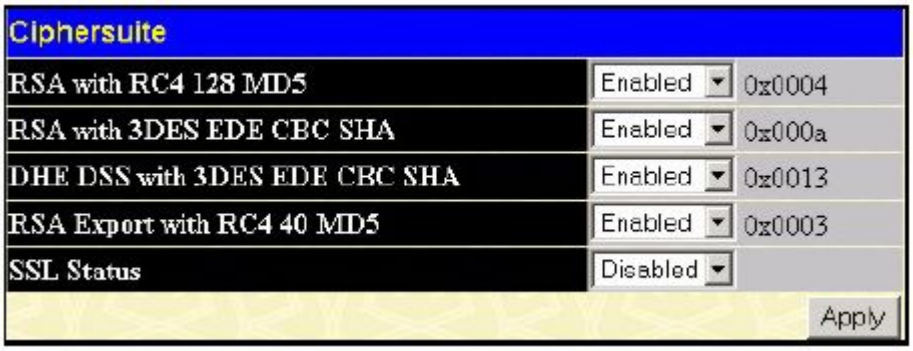


Рисунок 7.23 – Окно Ciphersuite

При настройке функции SSL на Коммутаторе настройте следующие параметры и кликните по **Apply**.

Параметр	Описание
RSA with RC4 128 MD5	Выбор данной опции задает использование ключа обмена RSA, 128-битное шифрование RC4 и алгоритм шифрования MD5 Hash Algorithm. Управление 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).
SSL Status	Используйте выпадающее меню для включения/выключения SSL-статуса Коммутатора. По умолчанию установлено значение *Disabled* (выключено).

Примечание: Некоторые настройки функции SSL не доступны в Web-интерфейсе данного коммутатора. Эти настройки должны осуществляться из командной строки. Для получения более подробной информации по настройке SSL следует обратиться к Руководству по интерфейсу командной строки для коммутаторов серии DES-3500, находящемуся на CD-диске.

Примечание: При выборе опции SSL переключатель на Web-интерфейс управления будет неактивным. Для того чтобы зарегистрироваться на Коммутаторе заново, адрес (URL) должен начинаться с http// (например, http://10.90.90.90). В противном случае Web-браузер выдаст ошибку и отказ в доступе.

Secure Shell (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 SSH

Данное окно предназначено для конфигурации и просмотра настроек SSH-сервера. Для открытия данного окна кликните **Security Management > Secure Shell (SSH) > SSH Configuration**:

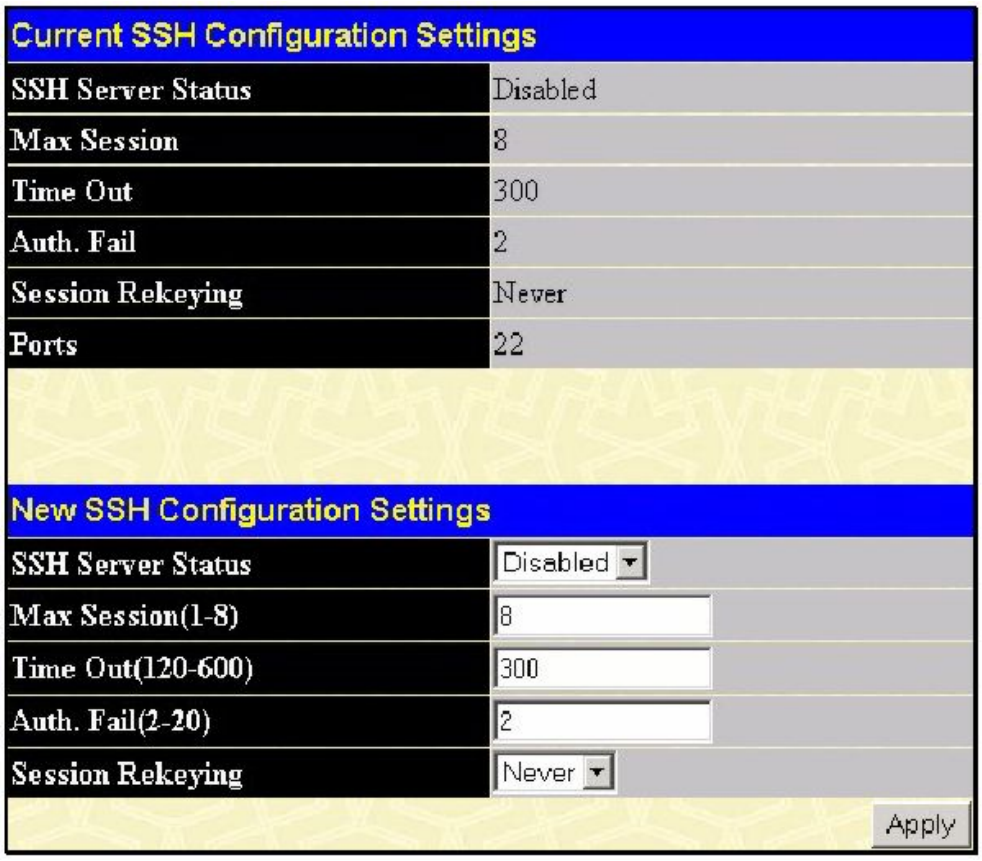


Рисунок 7.24 – Окно Current SSH Configuration Settings

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 300 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*.

SSH Algorithm (SSH-алгоритм)

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 Management > Secure Shell (SSH) > SSH Algorithm:**

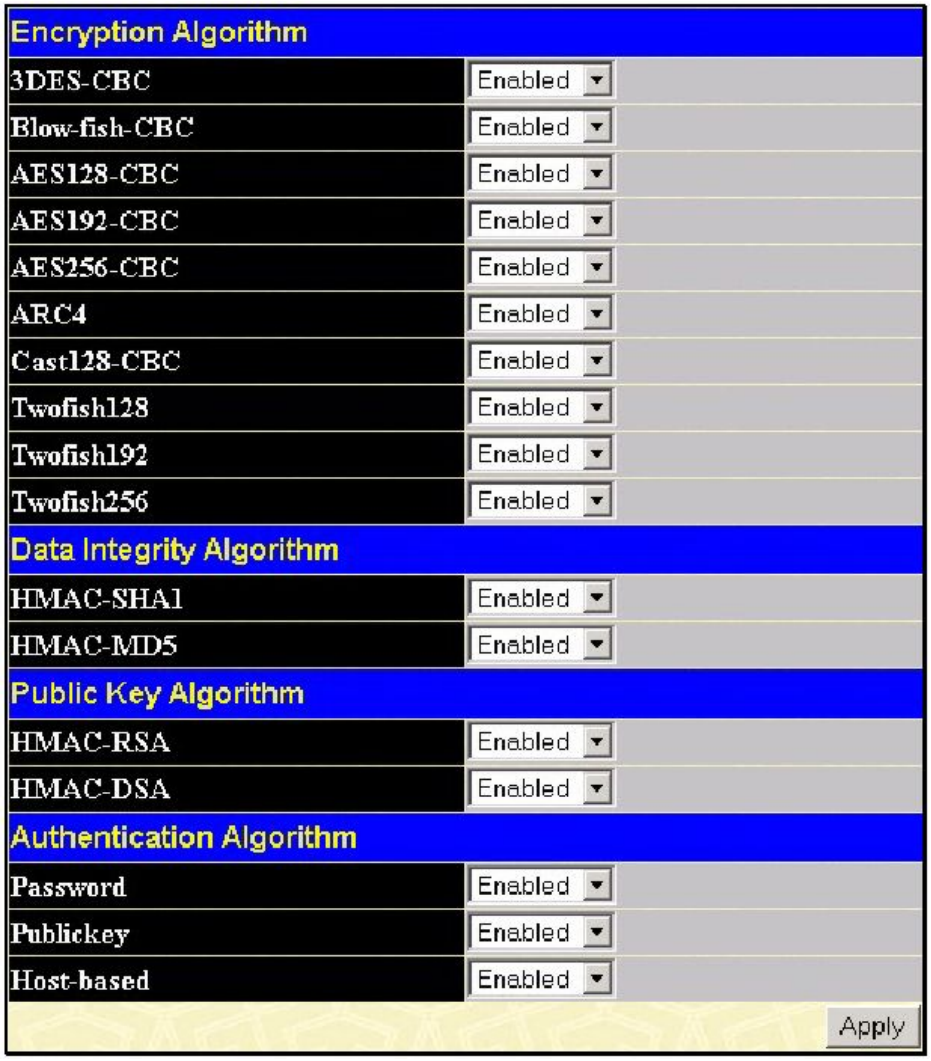


Рисунок 7.25 – Окно Encryption Algorithm

Могут быть заданы следующие алгоритмы:

Параметр	Описание
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).
Authentication Algorithm	
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*.

Кликните по **Apply** для принятия изменений.

Аутентификация SSH-пользователя

Данное окно используется для настройки параметров для подключения пользователей к Коммутатору через SSH. Для работы с эти окном кликните **Security Management > Secure Shell > SSH User Authentication**.

Рисунок 7.26 – Окно Current Accounts

Рассмотрим пример. Учетная запись «Trinity» была настроена ранее в окне **User Accounts** в папке **Security Management**. 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.

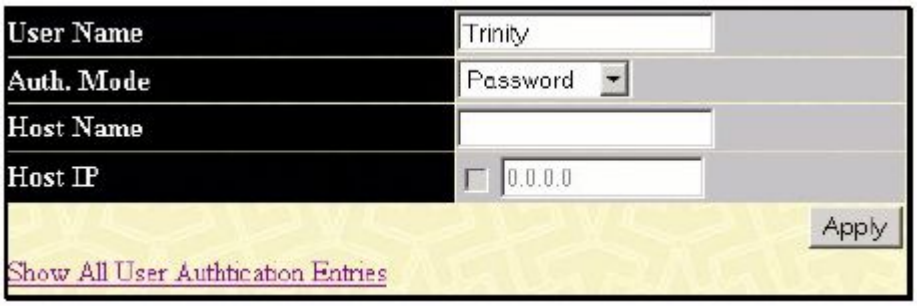


Рисунок 7.27 – Окно User Accounts Modify Table

Пользователь может задать 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 принятия 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.

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-3500 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 серии DES-3500 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 серии DES-3500 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.

Таблица SNMP-пользователей

Таблица **SNMP User Table** отображает всех сконфигурированных на коммутаторе SNMP-пользователей. Для открытия окна, показанного ниже, нажмите: **Security Management ⇨ SNMP Manager ⇨ SNMP User Table.**

Рисунок 7.28 – Окно SNMP User Table

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

Рисунок 7.29 – Окно «SNMP User Table Display»

В окне отображаются следующие параметры:

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

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

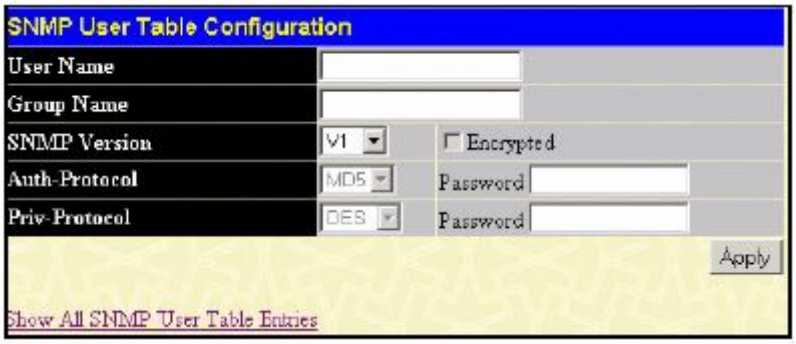


Рисунок 7.30 – Окно SNMP User Table Configuration

Можно установить следующие параметры:

Параметр	Описание
User Name	Имя пользователя может состоять из буквенно-цифровой последовательности длиной не более 32 символов, оно позволяет идентифицировать пользователей SNMP.
Group Name	Это поле используется для обозначения, какая созданная SNMP-группа может запрашивать SNMP -сообщения.
SNMP 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.

Для того чтобы изменения вступили в силу, кликните по **Apply**. Для возврата к SNMP User Table кликните по 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: **Security Management ⇨ SNMP Manager ⇨ SNMP View Table.**

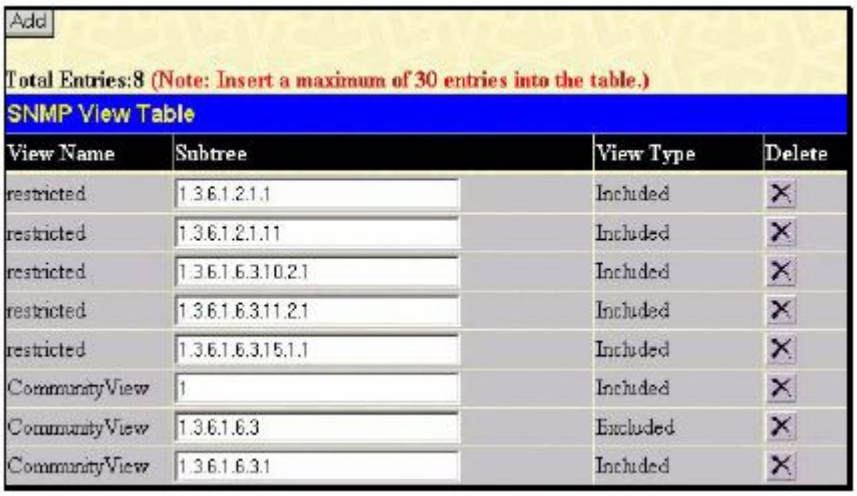


Рисунок 7.31 - Окно SNMP View Table

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

Рисунок 7.32 – Окно «SNMP View Table Configuration»

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

Могут быть установлены следующие параметры:

Параметр	Описание
View Name	Введите имя пользователя в виде буквенно-цифровой последовательности длиной не более 32 символов. Параметр используется для идентификации нового объекта SNMP.
Subtree OID	Введите Object Identifier Subtree (OID) для объекта. OID идентифицирует

	объект MIB tree, который будет включён или исключён SNMP-менеджером.
View Type	Отметьте (Included) в списке объектов те, к которым SNMP-менеджер сможет получать доступ. Отметьте (Excluded) в списке объектов те, к которым SNMP-менеджер не сможет получать доступ.

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

Таблица групп SNMP (SNMP Group Table)

SNMP группа, созданная в этой таблице, заносит SNMP-пользователей (определённых в таблице SNMP-пользователей (SNMP User Table)) в отображаемые элементы, созданные в предыдущем меню.
Для просмотра данного окна кликните: **Security Management ⇨ SNMP Manager ⇨ SNMP Group Table.**

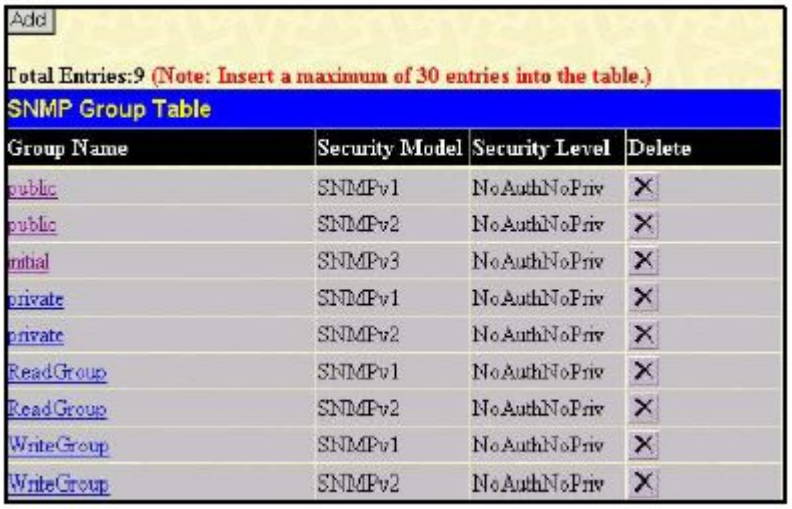


Рисунок 7.33 – Окно «SNMP Group Table»

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

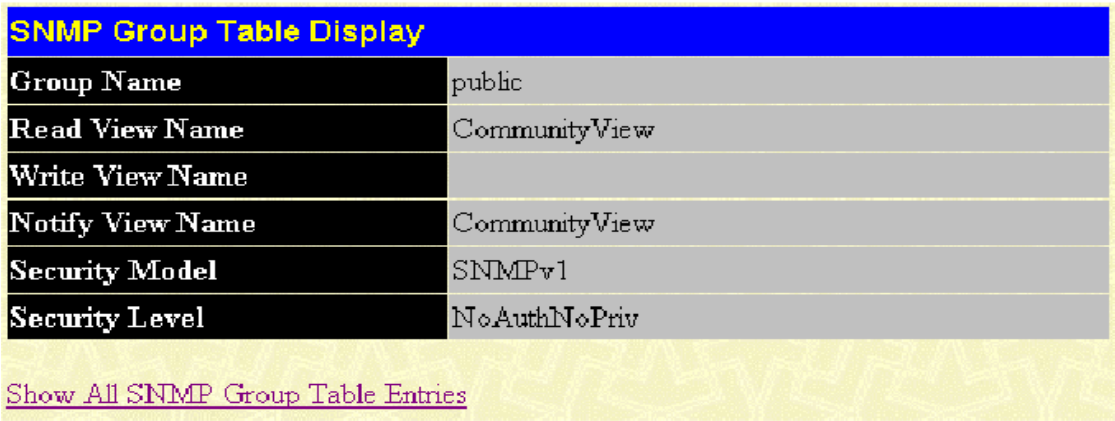


Рисунок 7.34 – Окно SNMP Group Table Display

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

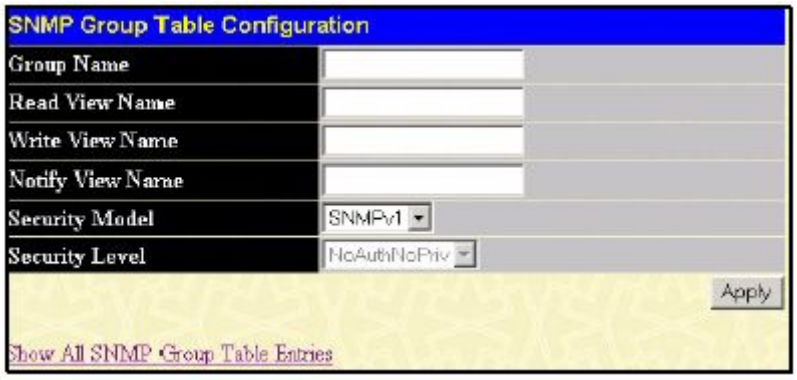


Рисунок 7.35 – Окно SNMP Group Table Configuration

Можно установить следующие параметры:

Параметр	Описание
Group Name	Введите имя группы, которое может состоять из буквенно-цифровой последовательности длиной не более 32 символов. Оно используется для идентификации 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 того чтобы новые настройки вступили в силу, нажмите **Apply**. Для возвращения к таблице SNMP Group Table, нажмите ссылку Show All SNMP Group Table Entries.

Таблица конфигурации SNMP Community

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

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

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

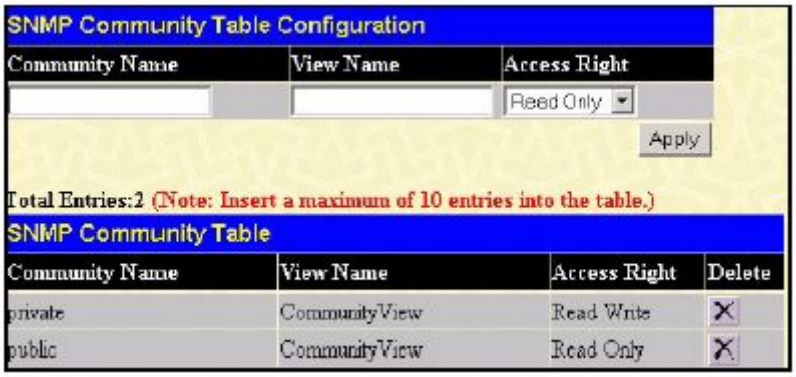


Рисунок 7.36 – Окно SNMP Community Table Configuration

Можно установить следующие параметры:

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

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

Таблица хоста SNMP

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

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

Рисунок 7.37 - Окно SNMP Host Table

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

Рисунок 7.38 – Окно SNMP Host Table Configuration

Можно установить следующие параметры:

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

Для применения новых настроек кликните по **Apply**. Для возвращения к **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 на Коммутаторе. Для отображения SNMP Engine ID Коммутатора, откройте **Administration ⇨ SNMP Manger ⇨ SNMP Engine ID,** что позволит открыть окно **SNMP Engine ID Configuration,** показанное ниже.

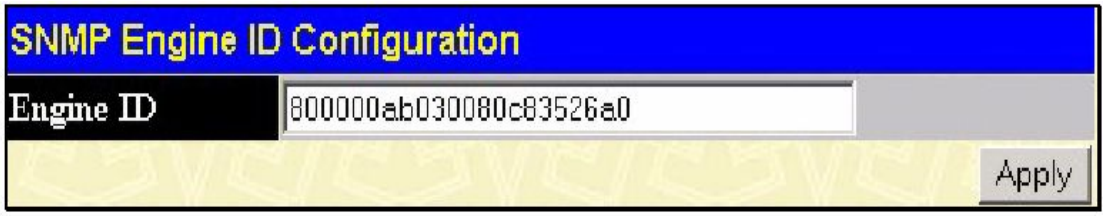


Рисунок 7.39 – Окно «SNMP Engine ID Configuration»

Для изменения Engine ID, введите новый Engine ID в нужном поле и кликните по кнопке **Apply**.

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.

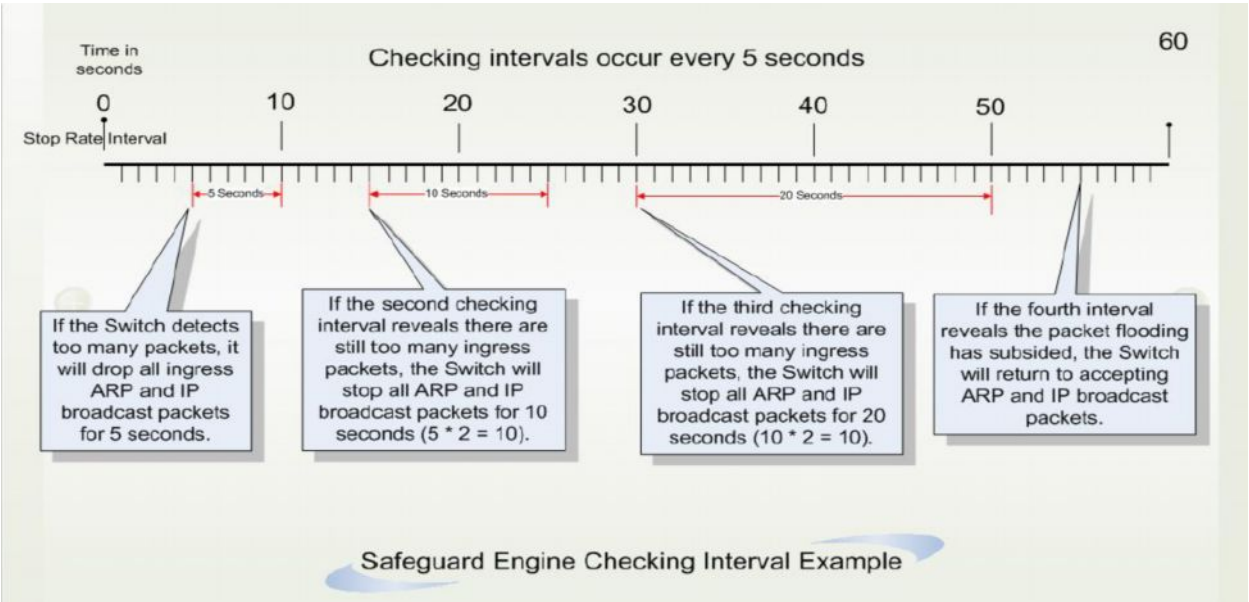


Рисунок 7- 40. Пример Safeguard Engine

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.

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

Рисунок 7- 41. Окно Safeguard Engine

Для настройки функции Safeguard Engine Коммутатора выберите в выпадающем меню **State** значение *Enabled*. Чтобы задать параметры Safeguard Engine, кликните по кнопке **Advanced Settings**. В результате откроется следующее окно:

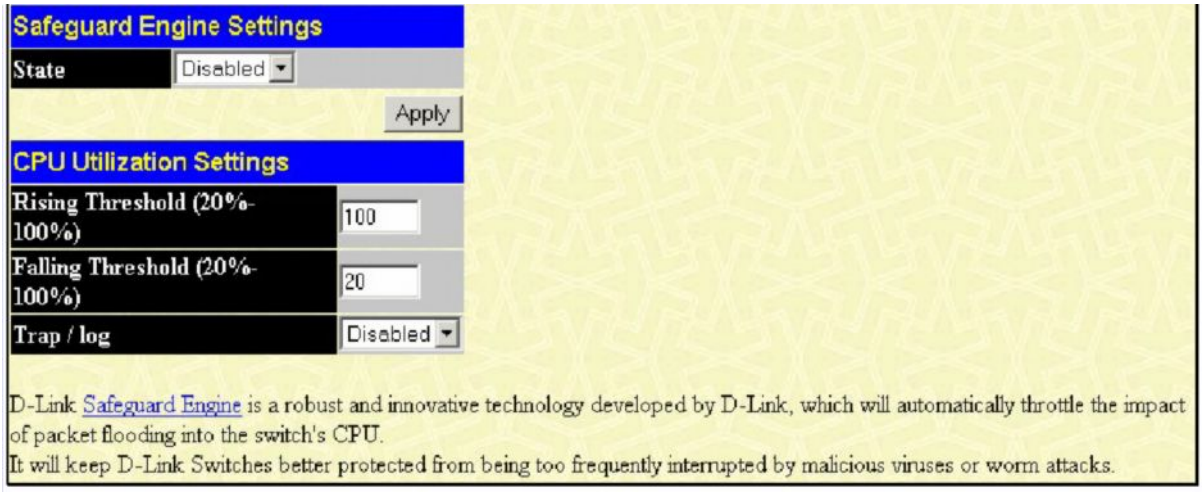


Рисунок 7- 42. Окно Safeguard Engine - Advanced Settings

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.

Фильтрация
Настройка сортировки DHCP-серверов

Использование этой функции позволяет не просто ограничить число пакетов от DHCP-сервера, а задать получение пакета от назначенного DHCP-сервера определенным DHCP-клиентом. Это осбенно важно, когда в сети существет несколько DHCP-серверов, каждый из которых предоставляет DHCP-сервис определенной группе клиентов. При включении DHCP-фильтра в первый раз будут созданы профиль доступа и правило доступа, затем необходимо создать другие правила доступа. Эти правила используются для блокировки пакетов DHCP-сервера. Аналогично при создании разрешающего правила DHCP будет создан один профиль доступа и одно правило доступа, где MAC-адрес DHCP-клиента является MAC-адресом клиента, а IP-адрес источника совпадает с IP-адресом DHCP-сервера (UDP-порт номер 67). Настройки выполняются в окне **DHCP Client Screening Setting**. Эти правила позволяют разрешить продвижение пакетов DHCP-сервера.

При включении функции DHCP-фильтра в окне **DHCP Server Screening Setting** все пакеты DHCP-сервера будут отфильтровываться с определенного порта.

DHCP Server Screening Setting

From	To	State	Apply
Port 1	Port 1	Disable	Apply

DHCP Server Screening Status

Port	State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable
12	Disable
13	Disable
14	Disable
15	Disable
16	Disable
17	Disable
18	Disable
19	Disable
20	Disable
21	Disable
22	Disable
23	Disable
24	Disable
25	Disable
26	Disable

Рисунок 7- 43. Окно DHCP Server Screening Setting

В показанном выше окне доступны для настройки следующие параметры:

Параметр	Описание
From/To	Данные выпадающие меню позволяют задать диапазон портов для настройки.
State	Данное поле позволяет включить (Enabled) или выключить (Disabled) DHCP-фильтр для заданного диапазона портов.

Для принятия выполненных настроек кликните по **Apply**. Текущие настройки будут отображены в таблице **DHCP Server Screening Status**.

Настройка фильтрации DHCP-клиента

Это окно позволяет создать записи связи определенного IP-адреса Сервера и MAC-адреса Клиента на основе портов. Пожалуйста, убедитесь сначала, что функция фильтра DHCP-сервера включена в окне **DHCP Server Screening Setting**. Когда все настройки DHCP-сервера выполнены, все пакеты DHCP-сервера будут отфильтровываться на определенном порту, за исключением тех, что удовлетворяют связке IP-адрес сервера – MAC-адрес Клиента, установленной в следующем окне **DHCP Client Screening Setting**.

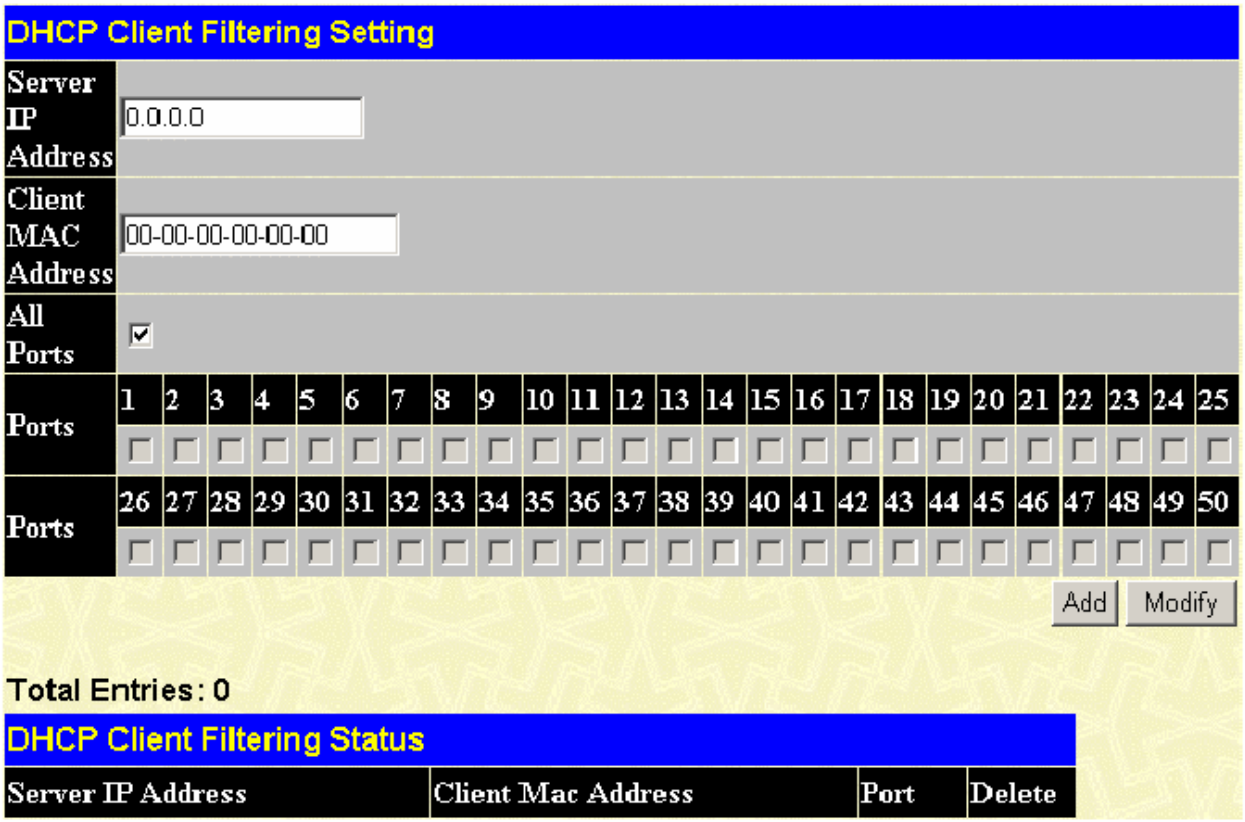


Рисунок 7- 44. Окно DHCP Client Filtering Setting

Ниже описаны параметры, доступные для настройки в данном окне:

Параметр	Описание
Server IP Address	Введите IP-адрес Сервера.
Client MAC Address	Введите MAC-адрес Киента.
All Ports	Поставьте галочку в данном поле, чтобы настроить сразу все порты.
Ports	Отметьте соответствующие порты для настройки.

Кликните по **Apply** для принятия новых настроек или по **Modify** для обновления настроек. В таблице **DHCP Client Filtering Status** отобразится текущий статус всех существующих записей. Для удаления существующей записи кликните по соответствующей кнопке под заголовком **Delete.**

Настройка фильтрации NetBIOS

При включении NetBIOS-фильтра все пакеты NetBIOS будут проходить фильтрацию на определенном порту. Включение функции NetBIOS-фильтра создаст один профиль доступа и три правила доступа на порт (номера UDP-портов 137 и 138, номер TCP-порта 139).
При включении опции Extensive NetBIOS Filter все пакеты NetBIOS поверх фреймоы 802.3 будут отфильтровываться на определенном порту.
Показанное ниже окно используется для настройки NetBIOS-фильтра. Включение опции Extensive NetBIOS filter приведет к созданию одного профиля доступа и одного правила доступа на порт (DSAP (Destination Service Access Point) =F0 и SASP (Source Service Access Point) =F0).

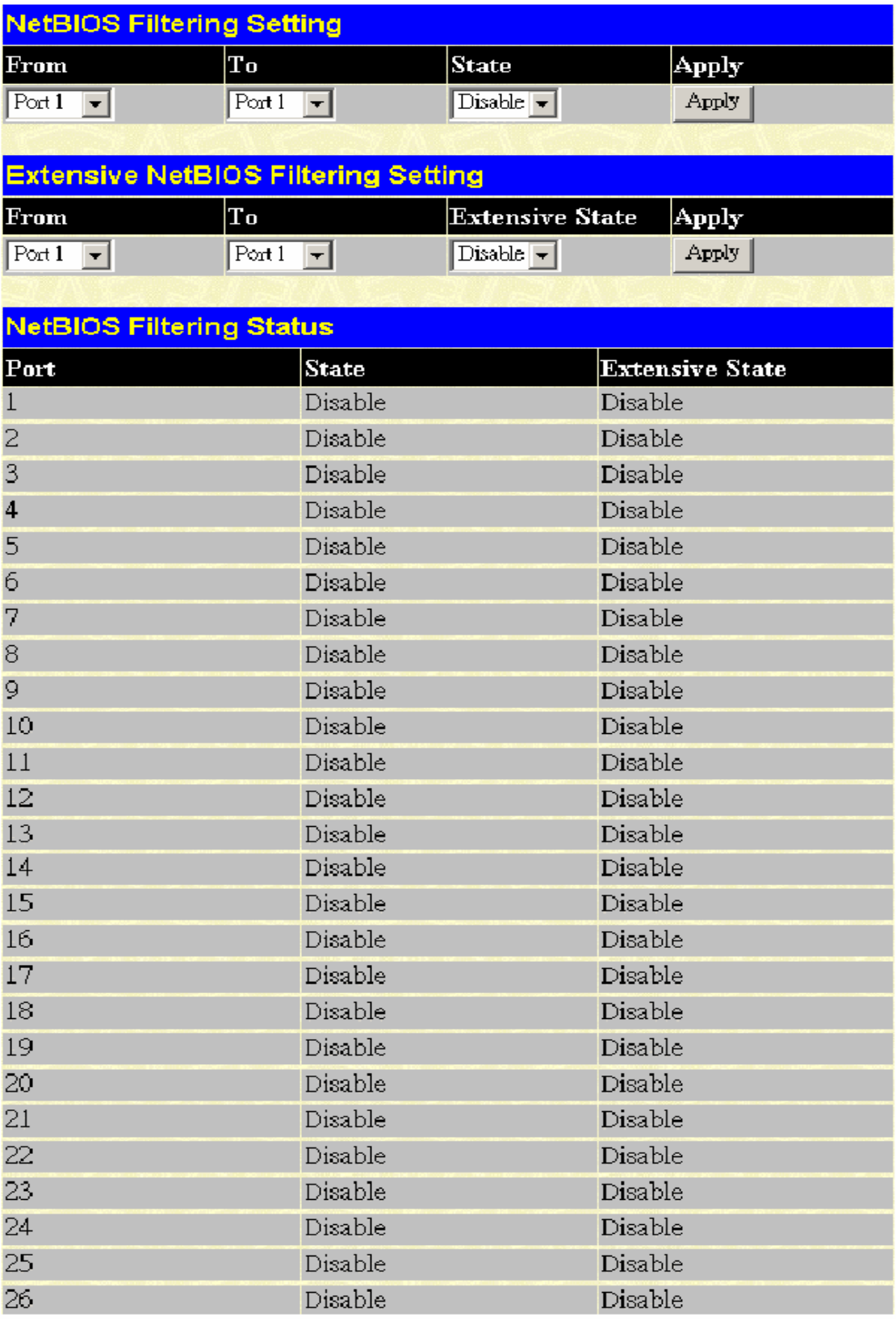


Рисунок 7- 45. Окно NetBIOS Filtering Setting и Extensive NetBIOS Filter Setting

Параметры, доступные для настройки, описаны ниже:

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

State	Данное выпадающее меню позволяет включить (Enable) или выключить (Disable) NetBIOS-фильтр для заданных портов. По умолчанию задано Disable.
Extensive State	Данное выпадающее меню позволяет включить (Enable) или выключить (Disable) Extensive NetBIOS-фильтр для заданных портов. По умолчанию задано Disable.

Для применения настроек кликните по **Apply**. В окне отобразится текущая конфигурация **NetBIOS Filtering Status**.

Раздел 8 - Мониторинг

Использование порта
Использование CPU
Пакеты
Ошибки
Размер
MAC-адрес
Системный журнал коммутатора
Группа IGMP Snooping
IGMP Snooping Forwarding
Статус VLAN
Порт маршрутизатора
Управление доступом порта
Функции уровня 3
Статус Safeguard Engine

Использование порта

Функция Port Utilization (Использование порта) является еще одним важным инструментом мониторинга состояния сети. Окно **«Utilization»** отображает процентное соотношение общей доступной полосы пропускания к полосе, приходящейся на порт. Для просмотра процентного соотношения использования портов откройте: **Monitoring ⇨ Port Utilization.**

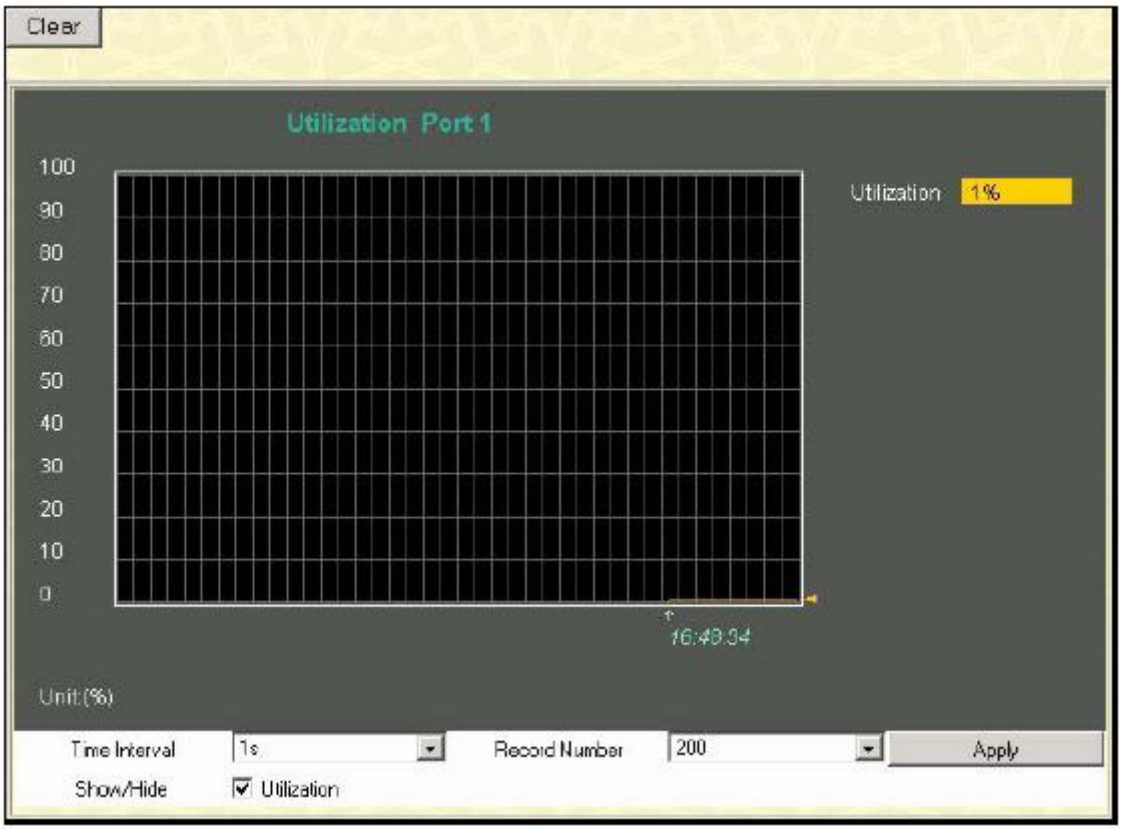


Рисунок 8.1 – Окно «Utilization»

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 1c. Этот параметр указывает временной интервал, через который будет проводиться измерение использования порта.
Record Number	В этом поле необходимо указать значение от 20 до 200 (по умолчанию указано 200). Этот параметр задает, сколько раз будет измеряться значение использования порта с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка

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

Использование CPU

Окно **«CPU Utilization»** позволяет получить процентное соотношение использования процессора CPU. Для работы с данным окном нажмите: **Monitoring ⇨ CPU Utilization.**

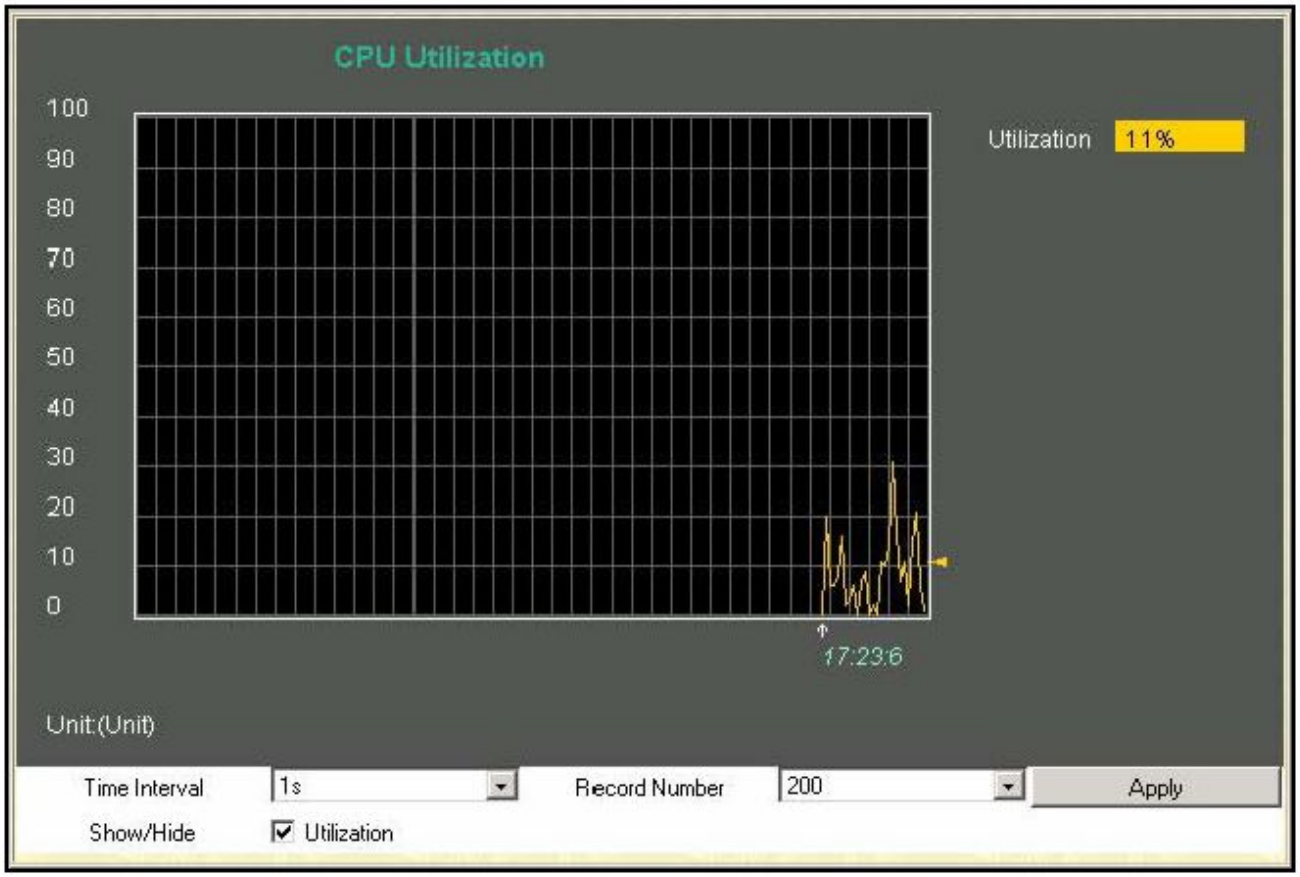


Рисунок 8.2 – Окно CPU Utilization

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.
Utilization	Отметьте, нужно ли отображать процентное использование процессора или нет.

Пакеты

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

Полученные пакеты(RX)

Для просмотра статистики по пакетам, полученным коммутатором, нажмите: **Monitoring ⇨ Packets ⇨ Received (RX).**

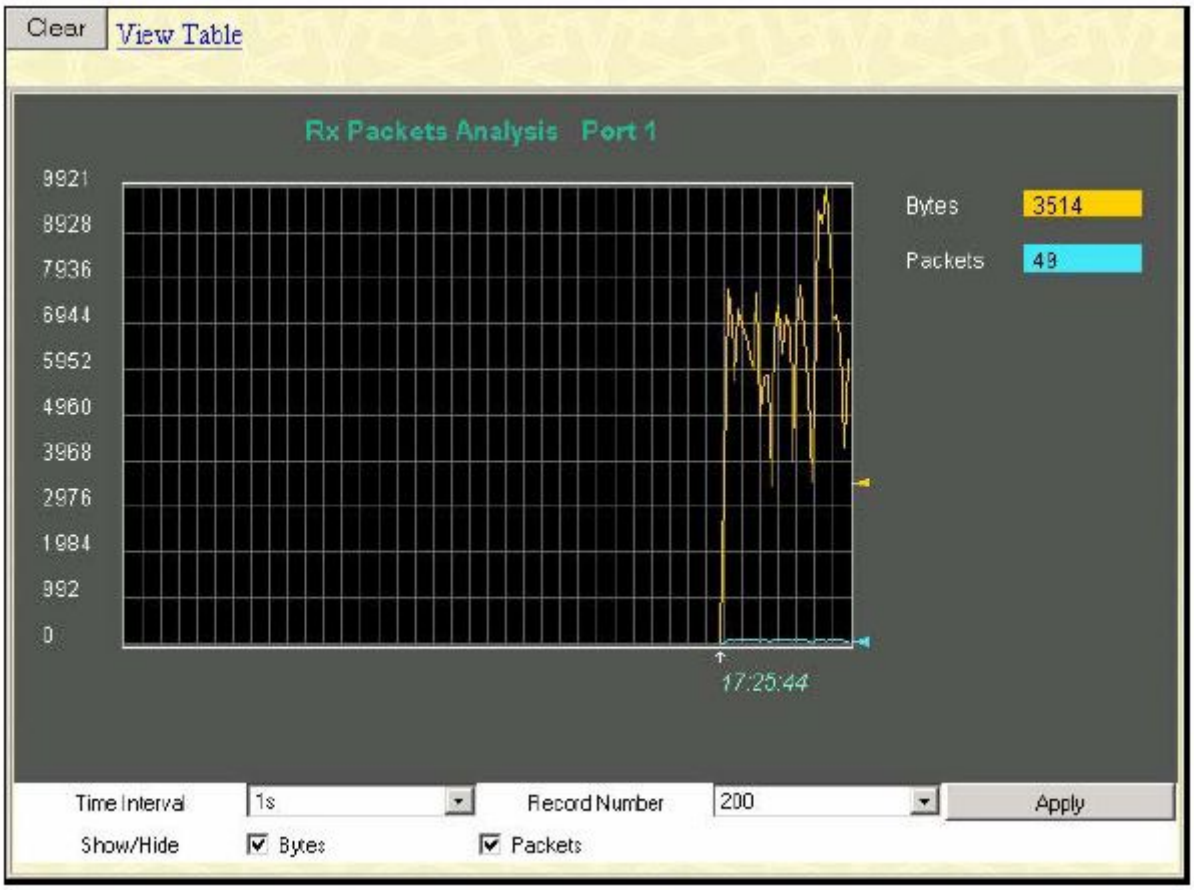


Рисунок 8.3 – Окно «Rx Packets Analysis» (график зависимости количества байт от количества переданных пакетов)

Для просмотра таблицы полученных пакетов кликните по ссылке View Table:

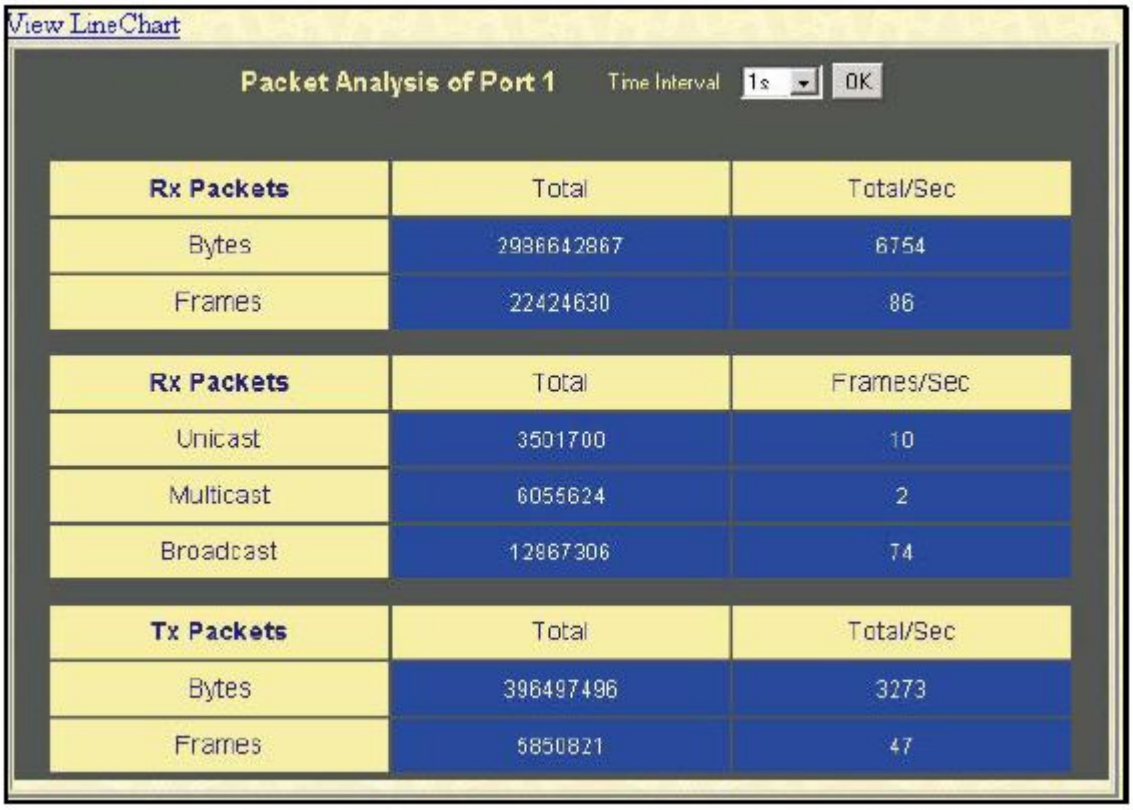


Рисунок 8.4 – Окно «Rx Packets Analysis» (таблица зависимости количества байт от количества переданных пакетов)

Можно настроить или просмотреть следующие поля:

Параметр	Описание
Time Interval	Выберите значение временного интервала в диапазоне от 1s до 60s, где s – это секунды. Данное значение по умолчанию равно 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). Данное значение по умолчанию равно 20.
Bytes	Подсчитывает число байт, полученных на порту.
Packets	Подсчитывает число пакетов, полученных на порту.
Show/Hide	Отметьте, нужно ли отображать байты и пакеты или нет.
Clear	Нажмите данную кнопку для обнуления всех счетчиков по статистике в этом окне.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Полученные одноадресные, многоадресные и широковещательные пакеты (RX)

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

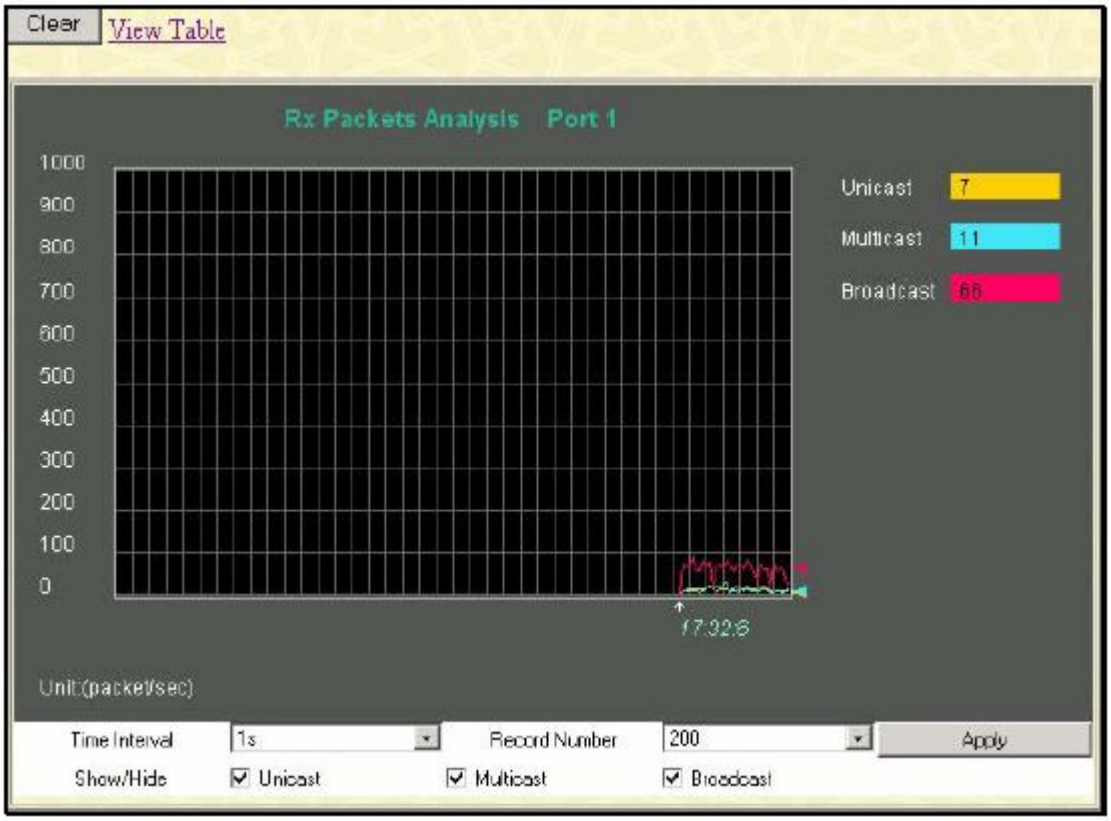


Рисунок 8.5 – Окно «Rx Packets Analysis» (график зависимости для одноадресных, многоадресных и широковещательных пакетов, полученных Коммутатором)

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

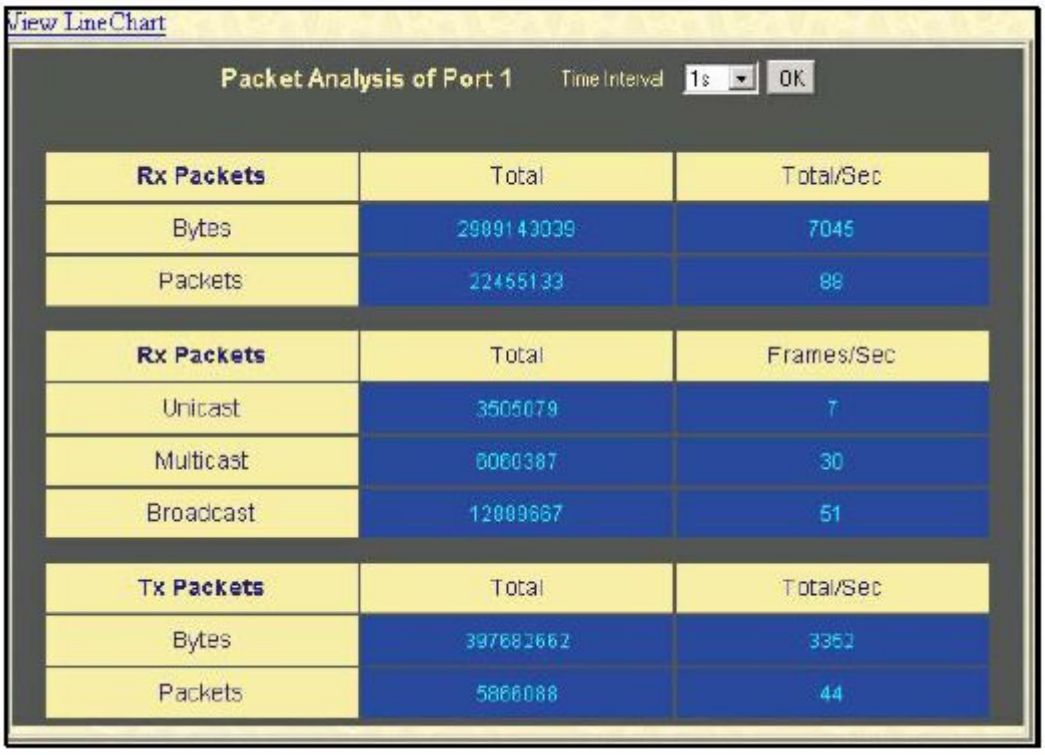


Рисунок 8.6 – Окно «Rx Packets Analysis» (таблица зависимости для одноадресных, многоадресных и широковещательных пакетов, полученных Коммутатором)

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 1сек. Через данный временной интервал каждый раз будет измеряться количество пакетов.
Record Number	Этот параметр задает, сколько раз будет измеряться количество пакетов с заданным временным интервалом (Time Interval). Чем больше это число, тем точнее будет выборка. Данное значение по умолчанию равно 20.
Unicast	Счетчик, отображающий количество пакетов, полученных портом, предназначенных для данного узла.
Multicast	Счетчик, отображающий количество пакетов, полученных данным портом, предназначенных для многоадресной группы, в которой он состоит.
Broadcast	Счетчик, отображающий количество широковещательных пакетов, полученных данным портом.
Show/Hide	Позволяет выбрать, какой тип пакетов будет отображаться: многоадресные (Multicast), широковещательные (Broadcast) и/или одноадресные (Unicast).
Clear	Кликните по этой кнопке для сброса значения всех счетчиков.
View Table	Нажмите на данную ссылку для отображения зависимости в виде таблицы.
View Line Chart	Нажмите на данную ссылку для отображения зависимости в виде линейного графика.

Отправленные пакеты (TX)

Для просмотра статистики по пакетам, отправленным коммутатором, нажмите: **Monitoring ⇨ Packets ⇨Transmitted (TX).**

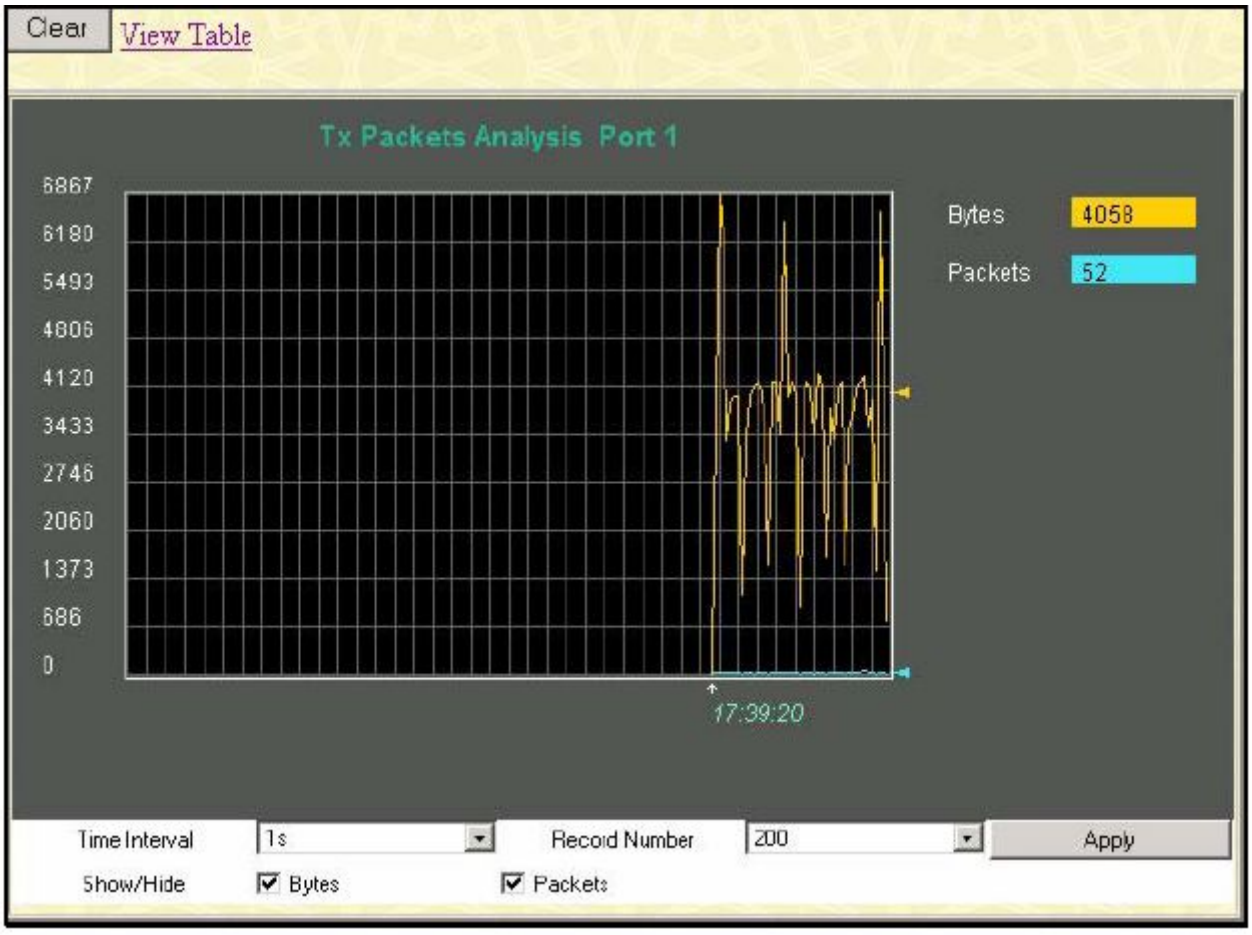


Рисунок 8.7 – Окно «Tx Packets Analysis» (график зависимости количества байт от количества переданных пакетов)

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

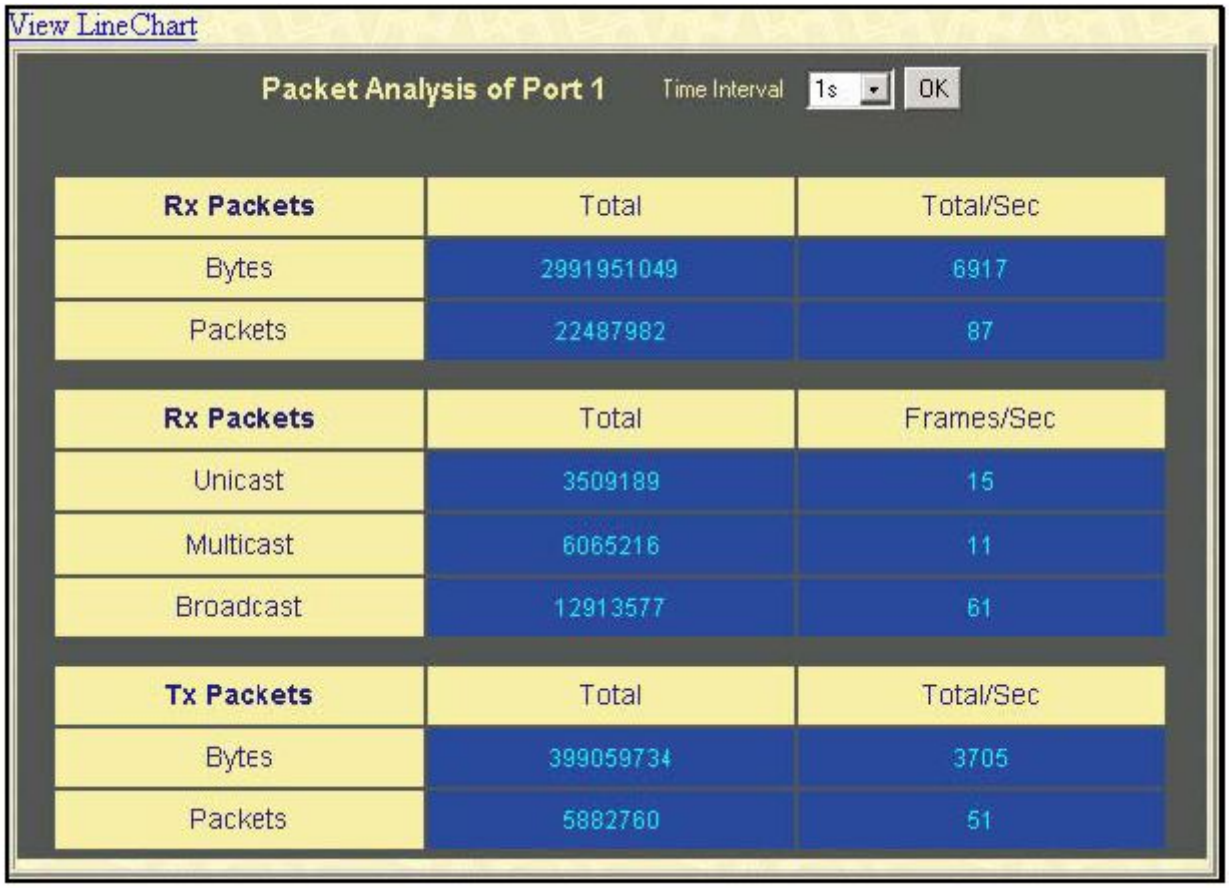


Рисунок 8.8 – Окно «Tx Packets Analysis» (таблица зависимости количества байт от количества переданных пакетов)

Можно настроить или просмотреть следующие поля:

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

Ошибки

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

Ошибки в полученных коммутатором пакетах (RX)

Для просмотра следующего графика, отражающего количество ошибок в полученных коммутатором пакетах, нажмите: **Monitoring ⇨ Error ⇨ Received (RX).**

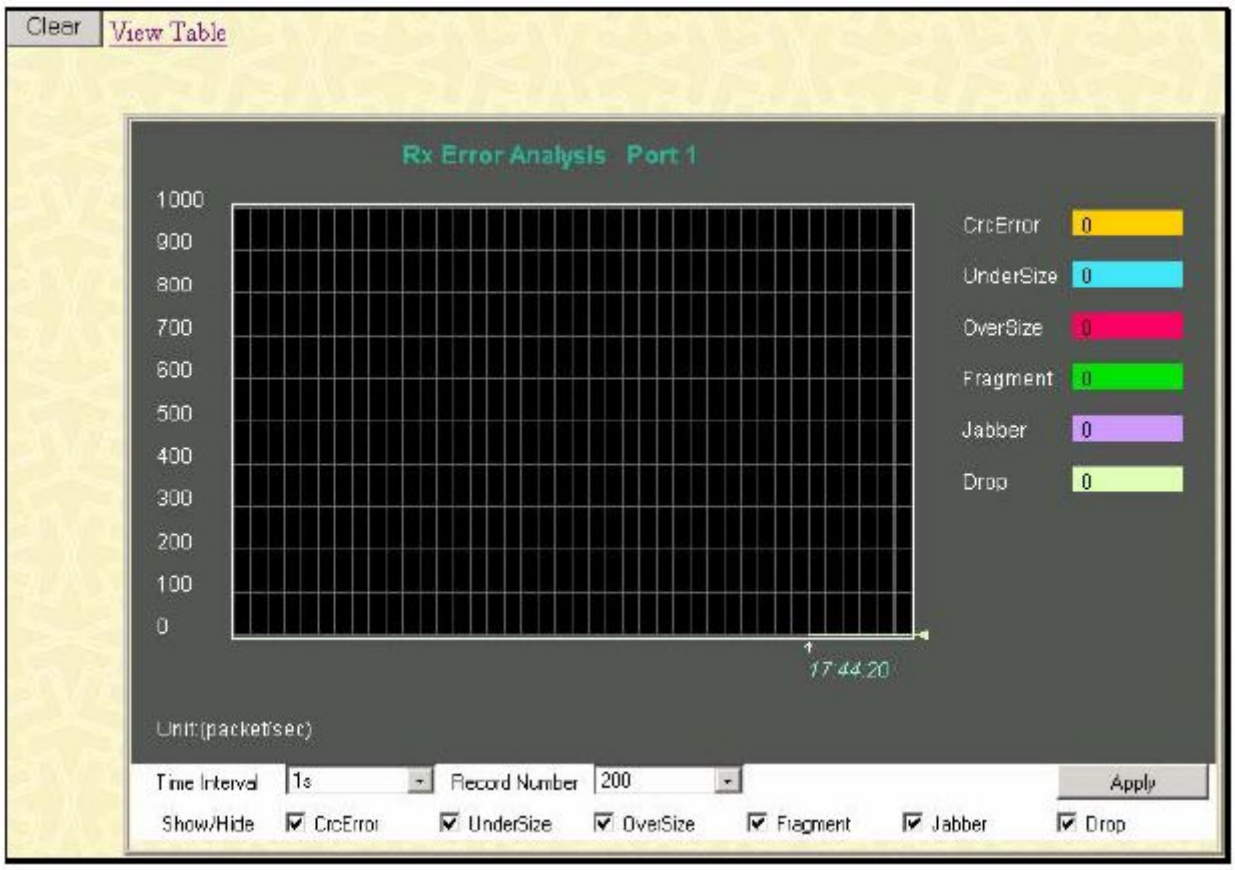


Рисунок 8.9 – Окно «Rx Error Analysis» (график зависимости)

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

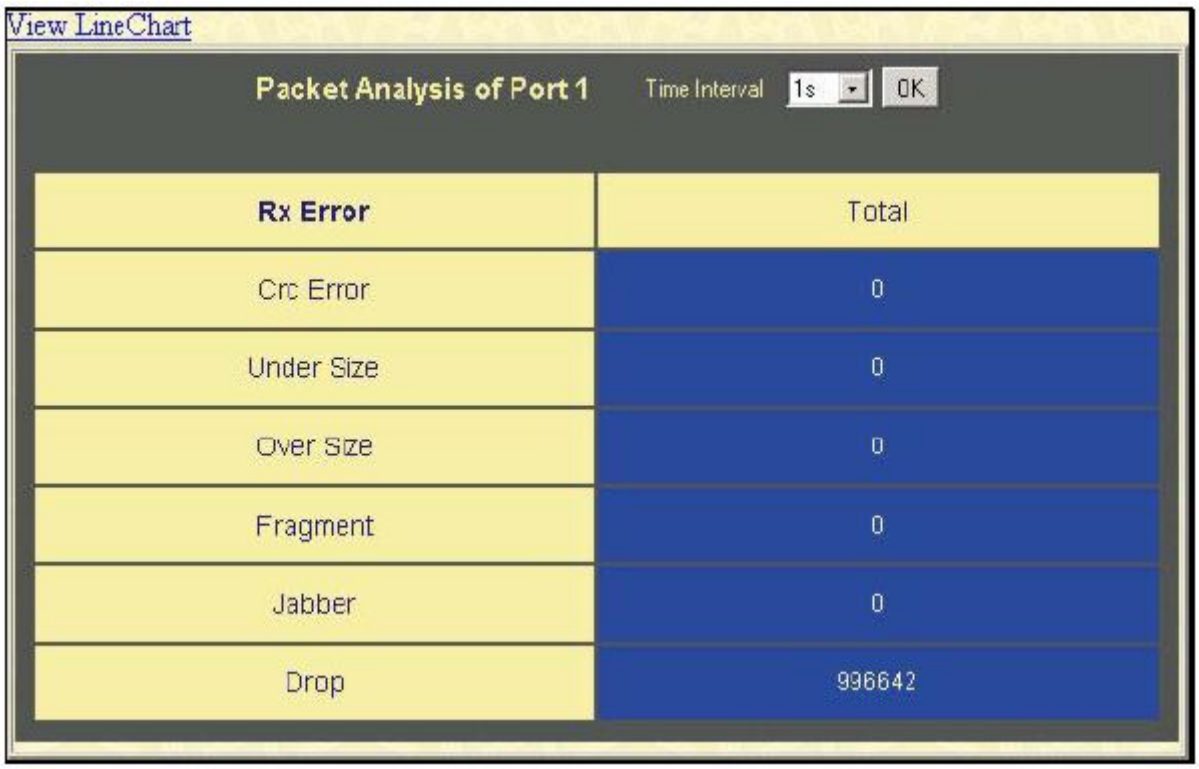


Рисунок 8.10 – Окно «Rx Error Analysis» (таблица)

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)

В следующем окне отображается график зависимости ошибок в отправленных коммутатором пакетов, для работы с данным окном нажмите: **Monitoring ⇨ Error ⇨Transmitted (TX).**

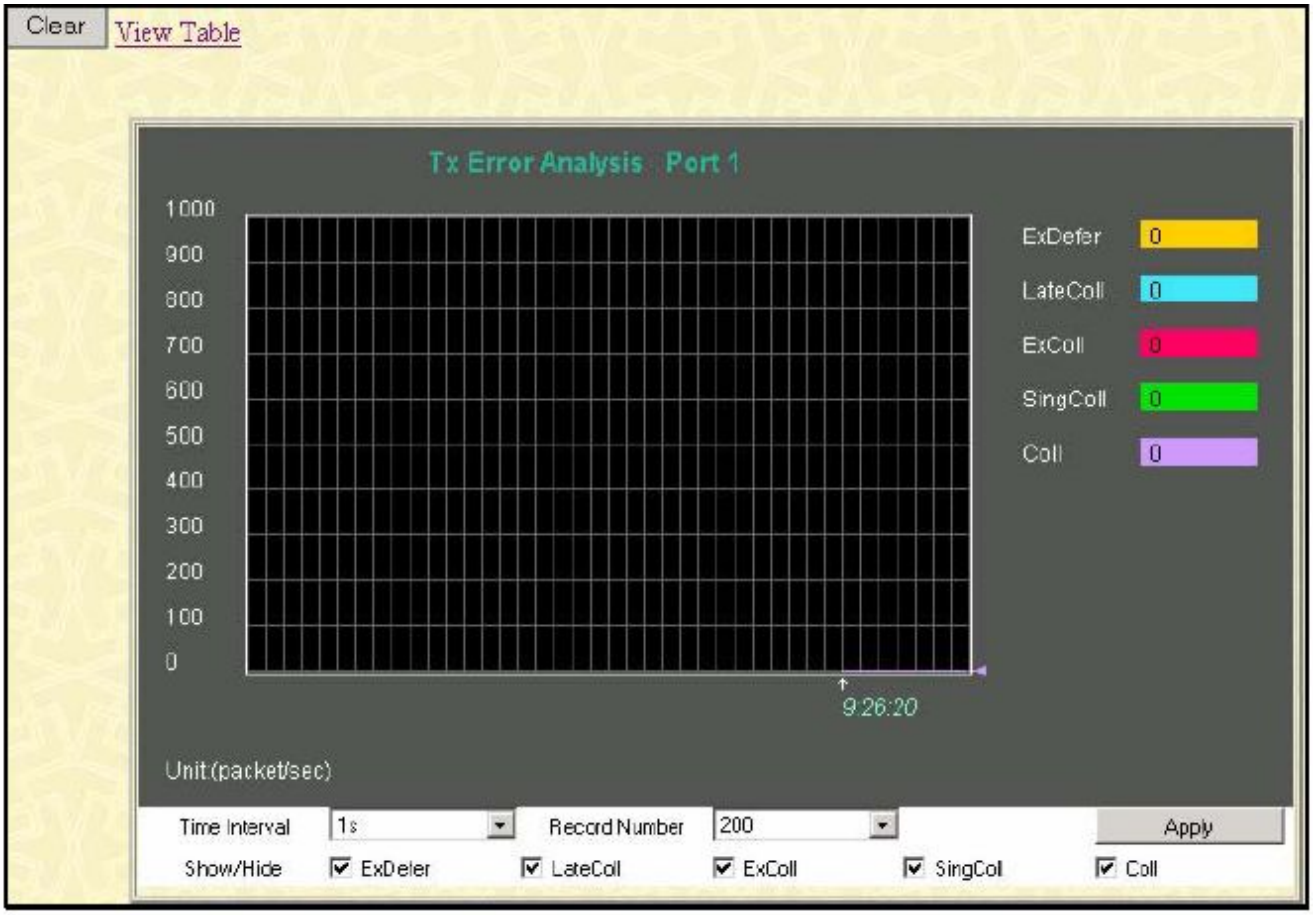


Рисунок 8.11 – Окно «Tx Error Analysis» (график зависимости)

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

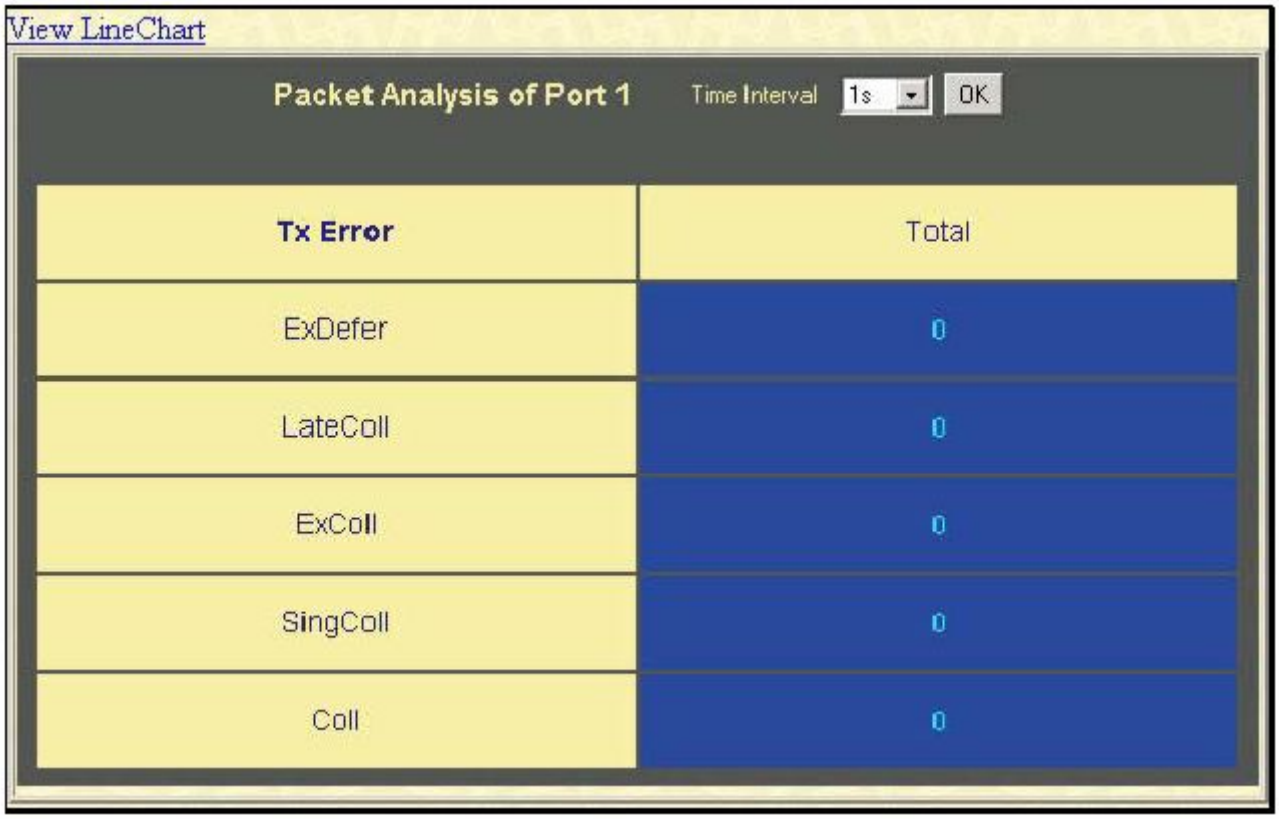


Рисунок 8.12 – Окно «Tx Error Analysis» (таблица)

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.

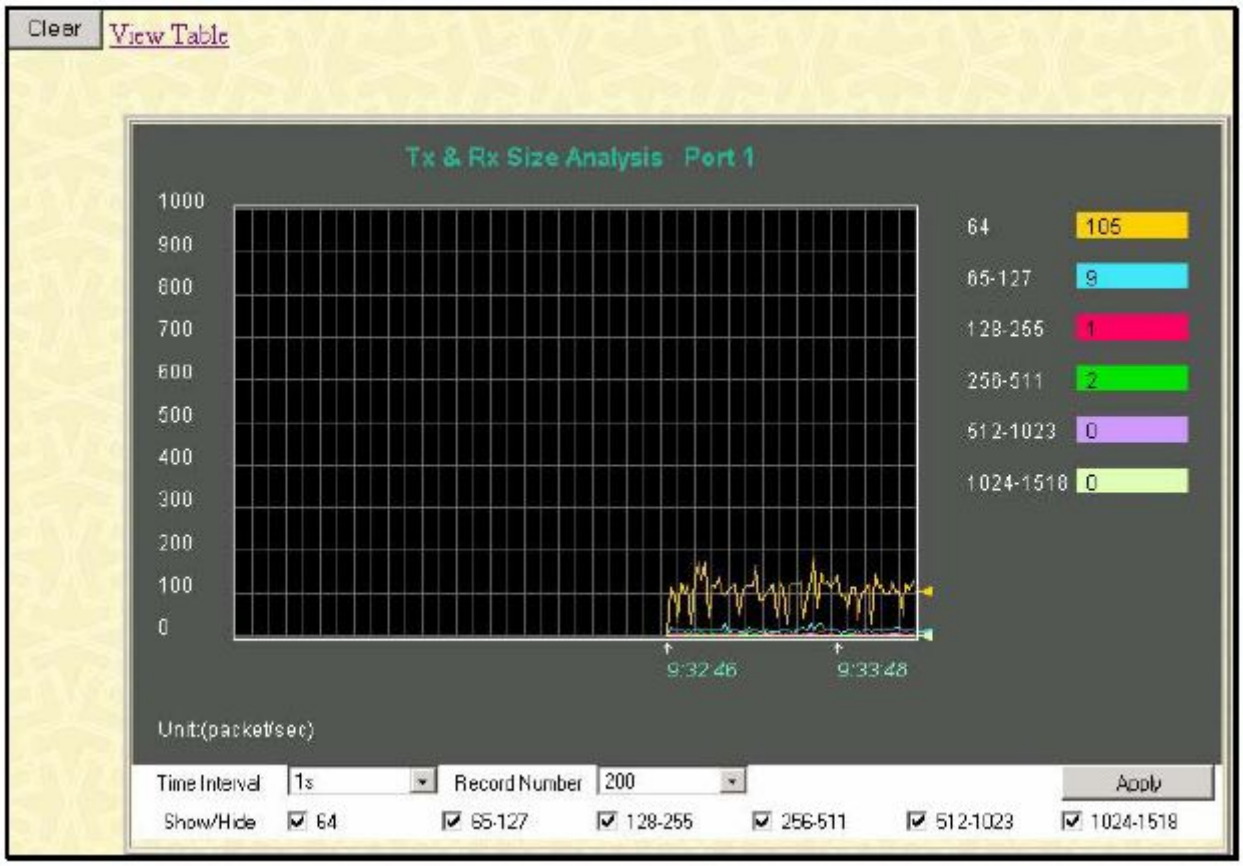


Рисунок 8.13 – Окно «Rx Size Analysis»(график зависимости)

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

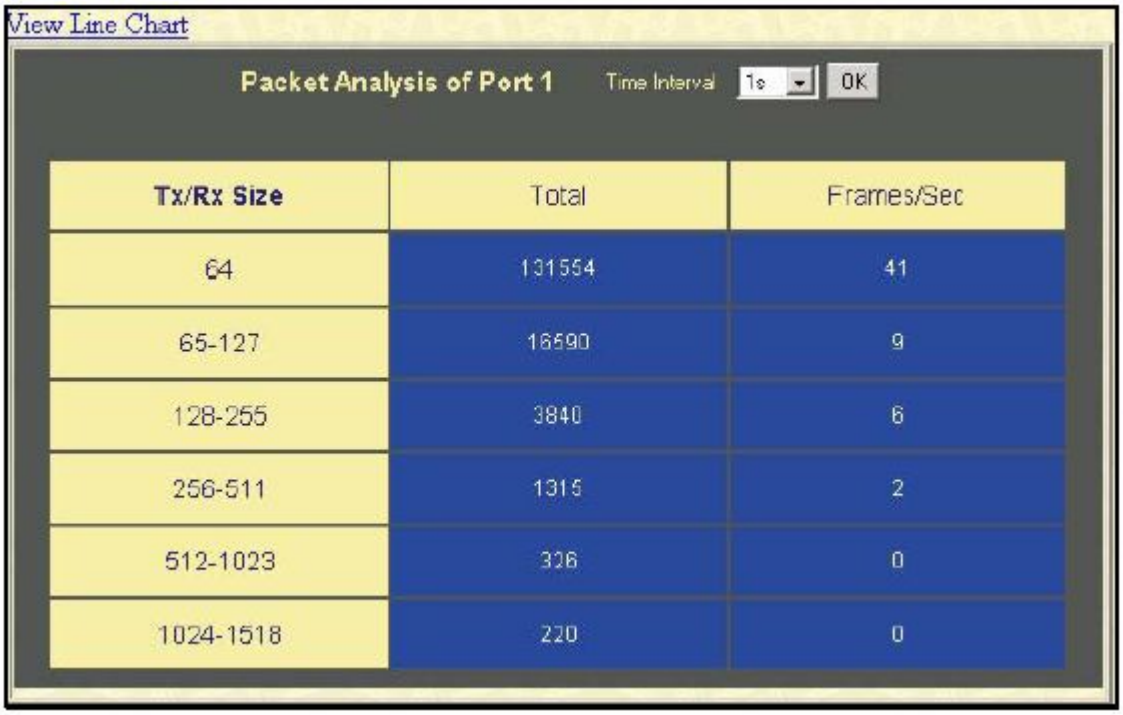


Рисунок 8.14 – Окно «Rx Size Analysis» (таблица)

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

Динамические MAC-адреса можно просмотреть в таблице, представленной ниже. Когда коммутатор узнает связь между MAC-адресом и номером порта, он делает запись в данной таблице. Эти записи используются при пересылке пакетов через коммутатор.

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

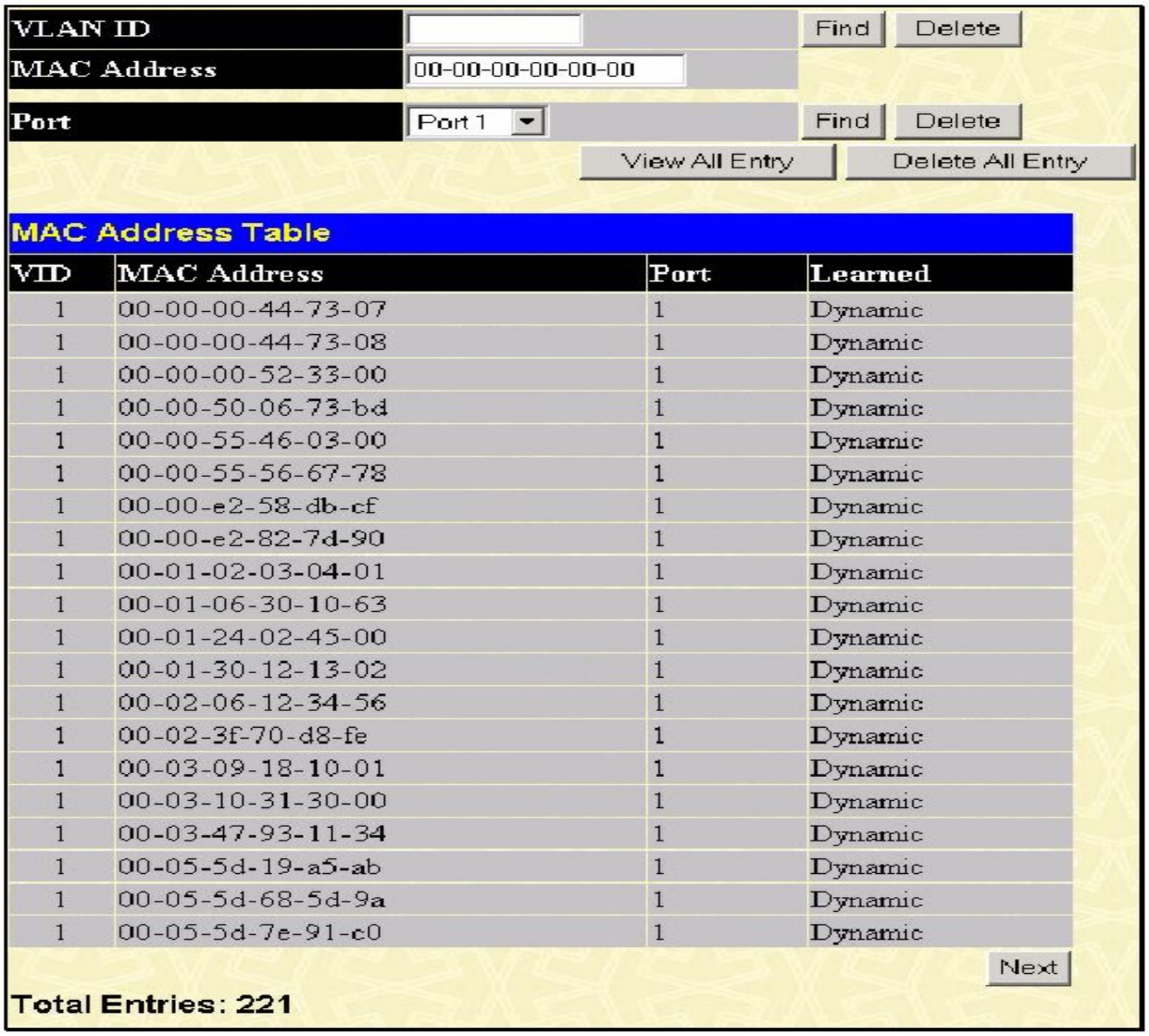


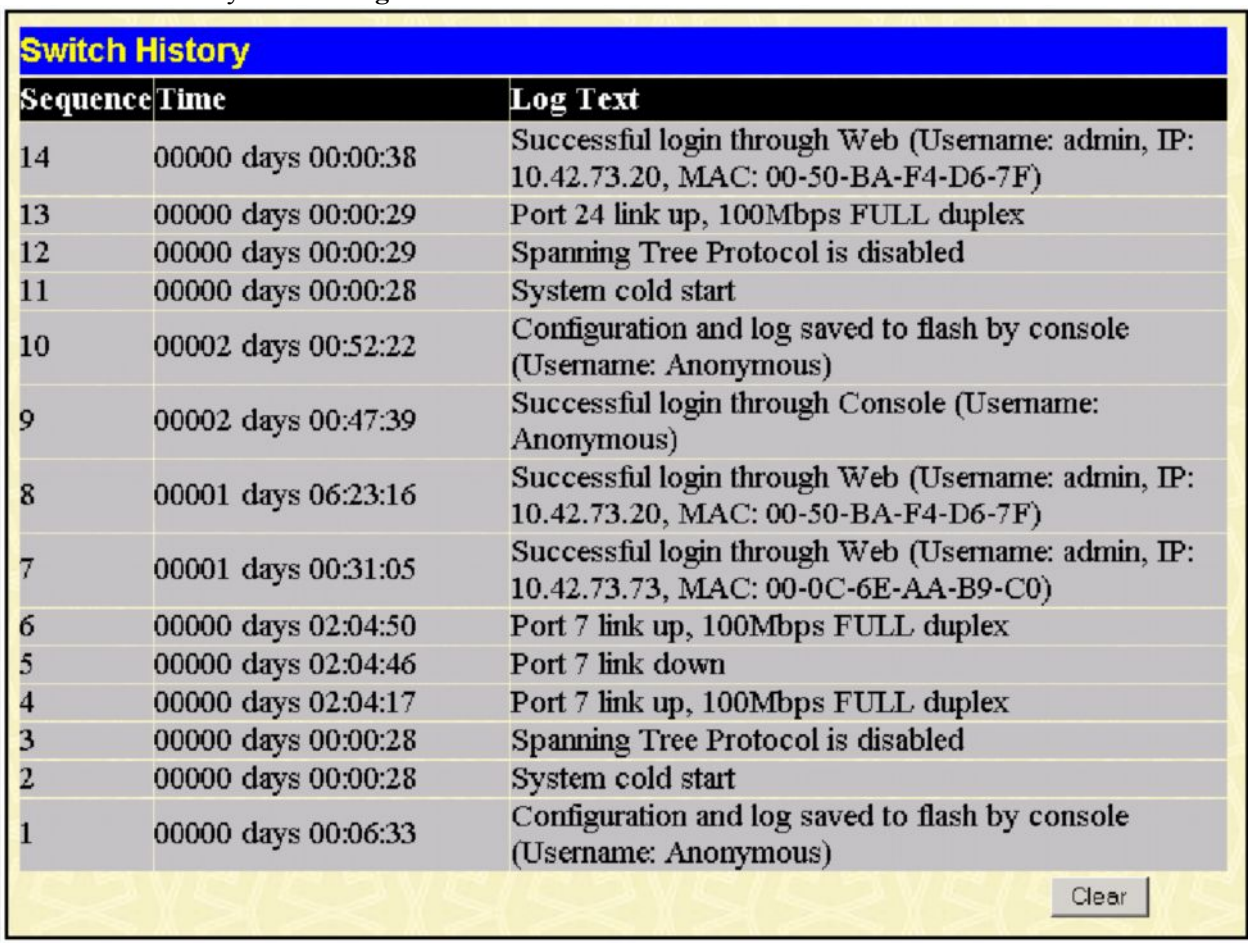
Рисунок 8.15 – Окно «MAC Address Table»

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.
Find	Задав в соответствующем поле 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.
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**.



Switch History

Sequence	Time	Log Text
14	00000 days 00:00:38	Successful login through Web (Username: admin, IP: 10.42.73.20, MAC: 00-50-BA-F4-D6-7F)
13	00000 days 00:00:29	Port 24 link up, 100Mbps FULL duplex
12	00000 days 00:00:29	Spanning Tree Protocol is disabled
11	00000 days 00:00:28	System cold start
10	00002 days 00:52:22	Configuration and log saved to flash by console (Username: Anonymous)
9	00002 days 00:47:39	Successful login through Console (Username: Anonymous)
8	00001 days 06:23:16	Successful login through Web (Username: admin, IP: 10.42.73.20, MAC: 00-50-BA-F4-D6-7F)
7	00001 days 00:31:05	Successful login through Web (Username: admin, IP: 10.42.73.73, MAC: 00-0C-6E-AA-B9-C0)
6	00000 days 02:04:50	Port 7 link up, 100Mbps FULL duplex
5	00000 days 02:04:46	Port 7 link down
4	00000 days 02:04:17	Port 7 link up, 100Mbps FULL duplex
3	00000 days 00:00:28	Spanning Tree Protocol is disabled
2	00000 days 00:00:28	System cold start
1	00000 days 00:06:33	Configuration and log saved to flash by console (Username: Anonymous)

Clear

Рисунок 8.16 – Окно «Switch History»

Коммутатор может записывать информацию о нештатных событиях в своем собственном жунале, на определенной станции для получения сообщений SNMP trap и на персональном комьютере 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 С 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 «подсмотрены», отображаются в поле Reports. Для просмотра таблицы **IGMP Snooping Table** кликните: **Monitoring ⇨ IGMP Snooping Group.**

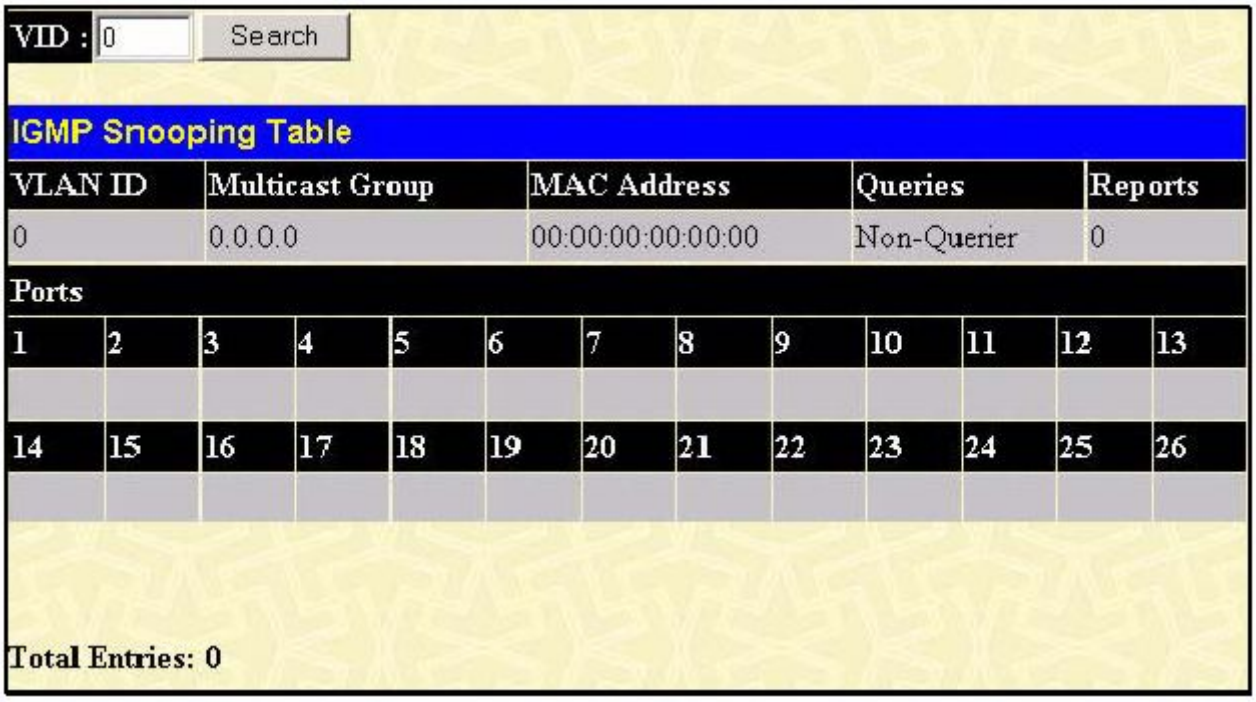


Рисунок 8- 17. Окно IGMP Snooping Table

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**.

Примечание: Коммутатор поддерживает до 128 групп IGMP Snooping.

Можно просмотреть следующие поля:

Параметр	Описание
VLAN ID	VLAN ID (VID) многоадресной группы.
Multicast Group	IP-адрес многоадресной группы.
MAC Address	MAC-адрес многоадресной группы.
Queries	Поле, предназначенное только для чтения, показывает статус состояния запроса. Disabled – означает, что коммутатор не передает пакеты запроса IGMP Snooping, Enabled – означает, что пакеты передаются
Reports	Общее количество отчетов, полученных для данной группы.
Port Map	Отображаются соответствующие порты.

Примечание: Для настройки IGMP Snooping на коммутаторе серии DES-3500 нажмите: **Configuration ⇨ IGMP.** Примеры настройки, а также другую информацию, касающуюся IGMP Snooping, можно найти в разделе 6 данного Руководства.

Таблица IGMP Snooping Forwarding

Ниже приведенное окно отображает записи в таблице IGMP Snooping Forwarding Table, для ее просмотра нажмите: **Monitoring ⇨ IGMP Snooping Forwarding.**

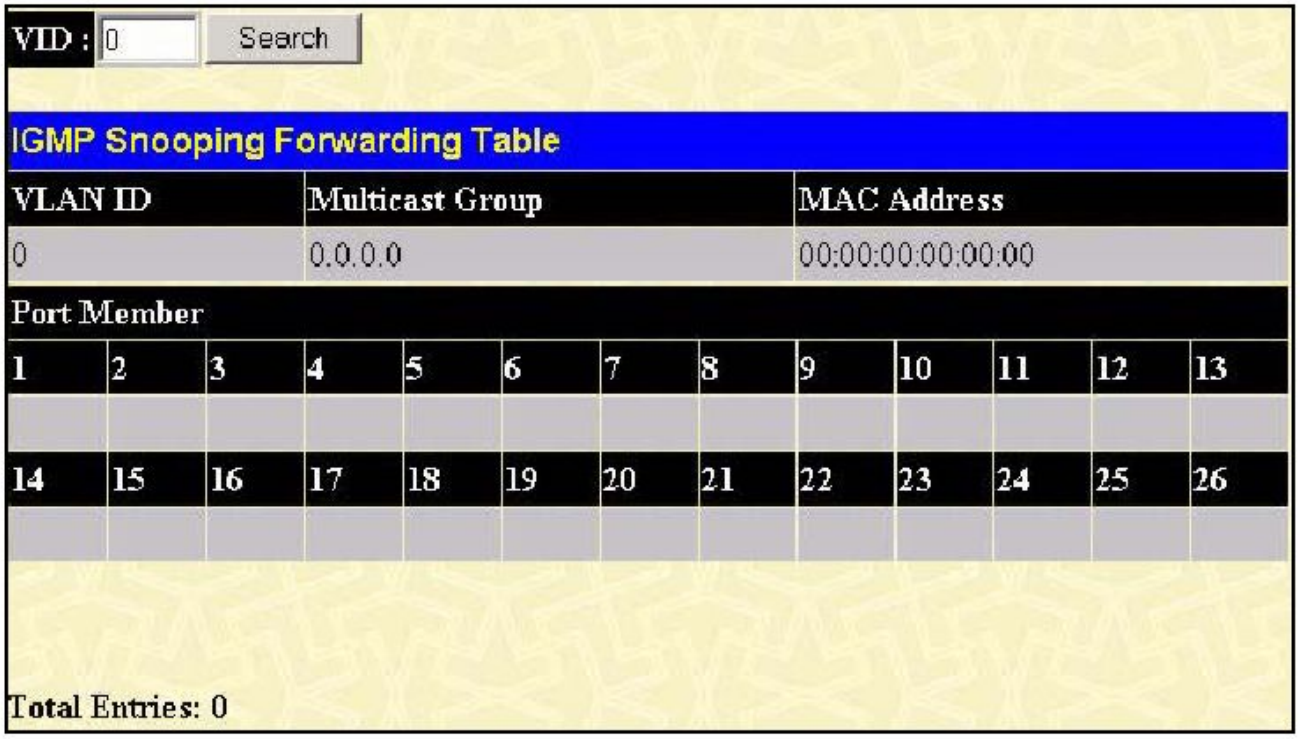


Рисунок 8.18 – Окно IGMP Snooping Forwarding Table

Для удобства пользователя предусмотрена возможность быстрого поиска строки в таблице IGMP Snooping Forwarding Table по VLAN ID (VID) путем введения VID в верхнем левом углу и нажатия на кнопку **Search**.

Можно просмотреть следующие поля:

Параметр	Описание
VLAN ID	VLAN ID (VID) многоадресной группы.
Multicast Group	IP-адрес многоадресной группы.
MAC Address	MAC-адрес многоадресной группы.
Port Map	Отображаются соответствующие порты.

Статус VLAN

Представленное ниже окно позволяет просмотреть статус каждого порта виртуальной сети VLAN коммутатора. Здесь отображаются Egress-порты и тегированные порты Коммутатора. Для просмотра следующей таблицы откройте: **Monitoring ⇨ VLAN Status.**

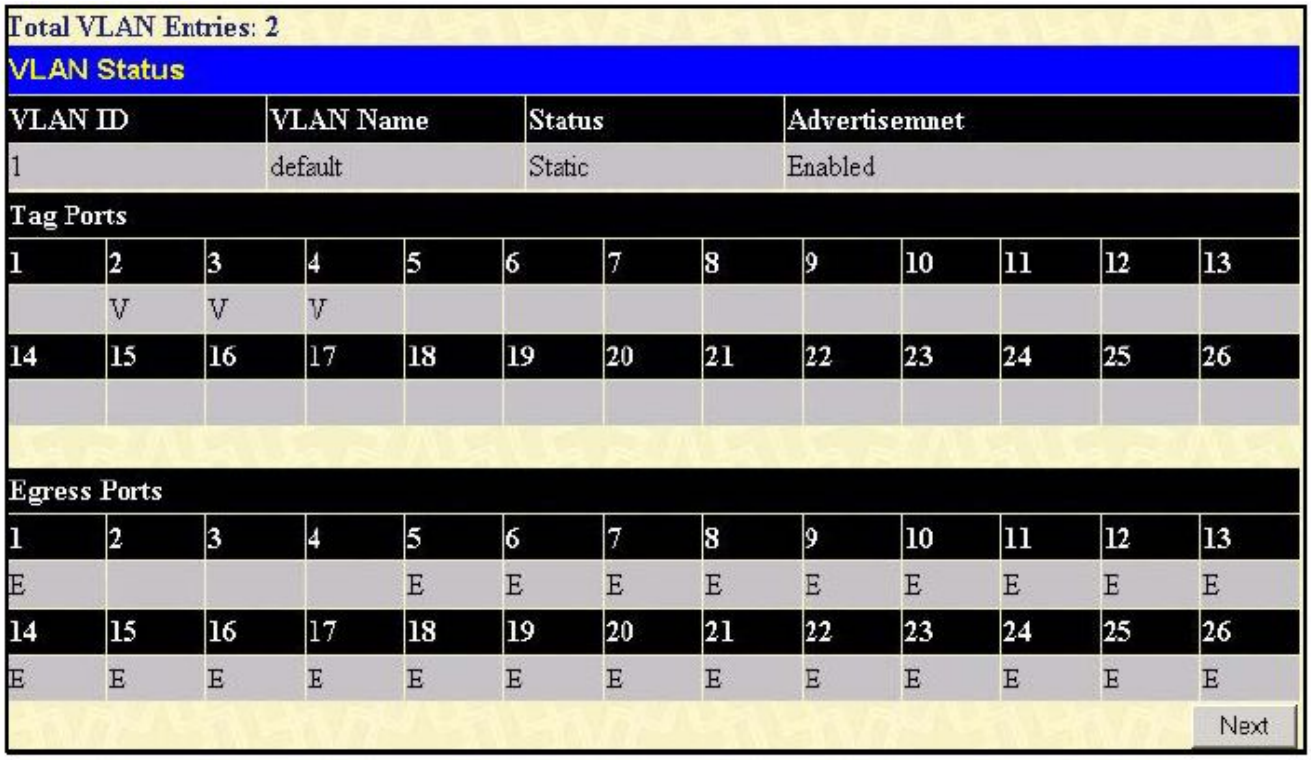


Рисунок 8.19 – Окно VLAN Status

Порт маршрутизатора

Окно **Router Port** отображает порты коммутатора, которые на данный момент времени подключены к маршрутизатору. Такие порты, настроенные пользователем через консоль или Web-интерфейс управления, отображаются в качестве статических портов и обозначаются буквой S. Буквой D обозначаются порты, динамически настроенные коммутатором. Для просмотра следующей таблицы откройте: **Monitoring ⇨ Router Port.**

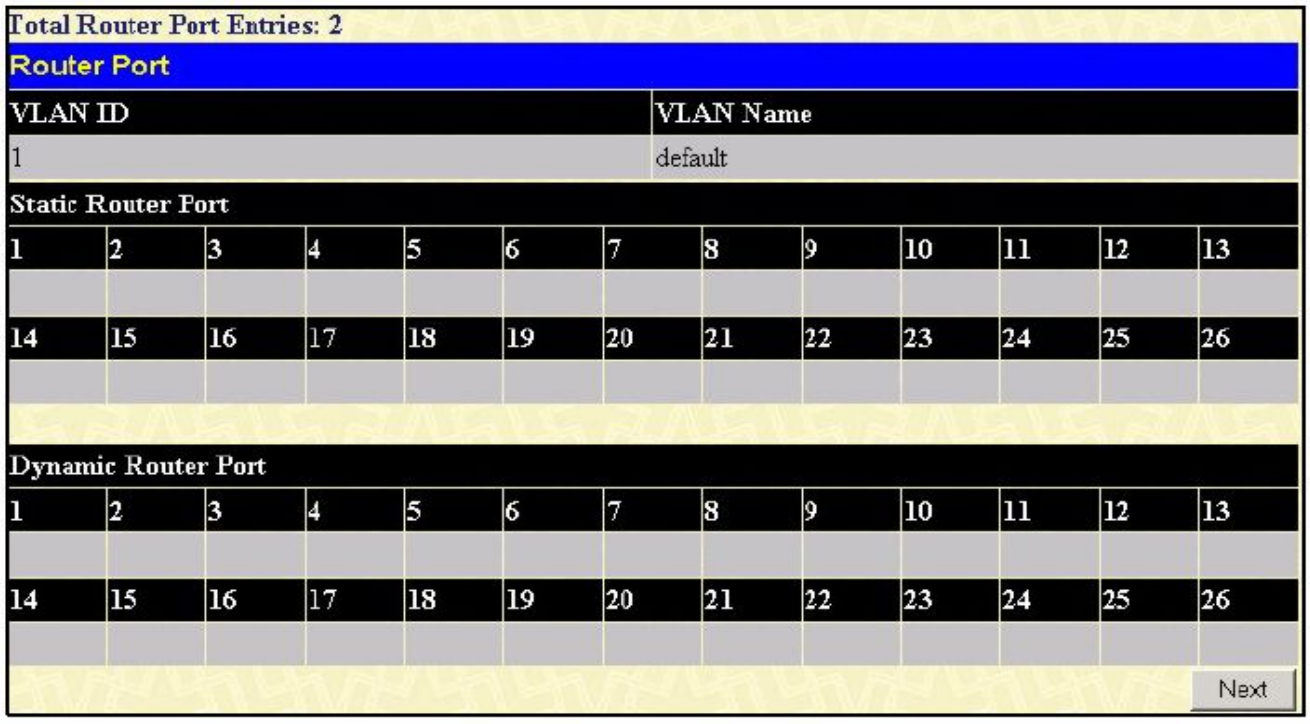


Рисунок 8.20 – Окно «Router Port»

Контроль доступа по портам

Окна «Port Access Control» используются для контроля статистики аутентификации 802.1x на основе портов. Для работы с указанными окнами нажмите: **Monitoring ⇨ Port Access Control.**

Состояние аутентификатора

В показанном ниже окне статус 802.1x на Коммутаторе**.** Для просмотра таблицы «**Authenticator State»** нажмите **Monitoring ⇨ Port Access Control ⇨Authenticator State.**

Рисунок 8.21 – Окно «Authenticator State» - при аутентификации 802.1x на основе портов

Рисунок 8.22 – Окно «Show Authenticator State» - при аутентификации 802.1x на основе MAC-адресов

Представленное окно отображает состояние аутентификатора (Authenticator State) для конкретного порта. Для выбора коммутатора в стеке используйте выпадающее меню в верхней части окна и кликните по **Apply**.

Интервал между опросами может быть от 1 до 60 сек., он устанавливается в выпадающем меню в верхней части таблицы, после чего следует нажать **OK.**

Информация, представленная в данном окне, описывается в таблице:

Параметр	Описание
Auth PAE State	В данном поле доступны опции *Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth* или *N/A*. N/A (Not available – не доступен) свидетельствует о том, что возможность аутентификации портов отключена.
Backend State	В данном поле доступны опции *Request, Response, Success, Fail, Timeout, Idle, Initialize* или *N/A*. N/A (Not available – не доступен) свидетельствует о том, что возможность аутентификации портов отключена.
Port Status	В данном поле доступны следующие опуии: *Authorized*, *Unauthorized* или *N/A*.

Функции уровня 3

Просмотр таблицы ARP

Для открытия окна **«ARP Table»** нажмите: **Monitoring ⇨ Layer 3 Feature.** Данное окно отобразит текущие ARP-записи, установленные на коммутаторе. Для поиска определенной ARP-записи введите имя интерфейса в поле Interface Name или IP-адрес в поле IP Address и кликните по **Find.**

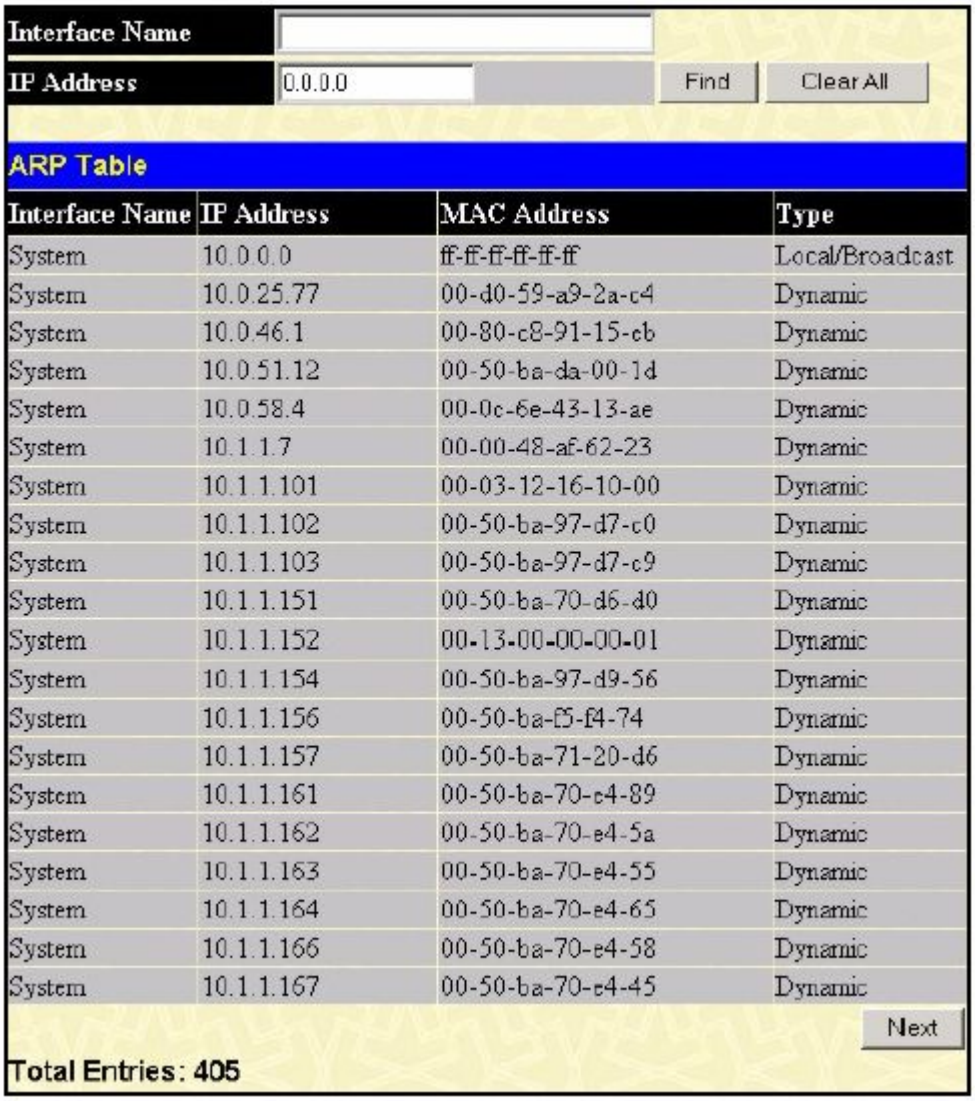


Рисунок 8.23 - Окно ARP Table

Статус Safeguard Engine

Окно «Safeguard Engine» отображает параметры настройки функции Safeguard Engine, которая является средством защиты процессора CPU. CPU коммутатора предназначен для обработки управляющей информации, такой как STP, SNMP, доступ по WEB-интерфейсу и т.д. Также CPU обрабатывает некоторый специфичный трафик, такой как ARP-широковещание, пакеты с неизвестным IP-адресом назначения, IP-широковещание и т.д. Но в современных сетях достаточно много вирусов и вредоносного трафика. Обычно они генерируют много «интересного» для CPU трафика (такого как ARP-широковещание например). Поэтому очень важно обеспечить защиту CPU. D-Link Safeguard Engine позволяет идентифицировать и приоритезировать этот

«интересный» для CPU трафик с целью отбрасывания ненужных пакетов для сохранения функциональности коммутатора.

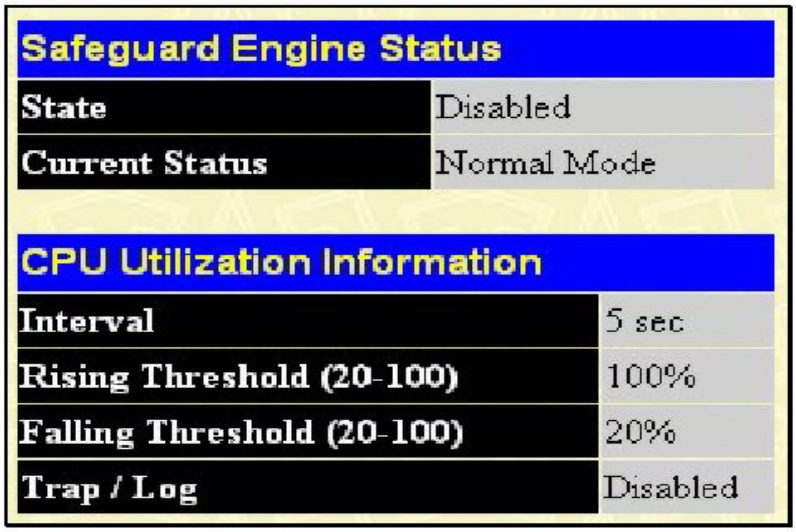


Рисунок 8- 24. Окно Safeguard Engine Status и CPU Utilization Information

В данном окне представлена следующая информация:

Параметр	Описание
State	В данном поле отображается текущее состояние функции Safeguard Engine: включена (Enabled) или выключена (Disabled).
Current Status	В данном поле отображается текущий режим работы CPU.
Interval	Отображает временной интервал, через который каждый раз будет проверяться загрузка CPU и сравниваться со значениями порогов **Rising Threshold** и **Falling Threshold**. По умолчанию составляет 5 секунд.
Rising Threshold	В данном поле отображается 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	В данном- поле отображается 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	Отображает статус отправки сообщений об активации механизма Safeguard Engine в журнал коммутатора / SNMP.

Раздел 9 – Техническая эксплуатация

Сервисы TFTP
Поддержка нескольких копий ПО
Журнал коммутатора
Ping-тест
Сохранение изменений
Перезагрузка
Выход из системы

Сервисы TFTP

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.

Загрузка программного обеспечения с TFTP-сервера

Для обновления программного обеспечения коммутатора откройте: **Maintenance ⇨ TFTP Services ⇨ Download Firmware.**

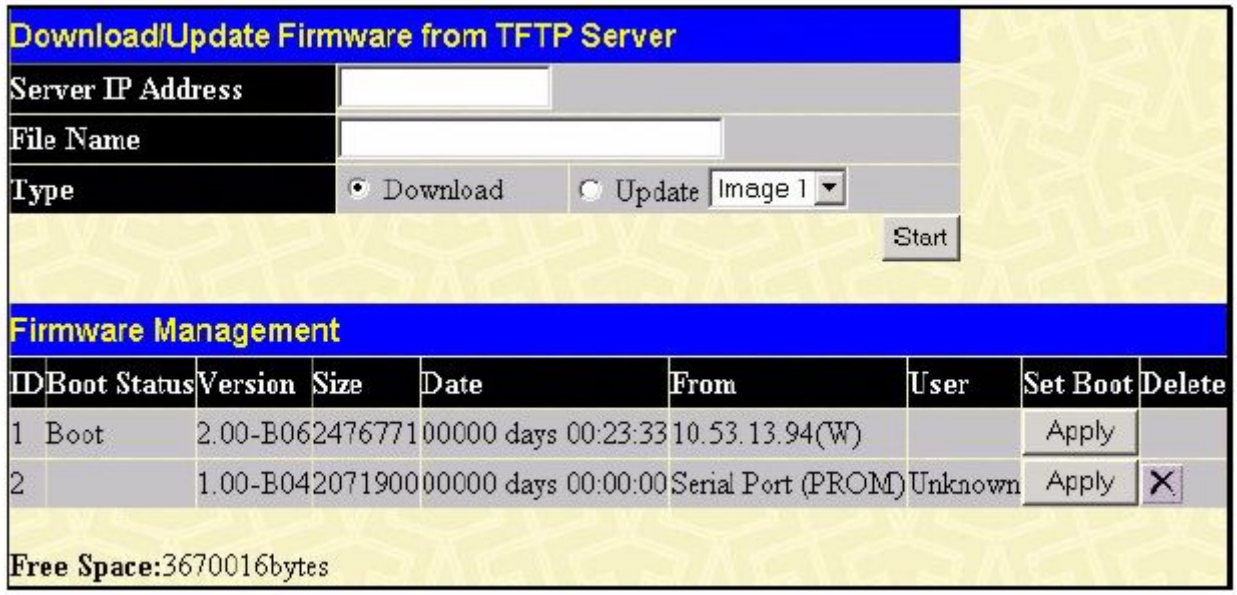


Рисунок 9.1 – Окно «Download/Update Firmware from TFTP Server»

Коммутатор может хранить две версии программного обеспечения, используемую версию программного обеспечения можно определить в поле **Type,** выбрав опцию Update и определить *Image 1* или *Image 2* в выпадающем меню. Для загрузки или обновления программного обеспечения настройте следующие поля и кликните по **Start**.

Параметр	Описание
Server IP	Введите IP-адрес сервера, с которого вы хотите загрузить прошивку.
File Name	Определите путь и имя файла с программным обеспечением на сервере.
Type	Выберите действие, которое необходимо произвести с программным обеспечением: *Download*: При выборе данной опции определяет загрузку программного обеспечения на коммутатор. Коммутатор сразу же начнет использовать

	данную версию программную обеспечения. *Update*: При выборе данной опции коммутатор сохранит программное обеспечение на коммутаторе, не используя его. Коммутатор поддерживае две версии программного обеспечения (Section 1 и Section 2).

Информация о программном обеспечении Коммутатора доступна в том же окне в таблице Firmware Management. Оно содержит следующую информацию:

Параметр	Описание
ID	ID программного обеспечения, определенный пользователем на коммутаторе.
Boot Status	Напротив текущей версии программного обеспечения коммутатора будет указано «Boot».
Version	Версия программного обеспечения.
Size	Размер файла программного обеспечения в байтах.
Date	Дата установки программного обеспечения на коммутатор.
From	IP-адрес сервера, с которого установлено программное обеспечение.
User	Имя пользователя, установившего программное обеспечение.
Set Boot	Нажатие кнопки **Apply** напротив соответствующего программного обеспечения приведет к тому, что данная версия программного обеспечения будет использоваться после перезапуска коммутатора в качестве основной.
Delete	Кликните по **X** в данной колонке для удаления соответствующего программного обеспечения с коммутатора.

Загрузка конфигурационного файла

Чтобы скачать конфигурационный файл с TFTP-сервера, нажмите **Maintenance ⇨ TFTP Services ⇨ Download Configuration File:**

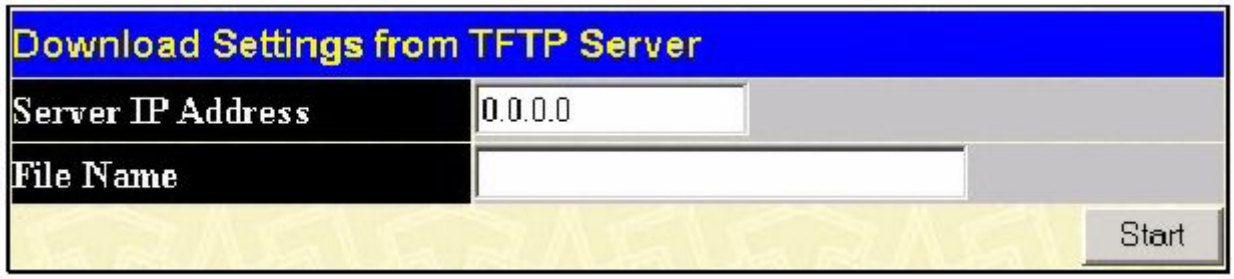


Рисунок 9.2 – Окно «Download Settings from TFTP Server»

Введите IP-адрес TFTP-сервера и задайте путь к конфигурационному файлу коммутатора на TFTP-сервере. Кликните по Start для записи IP-адреса TFTP-сервера и начала передачи файла.

Сохранение конфигурационного файла на TFTP-сервере

Для загрузки конфигурационного файла коммутатора на TFTP-сервер, нажмите **Maintenance ⇨ TFTP Services**, а затем кликните по ссылке **Upload Configuration:**

Рисунок 9.3 – Окно Upload Settings to TFTP Server

Введите IP-адрес TFTP-сервера, путь и имя конфигурационного файла на TFTP-сервере.
Кликните **Start** для начала передачи файла на TFTP-сервер.

Загрузка журнала Коммутатора на TFTP-сервер

Чтобы загрузить файл журнала Коммутатора на TFTP-сервер, откройте **Maintenance ⇨ TFTP Services,** а затем кликните по ссылке **Upload Log:**

Рисунок 9.4 – Окно «Upload Log to TFTP Server»

Введите IP-адрес TFTP-сервера, путь и имя файла с журналом Коммутатора на TFTP-сервере.
Нажмите **Start** для начала загрузки файла на TFTP-сервер.

Поддержка нескольких версий программного обеспечения

С помощью папки **Multiple Image Services** пользователи Коммутатора могут настроить и просмотреть информацию о программном обеспечении коммутатора. В памяти коммутатора может храниться две версии программного обеспечения, причем любая из них может быть настроена в качестве основной, т.е. используемой при загрузке коммутатора. Для получения информации о программном обеспечении коммутатора кликните по ссылке **Firmware Information.** По умолчанию при запуске коммутатора будет использоваться та версия программного обеспечения, которая хранится в Image 1, однако пользователь может изменить эту настройку с помощью окна **Config Firmware Image.**

Информация о программном обеспечении

Следующее окно содержит информацию о существующем программном обеспечении на коммутаторе. Для открытия данного окна кликните **Maintenance ⇨ MULTIPLE IMAGE Services ⇨ Firmware Information**.

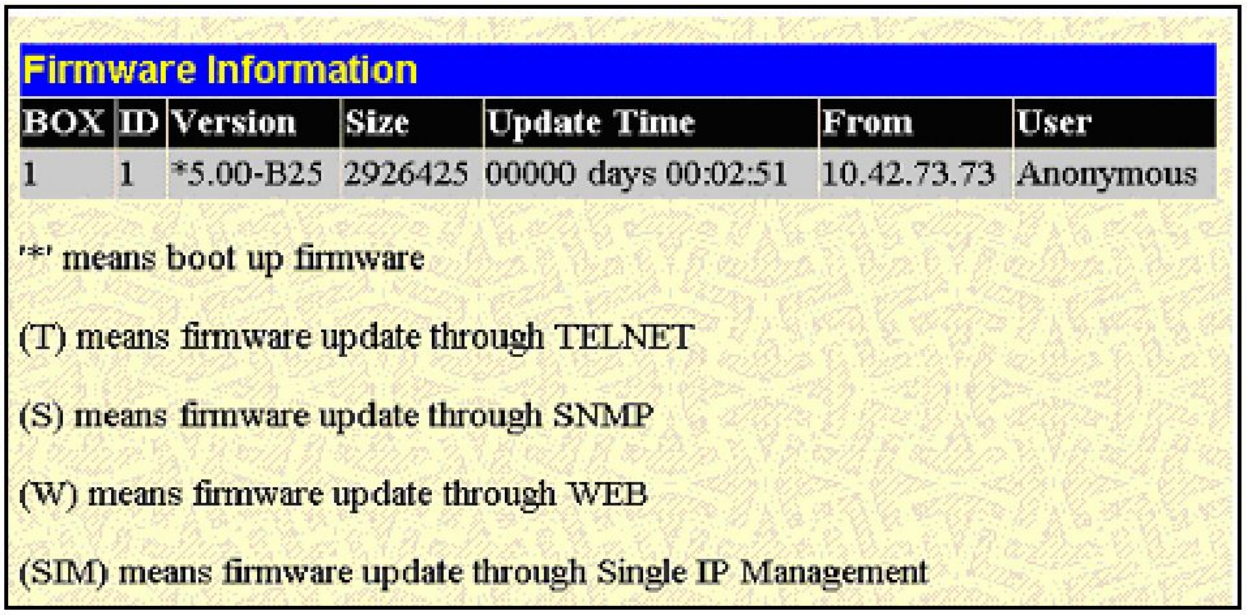


Рисунок 9.5 – Окно Firmware Information

Данное окно содержит следующую информацию:

Параметр	Описание
BOX	Определяет идентификационный номер коммутатора в стеке.
ID	Определяет ID программного обеспечения в памяти коммутатора. Коммутатор поддерживает два образа программного обеспечения. По умолчанию в качестве основного программного обеспечения будет использоваться Image ID 1, но пользователь может изменить эту настройку.
Version	Определяет версию программного обеспечения.
Size	Определяет размер соответствующего программного обеспечения в байтах.
Update Time	Дата установки программного обеспечения на коммутатор.
From	Задает IP-адрес устройства, с которого было установлено программное обеспечение. К IP-адресу в скобках дописываются следующие буквы: ▪ **R** – Если обновление программного обеспечения было произведено через консольный порт (RS-232). ▪ **T** – Если обновление программного обеспечения было произведено через Telnet. ▪ **S** – Если обновление программного обеспечения было произведено через SNMP (Simple Network Management Protocol). ▪ **W** – Если обновление программного обеспечения было произведено через Web-интерфейс управления. ▪ **SIM** – Если обновление программного обеспечения было произведено через Single IP Management.
User	Указывает имя пользователя, установившего программное обеспечение. Для неидентифицированных пользователей в данном поле будет указано «Anonymous» или «Unknown».

Настройка образа программного обеспечения

Окно «**Config Firmware Image**» позволяет пользователям настраивать образы программного обеспечения, сохраненные в памяти коммутатора. Для открытия следующего окна, нажмите **Maintenance ⇨ MULTIPLE IMAGE Services ⇨ Config Firmware Image**.

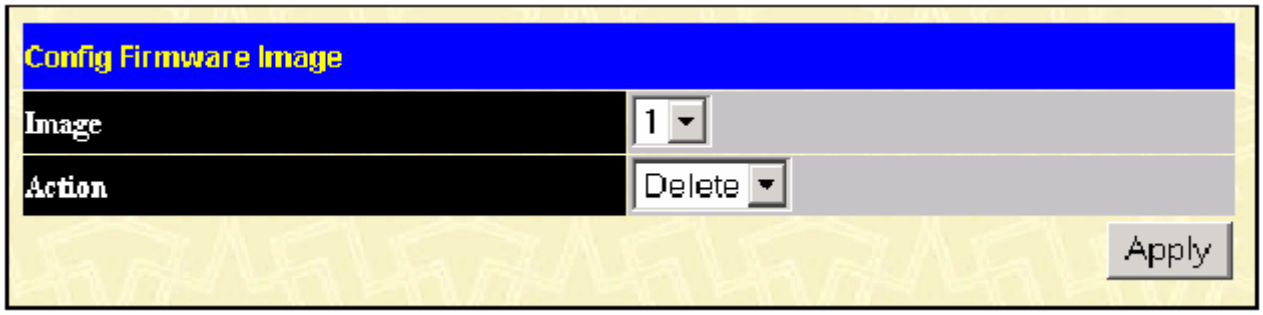


Рисунок 9.6 – Окно Config Firmware Image

В данном окне содержится следующая информация:

Параметр	Описание
Image	Выберите образ программного обеспечения для настройки, используя выпадающее меню. Коммутатор может хранить в памяти два образа программного обеспечения.
Action	В данном поле доступны две опции. ▪ Delete – выбор данной опции позволяет удалить программное обеспечение, указанное в поле Image. ▪ Boot – выбор данной опции позволяет установить образ программного обеспечения, указанный выше, в качестве основного при загрузке коммутатора. По умолчанию после перезагрузки загружается образ программного обеспечения ID 1.

Для того чтобы настройки вступили в силу, кликните по **Apply**.

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.

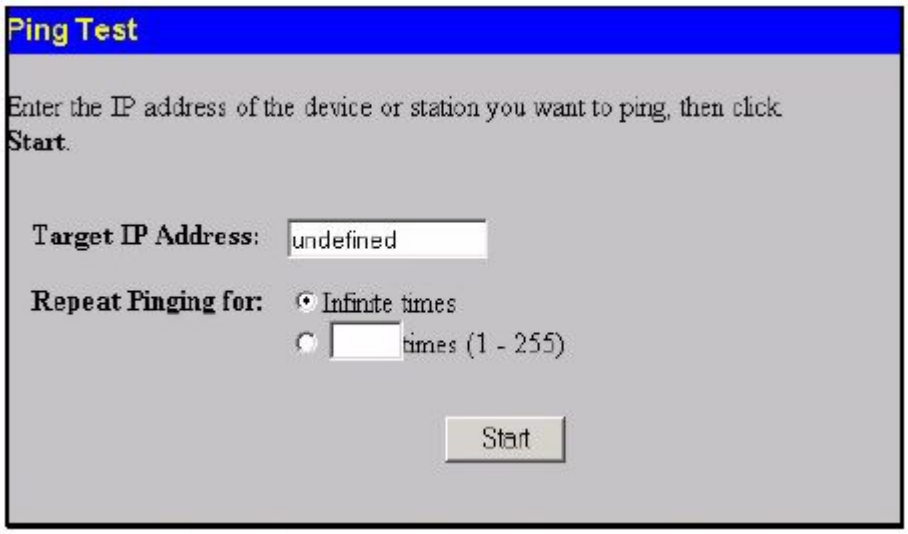


Рисунок 9.7 – Окно Ping Test

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.

Сохранение изменений

Коммутатор обладает двумя видами памяти: оперативная RAM и постоянная (энергонезависимая) NV-RAM. Выполняемые настройки записываются в RAM и вступают в силу после нажатия на кнопку **Apply** (Применить).

Если настройки не были сохранены в памяти NV-RAM, то во время перезапуска коммутатора они сотрутся, и коммутатор вернется к настройкам, сохраненным в NV-RAM.

Для сохранения выполненных изменений в настройках в энергонезависимой памяти NV-RAM кликните по **Save Changes** в папке **Maintenance.** Далее появится следующее окно.

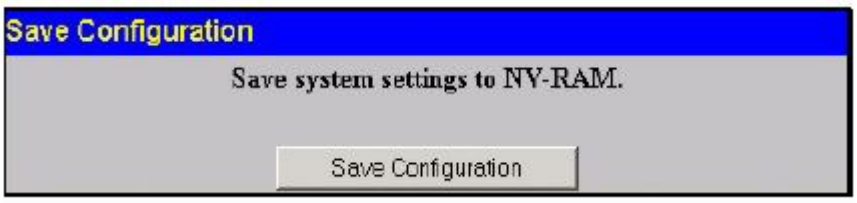


Рисунок 9.8 – Окно «Save Configuration»

Для сохранения текущих настроек коммутатора в NV-RAM нажмите кнопку **Save Configuration**. Следующее диалоговое окно подтвердит, что настройки сохранены:

Рисунок 9.9 – Диалоговое окно, подтверждающее сохранение настроек

Для продолжения кликните по **OK.** После сохранения конфигурационных настроек в памяти NV-RAM, они станут настройками по умолчанию для коммутатора и будут использоваться каждый раз при его перезапуске.

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 и затем перезапустить коммутатор. 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.

При выборе опции Reset будут сохранены учетные записи пользователей и журнал событий, в то время как все другие конфигурационные параметры будут сброшены к заводским по умолчанию. Если к коммутатору применить функцию Reset, используя данное окно, и сохранение изменений **Save Changes** при этом не было произведено, то после перезагрузки коммутатор вернется к последней сохраненной конфигурации.

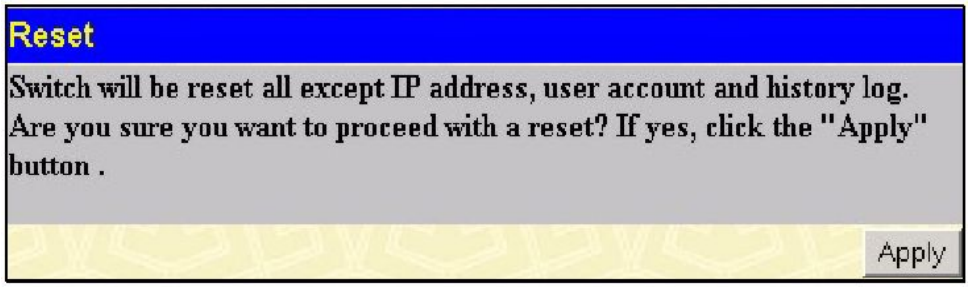


Рисунок 9- 10. Окно Reset

Reset System

При выборе опции Reset System все настройки будут сброшены к заводским и сохранены в памяти коммутатора NV-RAM. После этого произойдет перезапуск коммутатора. Аналогичный результат будет получен при выборе опции **Reset Config** и последующем сохранении изменений **Save Changes**.

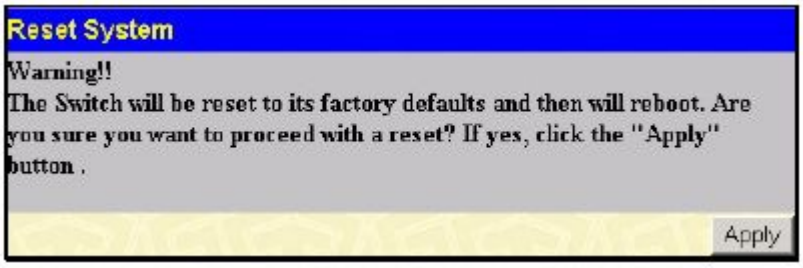


Рисунок 9.11 – Окно «Reset System»

Reset Config

При выборе опции Reset Config все настройки будут сброшены к заводским настройкам по умолчанию. При этом, в отличите от опции Reset system, не произойдет сохранения заводских параметров в энергонезависимой памяти NV-RAM. Если выбрать данную опцию, а затем не сохранить изменения с помощью **Save Changes,** то после перезагрузки коммутатор вернется к последней сохраненной конфигурации.

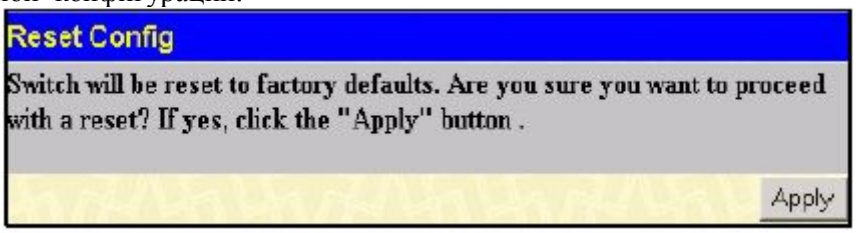


Рисунок 9.12 – Окно «Reset Config»

Перезапуск коммутатора

Следующее окно используется для перезапуска коммутатора. Все настройки, не сохраненные в энергонезависимой памяти коммутатора, будут утрачены. Кликните по кнопке **Reboot** для перезапуска коммутатора.

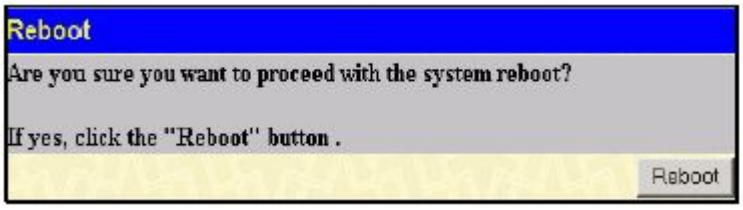


Рисунок 9.13 - Окно «Reboot»

Выход из системы (Logout)

Воспользуйтесь страницей завершения работы Web-интерфейса управления коммутатором, кликнув по кнопке **Log Out**.

Рисунок 9.14 – Окно Logout Web Setup

Раздел 10 - D-Link Single IP Management

Обзор технологии Single IP Management (SIM)
Топология сети
Обновление прошивки
Сохранение резервной копии/восстановление конфигурационных файлов

Обзор технологии Single IP Management (SIM)

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

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

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

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

Нет ограничений на количество SIM-групп в одной IP-подсети (широковещательном домене), однако один коммутатор может принадлежать только одной группе.
Если настроено большое количество VLAN, SIM-группа будет использовать на любом коммутаторе только VLAN *default*.
Технология SIM может использоваться в сетях, содержащих устройства, не поддерживающие SIM. Это позволяет пользователю контролировать работу коммутаторов, которые находятся на расстоянии более одного hop (перехода) от управляющего коммутатора CS.
SIM-группа – это группа коммутаторов, которые управляются как единый объект. Коммутаторы могут выполнять три различные функции:

1.**Commander Switch (CS) –** Это коммутатор, настраиваемый вручную в качестве управляющего устройства и обладающий следующими свойствами:

- Имеет IP-адрес.
- Не является управляющим коммутатором CS или членом другой SIM-группы.
- Подключен к другим коммутаторам, являющимися членами группы, через управляющую виртуальную локальную сеть VLAN.

2.**Member Switch (MS) –** Это коммутатор, который является членом SIM-группы и, к которому возможен доступ с управляющего коммутатора CS, он обладает следующими свойствами:

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

3.**Candidate Switch (CaS) –** это коммутатор, который готов стать членом SIM-группы, но не являющийся еще таковым. При помощи ручной настройки коммутатор Candidate Switch может стать членом SIM-группы. Коммутатор, настроенный в качестве CaS, который не является членом SIM-группы и обладает следующими свойствами:

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

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

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

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

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

Обновление технологии SIM до версии v1.6

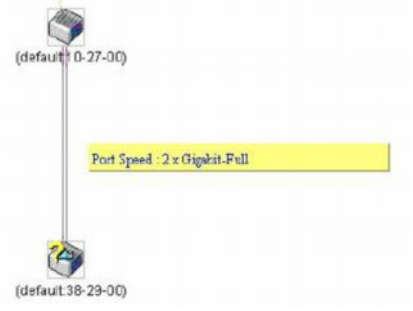
Коммутаторов серии xStack DES-3500 в данном релизе поддерживают управление согласно технологии SIM версии 1.6.

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.

Подключение функции SIM через Web-интерфейс

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

Рисунок 10.1 – 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:

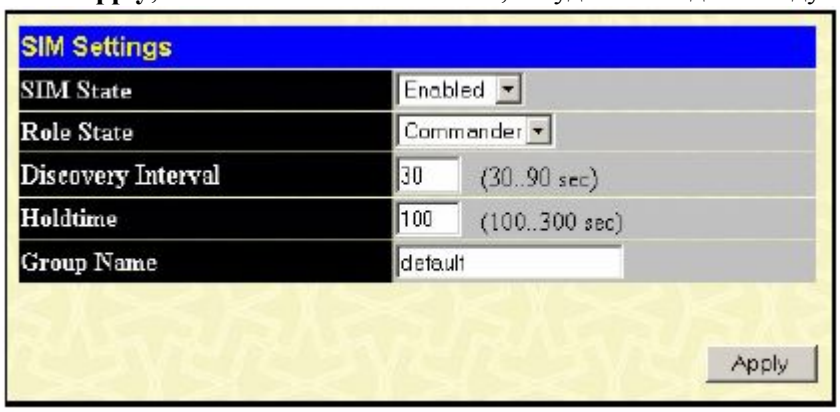


Рисунок 10.2 – Окно «SIM Settings» (enabled – включено)

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.
Group Name	Пользователь может задать имя группы длиной до 64 символов.

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 три ссылки: **Topology, Firmware Upgrade** и **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. Если кликнуть по **Topology** в папке **Single IP Management (Single IP Management ⇨ Topology),** появится следующее сообщение.

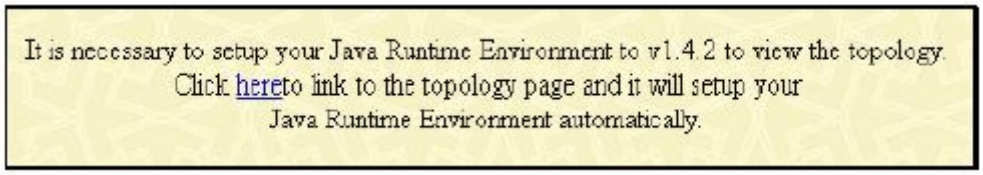


Рисунок 10.3 – Окно Java

Кликните по ссылке here, чтобы установить Java Runtime Environment на сервере, что приведет вас к окну Topology, показанному ниже.

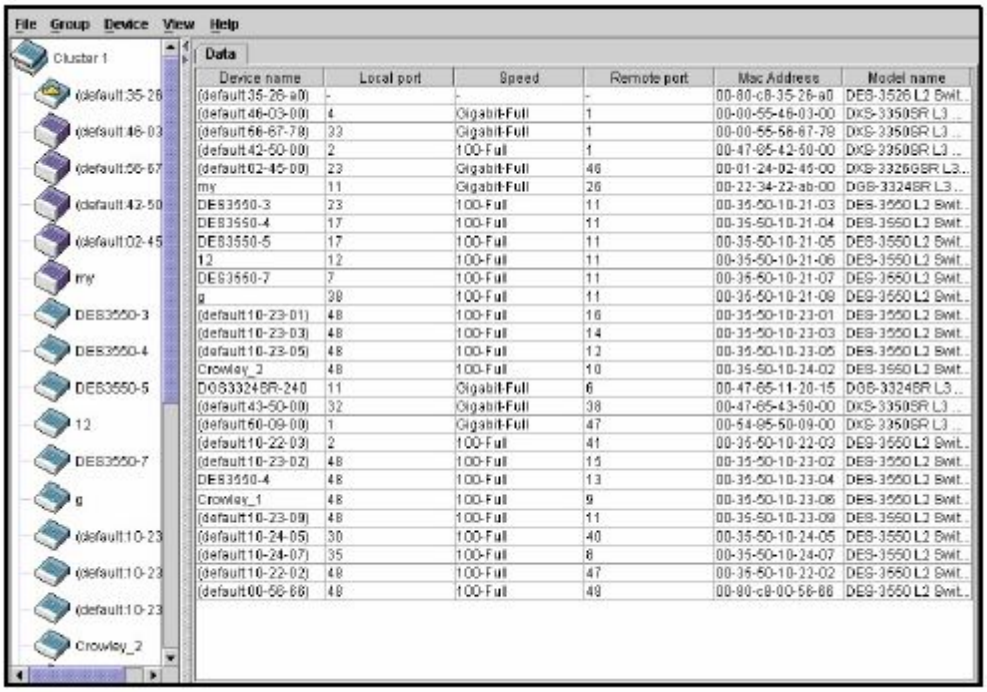


Рисунок 10.4 – Окно Single IP Management – Tree View

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).

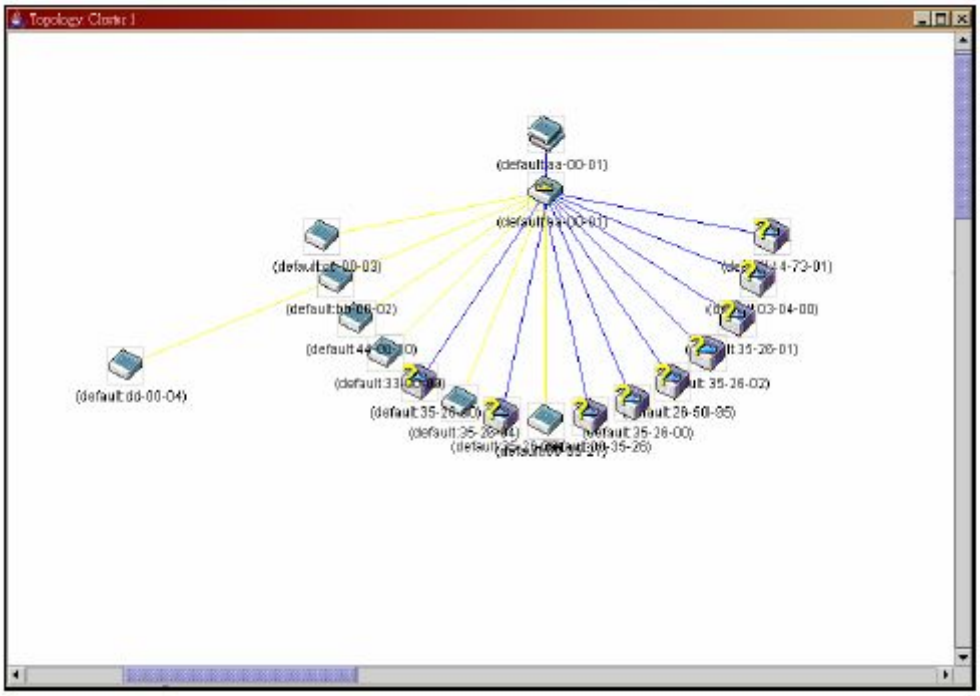


Рисунок 10.5 – Окно «Topology View»

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.

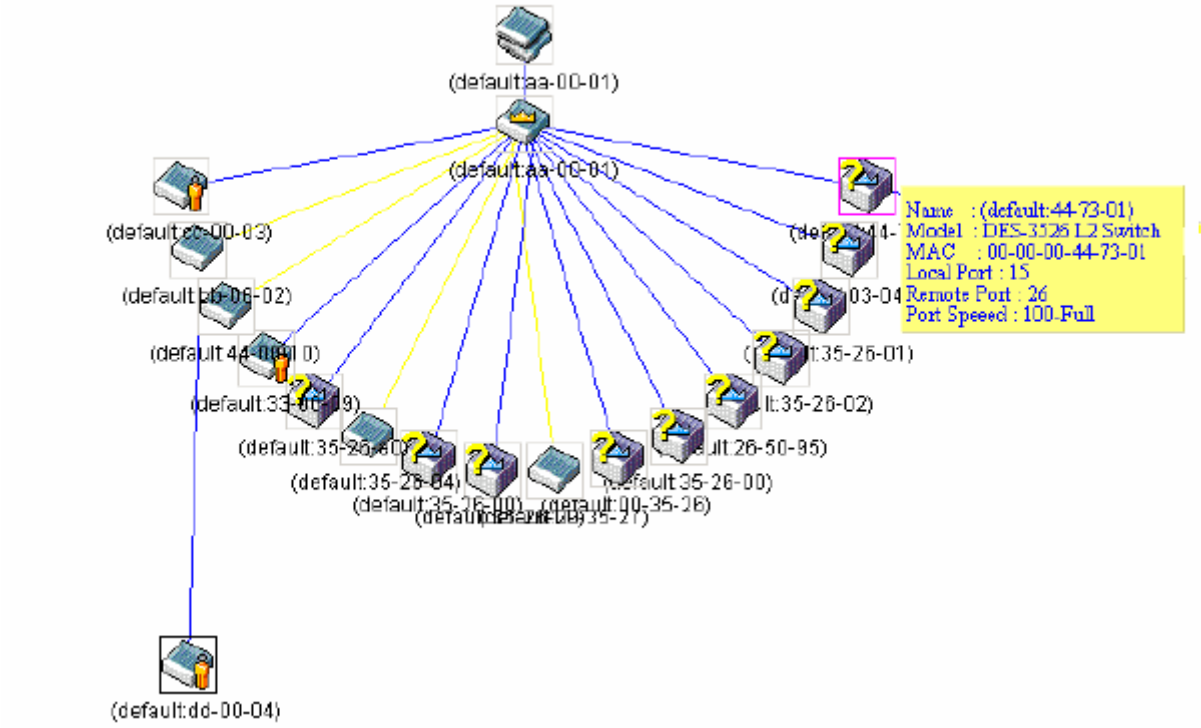


Рисунок 10.6 – Получение информации об устройстве, используя значки устройств

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

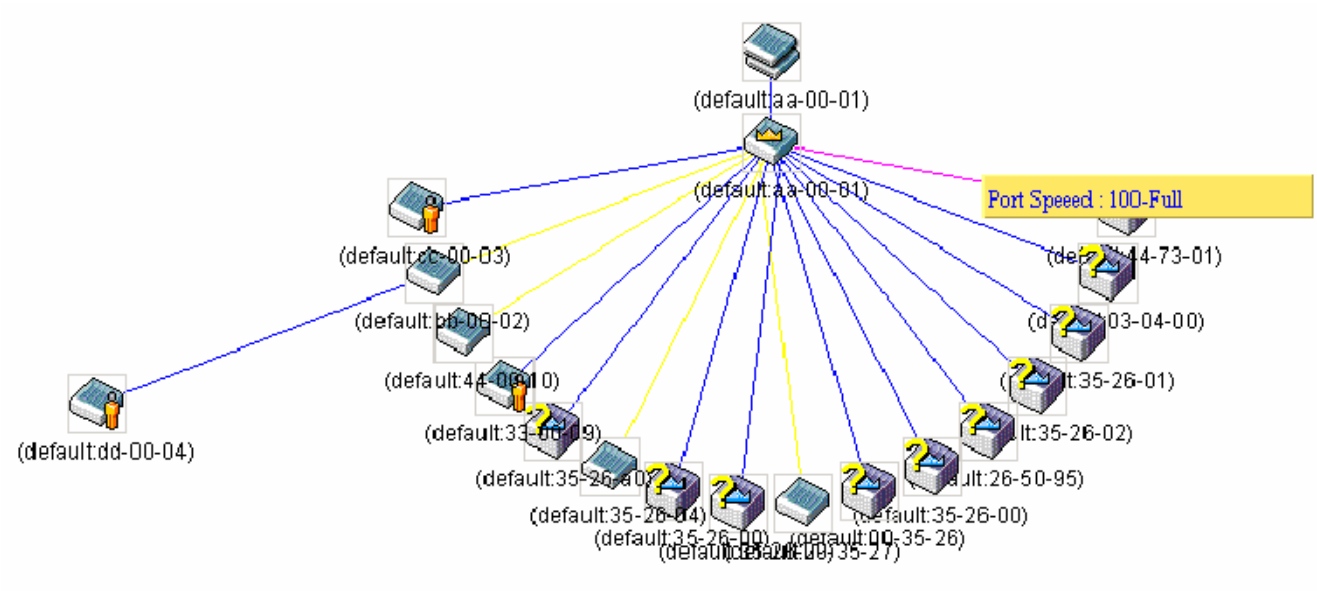


Рисунок 10.7 – Получение информации о скорости порта, используя значки устройства

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

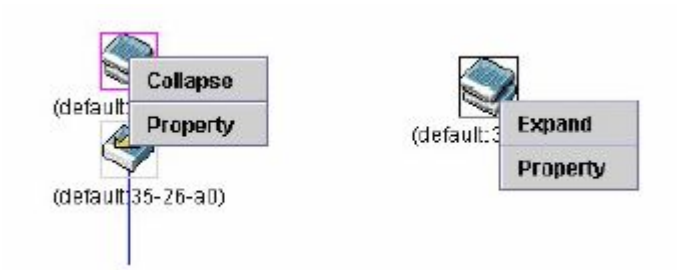


Рисунок 10.8 –Нажатие правой кнопкой мышки на значок группы

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.

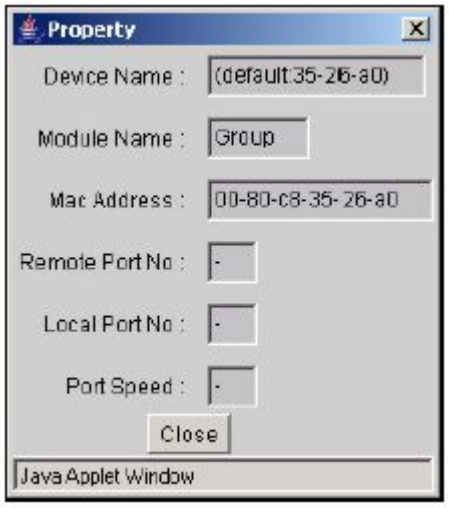


Рисунок 10.9 – Окно Property

Значок управляющего коммутатора

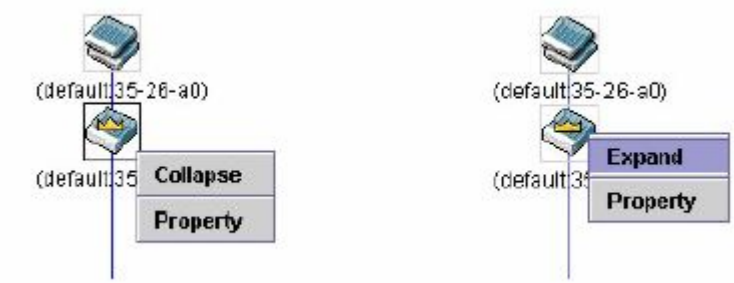


Рисунок 10.10 – Нажатие правой кнопкой мыши по значку управляющего коммутатора

Следующие опции могут быть доступны пользователю при настройке:

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

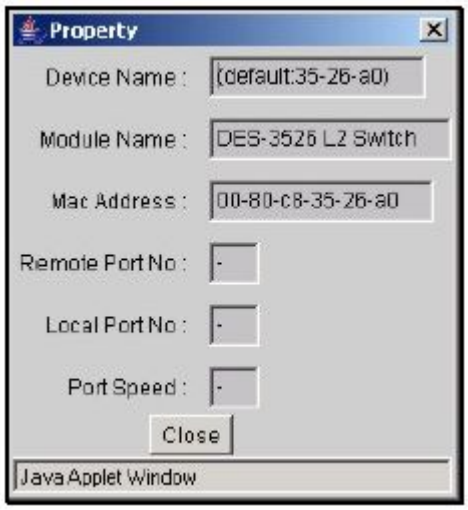


Рисунок 10.11 – Окно «Property»

Значок члена группы

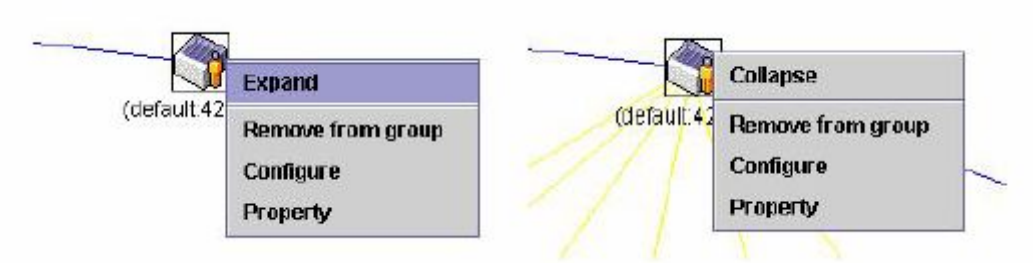


Рисунок 10.12 - Нажатие правой кнопки мышки по значку члена группы

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.

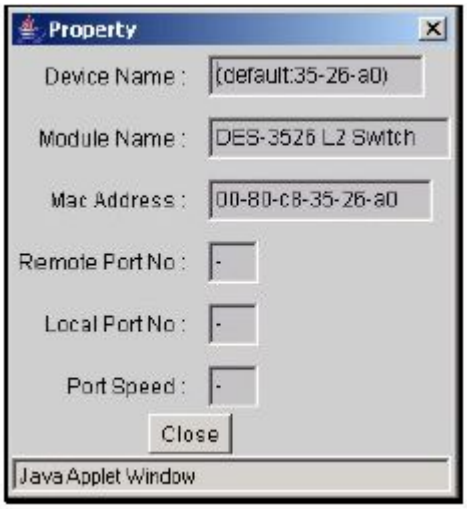


Рисунок 10.13 – Окно «Property»

Значок коммутатора CaS

Рисунок 10.14 - 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 **ОК** или **Cancel** для закрытия окна.

Рисунок 10.15 – Диалоговое окно Input password

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

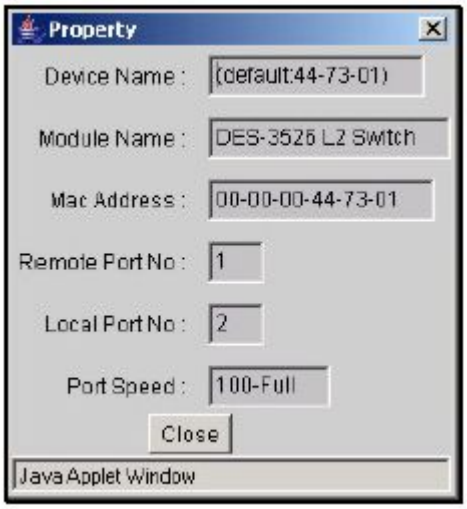


Рисунок 10.16 - Окно Property

Данное окно содержит следующую информацию:

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

Для закрытия окна **Property** кликните по **Close.**

Линейка меню

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

Рисунок 10.17 – Линейка меню в окне «Topology View»

Содержание пяти пунктов меню описывается далее.

File

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

Group

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

Рисунок 10.18 - Диалоговое окно Input password

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

Device

▪ **Configure** – открыть Web-интерфейс управления для настройки устройства.

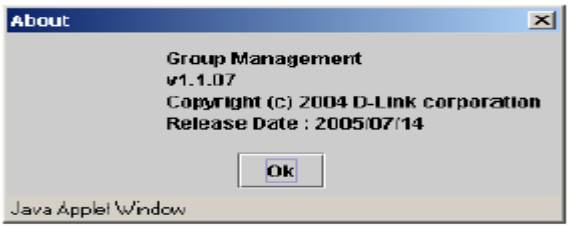
View

▪ **Refresh** – обновить окна просмотра.

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

Help

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



Примечание: В данной версии программного обеспечения некоторые функции SIM можно настроить только через интерфейс командной строки CLI (Command Line Interface). Для получения более полной информации о технологии SIM и ее настройках, обратитесь к ***Руководству по интерфейсу командной строки для коммутаторов серии DES-3500*** **.**

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. 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**.

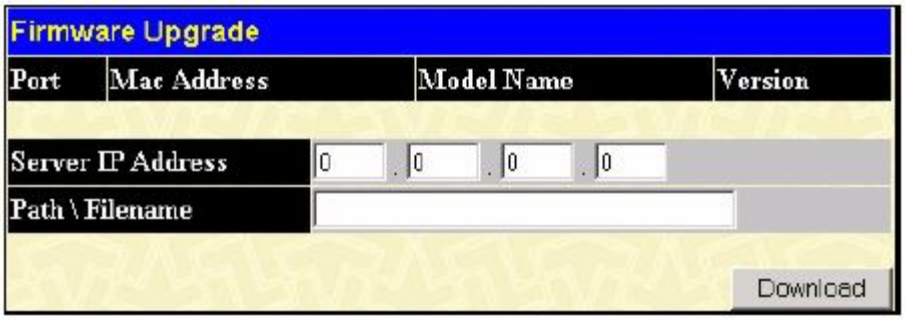


Рисунок 10.19 – Окно Firmware Upgrade

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**).

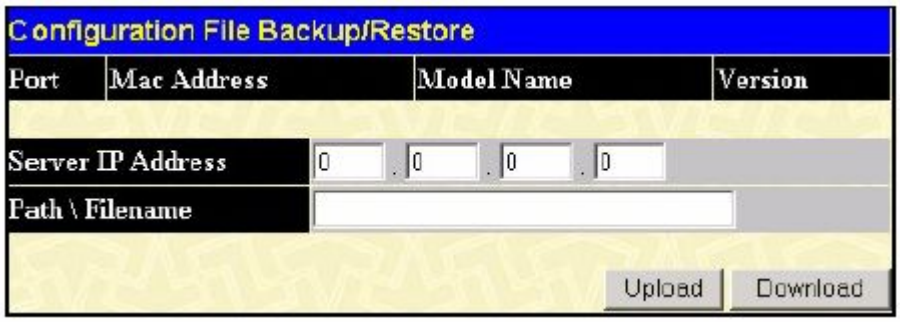


Рисунок 10.20 – Окно Configuration File Backup/Restore

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 **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**.

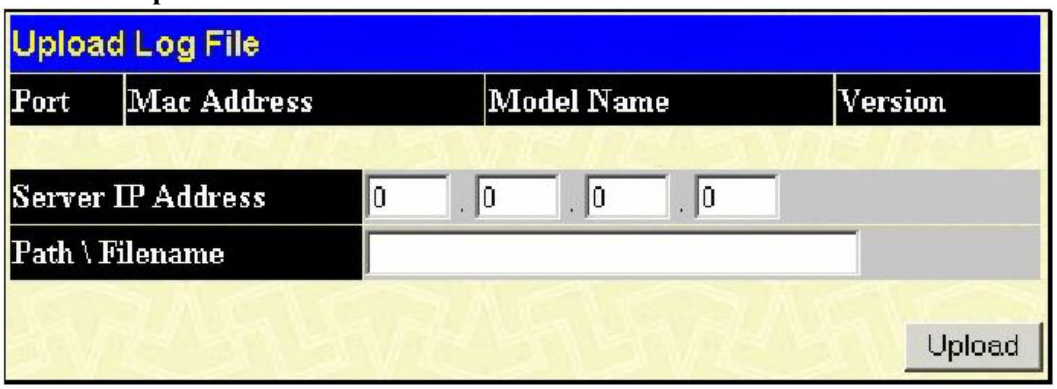


Рисунок 10- 21. Окно Upload Log File

Приложение А

Техническая спецификация

Основные	
Стандарты	Автосогласование NWay IEEE 802.3 IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP “Mini GBIC”) IEEE 802.1D Spanning Tree IEEE 802.1W Rapid Spanning Tree IEEE 802.1S Multiple Spanning Tree IEEE 802.1Q VLAN Очереди приоритетов IEEE 802.1p Агрегирование каналов IEEE 802.3ad Управление потоком в режиме полного дуплекса IEEE 802.3x
Протоколы	CSMA/CD
Канал связи **Ethernet** **Fast Ethernet** **Gigabit Ethernet** **Fiber Optic**	Полудуплекс Дуплекс 10 Мбит/с 20Мбит/с 100Мбит/с 200Мбит/с n/a 2000Мбит/с Поддержка SFP (Mini GBIC) IEEE 802.3z 1000BASE-LX (трансивер DEM-310GT) IEEE 802.3z 1000BASE-SX (трансивер DEM-311GT) IEEE 802.3z 1000BASE-LH (трансивер DEM-314GT) IEEE 802.3z 1000BASE-ZX (трансивер DEM-315GT)
Топология	Звезда
Сетевые кабели	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-ohm экранированная витая пара (STP)(100м)
Количество портов	24 порта 10/100/1000 Мбит/с (для DES-3526/DES-3526DC) 48 портов 10/100/1000 Мбит/с (для DES-3550) 2 комбо-порта 1000BASE-T/SFP

Физические параметры и условия эксплуатации		
Внешнее устройство питания	DES-3526/DES-3550	входное напряжение переменного тока: 100 – 120; 200 – 240 В, с частотой 50/60 Гц
	DES-3526 DC 60W	Входное напряжение постоянного тока: 48 В Выходное напряжение: 12В
Потребляемая мощность	Для DES-3526/DES-3526DC 23 Вт (макс.) Для DES-3550 40 Вт (макс.)	
Вентиляторы DC	Для DES-3526/DES-3526DC: один вентилятор 40мм Для DES-3550: два вентилятора 40мм	
Рабочая температура	От 0 до 40C	
Температура хранения	От -40 до 70C	
Влажность	От 5% до 95% без образования конденсата	
Размеры	Для DES-3526/DES-3526DC: 441 мм x 207 мм x 44 мм, стандартный размер для монтажа в 19” стойку Для DES-3550: 441 мм x 309 мм x 44 мм	
Масса	DES-3526 2.56 кг DES-3526DC 2.5 кг DES-3550 5 кг	
Электромагнитное	CE class A, FCC Class A, C-Tick	

излучение (EMI)	
Безопасность	CSA International

Производительность	
Метод коммутации	Store-and-forward
Размер буфера пакетов	16 MB на устройство
Скорость фильтрации/ продвижения пакетов	Одинаковая скорость для всех соединений. 1,488,095 pps на порт (для 1000Мбит)
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.

Приложение B
Кабели и коннекторы

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

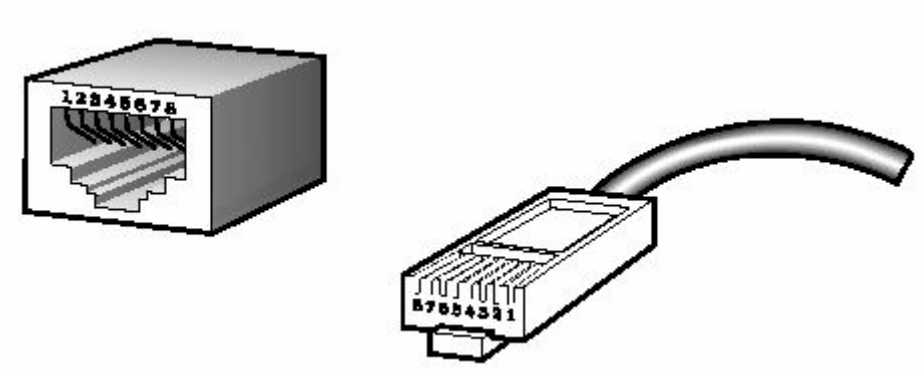


Рисунок B-1. Стандартный RJ-45 разъём с вилкой

Контакты разъёма RJ-45		
Контакты	Порт MDI-X	Порт MDI-II
1	RD+ (прием)	TD+ (передача)
2	RD- (прием)	TD- (передача)
3	TD+ (передача)	RD+ (прием)
4	не используется	не используется
5	не используется	не используется
6	TD- (transmit)	RD- (прием)
7	не используется	не используется
8	не используется	не используется

Таблица B-1. Стандартный разъём RJ-45

Приложение C
Записи системного журнала

В следующей таблице представлены возможные записи в Системном журнале и их значение.

Категория	Описание события	Содержимое записи	Уровень события	Примечание
system	Запуск системы в результате перезагрузки	**System warm start**	Critical	
system	Запуск системы в результате включения питания	**System cold start**	Critical	
	Сохранение конфигурации во Flash-памяти	**Configuration and log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Ошибка внутреннего блока питания	**Internal Power failed**	Critical	
	Восстановление внутреннего блока питания	**Internal Power is recovered**	Critical	
	Сбой в работе резервного источника питания	**Redundant Power failed**	Critical	
	Работа резервного источника питания восстановлена	**Redundant Power is working**	Critical	
up / download	Успешное обновление программного обеспечения	**Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Программное обеспечение обновить не удалось	**Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь

Категория	Описание события	Содержимое записи	Уровень события	Примечание
				зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Конфигурационный файл успешно загружен	**Configuration successfully downloaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Загрузить конфигурационный файл не удалось	**Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Конфигурационный файл успешно сохранен	**Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Сохранить конфигурационный файл не удалось	**Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и

Категория	Описание события	Содержимое записи	Уровень события	Примечание
				MAC-адресах не будет представлена в записи журнала.
	Журнал коммутатора успешно сохранен	**Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Informational	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Не удалось сохранить журнал коммутатора	**Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)**	Warning	«by console» и «IP: <ipaddr>, MAC: <macaddr>» связаны между собой XOR (исключающее или). Это значит, что если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
Interface	Соединение на порту	**Port <portNum> link up, <link state>**	Informational	Пример link state: , 100Mbps FULL duplex.
	Отсутствие соединения на порту	**Port <portNum> link down**	Informational	
Console	Успешная регистрация через консоль	**Successful login through Console (Username: <username>)**	Informational	Если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Не удалось зарегистрироваться через консоль	**Login failed through Console**	Warning	Если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Выход из системы через консоль	**Logout through Console (Username: <username>)**	Informational	Если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в

Категория	Описание события	Содержимое записи	Уровень события	Примечание
				записи журнала.
	Время сессии консоли истекло	**Console session timed out (Username: <username>)**	Informational	Если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
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	
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	**SNMP request received from**	Informational	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	некорректную community string	**<ipAddress> with invalid community string!**		
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 протокола Spanning Tree	**Spanning Tree Protocol is disabled**	Informational	
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 соовтетствии с локальным методом (local)	**Successful login through Console authenticated by AAA local method (Username: <username>)**	Informational	Если пользователь зарегистрирован через консоль, то информация об IP- и MAC-адресах не будет представлена в записи журнала.
	Регистраця через консоль не аутентифицирована	**Login failed through Console authenticated by AAA local method**	Warning	Если пользователь зарегистрирован через консоль, то

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	в соответствии с локальным методом (local)	**(Username: <username>)**		информация об IP- и MAC-адресах не будет представлена в записи журнала.
	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 Web (SSL) не аутентифицирована в соответствии с локальным методом (local)	**Login failed through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**	Warning	
	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	**Login failed through SSH from <userIP>**	Warning	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	SSH не аутентифицирована в соответствии с локальным методом (local)	**authenticated by AAA local method (Username: <username>, MAC: <macaddr>)**		
	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	
	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	**Login failed through Console**	Warning	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	аутентифицирована из-за таймаута или несоответствующей конфигурации сервера аутентификации	**due to AAA server timeout or improper configuration (Username: <username>)**		
	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	**Login failed through Web(SSL) from <userIP> due to AAA server timeout or improper configuration**	Warning	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	аутентификации	**(Username: <username>, MAC: <macaddr>)**		
	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	**Successful Enable Admin**	Informational	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	Admin через консоль аутентифицировано методом local_enable (локальный пароль)	**through Console authenticated by AAA local_enable method (Username: <username>)**		
	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 Admin через Web-интерфейс аутентифицировано методом local_enable (локальный пароль)	**Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Informational	
	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	**Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username:**	Informational	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	(локальный пароль)	**<username>, MAC: <macaddr>)**		
	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 не аутентифицировано методом local_enable (локальный пароль)	**Enable Admin failed through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>, MAC: <macaddr>)**	Warning	
	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**	Informational	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
		none method (Username: <username>, MAC: <macaddr>)		
	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-за таймаута или несоответствующей конфигурации сервера аутентификации	**Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)**	Warning	
	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:**	Warning	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
		<macaddr>)		
	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 сервера аутентификации	**Enable Admin failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>, MAC: <macaddr>)**	Warning	
	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	**Enable Admin failed through**	Warning	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	команды Enable Admin через Telnet не аутентифицировано сервером аутентификации	**Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>, MAC: <macaddr>)**		
	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	Вместо <protocol> будет представлено TACACS, XTACACS, TACACS+ или RADIUS
Port Security	Количество изученных адресов функции Port	**Port security violation (Port: <portNum>, MAC:**	Warning	

Категория	Описание события	Содержимое записи	Уровень события	Примечание
	Security достигло максимума, и новые адреса не могут быть изучены.	**<macaddr>)**		
IP-MAC-PORT Binding	IP-адрес не удовлетворяет связке IP-MAC Port Binding	**Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)**	Warning	
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	
Security	Получен пакет от источника, MAC-адрес которого совпадает с MAC-адресом устройства	**Possible spoofing attack from <mac> port <u16>**	Critical	

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-LHX, 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.