

D-Link™ DGS-3324SR

**Стекируемый коммутатор Gigabit Ethernet 3-его
уровня с высокой плотностью портов**

Руководство пользователя

Содержание

Для читателей	7
Типографские обозначения.....	7
Примечания, предупреждения и предостережения	8
Инструкции по технике безопасности	8
Меры предосторожности.....	8
Общие меры предосторожности для монтируемых в стойку устройств.....	10
Защита от электростатического разряда.....	11
Введение.....	12
Описание коммутатора.....	12
Характеристики	12
Компоненты передней панели.....	13
Светодиодные индикаторы.....	13
Описание задней панели	14
Разъем RPS	14
Опции управления	14
Web-интерфейс управления.....	14
Консольный интерфейс командной строки через последовательный порт или Telnet.....	14
SNMP-управление	14
Установка	16
Комплект поставки	16
Установка коммутатора.....	17
Установка коммутатора на поверхность	17
Установка коммутатора в стойку	17
Объединение коммутаторов в стек	18
Настройка группы коммутаторов на работу в составе стека.....	20
Индикатор порядкового номера устройства в стеке	21
Комбинированные порты Gigabit.....	22
Внешний резервный источник питания.....	22
Подключение к консольному порту.....	23
Защита паролем.....	24
Настройки SNMP	25
Traps	26
MIB.....	26
Установка IP-адреса.....	26
Подключение устройств к коммутатору.....	27
Введение в управление коммутатором	28
Введение	28
Регистрация в Web-менеджере	28
Пользовательский Web-интерфейс управления.....	29
Области интерфейса пользователя.....	29
Web-страницы.....	30
Основная настройка.....	31
Параметры IP коммутатора.....	32
Задание IP-адресов станций управления	34
Управление учетными записями пользователей	35
Привилегии Admin и User	36
Сохранение настроек.....	36

Сброс к заводским установкам.....	37
Перезагрузка коммутатора	37
Информация о коммутаторе.....	38
Дополнительные настройки	39
Настройка	41
Настройка идентификатора коммутатора.....	41
Настройка портов.....	42
Настройка зеркалирования портов.....	43
Настройка агрегирования каналов	44
Понятие транковой группы портов.....	44
Настройка порта LACP.....	47
Настройка IGMP.....	48
IGMP Snooping.....	48
Настройка статических портов Router Port.....	50
Настройка протокола Spanning Tree.....	51
Протокол 802.1w Rapid Spanning Tree.....	51
Состояния портов.....	51
Совместимость 802.1d/802.1w.....	52
Настройки STP на коммутаторе	53
Настройка STP на портах.....	54
Настройка продвижения и фильтрации пакетов	56
Статическая таблица MAC-адресов.....	56
Статическая таблица групповых MAC-адресов	57
Настройка VLAN	58
Понятие приоритета IEEE 802.1p.....	58
Виртуальные локальные сети VLAN.....	58
Реализация VLAN в DGS-3324SR	58
IEEE 802.1Q VLAN.....	59
Продвижение пакетов VLAN 802.1Q	59
Теги 802.1Q VLAN	60
Port VLAN ID.....	61
Tagging и Untagging.....	62
Фильтрация входящего трафика	62
Default VLAN.....	63
VLAN на основе портов.....	63
Сегментация с помощью VLAN	63
VLAN и транковые группы портов	64
Настройка статических VLAN	64
Настройка GVRP.....	65
Управление трафиком (контроль широковещательной/ групповой рассылки).....	67
Настройка функции Port Security.....	68
Настройка качества сервиса QoS.....	70
Понятие QoS.....	70
Контроль полосы пропускания	70
Выбор алгоритма обслуживания очередей	72
Настройка алгоритма обслуживания очередей.....	72
Приоритеты 802.1p по умолчанию	73
Приоритет пользователя 802.1p	74
Настройка сегментации трафика.....	75
Сервер System Log	76
Настройка параметров SNMP	78

Настройка системного времени	78
Настройка часового пояса и автоматического перехода на летнее время	79
Настройка таблицы профилей доступа	80
Управление доступом	87
Управление доступом к сети IEEE 802.1x на основе портов	87
Настройка аутентификации на коммутаторе	89
Настройка учетных записей локальных пользователей	92
Система контроля PAE	92
Настройка параметров аутентификации на портах	92
Инициализация портов	94
Повторная аутентификация портов	95
Сервер RADIUS	95
Сетевое взаимодействие на 3-ем уровне	96
Общие настройки функций 3-его уровня	97
Настройка IP-интерфейсов	97
Таблица ключей MD5	99
Настройка перераспределения маршрутов	99
Статическая таблица маршрутизации	101
Статическая ARP-таблица	102
Протокол RIP	103
Формат сообщения RIP версии 1	104
Сообщение RIP 1	105
Интерпретация маршрута RIP 1	105
Расширения RIP версии 2	105
Формат сообщения RIP 2	105
Настройка RIP	106
Настройка RIP на интерфейсе	106
Настройка протокола OSPF	107
Общие настройки OSPF	121
Настройка областей OSPF	122
Настройка OSPF на интерфейсе	123
Настройка виртуального интерфейса OSPF	125
Настройка агрегирования областей	127
Настройка маршрута OSPF к узлу	128
DHCP/BOOTP Relay	129
Информация DHCP/BOOTP Relay	129
Настройка DHCP/BOOTP Relay	129
DNS Relay	130
Настройка DNS Relay	131
Статическая таблица DNS Relay	131
Многоадресная рассылка	132
Настройка IGMP на интерфейсе	132
Настройка DVMRP на интерфейсе	133
Настройка PIM-DM на интерфейсе	135
SNMP-управление	137
Настройка SNMP	137
Traps	138
MIB	138
Таблица SNMP User Table	138

Таблица SNMP View Table.....	140
Таблица SNMP Group Table.....	141
Таблица SNMP Community Table.....	143
Таблица SNMP Host Table.....	144
SNMP Engine ID.....	145
Сетевой мониторинг.....	146
Загрузка портов.....	146
Пакеты.....	147
Принятые пакеты.....	148
Принятые одноадресные/групповые/широковещательные пакеты (UMB_cast).....	149
Отправленные пакеты.....	151
Ошибки.....	153
Принятые пакеты.....	153
Отправленные пакеты.....	156
Размер пакетов.....	157
Информация о стеке.....	160
Состояние коммутатора.....	161
Таблица MAC-адресов.....	161
Журнал событий коммутатора.....	163
Таблица IGMP Snooping.....	164
Порты Router Port.....	165
Управление доступом на портах.....	165
Состояние аутентификации на коммутаторе.....	165
Статистика сессий аутентификации.....	166
Диагностика аутентификации.....	168
Аутентификация на сервере Radius.....	169
Ведение учетных записей на сервере Radius.....	170
Мониторинг функций 3-его уровня.....	171
Таблица IP-адресов.....	172
Таблица маршрутизации.....	172
ARP-таблица.....	173
Таблица маршрутизации многоадресной рассылки.....	174
Таблица IGMP-групп.....	174
Мониторинг OSPF.....	174
Таблица состояния связей OSPF.....	174
Таблица OSPF-соседей.....	175
Таблица виртуальных OSPF-соседей.....	176
Мониторинг DVMPR.....	176
Таблица маршрутизации DVMPR.....	176
Таблица адресов DVMPR- соседей.....	177
Таблица переходов DVMPR.....	177
Мониторинг PIM.....	178
Таблица адресов PIM- соседей.....	178
Обслуживание коммутатора.....	179
Сервисы TFTP.....	179
Обновление ПО коммутатора с сервера TFTP.....	179
Загрузка конфигурационного файла с сервера TFTP.....	179
Сохранение конфигурационного файла на сервере TFTP.....	180
Сохранение файла журнала коммутатора на сервере TFTP.....	180
Ping - тест.....	180
Сохранение настроек.....	181

Сброс к заводским установкам	182
Перезагрузка коммутатора.....	183
Выход из системы	183
Технические характеристики.....	184
Физические и климатические.....	185
Производительность	185
Глоссарий	186
Аппаратные средства:.....	189
Программное обеспечение:.....	189
ОГРАНИЧЕНИЯ ГАРАНТИЙ	190
ОГРАНИЧЕНИЯ ОТВЕТСТВЕННОСТИ.....	190

Для читателей

Данное Руководство пользователя DGS-3324SR содержит информацию о настройке и управлении коммутатора DGS-3324SR. Оно предназначено для сетевых администраторов, знакомых с концепциями сетевого управления и терминологией.

Типографские обозначения

Обозначение	Описание
[]	Для командной строки квадратные скобки обозначают ввод дополнительного параметра. Например: [copy filename] обозначает, что можно ввести команду <code>copy</code> и далее имя файла. Скобки не вводятся.
Жирный шрифт	Обозначает кнопку, значок, меню или пункт меню. Например: откройте меню File и выберите Cancel . Используется для выделения. Также может обозначать системные сообщения или приглашения, возникающие на экране. Например: Вам почта . Жирный шрифт также используется для выделения имен файлов, имен программ и команд. Например: используйте команду copy .
Жирный моноширинный шрифт	Обозначает команды и ответы на команды, которые должны быть введены точно так, как написано в руководстве.
Начальная заглавная буква	Обозначает заголовок окна. Также имена клавиш клавиатуры начинаются с заглавной буквы. Например: нажмите Enter.
<i>Курсив</i>	Обозначает заголовок окна или поле ввода. Кроме того, обозначает переменную или параметр, которые должны быть заменены при вводе на подходящую строку. Например: параметр <i>filename</i> указывает, что нужно ввести фактическое имя файла, а не выделенное курсивом слово.
Имя меню > Опция меню	Обозначает структуру меню. Device > Port > Properties указывает на подменю Port Properties , расположенное в подменю Port в меню Device .

Примечания, предупреждения и предостережения



Примечание: **ПРИМЕЧАНИЕ** указывает на важную информацию, которая поможет более эффективно использовать устройство.




Внимание: **ВНИМАНИЕ** предупреждает о возможности повреждения устройства или на потерю данных и помогает избежать проблемы.



Осторожно: **ОСТОРОЖНО** предостерегает от возможного повреждения устройства или травмы персонала.

Инструкции по технике безопасности

Используйте следующие инструкции по технике безопасности, чтобы гарантировать безопасность работы персонала и защитить устройство от возможного повреждения. В этом разделе значок

«осторожно» () используется для указания мер безопасности и предостережений, которые необходимо прочесть.



Меры предосторожности

Для снижения риска травмы, поражения электротоком, воспламенения или повреждения устройства соблюдайте следующие меры предосторожности.

Обратите внимание на предупреждающие обозначения на устройстве. Не используйте устройство каким-либо образом, не описанным в документации к нему. Открытие или удаление крышки, помеченной треугольным символом со значком молнии, может привести к поражению электротоком. Внутренние компоненты этих отсеков должен обслуживать только технический специалист.

Если произошло что-либо из перечисленного, то отключите устройство от розетки сети питания и замените поврежденный элемент или обратитесь к техническому специалисту:

- Кабель питания, удлинитель кабеля или разъем кабеля поврежден.
- Какой-либо предмет попал в устройство.
- Устройство подверглось воздействию воды.
- Устройство упало или оказалось повреждено.
- Устройство работает неправильно, если Вы следуете инструкциям по эксплуатации
- Не размещайте устройство вблизи батарей отопления и источников тепла. Также не загораживайте вентиляционные отверстия.
- Не роняйте пищу и не разливайте жидкости на компоненты устройства и не используйте устройство во влажной среде. Если устройство подверглось воздействию влаги, то обращайтесь к подходящему разделу руководства по устранению неисправностей или к техническому специалисту.
- Не заталкивайте какие-либо предметы в отверстия устройства. Это может стать причиной воспламенения или поражения электротоком от внутренних компонентов.

- Используйте устройство только с протестированным на совместимость оборудованием
- Позвольте устройству охладиться, прежде чем снимать крышку или касаться внутренних компонентов.
- Используйте внешние источники питания только тех типов, которые удовлетворяют указанным на ярлыке устройства характеристикам. Если Вы не уверены в типе источника питания, то обратитесь в сервисный центр или к местной электроэнергетической компании.
- Чтобы избежать повреждения устройства, убедитесь, что переключатель напряжения (если он имеется) источника питания установлен в соответствии с Вашим регионом:
 - 115В/ 60Гц в большинстве стран Северной и Южной Америки и некоторых странах дальнего востока, таких как Корея и Тайвань.
 - 100В/ 50Гц в восточной Японии и 100В/ 60Гц в западной Японии.
 - 230В/ 50Гц в большинстве стран Европы, ближнего и дальнего востока.
- Кроме того, убедитесь, что подключенные устройства электрически совместимы с сетью питания Вашего региона.
- Используйте только утвержденные кабели питания. Если кабель питания не входит в комплект поставки устройства или необходим кабель питания для дополнительных компонентов устройства, то приобретайте кабель, протестированный и утвержденный для работы в Вашей стране. Кабель должен быть совместим с устройством и поддерживать напряжение питания и ток, указанные на ярлыке устройства. Номинальное напряжение и ток кабеля должны быть больше значений, указанных на устройстве.
- Для предотвращения удара электротоком подключайте системный и внешний кабели питания к правильно заземленным розеткам сети питания. Данные кабели комплектуются трехштырьковыми разъемами для правильного заземления. Не используйте разъемы адаптера и не удаляйте заземляющий контакт из кабеля. При необходимости использования удлинителя кабеля используйте 3-проводный кабель с правильно заземленными разъемами.
- Изучите характеристики удлинителя кабеля и силового фильтра. Убедитесь, что суммарный потребляемый ток всех подключенных к удлинителю или силовому фильтру устройств не превышает 80 процентов от максимального тока нагрузки удлинителя или силового фильтра.
- Для защиты устройства от внезапных скачков питания используйте силовой фильтр, линейный выпрямитель или источник бесперебойного питания (UPS).
- Осторожно разместите системные кабели и кабели питания; расположите их так, чтобы они не могли перекрутиться или сцепиться. Никакие предметы не должны лежать на кабелях.
- Не модифицируйте кабели или разъемы. Проконсультируйтесь с инженером-электриком местной электроэнергетической компании по поводу модификации кабеля. Всегда следуйте местным/национальным стандартам электромонтажа.
- При включении или отключении питания источников питания с возможностью «горячей» замены, поставляемых с устройством, следуйте следующим инструкциям:
 - Установите источник питания до подключения к нему кабеля питания.
 - Отключите кабель питания до удаления источника питания.
 - Если устройство имеет несколько источников питания, то отключите кабели питания от *всех* источников питания.
- Транспортируйте устройство осторожно; убедитесь, что все стабилизаторы устойчивости надежно прикреплены к устройству. Избегайте резких остановок и неровностей.



Общие меры предосторожности для монтируемых в стойку устройств

Следуйте следующим мерам предосторожности для надежной и безопасной установки устройства в стойку. Кроме того, обращайтесь к документации по установке в стойку, сопровождающей устройство и стойку, за описанием специфических мер безопасности и процедур установки.

Устройством считается любой компонент, установленный в стойку. Таким образом, «компонентом» является любое устройство, включая различную периферию и сопутствующую аппаратуру.



Осторожно: Установка устройств в стойку без передних и боковых стабилизаторов устойчивости может стать причиной падения стойки и возможных телесных повреждений при определенных обстоятельствах. Поэтому всегда устанавливайте стабилизаторы устойчивости до установки устройств в стойку.

После установки устройств в стойку никогда не вынимайте более одного устройства из стойки по направляющим за один раз. Вес более чем одного увеличенного устройства может стать причиной падения стойки и привести к серьезной травме.

- Перед работой со стойкой убедитесь, что стабилизаторы устойчивости прикреплены к стойке и к полу, и весь вес стойки опирается на пол. Прикрепите передний и боковые стабилизаторы устойчивости к одной стойке или боковые стабилизаторы для объединения нескольких стоек перед началом работы.

Меры предосторожности (продолжение)

- Всегда загружайте стойку снизу вверх, первым устанавливайте самое тяжелое устройство.
- Перед добавлением устройства убедитесь, что стойка находится в устойчивом положении.
- Будьте осторожны, когда нажимаете на защелки для освобождения направляющих устройства, и задвигаете или вынимаете устройство из стойки; направляющие могут зажать пальцы рук.
- Осторожно вставьте устройство полозьями по направляющим и задвиньте устройство в стойку.
- Не перегружайте разветвитель источника питания, обеспечивающий питание всей стойки. Общая нагрузка устройств в стойке не должна превышать 80 процентов от максимальной тока нагрузки разветвителя.
- Убедитесь, что обеспечивается достаточная вентиляция устройств в стойке.
- Не наступайте и не опирайтесь на какое-либо устройство в стойке при обслуживании других устройств.



Примечание: Квалифицированный инженер-электрик должен производить все подключения источников питания и заземления. Все электрические соединения должны выполняться в соответствии с местными или национальными стандартами и правилами.



Осторожно: Никогда не отключайте заземляющий провод и не используйте оборудование при отсутствии заземления. Обратитесь к специалисту по электрооборудованию или инженеру-электрику, если Вы не уверены, что обеспечено необходимое заземление.



Примечание: Шасси устройства должно быть непосредственно заземлено на раму стойки. Не пытайтесь подключить питание устройства до тех пор, пока не будет подключен заземляющий провод. Произведенное подключение питания и заземляющего провода должно быть проверено специалистом по электрооборудованию. Если не выполнено заземление, то возникнет риск поражения электротоком.

Защита от электростатического разряда

Статическое электричество может привести к повреждению чувствительных компонентов. Для предотвращения этого снимите заряд статического электричества с тела прежде, чем прикасаться к электронным компонентам устройства, таким как микропроцессор. Снять заряд можно, периодически прикасаясь к неокрашенной металлической поверхности шасси.

Кроме того, следуйте следующим инструкциям для предотвращения повреждения от электростатического разряда:

1. При распаковке чувствительных к статическому электричеству компонентов из картонной коробки не вынимайте их из антистатического упаковочного материала до тех пор, пока не готовы установить компоненты в устройство. Перед распаковкой чувствительных компонентов непременно снимите заряд статического электричества с тела.
2. При транспортировке чувствительных компонентов вначале поместите их в антистатическую упаковку.
3. Работайте со всеми чувствительными компонентами только в защищенном от статического электричества месте. Если возможно, используйте антистатические поверхности и антистатические материалы.

Раздел 1

Введение

Описание коммутатора

Характеристики

Компоненты передней панели

Описание задней панели

Описание дополнительных модулей

Опции управления

Описание коммутатора

DGS-3324SR – это модульный магистральный коммутатор Gigabit Ethernet, адаптируемый и масштабируемый. Коммутатор предоставляет возможность управления и подключения к магистрали сети стека из двенадцати коммутаторов 3-его уровня DGS-3324SR, объединенных по топологии кольцо. Кроме того, коммутатор может использовать до двадцати четырех портов Gigabit Ethernet в качестве центрального распределительного коммутатора для других коммутаторов или групп коммутаторов или маршрутизаторов. Четыре встроенных комбинированных порта Gigabit допускают как подключение 1000BASE-T, так и SFP.

Характеристики

- Четыре встроенных комбинированных порта 1000BASE-T/SFP
- Объединение в стек до 12 дополнительных коммутаторов DGS-3324SR по топологии кольцо или звезда
- Производительность внутренней магистрали 88 Гбит/с
- Поддержка 802.1D STP и 802.1w Rapid Spanning Tree для создания альтернативных резервных связей между коммутаторами
- Поддержка 802.1Q VLAN, IGMP Snooping, очередей приоритетов 802.1p, агрегирования каналов, зеркалирования портов
- Многоуровневые списки управления доступом ACL (на основе MAC-адресов, IP-адресов, VLAN, типе протокола, приоритета 802.1p, кода DSCP)
- Поддержка функций 3-го уровня, включая множество IP-интерфейсов, конфигурацию ключа MD5, перераспределение маршрутов, настройку статических маршрутов и маршрутов по умолчанию, настройку статической ARP-таблицы, RIP, OSPF, DNS Relay и протокола маршрутизации многоадресных IP-пакетов.
- Настройка качества сервиса QoS (Quality of Service)
- Управление доступом 802.1x (на основе портов) и поддержка клиента RADIUS
- Административно настраиваемая функция Port Security
- Управление полосой пропускания на портах
- Управление потоком IEEE 802.3z и IEEE 802.3x для всех портов Gigabit
- Сетевое управление SNMP v.1, v.2, v.3, поддержка RMON
- Поддержка внешнего резервного источника питания
- Поддержка Web-интерфейса управления.

- Поддержка управления CLI (Command Line Interface, Интерфейс командной строки)
- Поддержка клиента DHCP и BOOTP
- Доступ ко всем функциям настройки “in-band” (по сети) или “out-of-band” через последовательный порт RS-232
- Поддержка удаленного управления через консоль Telnet.
- Обновление ПО посредством TFTP
- Сегментация трафика
- Поддержка журналирования SysLog
- Поддержка протокола Simple Network Time Protocol
- Мониторинг трафика через Web-интерфейсу

Компоненты передней панели

На передней панели коммутатора располагаются индикаторы, порт RS-232 и 4 комбинированных порта SFP (Mini-GBIC).

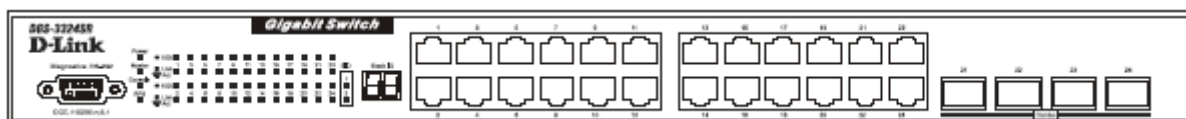


Рисунок 1-1 Вид передней панели коммутатора

Индикаторы показывают информацию о состоянии коммутатора и сети. Консольный порт RS-232 DCE предназначен для настройки и управления коммутатором через соединение с консольным терминалом или ПК, используя программу эмуляции терминала.

Светодиодные индикаторы

Светодиодные индикаторы коммутатора включают индикаторы Power, Master, Console и RPS. Группа из 24 индикаторов (по 2 для каждого порта) показывают состояние связи, активность и скорость работы для каждого порта.

Power	Горит зеленым цветом приблизительно 2 секунды после включения питания коммутатора, показывая готовность устройства к работе.
Master	Горит постоянно зеленым цветом, когда коммутатор работает в качестве мастер-коммутатора стека.
Console	Данный индикатор на передней панели должен гореть в течение выполнения теста по самодиагностике при включении питания Power-On Self Test (POST). Он загорается зеленым цветом при управлении коммутатором через out-of-band/локальную консоль при подключении к порту RS-232 с помощью последовательного кабеля.
RPS	Горит постоянно желтым цветом при работе коммутатора от внешнего источника питания. Это указывает на выход из строя внутреннего источника питания.
1000 Link/Act	Каждый порт Gigabit Ethernet имеет соответствующий индикатор. Постоянно горит зеленым цветом при правильном подключении и мигает при передаче или приеме данных портом.
Stack ID	Коммутатор имеет семисегментный индикатор (помеченный STACK ID), который показывает статус коммутатора в стеке.
SIO	Показывает, какой порт стекирования используется (если используется какой-либо).

Описание задней панели

На задней панели коммутатора располагается разъем питания, разъем для подключения резервного источника питания и два порта стекирования.

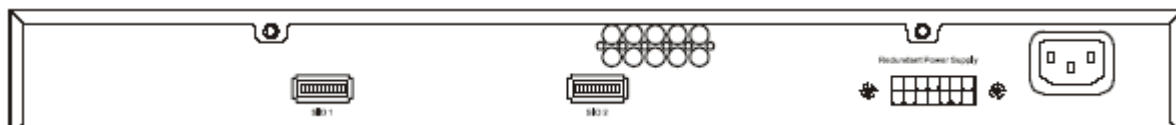


Рисунок 1-2 Вид задней панели коммутатора

Трехштырьковый разъем питания предназначен для подключения шнура питания. Вставьте один конец шнура питания в данный разъем, а другой конец с вилкой – в розетку сети питания. Поддерживается переменное напряжение питания 100-240В частотой 50-60Гц.

Разъем RPS

Внешний резервный источник питания подключается к разъему RPS. Если внутренний источник питания коммутатора выходит из строя, автоматически включается система резервного питания для обеспечения бесперебойной работы коммутатора. Коммутатора поддерживает модули резервного источника питания D-Link RPS-500.

Опции управления

Управление коммутатором осуществляется в терминальном режиме out-of-band через консольный порт, расположенный на передней панели, или по сети in-band с использованием Telnet или Web-браузера.

Web-интерфейс управления

После успешной установки коммутатора можно выполнять его настройку, следить за состоянием индикаторов и просматривать статистику работы коммутатора через любой Web-браузер, такой как Netscape Navigator (версии 6.2 или выше) или Microsoft Internet Explorer (версии 5.0).



Примечание: Для получения доступа к коммутатору через web-браузер компьютер, на котором запущен web-браузер, должен иметь доступ по IP-сети к коммутатору.

Консольный интерфейс командной строки через последовательный порт или Telnet

Также можно подключить компьютер или терминал к последовательному порту или использовать Telnet для доступа к коммутатору. Интерфейс командной строки предоставляет полный доступ ко всем функциям настройки и управления коммутатором. Полный список команд смотрите в *Руководстве по интерфейсу командной строки*, находящемся на CD с документацией.

SNMP-управление

Коммутатором можно управлять при помощи консольной программы с поддержкой SNMP. Коммутатор поддерживает SNMP версии 1.0, версии 2.0 и версии 3.0. SNMP-агент коммутатора декодирует входящие SNMP-сообщения и отвечает на запросы значений объектов MIB, хранящихся в базе данных. SNMP-агент обновляет объекты MIB для генерации статистики и счетчиков. Коммутатор поддерживает широкий набор расширений MIB:

- RFC1213 MIB II

- RFC1493 Bridge
- RFC1643 Ether-like MIB
- RFC1724 RIP 2
- RFC1757 RMON
- RFC1850 OSPF Version 2
- RFC1907 (SNMPv2-MIB)
- RFC2021 (RMON2)
- RFC2096 IP Forwarding
- RFC2233 Interface MIB
- RFC2571 (SNMP Frameworks)
- RFC2572 (Message Processing for SNMP)
- RFC2573 (SNMP Applications)
- RFC2574 (USM for SNMP)
- RFC2575 (VACM for SNMP)
- RFC2576 (Coexistence between SNMPS)
- RFC2618 (Radius-Auth-Client-MIB)
- RFC2620 (Radius-Acc-Client-MIB)
- RFC2932 IPv4 Multicast Routing
- RFC2933 IGMP
- RFC2934 PIM
- DVMRP MIB
- D-Link Enterprise MIB
- 802.1p RFC2674
- IEEE8021-PAE-MIB
- RSTP-MIB

Раздел 2

Установка

Комплект поставки

Перед подключением к сети

Установка коммутатора

Объединение коммутаторов в стек

Комбинированные порты Gigabit

Внешний резервный источник питания

Подключение к консольному порту

Защита паролем

Настройки SNMP

Установка IP-адреса

Подключение устройств к коммутатору

Комплект поставки

Прежде чем устанавливать коммутатор, убедитесь, что в комплект поставки входит следующее:

- Один коммутатор 3-его уровня DGS-3324SR Gigabit Ethernet
- Крепежный комплект: 2 уголка и винты
- Четыре самоклеящиеся резиновые ножки
- Один шнур питания
- Данное Руководство пользователя с регистрационной карточкой
- Руководство по командам CLI
- CD-ROM, содержащий Руководство пользователя и Руководство по командам CLI

Перед подключением к сети



Внимание: Не подключайте коммутатор к сети, не установив предварительно параметры IP коммутатора.

Прежде чем подключать коммутатор к сети, необходимо установить его на ровную поверхность или в стойку, настроить программу эмуляции терминала, подключить шнур питания и затем установить пароль и IP-адрес.

В комплект поставки входят резиновые ножки для крепления коммутатора на ровной поверхности и монтажные уголки и винты для установки коммутатора в стойку.



Внимание: Не подключайте стек коммутаторов к сети до тех пор, пока не настроите все коммутаторы на работу в стеке. Неверно настроенный стек коммутаторов может вызвать широкоэвещательный шторм.

Установка коммутатора

Установка коммутатора на поверхность

1. Установите коммутатор на поверхность, которая может выдержать вес коммутатора и подключенных кабелей. Вокруг коммутатора должно быть достаточно пространства для вентиляции и свободного доступа к разъемам кабелей.
2. Поставьте коммутатор на ровную поверхность и оставьте достаточно пространства для вентиляции – как минимум 5 см с каждой стороны коммутатора и 15 см с задней стороны для кабеля питания.
3. Прикрепите резиновые ножки в помеченных местах внизу коммутатора.
4. Резиновые ножки дополнительные, но рекомендуются для предотвращения скольжения коммутатора.

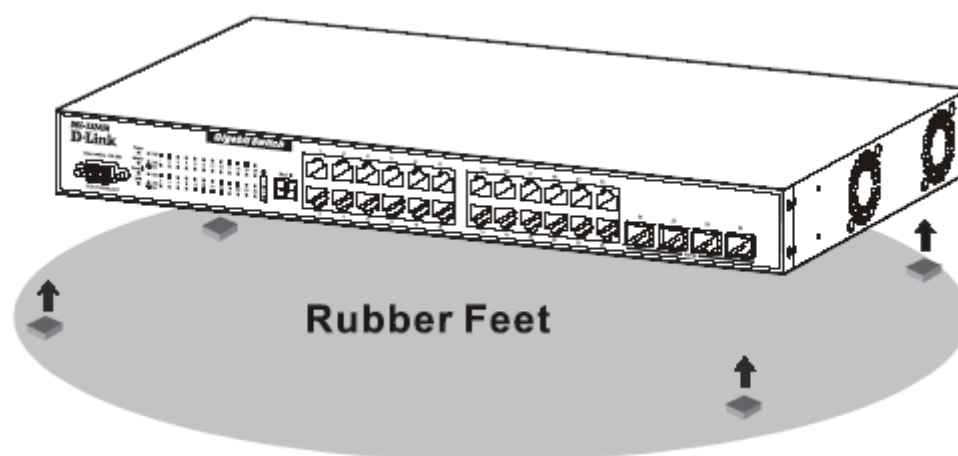


Рисунок 2-1 Крепление резиновых ножек для установки на поверхность

Установка коммутатора в стойку

Вы можете установить коммутатор в стандартную 19-дюймовую (48.3 см) стойку. Обратитесь к следующему рисунку.

1. Используйте прилагаемые винты для крепления монтажных уголков к каждой боковой стороне коммутатора.
2. Выровняйте отверстия в монтажных уголках с отверстиями в стойке.
3. Вставьте и крепко заверните два винта в каждом из уголков.

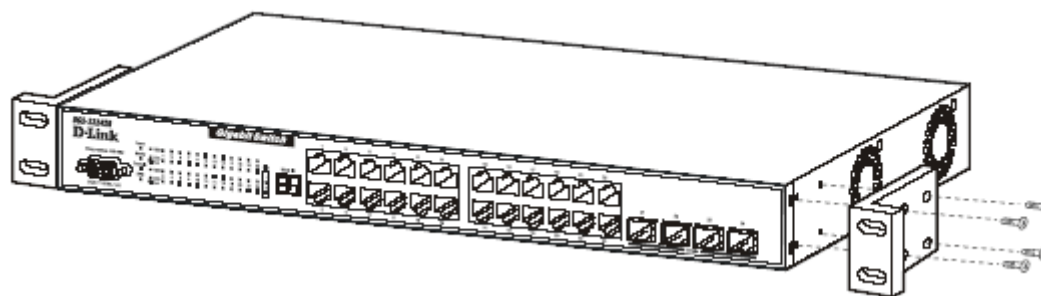


Рисунок 2-2 Крепление монтажных уголков

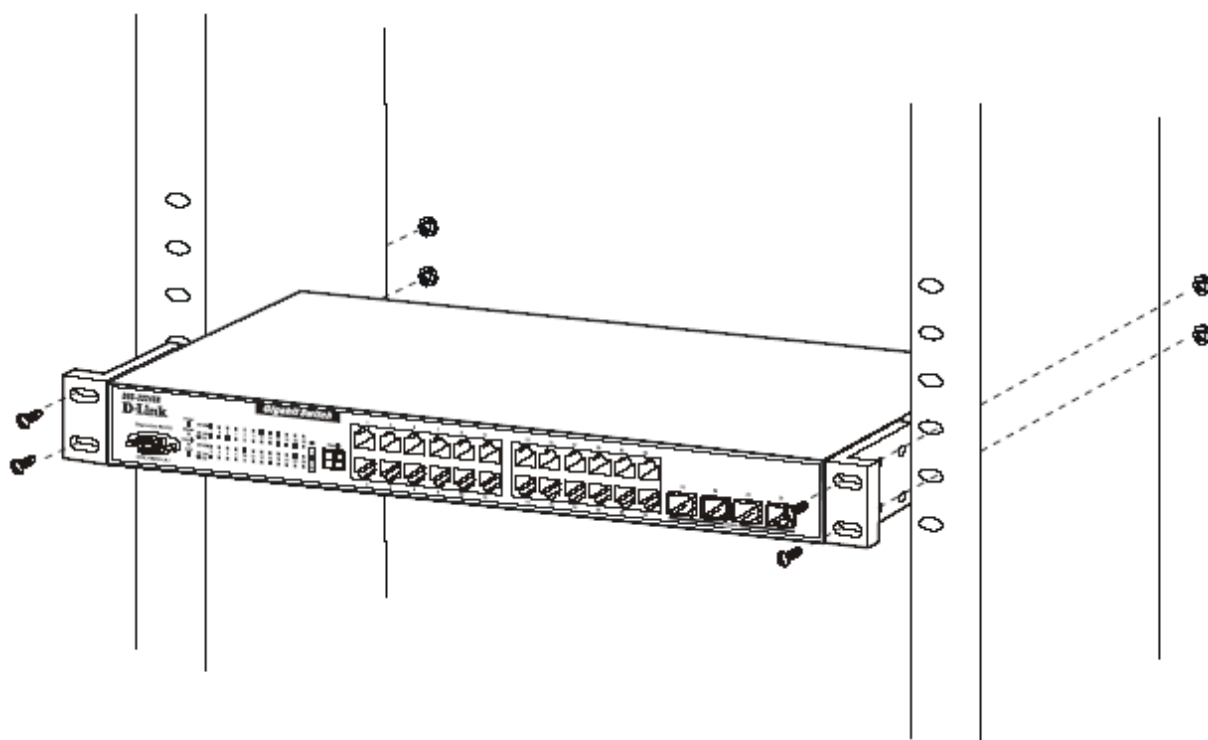


Рисунок 2-3 Установка коммутатора в стойку

Объединение коммутаторов в стек

Можно объединить в стек до 12 коммутаторов по топологии кольцо или звезда с одним мастер-коммутатором или в паре со вторым мастер-коммутатором через второй порт стекирования 10Gig. Пользователи могут добавлять устройства для достижения максимум 288 портов Gigabit Ethernet на стек, созданный по топологии кольцо, или 168 портов Gigabit Ethernet на стек, созданный по топологии звезда. Коммутаторы могут быть объединены в стек посредством высокоскоростных стековых кабелей, обеспечивающих скорость нескольких соединений Gigabit, что позволяет работать всему стеку как единому устройству в IP-сети. Пользователь может видеть количество объединенных в стек устройств на семисегментном индикаторе на передней панели. Пожалуйста, посмотрите на следующий рисунок.

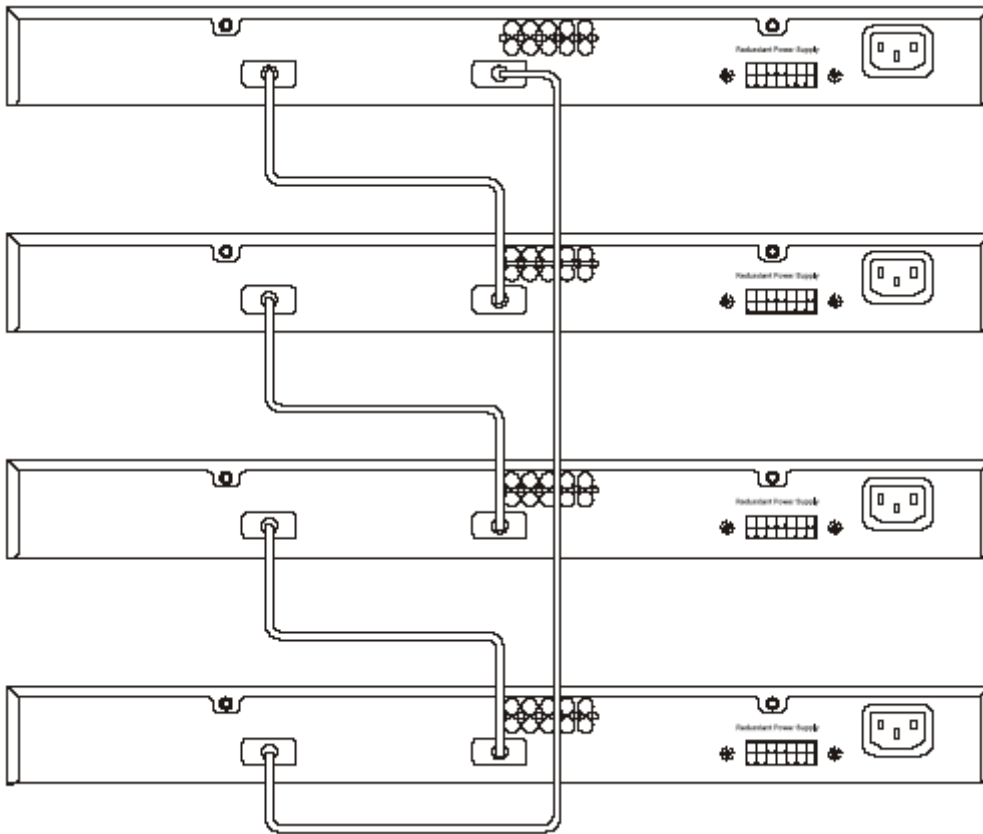


Рисунок 2-4 Топология кольцо (шина)

Пожалуйста, обратите внимание, что необходим DGS-3324Sri для объединения коммутаторов в стек по топологии звезда, как показано ниже.

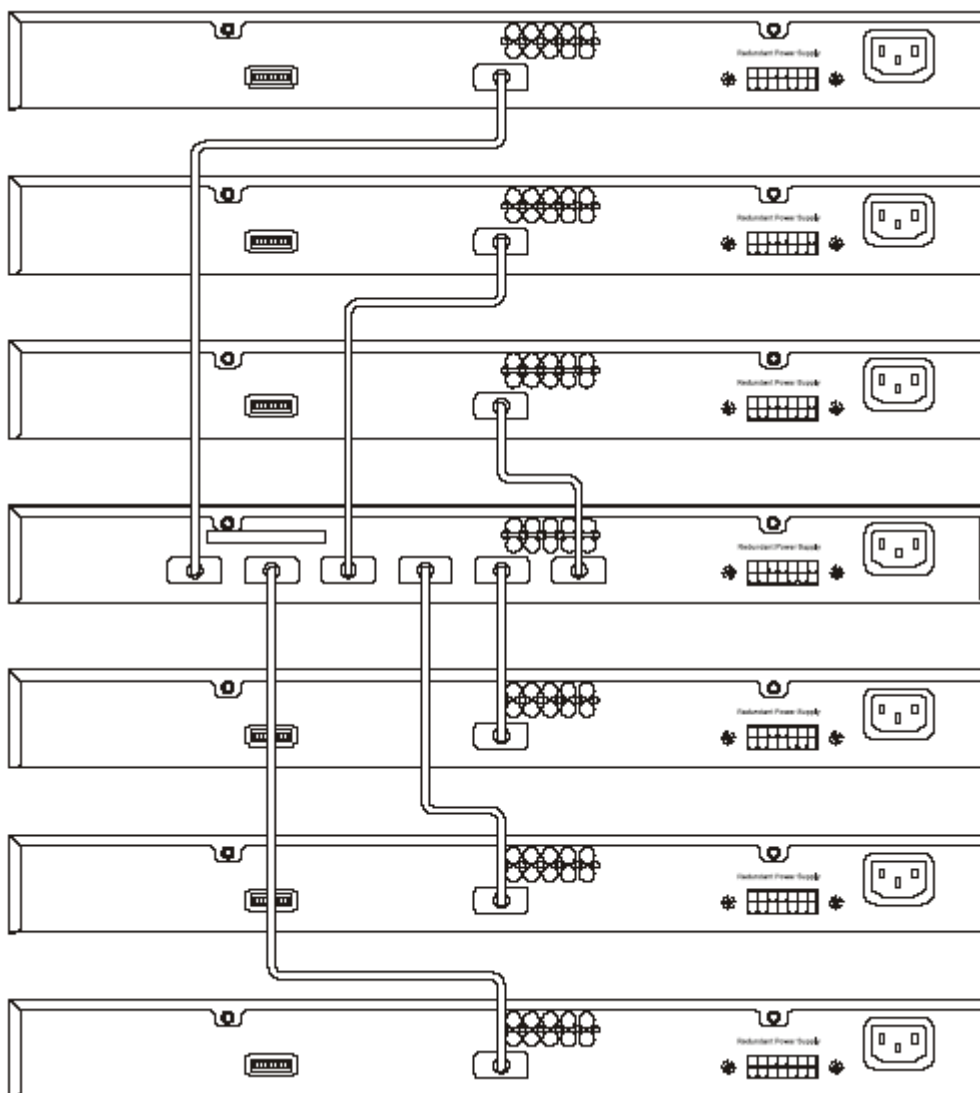


Рисунок 2-5 Объединение коммутаторов в стек по топологии звезда

Порты стекирования обозначены 1 и 2, и при использовании порта стекирования соответствующий ему индикатор (на передней панели) постоянно горит зеленым цветом. Соединение может быть установлено между двумя любыми портами стекирования. Поэтому порт стекирования 1 можно подключить к порту 1 или 2, и порт стекирования 2 можно подключить к порту 2 или 1.

Настройка группы коммутаторов на работу в составе стека

Следуйте приведенным далее инструкциям для настройки DGS-3324SR на работу в качестве мастер-коммутатора, а затем настройте ведомые устройства.

Для настройки DGS-3324SR на работу в составе стека в качестве мастер-коммутатора выполните следующее:

1. Начиная от приглашения командной строки введите **config box_priority current_box_id 1 priority 1** и нажмите Enter. (Коммутатор с наименьшим значением приоритета в стеке является мастер-коммутатором, приоритет со значением 2 выше, чем 5.)
2. Успешное выполнение команды будет подтверждено сообщением **Success**. Для изменения настроек потребуется всего несколько секунд. Смотрите далее пример для DGS-3324SR.
3. Сохраните изменения в настройках, используя команду CLI **save**.

4. Перезагрузите коммутатор.

```
DGS-3324SR:4#config box_priority current_box_id 1 priority 1
Command: config box_priority current_box_id 1 priority 1

Success.

DES-3324SR:4#.....
DES-3324SR:4#
```

Для настройки DGS-3324SR на работу в составе стека в качестве ведомого устройства выполните следующее:

1. Начиная от приглашения командной строки введите **config box_priority current_box_id 1 priority 2** и нажмите Enter.
2. Успешное выполнение команды будет подтверждено сообщением **Success**. Для изменения настроек потребуется всего несколько секунд. Смотрите далее пример для DGS-3324SR.
3. Сохраните изменения в настройках, используя команду CLI **save**.

```
DGS-3324SR:4#config box_priority current_box_id 1 priority 2
Command: config config box_priority current_box_id 1 priority 2

Success.

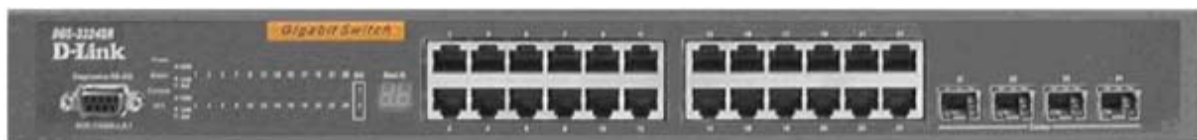
DGS-3324SR:4#.....
```



Примечание: Убедитесь, что все устройства имеют различные идентификаторы. Никакие два устройства не должны иметь одинаковые идентификаторы.

Индикатор порядкового номера устройства в стеке

Семисегментный индикатор **Stack ID** (как показано ниже) на передней панели показывает идентификатор Stack ID коммутатора в составе стека. Пожалуйста, обратите внимание, что индикатор **Master** горит, если коммутатор является мастер-коммутатором стека.



Комбинированные порты Gigabit

Кроме 24 портов 10/100/1000 Мбит/с коммутатор содержит 4 комбинированных порта Mini-GBIC. Данные 4 порта – это медные порты 10/100/1000BASE-T (встроенные) и порты Mini-GBIC (дополнительные). Пожалуйста, обратите внимание, что порты Mini-GBIC используются вместо встроенных портов 10/100/1000BASE-T. Порты Mini-GBIC не будут работать одновременно с соответствующими портами 10/100/1000BASE-T. Например, если порт 24х используется для модуля Mini-GBIC, то порт 24 будет недоступен в качестве встроенного порта 10/100/1000BASE-T, и наоборот.

Внешний резервный источник питания

Коммутатор поддерживает внешний резервный источник питания.

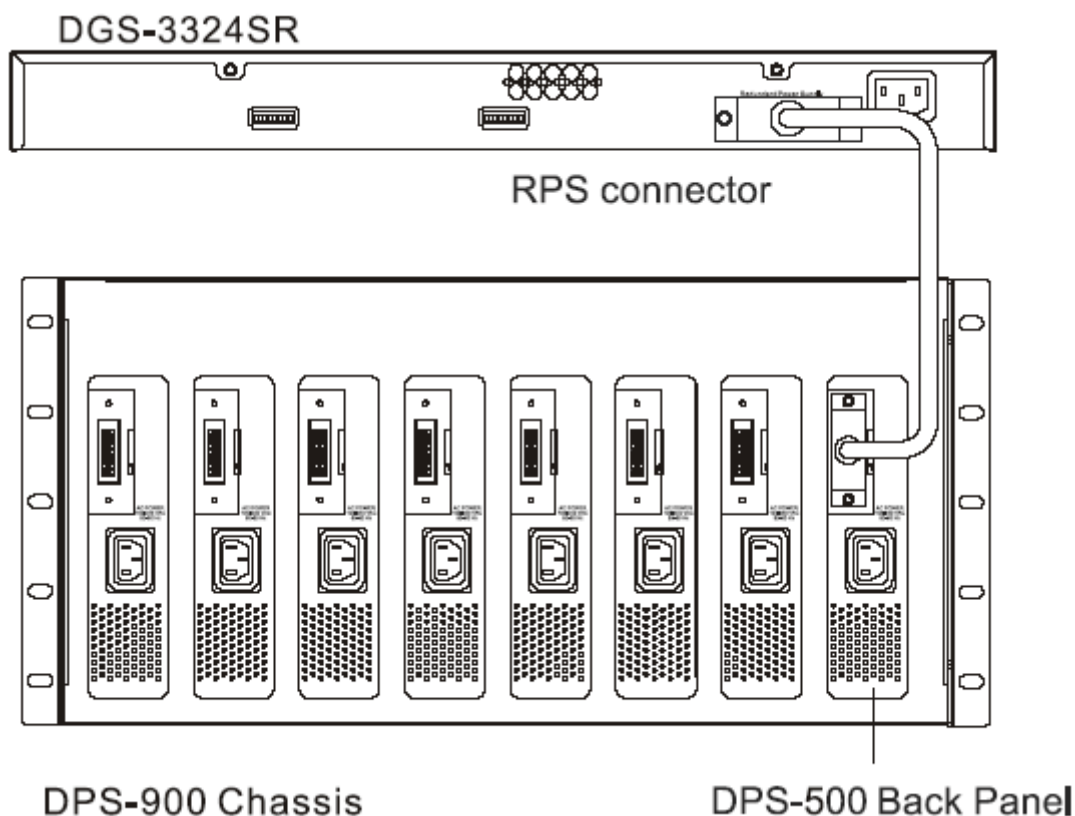


Рисунок 2-6 DPS-900 с DGS-3324SR

Figure 2-6. DPS-900 with DGS-3324SR

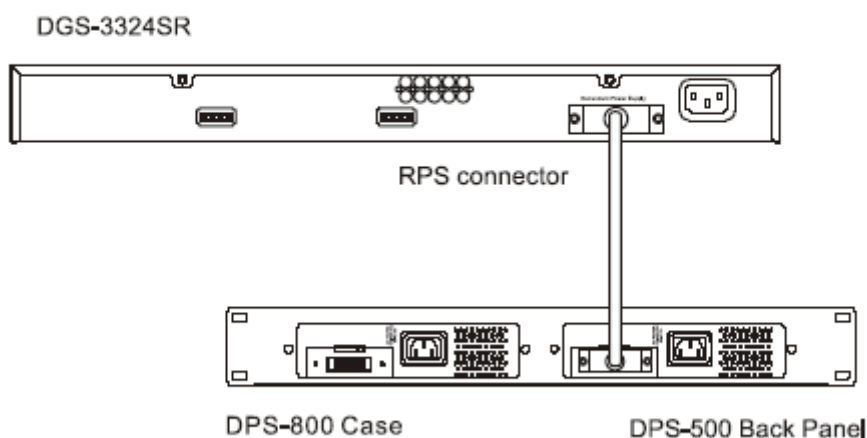


Рисунок 2-7 DPS-800 с DGS-3324SR



Примечание: За дополнительной информацией обращайтесь к документации DPS-900.



Осторожно: Не используйте для коммутатора любой другой резервный источник питания, кроме DPS-900.

Подключение к консольному порту

Коммутатор имеет последовательный порт RS-232, к которому подключается компьютер или терминал для управления и наблюдения за коммутатором. Порт имеет разъем DB-9, обеспечивающий соединение DCE.

Для использования консольного порта необходимо следующее оборудование:

- Терминал или компьютер с последовательным портом и возможностью эмуляции терминала.
- Кабель RS-232 с разъемом DB-9 «мама» для подключения к консольному порту коммутатора.

Для подключения терминала к консольному порту:

1. Подключите кабель RS-232 непосредственно к консольному порту коммутатора и закрепите его винтами.
2. Подключите другой конец кабеля к терминалу или последовательному порту компьютера, на котором работает программа эмуляции терминала. Настройте программу эмуляции терминала следующим образом:
 1. Выберите подходящий последовательный порт (COM-порт 1 или COM-порт 2).
 2. Установите скорость передачи в 115200 бод.
 3. Установите формат данных в 8 бит данных, 1 стоповый бит и без четности.
 4. Отключите управление потоком.
 5. В меню **Свойства** выберите **VT100** в поле **Эмуляция терминала**.

6. Установите опцию **Действие функциональных клавиш, Ctrl и стрелок** в значение **Клавиши терминала**. Убедитесь, что выбрано именно **Клавиши терминала** (а не **Клавиши Windows**).



Внимание: При использовании программы HyperTerminal в Microsoft Windows 2000 убедитесь, что установлен Windows 2000 Service Pack 2 или выше. Windows 2000 Service Pack 2 позволяет использовать клавиши-стрелки при эмуляции VT100 в программе HyperTerminal. За информацией о Windows 2000 Service Pack обращайтесь на сайт www.microsoft.com.

7. После правильной настройки терминала подключите кабель питания к разъему питания на задней панели коммутатора. На экране будет показана последовательность загрузки.
8. По завершении загрузки появится экран регистрации.
9. Если Вы ранее не регистрировались в консольной программе, то нажмите клавишу Enter в полях User Name и Password. По умолчанию имя пользователя (User Name) и пароль (Password) не установлены, поэтому администратор должен предварительно настроить учетные записи пользователей. Если учетные записи настроены, зарегистрируйтесь и продолжите настройку коммутатора.
10. Введите команды, необходимые для выполнения задачи. Многие команды требуют привилегий уровня администратора. За информацией о настройке учетных записей пользователей обращайтесь к следующему разделу. Список всех команд и дополнительная информация об их использовании приведены в *Руководстве по интерфейсу командной строки* на CD с документацией.
11. По окончании процедуры настройки коммутатора завершите сеанс работы командой **logout** или закройте программу эмуляции.

Защита паролем

По умолчанию для DGS-3324SR имя пользователя и пароль не заданы. Одной из первых задач при настройке коммутатора является создание учетных записей пользователей. Если Вы зарегистрировались, используя predetermined имя пользователя с правами администратора, то получите привилегированный доступ к программе управления коммутатором.

После начальной регистрации установите новые пароли для обоих пользователей по умолчанию для предотвращения неавторизованного доступа к коммутатору и запишите пароли на будущее.

Для создания учетной записи с привилегиями администратора выполните следующее:

1. Начиная от приглашения командной строки введите **create account admin** и далее <имя пользователя> и нажмите Enter.
2. Появится запрос на ввод пароля. Введите <пароль> для создаваемой учетной записи администратора и нажмите Enter.
3. Появится запрос на повторный ввод пароля для его подтверждения. Повторите ввод того же пароля и нажмите Enter.
4. При успешном создании новой учетной записи администратора появится сообщение **Success**.



Примечание: Пароль чувствителен к регистру.

Имена пользователей и пароли должны быть длиной до 15 символов.

В приведенном ниже примере показано создание учетной записи с привилегиями администратора и именем пользователя "newmanager".


```
DGS-3324SR:4#create account admin newmanager
Command: create account admin newmanager

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

Success.

DGS-3324SR:4#
```



Внимание: Команды настройки CLI изменяют только текущий конфигурационный файл и сохраняют изменения после перезагрузки коммутатора. Для сохранения изменений в энергонезависимой памяти коммутатора необходимо использовать команду **save** для копирования текущего конфигурационного файла в загрузочный.

Настройки SNMP

Протокол SNMP (Simple Network Management Protocol, Простой протокол сетевого управления) – это протокол уровня 7 модели OSI, используемый для удаленного контроля и настройки сетевых устройств. SNMP позволяет станциям сетевого управления просматривать и изменять настройки шлюзов, маршрутизаторов, коммутаторов и других сетевых устройств. Используйте SNMP для настройки системы, контроля производительности и обнаружения потенциальных проблем в коммутаторе или группе коммутаторов.

Управляемые устройства, поддерживающие SNMP, содержат программу (называемую «агентом»), которая работает локально на коммутаторе. Определенный набор переменных (управляемые объекты) обслуживается SNMP-агентом и используется для управления устройством. Данные объекты определены в MIB (Management Information Base, Информационная база управления), которая обеспечивает стандартное представление информации, управляемой встроенным SNMP-агентом. SNMP определяет формат MIB и протокола, используемого для доступа к данной информации по сети.

DGS-3324SR поддерживает SNMP версии 1, 2с и 3. Можно указать версию SNMP, используемую для управления коммутатором и мониторинга его работы. Три версии SNMP отличаются в обеспечиваемом уровне безопасности между станцией управления и сетевым устройством.

В SNMP v.1 и SNMP v.2 авторизация пользователя выполняется посредством «строки сообщества» - Community String, которая действуют как пароль. Удаленная пользовательская программа SNMP и агент SNMP должны использовать одни и те же Community Strings. Пакеты SNMP от любой станции, которая не была авторизована, игнорируются (отбрасываются).

По умолчанию определены следующие Community Strings, используемые для управления по SNMP v.1 и v.2:

public – позволяет авторизованным станциям управления получать объекты MIB.

private – позволяет авторизованным станциям управления получать и изменять объекты MIB.

SNMP v.3 использует более сложный процесс авторизации, который разделяется на две части. Первая часть используется для поддержания списка пользователей и их атрибутов, которым разрешено управлять по протоколу SNMP. Вторая часть описывает, что каждый пользователь из данного списка может делать при управлении по SNMP.

Коммутатор позволяет указывать и настраивать группы пользователей в данном списке с одинаковым набором привилегий. Для указанных групп может быть установлена версия SNMP. Таким образом, можно создать группу SNMP, которой разрешено просматривать информацию, предназначенную только для чтения, или получать сообщения traps, используя SNMP v.1, в то время как другой группе назначен

более высокий уровень безопасности, предоставляющий привилегии чтения/записи, посредством SNMP v.3.

Используя SNMP v.3 можно позволить или запретить индивидуальным пользователям или группам SNMP-менеджеров выполнять конкретные функции SNMP-управления. Разрешенные или запрещенные функции определяются с помощью идентификатора объекта Object Identifier (OID), ассоциированного с конкретной MIB. Дополнительным уровнем безопасности SNMP v.3 является возможность шифрования SNMP-сообщений. За дополнительной информацией о настройке SNMP v.3 обращайтесь к разделу *Управление*.

Traps

Traps – это сообщения, которые предупреждают о произошедших событиях при работе коммутатора. События могут быть как серьезными типа перезагрузки (кто-то случайно отключил питание коммутатора), так и менее серьезными типа изменения состояния порта. Коммутатор генерирует traps и посылает их станции сетевого управления. Типичными сообщениями traps являются сообщения Authentication Failure, Topology Change, Broadcast/Multicast Storm.

MIB

Управляющая информация и параметры коммутатора хранятся в информационной базе управления (Management Information Base, MIB). Коммутатор использует стандартный модуль информационной базы управления MIB-II. Следовательно, значения входящих в MIB объектов могут быть получены с помощью любых средств сетевого управления, основанных на SNMP. Кроме стандарта MIB-II, коммутатор также поддерживает собственную MIB в виде расширенной информационной базы управления. Объекты этой MIB также могут быть получены путем указания менеджером OID MIB (Object Identifier, идентификатор объекта MIB). Значения объектов MIB могут быть как открытыми только для чтения (read-only), так и для чтения, и для записи (read-write).

Установка IP-адреса

Каждому коммутатору должен быть назначен собственный IP-адрес, который используется для сетевого управления менеджером SNMP или другим TCP/IP приложением (например, BOOTP, TFTP). IP-адрес коммутатора по умолчанию равен 10.90.90.90. Вы можете изменить установленный по умолчанию IP-адрес коммутатора в соответствии со схемой адресации в сети.

При производстве коммутатору также назначается уникальный MAC-адрес. Этот MAC-адрес не может быть изменен, и его можно увидеть на экране консоли при начальной загрузке - как показано ниже.

```
Boot Procedure 1.00-B02
-----
Power On Self Test ..... 100 %
MAC Address : 00-01-02-03-04-00
H/W Version : 1A1
Please wait, loading Runtime image ..... 15 %_
```

Рисунок 2-4 Экран консоли при загрузке

Кроме того, MAC-адрес коммутатора можно посмотреть в меню *Информация о коммутаторе* Web-интерфейса управления.

IP-адрес коммутатора должен быть установлен перед началом управления им по Web-интерфейсу. IP-адрес коммутатора может быть установлен автоматически с помощью протоколов BOOTP или DHCP; в данном случае должен быть известен фактический адрес, назначаемый коммутатору.

IP-адрес можно установить, используя Интерфейс командной строки (CLI) через консольный последовательный порт, следующим образом:

1. Начиная от приглашения командной строки введите команды **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**, где **x** представляет собой IP-адрес, назначаемый IP-интерфейсу по имени **System**, а **y** - соответствующую маску подсети.
2. Кроме того, Вы можете ввести **config ipif System ipaddress xxx.xxx.xxx.xxx/z**, где **x** представляет собой IP-адрес, назначаемый IP-интерфейсу по имени **System**, а **z** - число подсетей в нотации CIDR.

IP-интерфейсу коммутатора **System** можно назначить IP-адрес и маску подсети, которые будут использоваться для подключения станции управления к серверу Telnet коммутатора или агенту управления по Web-интерфейсу.

```
DGS-3324SR:4#config ipif System ipaddress 10.52.19.13/255.0.0.0
Command: config ipif System ipaddress 10.52.19.13/8

Success.

DGS-3324SR:4#_
```

В приведенном выше примере коммутатору назначен IP-адрес 10.52.19.13 и маска подсети 255.0.0.0. Системное сообщение **Success** указывает на успешное выполнение команды. Теперь коммутатором можно управлять по Telnet и CLI или через Web-интерфейс.

Подключение устройств к коммутатору

После назначения IP-адреса к коммутатору можно подключать устройства.

Для подключения устройства к порту трансивера SFP:

1. Используйте требования к кабелю для выбора подходящего типа трансивера SFP.
2. Установите трансивер SFP (продается отдельно) в слот для трансивера SFP.
3. Используйте подходящий сетевой кабель для подключения устройства к разъемам трансивера SFP.



Внимание: Когда трансивер SFP установит соединение, соответствующий встроенный порт 10/100/1000BASE-T отключится.

Раздел 3

Введение в управление коммутатором

Регистрация в Web-менеджере

Пользовательский Web-интерфейс управления

Основная настройка

Информация о коммутаторе

IP-адрес

Учетные записи пользователей

Сохранение настроек

Сброс к заводским установкам

Перезагрузка коммутатора

Введение

Коммутатор DGS-3224SR предоставляет возможность управления через Web-интерфейс, позволяя использовать в качестве станции управления любой компьютер в сети, оснащенный Web-браузером, например, Netscape Navigator/Communicator или Microsoft Internet Explorer. Web-браузер выступает в качестве универсального средства управления и позволяет настраивать коммутатор, используя протокол HTTP.

Web-интерфейс управления и интерфейс консоли (и Telnet) являются разными способами доступа к одним и тем же настройкам коммутатора. Таким образом, все настройки, встречающиеся в Web-интерфейсе, имеются и в интерфейсе консоли.

Регистрация в Web-менеджере

Чтобы начать управление коммутатором, просто запустите установленный на компьютере браузер и введите в строке адреса IP-адрес коммутатора. Введенный URL должен выглядеть примерно так: `http://123.123.123.123`, где числа 123 представляют собой IP-адрес коммутатора.



Примечание: По умолчанию IP-адрес коммутатора равен 10.90.90.90.

В открывшейся странице нажмите кнопку **Login to make a setup**.



Рисунок 3-1 Страница регистрации

Откроется главная страница модуля управления.

Функции управления коммутатором, доступные через web-интерфейс, описаны ниже.



Рисунок 3-2 Окно регистрации

Оставьте поля **User Name** и **Password** пустыми и нажмите ОК. Откроется Web-интерфейс пользователя. Функции управления коммутатором, доступные через web-интерфейс, описаны ниже.

Пользовательский Web-интерфейс управления

Интерфейс пользователя предоставляет доступ к различным страницам настройки и управления коммутатором, позволяет просматривать статистику производительности и визуально контролировать состояние системы.

Области интерфейса пользователя

На приведенном ниже рисунке показан интерфейс пользователя, который делится на 3 области. Их назначение описано в следующей таблице.

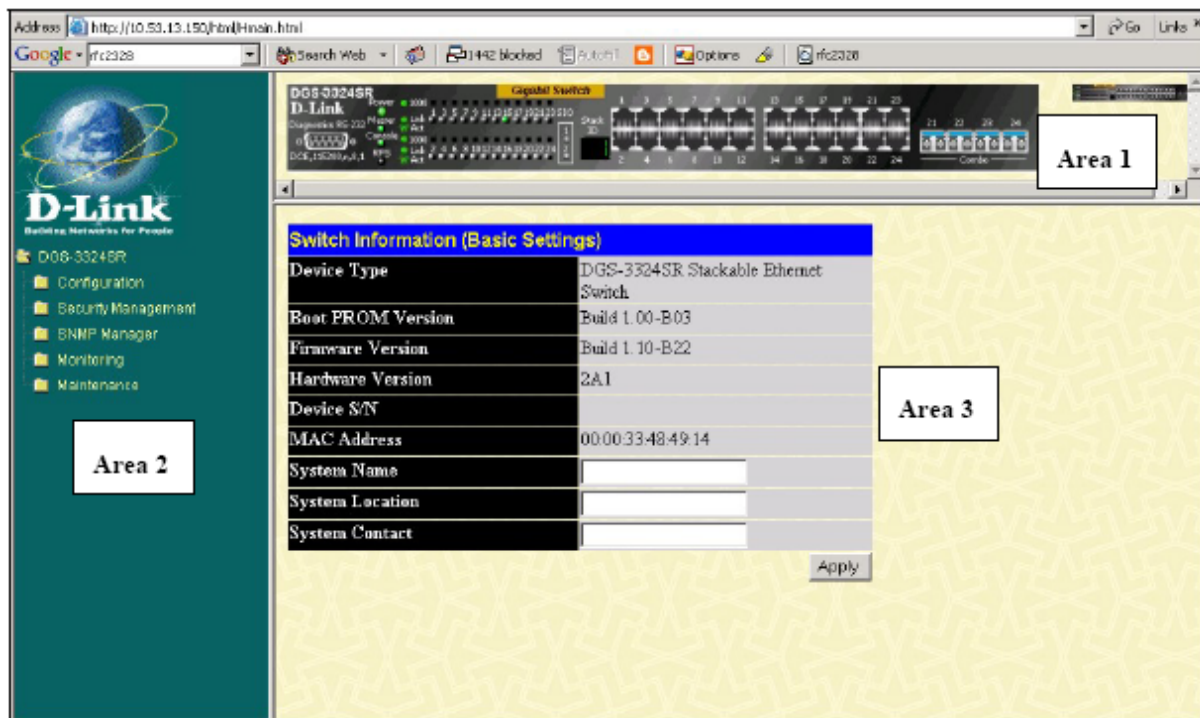


Рисунок 3-3 Главное окно Web-интерфейса управления

Область	Назначение
1	Предоставляет графическое изображение передней панели коммутатора практически в реальном времени. В этой области отображаются порты коммутатора и модули расширения, активность портов, режим дуплекса и управления потоком в зависимости от конкретного режима. Справа от передней панели коммутатора показана текущая конфигурация стека. Для выполнения функций управления можно выделять некоторые области изображения коммутатора, такие как порты, модули расширения, модуль управления или корпус.
2	Содержит папки, вложенные папки и гиперссылки для выбора набора команд и меню. Нажмите на логотип D-Link для перехода на web-сайт D-Link.
3	Показывает выбранную Вами информацию о коммутаторе и поля ввода значений параметров.



Внимание: Все изменения в настройках коммутатора, произведенные в текущем сеансе работы, должны быть сохранены через меню **Save Changes** или командой CLI **save**.

Web-страницы

После подключения к коммутатору через Web-браузер появится экран регистрации. Введите имя пользователя и пароль, чтобы войти в режим управления коммутатором.

Ниже приведен список доступных меню и их описание:

Папка **Configuration**: содержит меню настройки портов, контроля полосы пропускания, агрегирования каналов, зеркалирования портов, настройки VLAN, настройки протокола Spanning Tree, продвижения и фильтрации пакетов, качества сервиса QoS, контроля широковещательной/групповой рассылки, функции IGMP Snooping, настройки статических портов Router Port, сервера SysLog, функции Port Security,

настройки SNTP и таблицы профилей доступа. Кроме того, содержит меню Advanced Settings (Дополнительные настройки), которое используется для настройки последовательного порта, времени жизни MAC-адреса и для включения/отключения следующих функций: RMON, IGMP Snooping, доступа по Telnet и Web-интерфейсу, сегментации трафика и 802.1x. Страница Switch Information (Информация о коммутаторе) используется для ввода контактной информации и расположения коммутатора и содержит основную информацию, такую как MAC-адрес коммутатора, текущая версия ПО коммутатора и установленные модули.

Папка **Security Management**: содержит меню настройки 802.1x, включая информацию о сервере RADIUS и настройку PAE, настройку IP-адресов станций управления.

Папка **SNMP Manager**: содержит меню настройки параметров IP коммутатора, учетных записей пользователей и протокола SNMP, включая настройку SNMP v.3.

Папка **Monitoring**: содержит меню мониторинга производительности коммутатора, таблицу MAC-адресов, портов Router Port, информацию о функции IGMP Snooping и 802.1x.

Папка **Maintenance**: содержит меню для обновления ПО коммутатора, сохранения конфигурационных файлов (сервисы TFTP), сохранения изменений в настройках, сброса к заводским установкам и перезагрузки коммутатора, тестирования с помощью утилиты Ping и выхода из менеджера Web-управления.



Примечание: Убедитесь, что настроено имя пользователя и пароль в меню User Accounts (Учетные записи пользователей), прежде чем подключать коммутатор к большой сети.

Основная настройка

В последующих разделах описываются некоторые основные настройки коммутатора, такие как изменение IP-адреса, создание учетных записей пользователей, сохранение настроек и перезагрузка коммутатора.

Информация о коммутаторе

Нажмите на ссылку **Switch Information** в меню **Configuration**.

Switch Information (Basic Settings)	
Device Type	DGS-3324SR Stackable Ethernet Switch
Boot PROM Version	Build 1.00-B03
Firmware Version	Build 2.00-B19
Hardware Version	2A1
Device S/N	
MAC Address	00:00:33:48:49:14
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Apply	

Рисунок 3-4 Информация о коммутаторе – Основные настройки

Окно **Switch Information** показывает такую информацию, как установленные внешние модули (если есть), MAC-адрес устройства, версию **Boot PROM** и **Firmware**. Эта информация полезна при

обновлении PROM и ПО коммутатора, а MAC-адрес коммутатора может понадобиться для добавления его в адресную таблицу другого сетевого устройства.

Также можно ввести системное имя коммутатора, его расположение и имя и номер телефона администратора сети. Рекомендуется записать здесь контактную информацию для связи с человеком, отвечающим за обслуживание сети, в которой установлен данный коммутатор. После изменения настроек нажмите *Apply*.

Параметры IP коммутатора

Параметры IP коммутатора можно предварительно установить, используя интерфейс консоли, перед подключением через Ethernet. Если IP-адрес коммутатора еще не был изменен, то прочтите параграф *Введение* Руководства по интерфейсу командной строки или перейдите к концу данного раздела, где описано, как использовать консольный порт и команды CLI для настройки IP-адреса коммутатора.

Для изменения IP-адреса коммутатора через Web-интерфейс выберите меню **IP Address** в папке **Configuration**.

Для установки IP-адреса коммутатора:

В папке **Configuration** нажмите на ссылку **IP Address**. Появится меню **Switch IP Settings**.

Switch IP Settings	
Get IP From	Manual
IP Address	10.53.13.188
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
VLAN Name	default
<input type="button" value="Apply"/>	

Рисунок 3-5 Настройка параметров IP коммутатора



Примечание: IP-адрес коммутатора по умолчанию равен 10.90.90.90, маска подсети 255.0.0.0 и шлюз по умолчанию 0.0.0.0.

Для настройки вручную новых значений IP-адреса, маски подсети и шлюза по умолчанию:

- Выберите в меню **Get IP From** значение **Manual**.
- Введите новый IP-адрес и маску подсети.
- Если вы хотите иметь доступ к коммутатору из другой подсети, введите IP-адрес шлюза по умолчанию, в противном случае можно не менять адрес в данном поле.
- Если на коммутаторе не настроены VLAN, то можно использовать настройки по умолчанию – **default VLAN**. В default VLAN входят все порты коммутатора. Если же на коммутаторе настроены VLAN, то необходимо указать ту VLAN, в которую входит порт, к которому подключена станция управления.

Для автоматической настройки IP-адреса, маски подсети и шлюза по умолчанию с помощью протоколов BOOTP/DHCP:

Выберите в меню **Get IP From** значение *BOOTP* или *DHCP*. Это определяет, как будет назначен IP-адрес при следующей перезагрузке коммутатора.

Параметры для настройки:

Параметр	Описание
BOOTP	Коммутатор будет посылать при включении широковещательный запрос BOOTP. Протокол BOOTP позволяет назначать IP-адрес, маску подсети и шлюз по умолчанию через центральный сервер BOOTP. При включении этой опции коммутатор ищет сервер BOOTP, который предоставил бы необходимую информацию, прежде чем использовать заданные ранее настройки.
DHCP	Коммутатор будет посылать при включении широковещательный запрос DHCP. Протокол DHCP позволяет назначать IP-адрес, маску подсети и шлюз по умолчанию через центральный сервер DHCP. При включении этой опции коммутатор ищет сервер DHCP, который предоставил бы необходимую информацию, прежде чем использовать заданные ранее настройки.
Manual	Позволяет вручную задать IP-адрес, маску подсети и шлюз по умолчанию коммутатора. Эти значения должны быть введены в виде xxx.xxx.xxx.xxx, где каждое xxx - это десятичное число от 0 до 255. Этот адрес должен быть уникальным в сети и используется администратором сети. При выборе этой опции требуется ввести следующие значения:
Subnet Mask	Битовая маска, определяющая размер подсети, в которой находится коммутатор. Должна быть введена в виде xxx.xxx.xxx.xxx, где каждое xxx - это десятичное число от 0 до 255, и должна равняться 255.0.0.0 для сетей класса А, 255.255.0.0 для сетей класса В, 255.255.255.0 для сетей класса С, но допускается введение и произвольной маски.
Default Gateway	IP-адрес, определяющий, куда будут направляться пакеты с адресом назначения, находящимся вне данной подсети. Обычно это адрес маршрутизатора или компьютера, работающего в качестве IP-шлюза. Если Ваша сеть не является частью составной сети, или Вы не хотите иметь доступ к коммутатору из другой сети, то оставьте данное поле без изменений.
VLAN Name	В данное поле можно ввести имя VLAN, из которой станции управления будет позволено управлять коммутатором по протоколам стека TCP/IP (через web-интерфейс или Telnet). Станции управления, находящиеся в VLAN, отличных от введенной в поле VLAN Name, не будут иметь возможность управлять коммутатором по сети до тех пор, пока их IP-адреса не будут введены в меню Security IP Management. VLAN по умолчанию имеет имя default и включает в себя все порты коммутатора. По умолчанию в таблице Security IP Management нет ни одной записи, поэтому любая станция управления имеет доступ к коммутатору.

Установка IP-адреса коммутатора через интерфейс консоли

Каждому коммутатору должен быть назначен собственный IP-адрес, который используется для сетевого управления менеджером SNMP или другим TCP/IP приложением (например, BOOTP, TFTP). IP-адрес коммутатора по умолчанию равен 10.90.90.90. Вы можете изменить установленный по умолчанию IP-адрес коммутатора в соответствии со схемой адресации в сети.

IP-адрес коммутатора должен быть установлен перед началом управления им по Web-интерфейсу. IP-адрес коммутатора может быть установлен автоматически с помощью протоколов BOOTP или DHCP; в данном случае должен быть известен фактический адрес, назначаемый коммутатору.

IP-адрес можно установить, используя Интерфейс командной строки (CLI) через консольный последовательный порт, следующим образом:

Начиная от приглашения командной строки введите команды **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**, где **x** представляет собой IP-адрес, назначаемый IP-интерфейсу по имени **System**, а **y** - соответствующую маску подсети.

Кроме того, Вы можете ввести **config ipif System ipaddress xxx.xxx.xxx.xxx/z**, где **x** представляет собой IP-адрес, назначаемый IP-интерфейсу по имени **System**, а **z** - число подсетей в нотации CIDR.

IP-интерфейсе коммутатора **System** можно назначить IP-адрес и маску подсети, которые будут использоваться для подключения станции управления к серверу Telnet коммутатора или агенту управления по Web-интерфейсу.

Системное сообщение **Success** указывает на успешное выполнение команды. Теперь коммутатором можно управлять по Telnet и CLI или через Web-интерфейс, используя для подключения к коммутатору введенный выше IP-адрес.

Задание IP-адресов станций управления

В папке **Security Management** нажмите на ссылку **Security IP**, появится следующее окно.

Security IP Management	
IP1 Access to Switch	<input type="text" value="0.0.0.0"/>
IP2 Access to Switch	<input type="text" value="0.0.0.0"/>
IP3 Access to Switch	<input type="text" value="0.0.0.0"/>
IP4 Access to Switch	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/>	
<p>Note : Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.</p>	

Рисунок 3-6 Задание IP-адресов станций управления

Станциями управления являются определенные компьютеры в сети, которые используются для управления коммутатором. Можно ограничить число возможных станций управления указанием максимум 3 IP-адресов. Если все три поля содержат все нули ('0'), то любая станция управления с любым IP-адресом может получить доступ к коммутатору для управления и настройки. Если введен один или более IP-адресов, то только станции управления с данными IP-адресами смогут получить доступ к коммутатору для управления и настройки. После установки IP-адресов нажмите кнопку *Apply*.

Управление учетными записями пользователей

Используйте таблицу учетных записей для управления привилегиями пользователей. Для просмотра текущих учетных записей в папке **Security Management** нажмите на ссылку **User Accounts**. Появится окно **User Account Management**.

User Account Management		
User Name	Access Right	Add
Trinity	Admin	Modify

Рисунок 3-7 Таблица учетных записей пользователей

Для добавления нового пользователя нажмите кнопку *Add*. Для изменения или удаления текущей записи нажмите кнопку *Modify*.

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

Рисунок 3-8 Добавление новой учетной записи

Введите имя пользователя в поле **User Name**, пароль в поле **New Password** и повторите ввод пароля в поле **Confirm New Password**. Выберите уровень привилегий (**Admin** или **User**) из выпадающего меню **Access Right**. Для добавления нового пользователя через интерфейс CLI используйте команды **create account** и **config account**.

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

Рисунок 3-9 Изменение учетной записи пользователя

Для удаления учетной записи пользователя нажмите кнопку *Delete*. Для изменения пароля введите новый пароль в поле **New Password** и повторите его ввод в поле **Confirm New Password**. Выберите уровень привилегий (**Admin** или **User**) из выпадающего меню **Access Right**. Для удаления учетной записи через

интерфейс CLI используйте команду **delete account**. Для изменения существующей учетной записи используйте команду **config account**.

Привилегии Admin и User

Существует два уровня привилегий: **Admin** и **User**. Некоторые настройки и пункты меню, доступные пользователю с привилегиями **Admin**, недоступны пользователю с привилегиями **User**.

Следующая таблица описывает привилегии **Admin** и **User**.

Функции управления	Admin	User
Настройка коммутатора	Да	Только просмотр
Мониторинг сети -Network Monitoring	Да	Только просмотр
Community String и Trap Stations	Да	Только просмотр
Обновление ПО коммутатора и файла конфигурации	Да	Нет
Системные утилиты -System Utilities	Да	Только Ping – тест
Сброс к заводским установкам - Factory Reset	Да	Нет
Учетные записи пользователей		
Добавление/Изменение/Удаление учетной записи пользователя	Да	Нет
Просмотр учетных записей пользователей	Да	Нет

Привилегии Admin и User

После создания учетной записи пользователя с привилегиями **Admin** не забудьте сохранить настройки (смотрите далее).

Сохранение настроек

Произведенные изменения в настройках коммутатора необходимо сохранить. В папке **Maintenance** нажмите на ссылку **Save Changes**, появится окно **Save Configuration**.

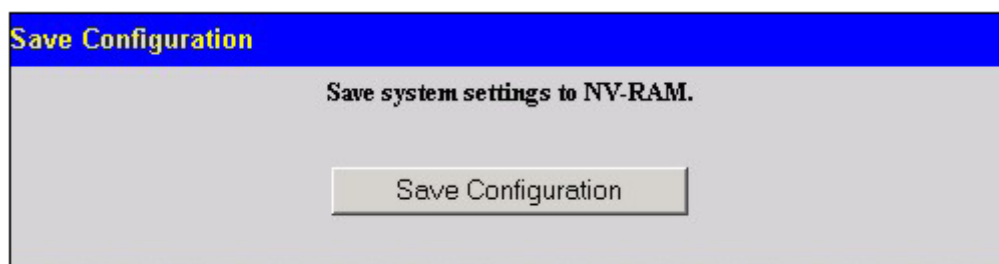


Рисунок 3-10 Окно Save Configuration

Коммутатор имеет два уровня памяти: обычное ОЗУ (RAM) и постоянную память, или NV-RAM. Для сохранения всех настроек, выполненных в течение текущего сеанса работы, во флэш-память коммутатора нажмите кнопку **Save Configuration**. В следующем появившемся окне нажмите кнопку **ОК**. После этого изменения немедленно применятся к ПО коммутатора, загруженному в ОЗУ, и немедленно вступят в силу. Как только настройки сохранены в NV-RAM, они становятся настройками коммутатора по умолчанию, и будут использоваться каждый раз, когда коммутатор перезагружается.

Однако для вступления в силу некоторых изменений в настройках коммутатора требуется перезагрузка. При перезагрузке все настройки в ОЗУ стираются и загружаются последние сохраненные в NV-RAM настройки. Таким образом, необходимо сохранять настройки коммутатора в NV-RAM.

Для сохранения настроек через интерфейс CLI используйте команду **save**.

Сброс к заводским установкам

В папке **Maintenance** нажмите на ссылку **Reset**, появится следующее меню.

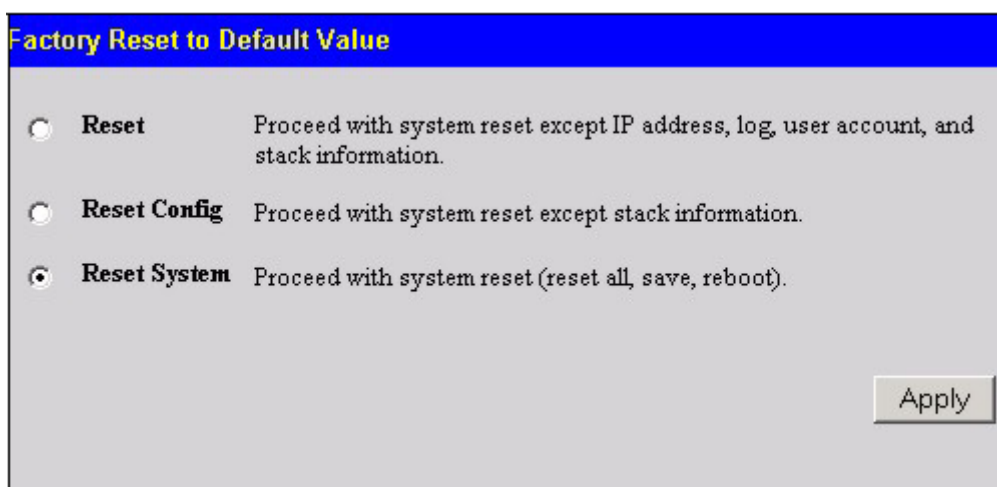


Рисунок 3-11 Меню Factory Reset To Default Value

Reset - сброс всех настроек к заводским установкам по умолчанию, кроме IP-адреса коммутатора, маски подсети, шлюза по умолчанию, журнала событий, учетных записей пользователей и параметров стекирования.

Reset Config - сброс всех настроек к заводским установкам по умолчанию, кроме параметров стекирования, но без их сохранения и перезагрузки коммутатора. Если сброс был выполнен с этой опцией, то заводские установки будут восстановлены только на текущий сеанс работы. После перезагрузки коммутатор вернется к последней сохраненной в NV-RAM конфигурации.

Reset System – сброс всех настроек к заводским установкам по умолчанию и сохранение их в NV-RAM коммутатора. Затем коммутатор будет перезагружен. После перезагрузки будет восстановлена конфигурация коммутатора, установленная на заводе.

Перезагрузка коммутатора

В папке **Maintenance** нажмите на ссылку **Reboot Device**, появится следующее меню.

Нажмите **Yes** после **Do you want to save the settings?** для того, чтобы коммутатор сохранил текущие настройки в NV-RAM перед перезагрузкой.

Нажмите **No**, если не хотите, чтобы коммутатор сохранял текущие настройки в NV-RAM перед перезагрузкой. Все изменения в настройках, произведенные с момента последнего исполнения команды **Save Changes**, будут потеряны.

Нажмите кнопку **Restart** для перезагрузки коммутатора.

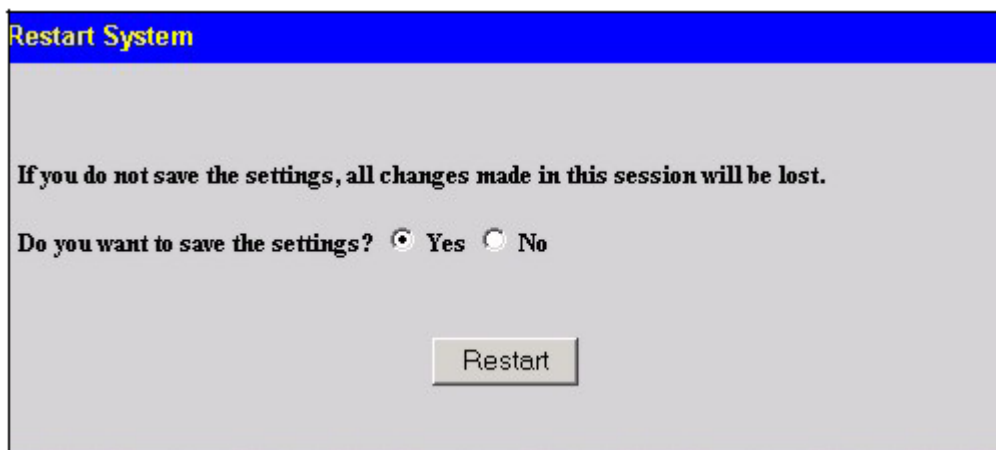


Рисунок 3-12 Меню перезагрузки коммутатора



Примечание: Выбор опции **Yes** эквивалентен выполнению команды **Save Changes** и перезагрузке коммутатора.

Информация о коммутаторе

Сразу после регистрации в системе управления появляется окно с информацией о коммутаторе **Switch Information (Basics Settings)**. К нему также можно получить доступ по ссылке **Switch Information** в меню **Configuration**.

Switch Information (Basic Settings)	
Device Type	DGS-3324SR Stackable Ethernet Switch
Boot PROM Version	Build 1.00-B03
Firmware Version	Build 2.00-B19
Hardware Version	2A1
Device S/N	
MAC Address	00:00:33:48:49:14
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Apply	

Рисунок 3-12 Информация о коммутаторе

Окно **Switch Information** показывает такую информацию, как установленные внешние модули (если есть), **MAC-адрес** устройства, версию **Boot PROM** и **Firmware**. Эта информация полезна при обновлении PROM и ПО коммутатора, а MAC-адрес коммутатора может понадобиться для добавлении его в адресную таблицу другого сетевого устройства.

Также можно ввести системное имя коммутатора, его расположение и имя и номер телефона администратора сети. Рекомендуется записать здесь контактную информацию для связи с человеком,

отвечающим за обслуживание сети, в которой установлен данный коммутатор. После изменения настроек нажмите *Apply*.

Кроме того, информацию о коммутаторе можно посмотреть через Telnet, используя команду CLI **show switch**.

Дополнительные настройки

Меню **Advanced Settings** позволяет настроить основные функции коммутатора. Для доступа к меню **Advanced Settings** нажмите на ссылку **Advanced Settings** в папке **Configuration**.

Switch Information (Advanced Settings)	
Serial Port Auto Logout	10 Minutes ▾
Serial Port Baud Rate	115200 ▾
MAC Address Aging Time (10-1000000)	300
IGMP Snooping	Disabled ▾
Multicast router Only	Disabled ▾
GVRP Status	Disabled ▾
Telnet Status	Enabled ▾
Web Status	Enabled ▾
RMON Status	Disabled ▾
Link Aggregation Algorithm	MAC Source ▾
Switch 802.1x	Disabled ▾
Auth Protocol	Radius Eap ▾
HOL Prevention	Enabled ▾
Jumbo Frame	Disabled ▾
Syslog state	Disabled ▾
Apply	

Рисунок 3-14 Информация о коммутаторе – дополнительные настройки

Опции меню **Advanced Settings** описаны в следующей таблице.

Параметр	Описание
Serial Port Auto Logout	Таймер автоматического выхода из интерфейса консоли. По истечении выбранного периода времени при отсутствии действий со стороны пользователя сеанс связи завершается автоматически. Возможные значения <i>2 Minutes.</i> , <i>5 Minutes.</i> , <i>10 Minutes.</i> , <i>15 Minutes.</i> или <i>Never (Никогда)</i> .
Serial Port Baud Rate	Фиксированное значение 115 200 бод.
MAC Address Aging Time	Данный параметр определяет время хранения MAC-адреса, изученного коммутатором, в таблице MAC-адресов при отсутствии обращений к нему. По умолчанию время жизни MAC-адреса равно 300 секунд. Оно может принимать значения от 10 до 1,000,000 секунд.

IGMP Snooping	Для активизации функции IGMP Snooping на коммутаторе выберите <i>Enabled</i> . По умолчанию функция IGMP Snooping отключена (<i>Disabled</i>). Активизация IGMP Snooping позволит определить выбрать опцию Multicast Router Only .
Multicast Router Only	Если выбрано <i>Enabled</i> и активизирована функция IGMP Snooping, то коммутатор будет передавать весь трафик групповой рассылки только на маршрутизатор многоадресной рассылки. В противном случае, коммутатор будет передавать весь групповой трафик на любой IP-маршрутизатор.
GVRP Status	Можно включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) GVRP на коммутаторе.
Telnet Status	По умолчанию разрешен (<i>Enabled</i>) доступ к коммутатору посредством Telnet. Для отключения этой возможности выберите <i>Disabled</i> .
Web Status	По умолчанию разрешено (<i>Enabled</i>) управление коммутатором на основе Web-интерфейса. Для отключения этой возможности выберите <i>Disabled</i> .
RMON Status	Можно включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) возможность удаленного мониторинга RMON коммутатора.
Link Aggregation Algorithm	Алгоритм, который использует коммутатор для балансировки нагрузки между портами в транковой группе. Доступны опции <i>MAC Source (no MAC-адресу источника)</i> , <i>MAC Destination (no MAC-адресу назначения)</i> , <i>MAC Src & Dest (no обоим MAC-адресам)</i> , <i>IP Source (no IP-адресу источника)</i> , <i>IP Destination (no IP-адресу назначения)</i> и <i>IP Src & Dest (no обоим IP-адресам)</i> . (смотрите раздел <i>Агрегирование каналов</i>)
Switch 802.1x	Можно включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) 802.1x на коммутаторе.
Auth Protocol	Доступны опции <i>Local</i> и <i>Radius Eap</i> .
HOL Prevention	Можно включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) HOL prevention на коммутаторе.
Jumbo Frame	Можно разрешить (<i>Enabled</i>) или запретить (<i>Disabled</i>) прием сверхбольших кадров Ethernet коммутатором.
Syslog State	Можно включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) ведение журнала на сервере Syslog.

Настройка

Раздел 4

- Настройка идентификатора коммутатора*
- Настройка портов*
- Настройка зеркалирования портов*
- Настройка агрегирования каналов*
- Настройка протокола IGMP*
- Настройка протокола Spanning Tree*
- Настройка продвижения и фильтрации пакетов*
- Настройка VLAN*
- Управление трафиком*
- Настройка функции Port Security*
- Настройка качества сервиса QoS*
- Сервер System Log*
- Настройка параметров SNMP*
- Настройка таблицы профилей доступа*
- Управление доступом*
- Сетевое взаимодействие на 3-ем уровне*

Настройка идентификатора коммутатора

В папке **Configuration** нажмите на ссылку **Box Information**, появится меню **Box Information Configuration**. Оно используется для настройки мастер-коммутатора стека коммутаторов. Мастер-коммутатор используется для настройки всего стека коммутаторов.

Рисунок 4-1 Меню Box Information Configuration

Параметры для настройки:

Параметр	Описание
Current Box ID	Текущий идентификатор Box ID мастер-коммутатора стека.
New Box ID	Новый идентификатор Box ID мастер-коммутатора стека.
Box Type	Позволяет выбрать модель мастер-коммутатора стека.
Priority	Показывает приоритет коммутатора. Меньшее значение означает больший приоритет. Коммутатор с наименьшим значением приоритета является мастер-коммутатором.

Настроенные параметры можно посмотреть в меню **Stack Information** в папке **Monitoring**.

Настройка портов

Данный раздел содержит информацию о настройке различных атрибутов и свойств физических портов коммутатора, включая скорость работы порта и управление потоком. Нажмите на ссылку **Port Configurations** в меню **Configuration**, появится следующее окно.

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

The Port Information Table						
Port	State	Speed/Duplex	Flow Control	Connection	Learning	
1	Enabled	Auto	Disabled	Link Down	Enabled	
2	Enabled	Auto	Disabled	Link Down	Enabled	
3	Enabled	Auto	Disabled	Link Down	Enabled	
4	Enabled	Auto	Disabled	Link Down	Enabled	
5	Enabled	Auto	Disabled	Link Down	Enabled	
6	Enabled	Auto	Disabled	Link Down	Enabled	
7	Enabled	Auto	Disabled	Link Down	Enabled	
8	Enabled	Auto	Disabled	Link Down	Enabled	
9	Enabled	Auto	Disabled	Link Down	Enabled	
10	Enabled	Auto	Disabled	Link Down	Enabled	
11	Enabled	Auto	Disabled	Link Down	Enabled	
12	Enabled	Auto	Disabled	Link Down	Enabled	
13	Enabled	Auto	Disabled	Link Down	Enabled	
14	Enabled	Auto	Disabled	Link Down	Enabled	
15	Enabled	Auto	Disabled	Link Down	Enabled	
16	Enabled	Auto	Disabled	Link Down	Enabled	
17	Enabled	Auto	Disabled	Link Down	Enabled	
18	Enabled	Auto	Disabled	Link Down	Enabled	
19	Enabled	Auto	Disabled	Link Down	Enabled	
20	Enabled	Auto	Disabled	Link Down	Enabled	
21	Enabled	Auto	Disabled	Link Down	Enabled	
22	Enabled	Auto	Disabled	Link Down	Enabled	
23	Enabled	Auto	Disabled	1000M/Full/None	Enabled	
24	Enabled	Auto	Disabled	Link Down	Enabled	

Рисунок 4-2 Меню настройки портов

Для настройки портов коммутатора:

1. Выберите коммутатор из выпадающего меню **Unit**.
2. Выберите порт или диапазон последовательных портов из выпадающих меню **From ... To ...**.
3. Используйте соответствующие меню для настройки следующих параметров:

Параметр	Описание
State <Enabled>	Используйте поле State , чтобы заблокировать (<i>Disabled</i>) или разблокировать (<i>Enabled</i>) данный порт

Speed/Duplex<Auto> Используйте поле **Speed/Duplex**, чтобы выбрать скорость и полу- или полнодуплексный режим работы порта. Режим *Auto* разрешает автосогласование устройствами скорости работы между 10 и 1000 Мбит/с, полу- или полнодуплексного режима; данный режим позволяет порту коммутатора автоматически определить наиболее эффективные параметры взаимодействия с подключенным к нему устройством. Остальные опции *10M/Full*, *10M/Half*, *100M/Full*, *100M/Half*, *1000M/Full_M* (Master) и *1000M Full_S* (Slave) точно определяют режим работы порта коммутатора.

Flow Control Показывает используемый метод управления потоком для различных настроек порта. При работе в полнодуплексном режиме используется управление потоком 802.3х, в полудуплексном режиме - метод обратного давления *backpressure*; в режиме *Auto* порт автоматически выбирает из данных двух методов необходимый. По умолчанию управление потоком отключено (*Disabled*).

Learning Позволяет для выбранного порта (или портов) заблокировать динамическое изучение MAC-адресов так, что новые MAC-адреса источников не будут добавляться в адресную таблицу заблокированного порта. Блокировку можно установить/снять выбором опции *Disabled/Enabled*. Используется в целях безопасности или повышения эффективности. Обращайтесь к разделу **Продвижение и фильтрация пакетов** за информацией о том, как внести MAC-адреса в адресную таблицу коммутатора.

Нажмите *Apply*, чтобы изменения вступили в силу.

Настройка зеркалирования портов

Коммутатор позволяет перенаправлять копии принятых и отправленных портом кадров на другой порт. Можно подключить устройство мониторинга к зеркалирующему порту, такое как Sniffer или RMON, для просмотра информации о проходящих через зеркалируемый порт пакетах. Это используется при сетевом мониторинге и с целью устранения проблем. В папке **Configuration** нажмите на ссылку **Port Mirroring**, появится меню зеркалирования портов **Setup Port Mirroring**.

Setup Port Mirroring

Target Port Unit: 1 Port: Port1

Status Disabled

Source Port

Port Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ingress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Both	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply

Note(1): The "Source Port" and "Target Port" should be different, or the setup will be invalid.

Note(2): The target port should be a non-trunked port.

Рисунок 4-3 Меню Setup Port Mirroring

Для настройки зеркалирования портов:

1. Выберите порт – источник кадров - в поле **Source Port**, и порт назначения в поле **Target Port**, который будет принимать копии пакетов от источника.
2. Выберите тип перенаправляемых пакетов – **Ingress** (входящие), **Egress** (исходящие) или **Both** (оба типа пакетов) и из выпадающего меню **Status** выберите **Enabled**.
3. Нажмите *Apply*, чтобы изменения вступили в силу.



Примечание: Более быстрый порт нельзя зеркалировать на медленный, например, порт 100 Мбит/с нельзя зеркалировать на порт 10 Мбит/с, так как много пакетов будет просто отбрасываться. Зеркалирование невозможно при использовании одного порта как в качестве источника, так и в качестве порта назначения. Кроме того, порт назначения не может входить в состав транковой группы.

Настройка агрегирования каналов

Понятие транковой группы портов

Агрегирование каналов, или транкинг портов, позволяет объединить несколько портов в один высокоскоростной канал связи.

DGS-3324SR поддерживает до 32 транковых групп портов, от 2 до 8 портов в каждой. Теоретически может быть достигнута пропускная способность в 8000 Мбит/с.

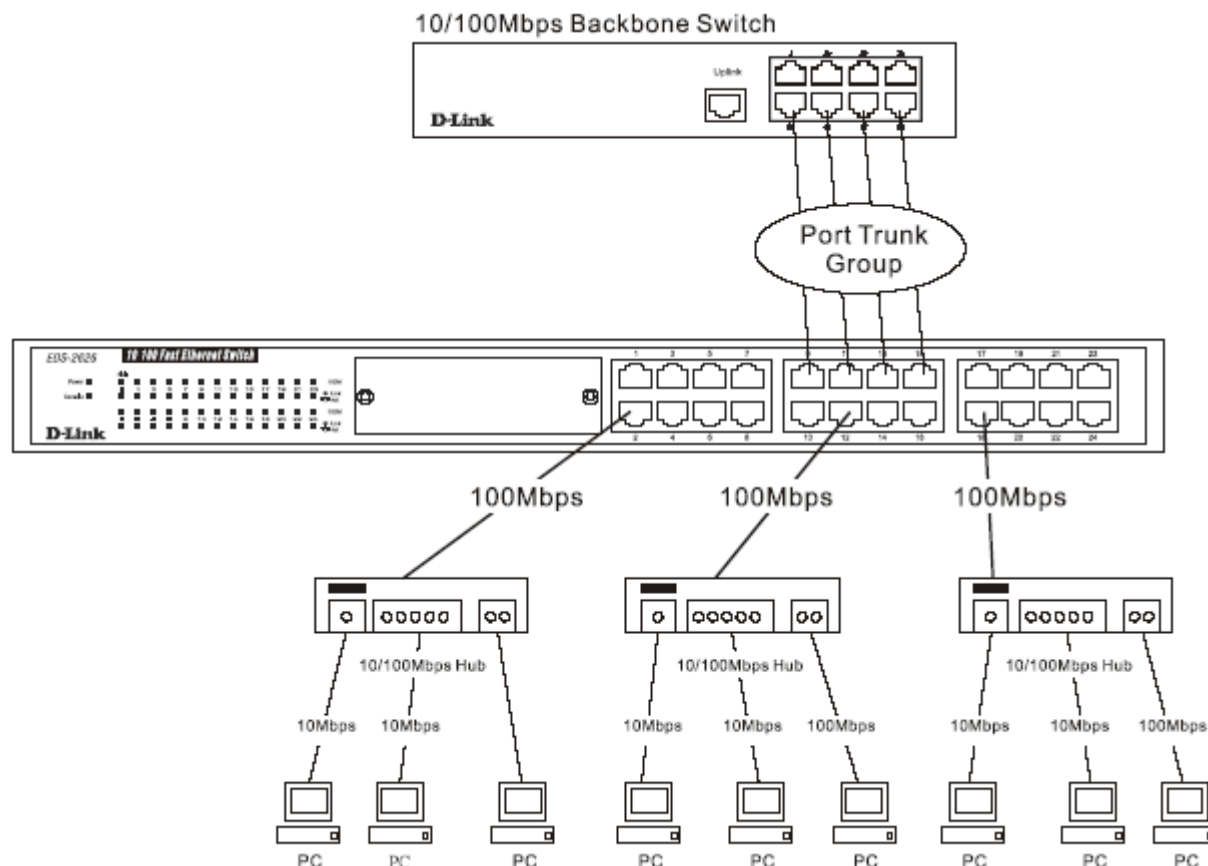


Рисунок 4-4 Пример агрегирования каналов

Коммутатор DGS-3324SR рассматривает транковую группу портов как один порт. Данные, передаваемые конкретному узлу (по адресу назначения), всегда будут передаваться через один и тот же порт в транковой группе портов. Это позволяет пакетам одного потока данных прибывать в том порядке, в котором они были отправлены.



Примечание: Если в составе транковой группы портов какой-либо из портов отключается, то пакеты, предназначенные данному порту, будут распределяться по оставшимся портам в группе.

Агрегирование каналов (объединение портов в транк) позволяет группировать порты для работы в качестве единого канала, пропускная способность которого равна сумме пропускных способностей каждого из портов.

Агрегирование каналов чаще всего используется для подключения высокоскоростных устройств - таких как серверы - к магистрали сети.

Коммутатор позволяет организовывать до 32 транковых групп портов, в каждую из которых может входить от 2 до 8 портов. Транк должен состоять из группы последовательных портов, за исключением 2 (дополнительных) гигабитных портов, которые могут составлять только отдельные каналы связи. Количество портов в транке не может превышать 8 (например, транк, начинающийся с порта номер 1, не может включать порты 9 или 10), и все порты должны принадлежать одной и той же VLAN. Кроме того, порты в транке должны работать на одной скорости и в полнодуплексном режиме.

Настройка всех портов, входящих в транк, сводится к настройке одного порта, который выбирается при конфигурировании транка и называется «связующим» портом, при этом все настройки этого порта - включая настройки VLAN – применяются ко всей группе портов.

При работе транкового соединения осуществляется балансировка нагрузки, поэтому, если один из портов, входящих в транк, выйдет из строя, то его трафик будет перенаправлен на оставшиеся работоспособные порты транка.

Для протокола STP на уровне коммутатора транк представляет собой одно соединение. На уровне портов STP будет использовать параметры «связующего» порта при вычислении значения Port Cost и определении состояния агрегированного канала. Если на коммутаторе настроены два агрегированных канала, и один из каналов избыточен, то STP заблокирует данный канал так же, как заблокировал бы отдельный порт коммутатора.

Для настройки транковых групп портов в папке **Configuration** нажмите на ссылку **Link Aggregation**, появится таблица **Current Link Aggregation Group Entries**:

Current Link Aggregation Group Entries		
Group ID	State	Delete
2	Enabled	

Рисунок 4-5 Таблица транковых групп портов

Для создания нового агрегированного канала нажмите кнопку *Add* и с помощью меню **Link Aggregation Group Configuration** (смотрите ниже) настройте агрегированный канал. Для изменения существующего агрегированного канала дважды щелкните на его названии. Для удаления существующего агрегированного канала нажмите кнопку **Delete** в таблице **Current Link Aggregation Group Entries**.

Link Aggregation Group Configuration																																																	
Group ID	<input type="text"/>																																																
Type	LACP																																																
State	Disabled																																																
Master Port	1 Port 1																																																
Unit	1																																																
Choose Member Ports	<table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td> </tr> <tr> <td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24																										
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																										
Flooding Port	X																																																
Apply																																																	
<p>Note(1): It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Link Aggregation Group Entries</p>																																																	

Рисунок 4-6 Меню Link Aggregation Group Configuration

Link Aggregation Group Configuration																																																	
Group ID	2																																																
Type	LACP																																																
State	Enabled																																																
Master Port	1 Port 1																																																
Unit	1																																																
Choose Member Ports	<table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td> </tr> <tr> <td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24																										
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																										
Flooding Port	X																																																
Apply																																																	
<p>Note(1): It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Link Aggregation Group Entries</p>																																																	

Рисунок 4-7 Окно Link Aggregation Group Configuration – Modify

Параметры для настройки:

Параметр	Описание
Group ID	Введите идентификатор Group ID транковой группы портов.
Type	Выберите тип создаваемого транкового соединения LACP (Link Aggregation Control Protocol) или Static из выпадающего меню. Протокол LACP позволяет автоматически обнаруживать каналы в транковой группе портов.
State	Позволяет включить (Enabled) или отключить (Disabled) транковое соединение. Полезно использовать для диагностики соединения, быстрого отключения сетевого устройства или для создания резервного транкового соединения, управляемого вручную.
Master Port	«Связующий» порт настраиваемого транка.

Unit	Позволяет выбрать номер коммутатора в стеке, для которого будет настраиваться Link Aggregation Group.
Choose Member Ports	Позволяет выбрать порты, которые будут входить в данную транковую группу (до 8 портов в группе).
Flooding Port	Можно назначить один из портов в составе транковой группы, на который будут передаваться широковещательные пакеты или пакеты с неизвестным адресом назначения.

После настройки параметров нажмите *Apply*, чтобы настройки вступили в силу. Созданная транковая группа портов появится в таблице **Current Link Aggregation Group Entries**, показанной на рисунке 4-5.

Настройка порта LACP

Меню **LACP Port Setting** используется совместно с меню **Link Aggregation** для создания транковых групп портов на коммутаторе. С его помощью можно определить, какие порты будут работать в активном или пассивном режиме при обработке и отправке управляющих кадров LACP.

Unit	From	To	Mode	Apply
1	Port 1	Port 1	Active	Apply

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

Рисунок 4-8 Меню настройки портов LACP и таблица LACP Port Information

Параметры для настройки:

Параметр	Описание
Unit	Позволяет выбрать номер коммутатора в стеке, для которого будет изменен LACP режим порта.
From/To	Группа последовательно пронумерованных портов, подлежащих

Mode	<p>настройке.</p> <p><i>Active</i> – Активные порты LACP имеют возможность обрабатывать и отправлять управляющие кадры LACP. Это позволяет поддерживающим протокол LACP устройствам согласовывать параметры агрегированного канала так, что его состав может быть изменен динамически при необходимости. Для возможности изменения состава транковой группы портов, то есть для добавления или удаления портов из группы, как минимум одно из участвующих в агрегированном соединении устройств должно настроить порты LACP как Active. Оба устройства должны поддерживать протокол LACP.</p> <p><i>Passive</i> – Пассивные порты LACP изначально не могут отправлять управляющие кадры LACP. Для возможности динамического создания и изменения агрегированного канала порты LACP на одном из концов этого канала должны быть настроены как Active (активные).</p>
------	---

После настройки параметров нажмите кнопку *Apply*, чтобы изменения вступили в силу. В таблице **LACP Port Information** показано, какие порты настроены как активные и/или пассивные.

Настройка IGMP

Функция IGMP Snooping (Internet Group Management Protocol, Межсетевой протокол управления группами) позволяет коммутатору распознавать IGMP-запросы и отчеты, передаваемые между сетевыми станциями или сетевыми устройствами и IGMP-узлом. При активизации IGMP Snooping коммутатор может заблокировать или разблокировать порт для определенного устройства, основываясь на проходящих через него сообщениях IGMP.

Для использования IGMP Snooping необходимо вначале активизировать данную функцию глобально на коммутаторе (смотрите **Дополнительные настройки**). Затем можно произвести настройку для каждой VLAN, используя меню **IGMP Snooping** в папке **Configuration**. После включения функции IGMP Snooping коммутатор может заблокировать или разблокировать порт для определенного члена группы многоадресной рассылки на основании сообщений IGMP, отправляемых устройством IGMP-узлу и наоборот. Коммутатор просматривает сообщения IGMP и прекращает передачу многоадресных пакетов, если больше нет узлов, запрашивающих продолжение рассылки.

IGMP Snooping

Используйте таблицу **Current IGMP Snooping Group Entries** для просмотра статуса IGMP Snooping. Для изменения настроек нажмите кнопку *Modify* напротив записи с нужным идентификатором VLAN ID.

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

Рисунок 4-9 Таблица Current IGMP Snooping Group Entries

Нажмите кнопку *Modify*, появится меню **IGMP Snooping Settings**.

IGMP Snooping Settings	
VLAN ID	<input type="text" value="1"/>
VLAN Name	<input type="text" value="default"/>
Query Interval	<input type="text" value="125"/>
Max Response Time	<input type="text" value="10"/>
Robustness Value	<input type="text" value="2"/>
Last Member Query Interval	<input type="text" value="1"/>
Host Timeout	<input type="text" value="260"/>
Route Timeout	<input type="text" value="260"/>
Leave Timer	<input type="text" value="2"/>
Querier State	<input type="text" value="Disabled"/>
Querier Router Behavior	Non-Querier
State	<input type="text" value="Disabled"/>

[Show All IGMP Group Entries](#)

Рисунок 4-10 Меню IGMP Snooping Settings

Параметры для настройки:

Параметр	Описание
Query Interval	Позволяет ввести интервал времени между передачей IGMP-запросов; может принимать значения от 1 до 9999 секунд, значение по умолчанию 125 секунд.
VLAN ID	Идентификатор VLAN ID, определяющий вместе с именем VLAN Name ту VLAN, для которой производятся настройки IGMP Snooping.
VLAN Name	Имя VLAN Name, определяющее вместе с идентификатором VLAN ID ту VLAN, для которой производятся настройки IGMP Snooping.
Max Response Time	Максимальное время ожидания IGMP-отчета; может принимать значения от 1 до 25 секунд, значения по умолчанию 10 секунд.
Robustness Variable	Разрешенное количество потерь пакетов в подсети; можно установить значение от 2 до 255, причем это значение должно быть больше для тех подсетей, где ожидается большее количество потерянных пакетов. Значение по умолчанию 2.
Last Member Query Interval	Укажите максимальный интервал времени между запросами о вхождении в группу, включая те, которые отправляются в ответ на запрос о намерении покинуть группу. Значение по умолчанию 1.
Host Timeout	Задаёт максимальное время, в течение которого узел может быть членом группы многоадресной рассылки без отправки коммутатору отчёта о нахождении в группе. Значение по умолчанию 260 сек.
Route Timeout	Задаёт максимальный интервал времени, в течение которого информация о маршруте будет оставаться в адресной таблице коммутатора, если не был получен отчет о вхождении в группу. Значение по умолчанию 260 сек.
Leave Timer	Если коммутатор не получит ответ на запрос о вхождении узлов в группу прежде, чем истечет интервал времени Leave Timer, то адрес узла удаляется из адресной таблицы коммутатора.

Querier State	Можно разрешить передачу пакетов IGMP-запросов (<i>Querier</i>) или запретить (<i>Non-Querier</i>). Значение по умолчанию <i>Non-Querier</i> .
State	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) функцию IGMP Snooping для указанной VLAN. Значение по умолчанию <i>Disabled</i> .

Нажмите кнопку *Apply*, чтобы новые параметры вступили в силу. Для возврата в таблицу **Current IGMP Snooping Group Entries** нажмите ссылку [Show All IGMP Group Entries](#).

Настройка статических портов Router Port

Статическим портом Router Port является порт, к которому подключен маршрутизатор многоадресной рассылки. Как правило, данный маршрутизатор должен иметь соединение с WAN или Интернет. Настройка порта Router Port позволяет многоадресным пакетам от маршрутизатора распространяться по сети так же, как и многоадресным сообщениям (IGMP) из сети распространяться к маршрутизатору.

Порт Router Port работает следующим образом:

- Все IGMP-отчеты передаются на порт Router Port.
- IGMP-запросы (от порта Router Port) передаются на все порты.
- Все пакеты UDP многоадресной рассылки будут переданы на порт Router Port. Поскольку маршрутизаторы не генерируют IGMP-отчеты и не реализуют механизм IGMP Snooping, то маршрутизатор многоадресной рассылки, подключенный к порту Router Port коммутатора 3-его уровня, не сможет принимать потоки данных UDP до тех пор, пока все пакеты UDP многоадресной рассылки не будут передаваться на порт Router Port.

Порт Router Port может быть настроен динамически, если были обнаружены входящие на порт пакеты IGMP-отчетов, пакеты групповой рассылки RIPv2, DVMRP или PIM-DM.

Откройте папку **IGMP** и нажмите на ссылку **Static Router Ports Entry**, появится меню **Current Static Router Ports Entries**.

Current Static Router Ports Entries		
VLAN ID	VLAN Name	Modify
1	default	<input type="button" value="Modify"/>

Рисунок 4-11 Меню Current Static Router Ports Entries

В меню **Current Static Router Ports Entries** показаны все записи о настроенных статических портах Router Port. Для добавления или изменения записи нажмите кнопку *Modify*. Появится меню **Static Router Port Settings**.

Рисунок 4-12 Меню Static Router Port Settings

Параметры для настройки:

Параметр	Описание
VID (VLAN ID)	Идентификатор VLAN ID вместе с именем VLAN определяет VLAN, в которую входит маршрутизатор многоадресной рассылки.
VLAN Name	Имя VLAN, в которую входит маршрутизатор многоадресной рассылки.
Unit	Идентификатор Unit ID коммутатора в стеке коммутаторов, для которого создается запись в таблице статических портов Router Port.
Member Ports	Порты коммутатора, к которым подключены маршрутизаторы многоадресной рассылки.

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в таблицу **Current Static Router Ports Entries** нажмите на ссылку [Show All Static Router Port Entries](#).

Настройка протокола Spanning Tree

Коммутатор поддерживает протоколы 802.1d Spanning Tree Protocol (STP) и 802.1w Rapid Spanning Tree Protocol (RSTP). Протокол 802.1d хорошо знаком многим сетевым специалистам. Но поскольку 802.1w RSTP был недавно реализован в управляемых коммутаторах Ethernet D-Link, далее приведено его краткое описание и описание настройки 802.1d STP и 802.1w RSTP.

Протокол 802.1w Rapid Spanning Tree

DGS-3324SR поддерживает две версии протокола Spanning Tree Protocol, Rapid Spanning Tree Protocol (RSTP), определенный спецификацией IEEE 802.1w, и версию совместимую с IEEE 802.1d STP. RSTP может работать с оборудованием, поддерживающим STP, однако все преимущества от его использования будут потеряны.

Протокол IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) является развитием стандарта 802.1d STP. Он был разработан для преодоления отдельных ограничений STP, которые мешали внедрению некоторых новых функций коммутаторов, например, функций 3-его уровня, всё больше и больше применяемых в коммутаторах Ethernet. Основные функции и терминология остались такими же, как и в STP. Многие настройки, определенные для STP, также используются и RSTP. Данный раздел описывает некоторые новые концепции алгоритма Spanning Tree и показывает основные различия между протоколами STP и RSTP.

Состояния портов

Существенным отличием протоколов STP 802.1d и RSTP 802.1w является способ перехода портов в состояние продвижения и то, каким образом этот переход влияет на роль порта в топологии сети. RSTP

объединяет состояния Disabled, Blocking и Listening, используемые в STP, и создает единственное состояние *Discarding* (отбрасывание), при котором порт не активен. В любом случае порты не передают пакеты в этих состояниях; функционально нет различия между состояниями порта Disabled, Blocking и Listening для STP и состоянием порта Discarding для RSTP - порт не активен в сетевой топологии. В приведенной ниже таблице показаны отличия обоих протоколов относительно состояния портов.

Процесс определения стабильной топологии сети для обоих протоколов одинаков. Каждый сегмент имеет единственный путь к корневому мосту. Все мосты принимают и обрабатывают пакеты BPDU. Тем не менее, пакеты BPDU генерируются чаще - с каждым пакетом Hello. BPDU генерируются, даже если пакет BPDU не был принят. Следовательно, каждое соединение между мостами чувствительно к состоянию данной связи. Данное отличие приводит к более быстрому обнаружению сбойных связей и, поэтому, к более быстрой установке топологии сети. Недостатком протокола 802.1d является отсутствие мгновенных обратных связей от смежных мостов.

802.1d STP	802.1w RSTP	Продвижение?	Обучение?
Disabled	Discarding	Нет	Нет
Blocking	Discarding	Нет	Нет
Listening	Discarding	Нет	Нет
Learning	Learning	Нет	Да
Forwarding	Forwarding	Да	Да

Таблица 5-4 Сравнение состояний портов

При работе RSTP порт может перейти в состояние продвижения значительно быстрее – он больше не зависит от конфигурации таймеров - поддерживающий RSTP мост «чувствует» состояние соединения с другим мостом, совместимым с RSTP, посредством обратной связи. Порты больше не должны ждать стабилизации топологии, чтобы перейти в режим продвижения пакетов. Для того чтобы обеспечить быстрый переход в это состояние, протокол RSTP вводит два новых понятия: пограничный порт (edge port) и порт типа «точка-точка» (point-to-point, P2P).

Пограничный порт – Edge Port

Пограничным (Edge) портом объявляется порт, непосредственно подключенный к сегменту, в котором не могут быть созданы маршрутные петли. Например, непосредственно подключенный к рабочей станции порт. Порт, который определен как пограничный, мгновенно переходит в состояние продвижения, минуя состояния прослушивания и обучения. Пограничный порт теряет свой статус и становится обычным портом связующего дерева в том случае, если получит пакет BPDU.

Порт P2P

Порт P2P, обычно используемый для подключения к другим мостам, также способен быстро перейти в состояние продвижения. При работе RSTP все порты, функционирующие в полнодуплексном режиме, рассматриваются как порты P2P, до тех пор, пока не будут переконфигурированы вручную.

Совместимость 802.1d/802.1w

Протокол RSTP способен взаимодействовать с оборудованием, поддерживающим STP, и если необходимо, может автоматически преобразовывать пакеты BPDU в формат 802.1d. Однако, преимущество быстрой сходимости этого протокола (когда все коммутаторы переходят в состояние продвижения или блокировки и обладают тождественной информацией) теряется. Протокол также предоставляет возможность использования переменной для миграции, в случае обновления программного обеспечения оборудования в сегменте сети для использования RSTP.

Настройки STP на коммутаторе

Протокол Spanning Tree (STP) работает на двух уровнях: на уровне коммутатора, где задаются общие настройки, и на уровне портов, где настройки задаются индивидуально для портов или групп портов. В папке **Configuration** выберите папку **Spanning Tree** и нажмите на ссылку **STP Switch Settings**, появится следующее меню.

Switch Spanning Tree Settings	
Spanning Tree Protocol	Enabled ▾
Bridge Max Age (6-40 Sec)	20
Bridge Hello Time (1-10 Sec)	2
Bridge Forward Delay (4-30 Sec)	15
Bridge Priority (0-61440 Sec)	32768
STP Version	rstp ▾
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled ▾
Apply	
Designated Root Bridge	00-00-33-48-49-14
Root Priority	32768
Cost to Root	0
Root Port	None
Time Topology Change(secs)	9
Topology Changes Count	1
Protocol Specification	3
Max Age	20
Hello Time	2
Forward Delay	15
Hold Time	3
<i>Note: 2*(Forward Delay-1) >= Max Age, Max Age >= 2*(Hello Time +1)</i>	

Рисунок 4-13 Настройки STP на коммутаторе

Параметры для настройки:

Параметр	Описание
Spanning Tree Protocol <Disabled>	Позволяет включать (<i>Enabled</i>) или отключать (<i>Disabled</i>) работу Spanning Tree Protocol на коммутаторе.
Max Age: (6 – 40sec) <20>	Данный параметр может изменяться в пределах от 6 до 40 секунд. Если по истечении времени, заданного в параметре Max Age, от корневого коммутатора не будет получен пакет BPDU, то коммутатор начнет рассылать соседним коммутаторам пакеты BPDU, в которых корневым коммутатором назначит себя. Если коммутатора окажется наименьший идентификатор Bridge ID, то он станет корневым.
Hello Time: (1 – 10sec) <2>	Данный параметр может изменяться в пределах от 1 до 10 секунд. Это интервал времени, через который корневой коммутатор рассылает служебные пакеты BPDU, уведомляющие другие коммутаторы сети, что он является корневым и доступен.

Forward Delay: (4 - 30sec) <15>	Данный параметр может изменяться в пределах от 4 до 30 секунд. Это время, в течении которого каждый порт коммутатора находится в состоянии прослушивания, прежде чем перейти в состояние продвижения пакетов.
Bridge Priority: (0 - 61440) <32768>	Приоритет коммутатора может быть установлен в пределах от 0 до 61440. Данный параметр используется при выборе корневого коммутатора. Чем меньше значение данного параметра, тем выше приоритет коммутатора, и тем выше вероятность, что коммутатор станет корневым.
STP Version <RSTP>	Позволяет выбрать версию STP: RSTP (установлено по умолчанию) или STP. Обе версии используют параметры STP одинаковым образом. RSTP полностью совместим с IEEE 802.1d STP.
Tx Hold Count <3>	Максимальное количество пакетов Hello, отправляемых за интервал Hello Time, изменяется в пределах от 1 до 10. Значение по умолчанию равно 3.
Forwarding BPDU <Enabled>	Доступны опции Enabled и Disabled. При установке Enabled коммутатор будет продвигать пакеты BPDU, полученные от других сетевых устройств, когда работа STP выключена на коммутаторе. Значение по умолчанию - Enabled.

Нажмите *Apply*, чтобы изменения вступили в силу.



Примечание: Значение Hello Time не может быть больше, чем значение Max Age. Иначе возникнет ошибка конфигурации.

При настройке применяйте следующую формулу для расчета значений:

Max. Age $\leq 2 \times$ (Forward Delay - 1 second)

Max. Age $\geq 2 \times$ (Hello Time + 1 second)

Настройка STP на портах

Если коммутаторы объединены в стек, вначале выберите порядковый номер коммутатора в стеке.

STP Port Settings

Unit	From	To	State	Cost(0=Auto)	Priority	Migration	Edge	P2P
1	Port 1	Port 1	Disabled	0	0	No	No	No

The STP Port Information

Port	Connection	State	Cost	Priority	Edge	P2P	STP Status	Role
1	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
2	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
3	100M/Full/None	Yes	*200000	128	No	Yes	Forwarding	NonStp
4	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
5	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
6	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
7	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
8	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
9	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
10	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
11	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
12	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
13	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
14	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
15	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
16	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
17	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
18	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
19	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
20	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
21	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
22	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
23	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled
24	Link Down	Yes	*200000	128	No	Yes	Disabled	Disabled

Рисунок 4-14 Настройка STP на портах

Кроме настройки параметров Spanning Tree на уровне коммутатора, можно настроить параметры STP для определенных групп портов. Группа портов будет использовать параметры STP уровня коммутатора и дополнительные параметры **Port Priority** и **Port Cost**.

Алгоритм Spanning Tree работает на уровне групп портов таким же образом, как и на уровне коммутаторов, но понятие корневого коммутатора заменяется понятием корневого порта. Корневой порт – это один из портов группы, который выбирается на основании параметров Port Priority и Port Cost для соединения данной группы с сетью. Избыточные связи будут блокированы так же, как они блокируются на уровне коммутаторов.

STP на уровне коммутатора блокирует избыточные связи между коммутаторами (и аналогичными сетевыми устройствами). STP на уровне портов блокирует избыточные связи в пределах группы портов.

Желательно определять группу портов STP в соответствии с группой портов VLAN.

Параметры для настройки:

Параметр	Описание
Unit	Идентификатор Unit ID коммутатора в составе стека.
From/To <Port 1>	Группа последовательно пронумерованных портов, подлежащих настройке.
State <Disabled>	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) протокол STP для указанной группы портов.
Cost (0=Auto) <0>	Параметр Port Cost может изменяться от 1 до 200 000 000. Чем меньше значение параметра для данного порта, тем больше вероятность, что порт будет выбран для продвижения пакетов. Значения по умолчанию: Для порта 100 Мбит/с = 200 000 Для порта 1 Гбит/с = 20 000

Priority <0>	Параметр Port Priority может изменяться от 0 до 240. Чем меньше значение параметра для заданного порта, тем больше вероятность, что порт будет выбран в качестве корневого (Root Port).
Migration <No>	Выбор опции Yes разрешает порту переход от 802.1d STP к 802.1w RSTP. RSTP может сосуществовать со стандартом STP, однако, преимущества от его использования теряются при подсоединении к порту сегмента, поддерживающего только 802.1d. Переход должен быть разрешен для тех портов, к которым присоединены сегменты сети или отдельные станции, которые будут модернизированы для поддержки RSTP во всем сегменте или его части.
Edge <No>	Выбор опции Yes назначает данный порт в качестве «пограничного». Такие порты не могут создавать петель в сети, однако, порт может потерять этот статус, если топология сети изменяется так, что возникает возможность образования петель. В нормальном состоянии «пограничный» порт не принимает пакеты BPDU. Если он примет пакет BPDU, то автоматически теряет статус «пограничного». Опция No указывает, что порт не является «пограничным».
P2P <No>	Выбор опции Yes определяет, что данный порт входит в соединение точка-точка. Такой порт похож на «пограничный» порт, но порт при соединении точка-точка может работать в полнодуплексном режиме в отличие от «пограничного» порта. Подобно «пограничным» портам, данные порты переходят в состояние продвижения также быстро, как и при использовании протокола RSTP.

Нажмите *Apply*, чтобы изменения вступили в силу.

Настройка продвижения и фильтрации пакетов

Статическая таблица MAC-адресов

В папке **Configuration** откройте папку **Forwarding & Filtering** и нажмите на ссылку **Unicast Forwarding**, появится меню **Setup Static Unicast Forwarding Table**.


Setup Static Unicast Forwarding Table					
VLAN ID	MAC Address	Unit	Port		
1	00:00:00:00:00:00	1	Port 1		
Add/Modify					
Static Unicast Forwarding Table					
Mac Address	VID	VLAN Name	Unit	Port	Delete
00:00:00:00:00:00	1	default	1	1	X
End of data!					

Рисунок 4-15 Статическая таблица MAC-адресов

Параметры для настройки:

Параметр	Описание
VLAN ID	Идентификатор VLAN ID той VLAN, которой принадлежит введенный MAC-адрес.
MAC Address	MAC-адрес, по которому пакеты будут передаваться статически. Это должен быть обычный одноадресный (уникальный) MAC-адрес.

Unit	Позволяет выбрать коммутатор в стеке по его идентификатору Unit ID при объединении коммутаторов в стек.
Port	Позволяет задать порт коммутатора, к которому подключено устройство с данным MAC-адресом.

Нажмите *Apply*, чтобы изменения вступили в силу. Для удаления записи из статической таблицы MAC-адресов нажмите  в колонке **Delete** рядом с удаляемой записью.

Статическая таблица групповых MAC-адресов

Далее описывается настройка таблицы групповых MAC-адресов на коммутаторе. Откройте папку **Forwarding & Filtering** и нажмите на ссылку **Multicast Forwarding**, появится следующее окно.

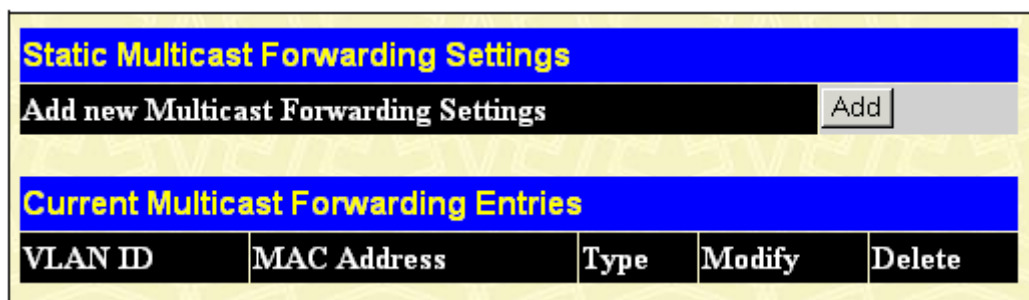


Рисунок 4-16 Таблица групповых MAC-адресов

Для добавления новой записи в таблицу групповых MAC-адресов нажмите кнопку *Add*, появится меню **Setup Static Multicast Forwarding Table**.

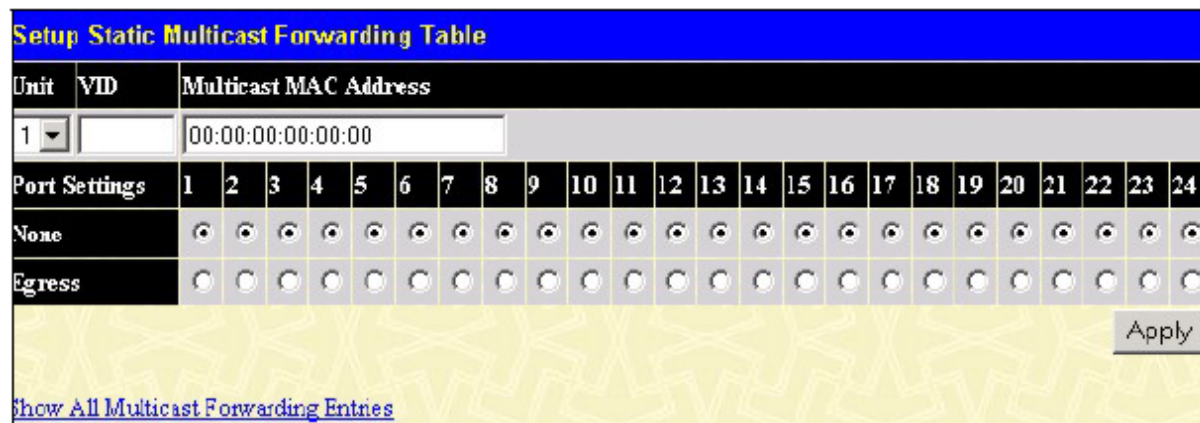



Рисунок 4-17 Добавление записи в таблицу групповых MAC-адресов

Параметры для настройки:

Параметр	Описание
Unit	Номер коммутатора в стеке коммутаторов.
VID	Идентификатор VLAN ID той VLAN, которой принадлежит введенный MAC-адрес.
Multicast MAC Address	MAC-адрес многоадресной рассылки. Это должен быть групповой MAC-адрес.
Port Settings	Позволяет указать порты, которые являются членам статической группы многоадресной рассылки, и порты, которым будет запрещено или разрешено присоединяться к группе многоадресной рассылки динамически по протоколу GVRP. Доступны следующие опции: None – порту разрешено динамически присоединяться к группе многоадресной

рассылки. Опция **None** выбирается, когда подключенная к порту станция может присоединяться к группе многоадресной рассылки, используя протокол GMRP. **Egress** – порт статически входит в группу многоадресной рассылки.

Нажмите *Apply*, чтобы изменения вступили в силу. Для удаления записи из статической таблицы групповых MAC-адресов нажмите  в колонке **Delete** рядом с удаляемой записью. Для возврата в таблицу групповых MAC-адресов нажмите на ссылку [Show All Multicast Forwarding Entries](#).

Настройка VLAN

Понятие приоритета IEEE 802.1p

Функция добавления приоритета в пакеты определена стандартом IEEE 802.1p, который был разработан в качестве средства управления трафиком в сети, где одновременно могут передаваться различные типы данных. Он помогает разрешить проблемы, связанные с передачей критических по времени доставки данных в загруженной сети. Качество работы приложений, зависящих от времени передачи данных, например видеоконференций, может быть сильно снижено даже очень небольшими задержками при передаче данных.

Сетевые устройства, поддерживающие стандарт IEEE 802.1p, имеют возможность распознавать приоритет пакетов. Эти устройства также могут добавлять тег приоритета в пакеты. Кроме того, они могут извлекать тег приоритета из пакета. Тег приоритета определяет срочность доставки пакета и очередь, в которую пакет будет назначен.

Значение приоритета находится в пределах от 0 до 7, значение 0 назначается пакетам с наименьшим приоритетом, а 7 – с наивысшим. Тег наивысшего приоритета обычно используется для передачи данных видео и аудиоприложений, которые чувствительны даже к небольшим задержкам, или для передачи данных от конечных пользователей, которым нужны особые гарантии доставки данных.

Коммутатор DGS-3324SR позволяет настроить обработку пакетов с тегом приоритета. Используя очереди для управления приоритетами можно определить относительный приоритет передаваемого пакета в соответствии с требованиями сети. Может возникнуть ситуация, когда будет выгодно определить несколько пакетов с различными значениями приоритетов в одну очередь. Однако рекомендуется резервировать очередь с наивысшим приоритетом, очередь Queue 1, для пакетов со значением приоритета 7. Пакеты без тега приоритета назначаются в очередь Queue 0, и поэтому получают низший приоритет доставки.

Для обслуживания очередей пакетов в коммутаторе реализован алгоритм Weighted Round Robin (взвешенный циклический алгоритм). Соотношение обслуживания очередей равно 4:1. Это значит, что на каждый обслуженный пакет в низкоприоритетной очереди Queue 0 приходится 4 пакета из очереди Queue 1 с наивысшим приоритетом.

Помните, что настройка очередей приоритетов распространяется на все порты коммутатора и воздействует на все подключенные устройства. Система очередей приоритетов будет особенно эффективна, если все коммутаторы сети поддерживают теги приоритета.

Виртуальные локальные сети VLAN

Виртуальной сетью - VLAN - называется топология сети, при которой узлы объединяются не физически, а логически. То есть узлы, которые взаимодействуют наиболее часто друг с другом, могут быть объединены в VLAN в независимости от их реального расположения в сети. VLAN позволяют логически сегментировать сеть на широкоэвещательные домены так, что пакеты будут пересылаться только между узлами, входящими в одну и ту же VLAN.

Реализация VLAN в DGS-3324SR

Пакеты **не могут** передаваться между VLAN без помощи устройства, выполняющего функцию маршрутизации между ними.

DGS-3324SR поддерживает IEEE 802.1Q VLAN и VLAN на основе портов. Функция извлечения тегов может использоваться для удаления тега 802.1Q из заголовка пакета для сохранения совместимости с устройствами, не поддерживающими тегирование.

По умолчанию, все порты коммутатора назначены в единственную 802.1Q VLAN с именем “default”. “default” VLAN имеет VID = 1.

Порты в разных VLAN, построенных на основе портов, могут перекрываться.

IEEE 802.1Q VLAN

Некоторые определения:

Tagging (Маркировка пакета) - процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра.

Untagging – процесс извлечения информации 802.1Q VLAN из заголовка пакета.

Ingress port (Входящий порт) - порт коммутатора, на который поступают пакеты, и при этом принимается решение о принадлежности к VLAN.

Egress port (Исходящий порт) – порт коммутатора, с которого пакеты передаются на другие сетевые устройства – коммутаторы или рабочие станции, и соответственно, на нем должно приниматься решение о маркировке.

В коммутаторе DGS-3324SR реализована поддержка IEEE 802.1Q (tagged) VLAN. 802.1Q VLAN требует тегирования, что позволяет разбить всю сеть на несколько VLAN (при условии, что все коммутаторы сети совместимы с IEEE 802.1Q).

VLAN позволяют сегментировать сеть для уменьшения размера широковещательных доменов. Все входящие в VLAN пакеты могут быть переданы только на те конечные станции (и другие коммутаторы с поддержкой IEEE 802.1Q), которые являются членами данной VLAN. Это относится к широковещательным, многоадресным пакетам и пакетам с неизвестным адресом источника.

Кроме того, VLAN могут обеспечить некоторый уровень безопасности в сети, поскольку IEEE 802.1Q VLAN передают пакеты только между станциями, входящими в одну VLAN.

Любой порт может быть настроен как *tagging* или как *untagging*. Функция *untagging* позволяет VLAN работать с теми сетевыми устройствами, которые не понимают меток в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q, и позволяет нормально функционировать протоколу Spanning Tree.

Стандартом IEEE 802.1Q ограничено продвижение немаркированных пакетов только в ту VLAN, в которую входит порт назначения.

Основные характеристики IEEE 802.1Q:

- Определение пакетов в VLAN при фильтрации.
- Допускает наличие единственного глобального покрывающего дерева.
- Использует явную одноуровневую схему тегирования.

Продвижение пакетов VLAN 802.1Q

Решение о продвижении пакета принимается на основе 3 следующих видов правил:

- Правила входящего трафика - правила классификации получаемых пакетов относительно принадлежности VLAN.
- Правила продвижения между портами - принимается решение о продвижении или отбрасывании пакета.
- Правила исходящего трафика - определяется, нужно ли маркировать пакет перед передачей его или нет.

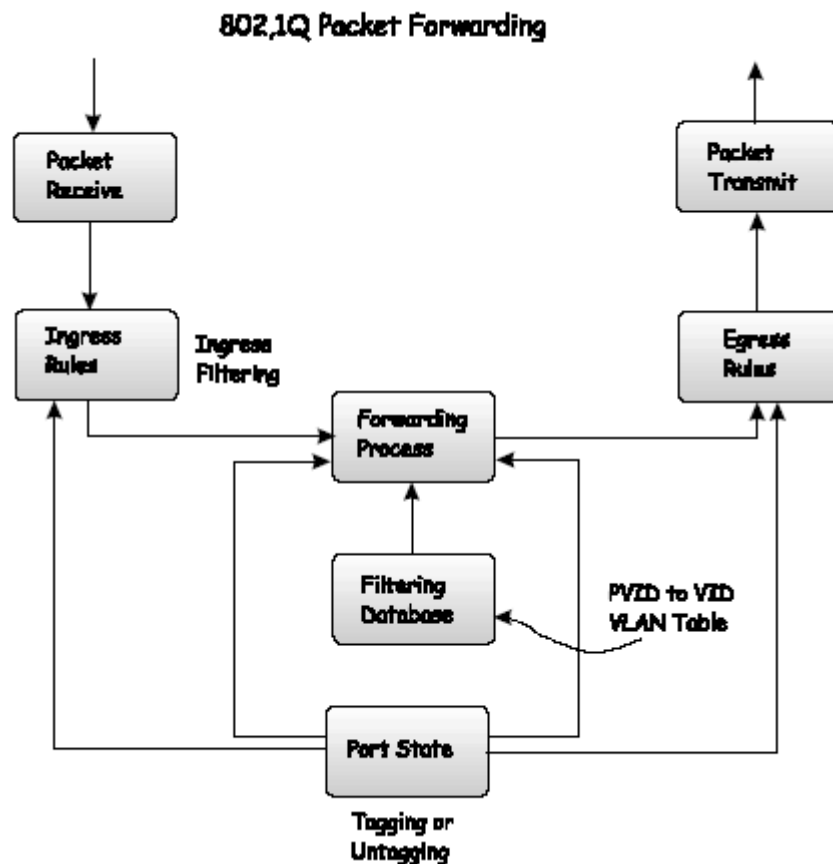


Рисунок 4-18 Продвижение пакетов IEEE 802.1Q

Теги 802.1Q VLAN

Приведенный ниже рисунок показывает тег 802.1Q VLAN. После MAC-адреса назначения добавлены 4 дополнительных байта. На их наличие указывает значение 0x8100 в поле типа протокола EtherType. Если поле EtherType равно 0x8100, то кадр содержит тег IEEE 802.1Q/802.1p. Тег располагается в 2 следующих байтах и состоит из 3 битов приоритета кадра, 1 бита Canonical Format Identifier (CFI - используемого для инкапсуляции пакетов Token Ring при передаче их по магистральям Ethernet) и 12 бит идентификатора VLAN - VLAN ID (VID). 3 бита приоритета используются стандартом 802.1p. VID является идентификатором VLAN и используется стандартом 802.1Q. Поскольку под поле VID отведено 12 бит, то можно определить 4096 уникальных VLAN.

Добавление тега в заголовок пакета делает пакет длиннее на 4 байта. Вся содержащаяся в исходном пакете информация сохраняется.

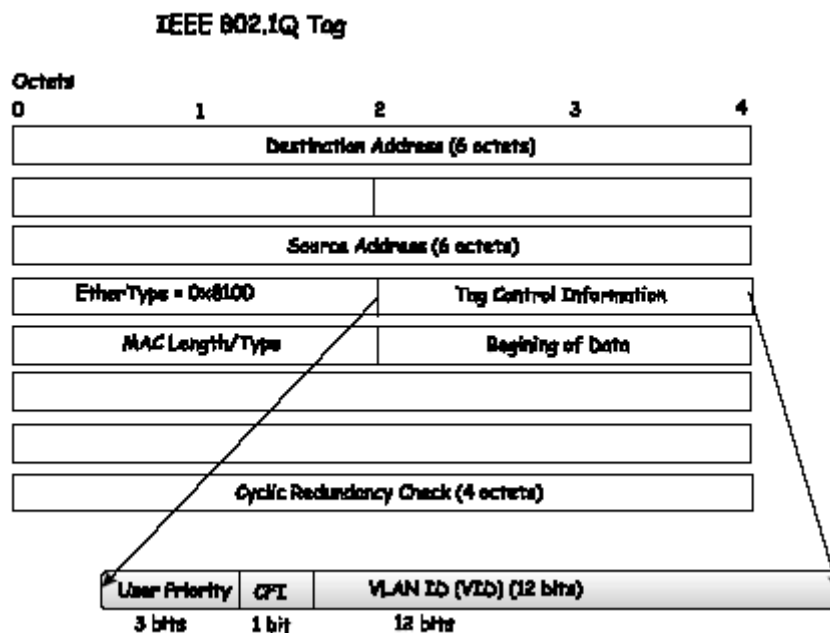


Рисунок 4-19 Тег IEEE 802.1Q

Поля EtherType и VLAN ID добавляются после MAC-адреса назначения, но перед исходным полем EtherType/Length или полем Logical Link Control. Поскольку сформированный пакет несколько длиннее исходного, то должна быть заново вычислена контрольная сумма Cyclic Redundancy Check (CRC).

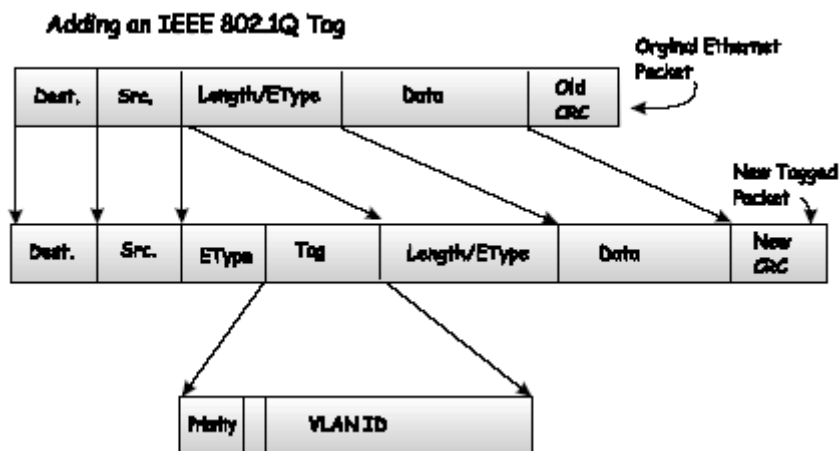


Рисунок 4-20 Добавление тега IEEE 802.1Q

Port VLAN ID

Маркированные пакеты (несущие информацию о 802.1Q VID) могут быть переданы от одного устройства, совместимого со стандартом 802.1Q, к другому с сохранением информации о принадлежности к VLAN. Это позволяет создавать несколько VLAN на многих сетевых устройствах (в действительности, на всей сети - если все сетевые устройства поддерживают стандарт 802.1Q).

К сожалению, не все устройства поддерживают стандарт 802.1Q. Такие устройства называются *tag-unaware* (не поддерживающие тегирование). Устройства, совместимые с 802.1Q, называются *tag-aware* (поддерживающие тегирование).

Перед принятием стандарта 802.1Q VLAN использовались VLAN на основе портов и MAC-адресов. Они полагались на Port VLAN ID (PVID) при продвижении пакетов. Принятому на данном порту пакету должен быть присвоен PVID этого порта, и далее пакет должен быть передан на порт, который соответствует адресу назначения пакета (найденному в адресной таблице коммутатора). Если PVID порта, принявшего пакет, отличается от PVID порта назначения, то коммутатор отбрасывает пакет.

На одном коммутаторе различные PVID означают различные VLAN (помните, что две VLAN не могут взаимодействовать между собой без маршрутизатора). Таким образом, VLAN на основе портов не могут выходить за пределы данного коммутатора (или стека коммутаторов).

Каждый физический порт коммутатора имеет PVID. В стандарте 802.1Q портам также назначается PVID для использования в пределах одного коммутатора. Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1. Немаркированным пакетам присваивается PVID порта, на котором они были приняты. Решение о продвижении пакета принимается на основании этого PVID. Маркированные пакеты продвигаются в соответствии с идентификатором VID, содержащемся в теге. Маркированным пакетам также присваивается PVID, но PVID не используется при принятии решения о продвижении пакета, используется только VID.

Поддерживающие тегирование коммутаторы должны хранить таблицу, связывающую идентификаторы PVID коммутатора с идентификаторами VID сети. Коммутатор сравнивает VID пакета, который нужно передать, с VID порта, на который нужно передать пакет. Если VID порта и пакета различаются, то коммутатор отбросит пакет. Поскольку существуют PVID для немаркированных пакетов и VID для маркированных пакетов, то можно использовать в одной сети как устройства, поддерживающие тегирование, так и не поддерживающие тегирование. Порт коммутатора может иметь только один PVID и так много идентификаторов VID, насколько позволяет память коммутатора, используемая для хранения таблицы VLAN.

Поскольку некоторые сетевые устройства могут не поддерживать тегирование, то перед передачей пакета устройство, поддерживающее тегирование, должно принять решение – нужно ли добавить тег в передаваемый пакет или нет. Если передающий порт подключен к не поддерживающему тегирование устройству, то пакет должен быть немаркированным. Если же передающий порт подключен к поддерживающему тегирование устройству, то пакет должен быть маркированным.

Tagging и Untagging

Каждый порт устройства, поддерживающего стандарт 802.1Q, может быть настроен как *tagging* или как *untagging*.

Порт, настроенный как *tagging*, будет добавлять номер VID, приоритет и другую информацию о VLAN в заголовок всех проходящих через него пакетов. Если пакет приходит на порт уже маркированным, то данный пакет не изменяется, и таким образом сохраняется вся информация о VLAN. Информация о VLAN в теге может быть использована другими сетевыми устройствами, поддерживающими стандарт 802.1Q, при принятии решения о продвижении пакета.

Порт, настроенный как *untagging*, будет извлекать тег 802.1Q из всех проходящих через него пакетов. Если же пакет не содержит тег VLAN 802.1Q, то порт не изменяет такой пакет. Таким образом, все принятые и переданные этим портом пакеты не будут содержать информацию о VLAN (помните, что PVID используется только внутри коммутатора). Функция *untagging* используется при передаче пакетов от сетевых устройств, поддерживающих стандарт 802.1q, на устройства, не поддерживающие этот стандарт.

Фильтрация входящего трафика

Порт коммутатора, на который поступают пакеты из сети и который должен принять решение о принадлежности пакета VLAN, называется *ingress port* (входящим портом). При включении на порту функции фильтрации входящего трафика коммутатор проверяет пакет на наличие информации VLAN и на ее основании принимает решение о продвижении пакета.

Если пакет содержит информацию о VLAN, входной порт сначала определяет, является ли он сам членом данной VLAN. Если нет, то пакет отбрасывается. Если да, то определяется, является ли порт назначения членом данной VLAN. Если нет, то пакет отбрасывается. Если же порт назначения входит в данную VLAN, то он передает пакет в подключенный к нему сегмент сети.

Если пакет не содержит в заголовке информацию о VLAN, то входной порт добавляет в заголовок пакета тег с идентификатором VID, равным собственному PVID (если порт является маркированным - *tagging*). Затем коммутатор определяет, принадлежат ли входной порт и порт назначения одному VLAN (имеют одинаковые VID). Если нет, пакет отбрасывается. В противном случае порт назначения передает пакет в подключенный к нему сегмент сети.

Этот процесс называется *ingress filtering* (входной фильтрацией) и используется для сохранения пропускной способности внутри коммутатора путем отбрасывания на стадии приема пакетов, не входящих в ту же VLAN, что и входной порт.

Default VLAN

Изначально на коммутаторе настроена одна VLAN с VID = 1, называемая “default”. По умолчанию все порты коммутатора входят в default VLAN. При настройке VLAN на основе портов соответствующие порты новых VLAN удаляются из default VLAN.

Пакеты не могут перемещаться между VLAN. Связь между двумя VLAN должна проходить через внешний маршрутизатор.



Примечание: Если VLAN не настроены на коммутаторе, то все пакеты будут передаваться на любой требуемый порт назначения. Пакеты с неизвестным адресом назначения будут передаваться на все порты коммутатора, так же как и широковещательные и многоадресные пакеты.

Далее приведен пример:

Имя VLAN	VID	Порты коммутатора
System (по умолчанию)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Таблица 4 -2 Пример назначения портов в VLAN

VLAN на основе портов

VLAN на основе портов ограничивают входящий и исходящий трафик портов коммутатора. Таким образом, все подключенные к порту устройства (один компьютер или целый отдел), являются членами той VLAN, в которую входит порт.

При создании VLAN на основе портов нет необходимости в поддержке сетевыми адаптерами тегов 802.1Q в заголовке пакетов. Сетевые адаптеры отправляют и принимают обычные кадры Ethernet. Если узел назначения находится в том же сегменте, то взаимодействие происходит по обычному протоколу Ethernet. Если же узел назначения подключен к другому порту коммутатора, то решение о продвижении пакета принимается коммутатором на основе VLAN.

Сегментация с помощью VLAN

Для примера, пусть пакет отправлен компьютером, подключенным к порту Port 1, который является членом VLAN 2. Если узел назначения подключен к другому порту (найденному после поиска в обычной адресной таблице коммутатора), коммутатор проверяет, является ли другой порт (Port 10) членом VLAN 2 (и, следовательно, может принимать пакеты от VLAN 2). Если порт Port 10 не является членом VLAN 2, то пакет отбрасывается коммутатором и не достигает адреса назначения. Если же порт Port 10 является членом VLAN 2, то коммутатор передает пакет. Выборочное продвижение пакетов на основе тега VLAN позволяет сегментировать сеть при помощи VLAN. Ключевым моментом является то, что порт Port 1 может отправлять пакеты только в VLAN 2.

Можно организовать совместный доступ к сетевым ресурсам, например принтерам, серверам, из нескольких VLAN. Это достигается путем перекрытия VLAN – то есть порт может входить

одновременно в более чем одну VLAN. Например, порты 1, 2, 3 и 4 являются членами VLAN 1, а порты 1, 5, 6 и 7 входят в VLAN 2. Порт 1 принадлежит двум VLAN. Порты 8, 9 и 10 не определены в какую-либо VLAN. Это значит, что порты 8, 9 и 10 входят в одну и ту же VLAN.

VLAN и транковые группы портов

Порты, входящие в транк, должны принадлежать одной VLAN. Любые изменения членства VLAN одного из портов транковой группы распространяются на все остальные порты транка.



Примечание: Если Вы хотите использовать сегментацию по VLAN вместе транковыми группами портов, то вначале необходимо настроить транки портов, а затем настроить VLAN. Если требуется изменить настройки транковой группы портов с уже сформированными VLAN, то нет необходимости изменять настройки VLAN после изменения параметров транковой группы, поскольку в данном случае настройки VLAN изменятся автоматически.

Настройка статических VLAN

Для создания или изменения 802.1Q VLAN:

В папке **Configuration** откройте папку **VLAN** и нажмите на ссылку **Static VLAN Entry**, появится следующее окно.

Add			
Current 802.1Q Static VLANs Entries			
VLAN ID	VLAN name	Advertisement	Delete
1	default	Enabled	

Рисунок 4-21 Таблица Current 802.1Q Static VLANs Entries

В данном окне приведен полный список настроенных на коммутаторе VLAN по имени и идентификатору VLAN ID. Для удаления существующей VLAN 802.1Q нажмите соответствующую кнопку в колонке **Delete**.

Для создания новой VLAN 802.1Q нажмите кнопку *Add*, появится следующее меню.

802.1Q Static VLANs																								
Unit	VID	VLAN Name												Advertisement										
1														Disabled										
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply																								
Show All Static VLAN Entries																								

Рисунок 4-22 Добавление записи о статической VLAN 802.1Q

Для возврата в таблицу **Current 802.1Q Static VLANs Entries** нажмите на ссылку **Show All Static VLANs Entries**. Для изменения настроек существующей VLAN дважды щелкните на нужную запись, появится следующее меню.

802.1Q Static VLANs																									
Unit	VID	VLAN Name													Advertisement										
1	1	default													Enabled										
Port Settings		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
None		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Forbidden		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Apply																									
Show All Static VLAN Entries																									

Рисунок 4-23 Изменение настроек VLAN 802.1Q

Параметры для настройки:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке при объединении коммутаторов в стек.
VID (VLAN ID)	Позволяет ввести VLAN ID в при добавлении или отображает VLAN ID существующей VLAN при редактировании. VLAN обозначаются по имени или по VID.
VLAN Name	Позволяет задать имя VLAN при добавлении или показывает имя существующей VLAN при редактировании.
Advertisement	Можно включить данную функцию (<i>Enabled</i>), чтобы позволить узлам сети присоединяться к данной VLAN с помощью протокола GVRP.
Port	Позволяет назначить данный порт в VLAN.
Tag	Позволяет настроить данный порт как Tagged . Когда такой порт передает немаркированный пакет, то добавляет в заголовок пакета 32-битный тег, содержащий VID. При передаче маркированного пакета заголовок пакета не изменяется.
None	Позволяет указать, что порт не является членом данной VLAN.
Egress	Указывает, что порт статически входит в VLAN; такой порт может передавать трафик в VLAN и может быть настроен как tagged и как untagged.
Forbidden	Указывает, что порт не является членом VLAN и не сможет стать членом VLAN динамически.

Настройка GVRP

В папке **Configuration** откройте папку **VLAN** и нажмите на ссылку **GVRP Setting**.

Диалоговое окно **Port VLAN ID (PVID)**, показанное ниже, позволяет определить, будет ли коммутатор распространять информацию о настроенных на нем VLAN другим коммутаторам по протоколу **GARP VLAN Registration Protocol (GVRP)**. Кроме того, опция **Ingress Checking** позволяет ограничить входящий трафик коммутатора: пакеты, VID которых не совпадает с PVID порта, будут отбрасываться.

GVRP Settings							
Unit	From	To	GVRP	Ingress Check	Acceptable Frame Type	PVID	Apply
1	Port 1	Port 1	Disabled	Disabled	Tagged_Only		Apply

GVRP Table				
Port	PVID	GVRP	Ingress Check	Acceptable Frame Type
1	1	Disabled	Enabled	All Frames
2	1	Disabled	Enabled	All Frames
3	1	Disabled	Enabled	All Frames
4	1	Disabled	Enabled	All Frames
5	1	Disabled	Enabled	All Frames
6	1	Disabled	Enabled	All Frames
7	1	Disabled	Enabled	All Frames
8	1	Disabled	Enabled	All Frames
9	1	Disabled	Enabled	All Frames
10	1	Disabled	Enabled	All Frames
11	1	Disabled	Enabled	All Frames
12	1	Disabled	Enabled	All Frames
13	1	Disabled	Enabled	All Frames
14	1	Disabled	Enabled	All Frames
15	1	Disabled	Enabled	All Frames
16	1	Disabled	Enabled	All Frames
17	1	Disabled	Enabled	All Frames
18	1	Disabled	Enabled	All Frames
19	1	Disabled	Enabled	All Frames
20	1	Disabled	Enabled	All Frames
21	1	Disabled	Enabled	All Frames
22	1	Disabled	Enabled	All Frames
23	1	Disabled	Enabled	All Frames
24	1	Disabled	Enabled	All Frames

Рисунок 4-24 Настройка GVRP

Параметры для настройки:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке при объединении коммутаторов в стек.
From/To	Группа последовательно пронумерованных портов, подлежащих настройке.
GVRP	Можно включить (<i>Enabled</i>) работу протокола GARP VLAN Registration Protocol (<i>GVRP</i>), который позволяет порту динамически становится членом VLAN. По умолчанию протокол GVRP отключен (<i>Disabled</i>).
Ingress Check	Позволяет включить (<i>Enabled</i>) функцию фильтрации входящего трафика. При этом порт будет сравнивать метку VID в пришедшем пакете с PVID данного порта. Если они не совпадают – пакет отбрасывается. Значение <i>Disabled</i> отключает фильтрацию входящего трафика.
Acceptable Frame Type	Показывает тип кадров, которые разрешено принимать порту. При выборе опции <i>Tagged_Only</i> порту будет разрешено принимать только маркированные кадры VLAN, а при выборе <i>Admit_All</i> – и маркированные, и немаркированные. Значение по умолчанию <i>Tagged_Only</i> .

PVID	<p>В таблице GVRP Table в данном поле указан текущий идентификатор PVID порта. По умолчанию все порты коммутатора входят в default VLAN с VID = 1.</p> <p>Идентификатор PVID используется для тегирования исходящих немаркированных пакетов и при принятии решения о продвижении входящих пакетов. Если порт настроен как tagged и принимает немаркированный пакет, то он добавит в заголовок пакета тег 802.1Q, используя PVID в качестве VID в теге. Когда пакет приходит по адресу назначения, то принявшее его устройство использует PVID для принятия решения о продвижении пакета.</p> <p>Если пакет приходит на порт, на котором включена функция фильтрации входящего трафика, то порт сравнивает VID пакета со своим PVID. Если они не равны, пакет отбрасывается, иначе порт принимает пакет.</p>
------	---

Управление трафиком (контроль широковещательной/ групповой рассылки)

Используйте меню **Traffic Control** для включения или отключения функции контроля широковещательной/групповой рассылки и установки порогового значения количества принимаемых пакетов широковещательной/групповой рассылки и пакетов DLF (Destination Look Up Failure). Настройка контроля трафика выполняется для отдельных портов.

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

Traffic Control Table				
Port	Broadcast Storm	Multicast Storm	Destination Lookup Fail	Threshold
1	Disabled	Disabled	Disabled	128
2	Disabled	Disabled	Disabled	128
3	Disabled	Disabled	Disabled	128
4	Disabled	Disabled	Disabled	128
5	Disabled	Disabled	Disabled	128
6	Disabled	Disabled	Disabled	128
7	Disabled	Disabled	Disabled	128
8	Disabled	Disabled	Disabled	128
9	Disabled	Disabled	Disabled	128
10	Disabled	Disabled	Disabled	128
11	Disabled	Disabled	Disabled	128
12	Disabled	Disabled	Disabled	128
13	Disabled	Disabled	Disabled	128
14	Disabled	Disabled	Disabled	128
15	Disabled	Disabled	Disabled	128
16	Disabled	Disabled	Disabled	128
17	Disabled	Disabled	Disabled	128
18	Disabled	Disabled	Disabled	128
19	Disabled	Disabled	Disabled	128
20	Disabled	Disabled	Disabled	128
21	Disabled	Disabled	Disabled	128
22	Disabled	Disabled	Disabled	128
23	Disabled	Disabled	Disabled	128
24	Disabled	Disabled	Disabled	128

Рисунок 4-25 Меню Traffic Control Settings

Контроль трафика используется для предотвращения «штормовой» рассылки широковещательных/ групповых пакетов или ARP-запросов, которая возникает в результате образования маршрутной петли в сети. Контроль **Destination Lookup Failure** используется для предотвращения «штормовой» рассылки пакетов, MAC-адрес назначения которых не найден в адресной таблице коммутатора, и поэтому эти пакеты должны быть переданы на все порты коммутатора или на все порты VLAN.

Для настройки контроля трафика в поле **Unit** выберите идентификатор нужного коммутатора в составе стека. С помощью полей **Broadcast Storm** (широковещательная рассылка), **Multicast Storm** (групповая рассылка) и **Destination Unknown** (неизвестен адрес назначения) можно включить (*Enabled*) или отключить (*Disabled*) контроль соответствующей рассылки. Параметр **Threshold** определяет пороговое значение количества принятых пакетов (в Кбит/с), при котором включается контроль, и коммутатор ограничивает принятие большего количества пакетов. Значение **Threshold** находится в пределах от 0 до 255 пакетов. Значение по умолчанию 128.

Настройка функции Port Security

Коммутатор позволяет заблокировать динамическое изучение MAC-адресов для указанного диапазона портов таким образом, что текущий MAC-адрес источника, введенный в адресную таблицу, невозможно будет изменить до тех пор, пока порт не будет разблокирован. Порт можно заблокировать, выбрав опцию *Disabled* из выпадающего меню **Learn**<*Disabled*> и нажав кнопку *Apply*.

Запрет изучения портом MAC-адресов обеспечивает дополнительную безопасность, так как предотвращает получение доступа к сети неавторизованных компьютеров через заблокированные порты. Если компьютер с неизвестным коммутатору MAC-адресом попытается передать пакет через заблокированный порт, то пакет будет отброшен.

Port Security Settings						
Unit	From	To	Admin State	Max.Addr(0-64)	Mode	Apply
1	Port 1	Port 1	Disabled	0	DeleteOnReset	Apply

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

Рисунок 4-25 Настройка функции Port Security

Нажмите *Apply*, чтобы изменения вступили в силу.

Параметры для настройки:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке при объединении коммутаторов в стек.
From/To	Группа последовательно пронумерованных портов, подлежащих настройке.
Admin State	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) функцию Port Security (заблокировать таблицу MAC-адресов для указанного порта).

Max. Addr (0-64)	Выберите максимальное количество изучаемых портом MAC-адресов.
Mode	Выберите DeleteOnTimeout для удаления из FDB (Forwarding Data Base, База данных продвижения) динамических записей с истекшим временем жизни. Выберите DeleteOnReset для удаления всех записей из FDB, включая статические записи, при сбросе системы или перезагрузке.

Настройка качества сервиса QoS

Понятие QoS

Коммутатор DGS-3324SR поддерживает очереди приоритетов 802.1p. В коммутаторе имеется 7 очередей приоритетов. Эти очереди нумеруются от 0 - очередь с наименьшим приоритетом - до 6 - очередь с наивысшим приоритетом. Восемь очередей приоритетов, определенных в стандарте IEEE 802.1p (от 0 до 7), ставятся в соответствие аппаратным очередям коммутатора следующим образом:

- Приоритет 0 назначается в очередь коммутатора Q2.
- Приоритет 1 назначается в очередь коммутатора Q0.
- Приоритет 2 назначается в очередь коммутатора Q1.
- Приоритет 3 назначается в очередь коммутатора Q3.
- Приоритет 4 назначается в очередь коммутатора Q4.
- Приоритет 5 назначается в очередь коммутатора Q5.
- Приоритет 6 назначается в очередь коммутатора Q6.
- Приоритет 7 назначается в очередь коммутатора Q6.

При использовании алгоритма строгой очереди приоритетов вначале обслуживаются все пакеты из очереди с наивысшим приоритетом. При этом пока более приоритетная очередь не опустеет, пакеты из менее приоритетных очередей передаваться не будут.

При использовании взвешенного циклического алгоритма для каждой очереди приоритетов задается ее «вес», который определяет количество обслуживаемых за один раз пакетов в этой очереди. Если существует 8 очередей CoS от А до Н, и им соответствуют «веса» от 8 до 1, то очереди будут обслуживаться в следующем порядке: А1, В1, С1, D1, E1, F1, G1, H1, А2, В2, С2, D2, E2, F2, G2, А3, В3, С3, D3, E3, F3, А4, В4, С4, D4, E4, А5, В5, С5, D5, А6, В6,С6, А7, В7, А8, А1, В1, С1, D1, E1, F1, G1, H1.

Если каждая очередь CoS имеет одинаковое значение «веса», то взвешенный циклический алгоритм обслуживания очередей работает как обычный циклический алгоритм.

Если значение «веса» какой-либо очереди равно 0, то коммутатор будет обслуживать очередь до тех пор, пока она не опустеет. Очереди с «весом» не равным 0 будут обслуживаться по обычному взвешенному циклическому алгоритму.

Помните, что коммутатор DGS-3324SR поддерживает 8 очередей приоритетов (и 7 классов сервиса CoS) для каждого порта.

Контроль полосы пропускания

Контроль полосы пропускания обычно используется для ограничения скорости передачи и приема данных для указанного порта. В папке **Configuration** откройте папку **QoS** и нажмите на ссылку **Bandwidth Control**, появится следующее окно.

Bandwidth Settings						
Unit	From	To	Type	no_limit	Rate	Apply
1	Port 1	Port 1	Both	Disabled	1	Apply

Port Bandwidth Table		
Port	RX Rate (Mbit/sec)	TX Rate (Mbit/sec)
1	no_limit	no_limit
2	no_limit	no_limit
3	no_limit	no_limit
4	no_limit	no_limit
5	no_limit	no_limit
6	no_limit	no_limit
7	no_limit	no_limit
8	no_limit	no_limit
9	no_limit	no_limit
10	no_limit	no_limit
11	no_limit	no_limit
12	no_limit	no_limit
13	no_limit	no_limit
14	no_limit	no_limit
15	no_limit	no_limit
16	no_limit	no_limit
17	no_limit	no_limit
18	no_limit	no_limit
19	no_limit	no_limit
20	no_limit	no_limit
21	no_limit	no_limit
22	no_limit	no_limit
23	no_limit	no_limit
24	no_limit	no_limit

Рисунок 4-27 Меню Bandwidth Settings

Параметры для настройки:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке при объединении коммутаторов в стек.
From/To	Группа последовательно пронумерованных портов, подлежащих настройке.
Type	Определяет, будет ли влиять ограничение полосы пропускания на входящий трафик (RX), исходящий (TX) или на оба вида трафика (Both).
no_limit	Позволяет снять ограничение полосы пропускания (Enabled) или установить его (Disabled).
Rate	Позволяет ввести скорость передачи данных в Мбит/с, которой будет ограничена пропускная способность данного порта.

Нажмите *Apply*, чтобы изменения вступили в силу. Результаты настройки полосы пропускания показаны в таблице **Port Bandwidth Table**.

Выбор алгоритма обслуживания очередей

Данное меню позволяет выбрать алгоритм обслуживания очередей приоритетов: **Weighted Fair** (взвешенный циклический алгоритм) или **Strict** (строгая очередь приоритетов). В папке **Configuration** откройте папку **QoS** и нажмите на ссылку **QoS Scheduling Mechanism**, появится следующее меню.

Scheduling Mechanism Configuration	
Scheduling Mechanism	Strict
Apply	
QoS Scheduling Mechanism Table	
Class ID	Mechanism
Class-0	Strict
Class-1	Strict
Class-2	Strict
Class-3	Strict
Class-4	Strict
Class-5	Strict
Class-6	Strict

Рисунок 4-28 Меню выбора алгоритма обслуживания очередей

После выбора нажмите кнопку *Apply*, чтобы изменения вступили в силу.

Параметр	Описание
Strict	Алгоритм строгой очереди приоритетов. Сначала обслуживается очередь с наивысшим приоритетом. При этом пока более приоритетная очередь не опустеет, пакеты из менее приоритетных очередей передаваться не будут.
Weight Fair	Взвешенный циклический алгоритм обслуживания очередей приоритетов.

Настройка алгоритма обслуживания очередей

Качество сервиса QoS можно настроить путем изменения параметров алгоритм обслуживания аппаратных очередей коммутатора. При внесении изменений в реализацию QoS необходим тщательный анализ влияния этих изменений на сетевой трафик с наименьшим приоритетом. Изменение параметров алгоритма обслуживания очередей может привести к недопустимому уровню потерь пакетов или значительным задержкам при передаче. Если Вы решили изменить настройки QoS, то необходимо провести мониторинг производительности сети, особенно при максимальной загрузке, поскольку могут мгновенно возникнуть узкие места в сети, если настройки QoS непригодны. В папке **Configuration** выберите папку **QoS** и нажмите на ссылку **QoS Output Scheduling**, появится следующее окно.

QoS Output Scheduling Configuration	
	Max. Packets
Class-0	<input type="text" value="1"/>
Class-1	<input type="text" value="2"/>
Class-2	<input type="text" value="3"/>
Class-3	<input type="text" value="4"/>
Class-4	<input type="text" value="5"/>
Class-5	<input type="text" value="6"/>
Class-6	<input type="text" value="7"/>

Рисунок 4-29 Настройка алгоритма QoS

После назначения приоритетов портам коммутатора можно поставить в соответствие каждому из 7 уровней приоритетов 802.1p данный класс сервиса (от Class-0 до Class-6).



Примечание: Числа от 0 до 7 в настройках очередей коммутатора представляют собой приоритеты 802.1p. Не путайте их с номерами портов.

Приоритеты 802.1p по умолчанию

Коммутатор позволяет определить для каждого порта коммутатора приоритет 802.1p, используемый по умолчанию. В папке **Configuration** выберите папку **QoS** и нажмите на ссылку **802.1p Default Priority**, появится следующее окно.

Port Default Priority assignment				
Unit	From	To	Priority(0~7)	Apply
1	Port 1	Port 1	0	Apply

The Port Priority Table	
Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0

Рисунок 4-30 Определенные для портов приоритеты 802.1p

Эта страница позволяет назначить приоритет 802.1p по умолчанию любому порту коммутатора. Очереди приоритетов нумеруются от 0 (низший приоритет) до 7 (наивысший приоритет). Нажмите *Apply*, чтобы изменения вступили в силу.

Приоритет пользователя 802.1p

Коммутатор DGS-3324SR позволяет назначить каждый из приоритетов 801.1p в определенную очередь приоритетов коммутатора. В папке **Configuration** выберите папку **QoS** и нажмите на ссылку **802.1p User Priority**, появится следующее окно.

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

Рисунок 4-31 Соответствие очередей приоритетов 802.1p и классов сервиса

После назначения приоритетов портам коммутатора, можно поставить в соответствие каждому из 8 уровней приоритетов 802.1p определенный класс сервиса (от Class-0 до Class -6). Нажмите *Apply*, чтобы изменения вступили в силу.

Настройка сегментации трафика

Таблица сегментации трафика используется для ограничения трафика от одного порта к другим портам в пределах одного коммутатора (при работе в автономном режиме) или к группе портов другого коммутатора в составе стека. Техника сегментации трафика похожа на использование VLAN для сегментации сети и ограничения трафика между сегментами, но она менее гибкая. Таблица сегментации трафика предоставляет дополнительное средство управления трафиком без загрузки центрального процессора. В папке **Configuration** выберите папку **QoS** и нажмите на ссылку **Traffic Segmentation**, появится следующее окно.

Unit	Port	Configuration	Setup
1	Port1	<input type="button" value="View"/>	<input type="button" value="Setup"/>

Current Traffic Segmentation Table	
Unit	Port Map
1	1-3, 5-7, 9-24
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Рисунок 4-32 Таблица сегментации трафика

Нажмите кнопку **Setup**, появится меню **Setup Forwarding Ports**.

Unit	Port	Apply
1	Port 1	Apply

Setup Forwarding ports

Unit	1																																																
Forward Port	<table border="1"> <thead> <tr> <th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24																										
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																										

Apply

[View Settings of Unit 1 Port 1](#)

Рисунок 4-33 Меню Setup Forwarding ports

В данном меню можно указать, какому порту выбранного коммутатора в составе стека будет позволено передавать пакеты на другие указанные порты какого-либо коммутатора в стеке.

Настройка сегментации трафика на DGS-3324SR выполняется в два этапа. Вначале выбирается коммутатор в стеке, а затем порт этого коммутатора. Далее выбирается второй коммутатор в составе стека и порты этого коммутатора (или другие порты того же коммутатора), которым будет разрешено принимать пакеты от выбранного на первом этапе коммутатора и его порта.

Например, выбирается коммутатор 1 и его порт 1 в качестве передающего порта. Выбираются порты 1-3, 5-7 и 9-24, и им разрешается принимать пакеты от порта 1.

Нажмите кнопку **Apply** для занесения выбранных портов в таблицу сегментации трафика коммутатора.

Выпадающее меню **Unit** в верхней части окна позволяет выбрать коммутатор в составе стека по его идентификатору Unit ID. Выпадающее меню **Port** позволяет выбрать порт на данном коммутаторе. Это порт является источником пакетов.

Выпадающее меню **Unit** под заголовком **Setup Forwarding ports** позволяет выбрать коммутатор в составе стека по его идентификатору Unit ID. В поле **Forward Port** можно указать, каким портам выбранного коммутатора будет позволено принимать пакеты от выбранного ранее порта.

Нажмите кнопку **Apply** для занесения выбранных портов в таблицу сегментации трафика коммутатора.

Сервер System Log

Можно назначить до 4 серверов **System Log**, которым коммутатор будет отправлять сообщения SysLog (журнала событий). В папке **Configuration** нажмите на ссылку **System Log Server**, появится следующее меню.

Index	Server IP	Status	Delete
1	10.53.13.94	Enabled	<input type="checkbox"/>

Рисунок 4-34 Список серверов System Log


Параметры, задаваемые для добавления и редактирования настроек сервера **System Log Server** те же самые. Смотрите таблицу, приведенную ниже.

Configure System Log Server	
Index(1-4)	<input type="text" value="0"/>
Server IP	<input type="text" value="0.0.0.0"/>
Severity	Warning ▾
Facility	Local0 ▾
UDP Port(514 or 6000-65535)	<input type="text" value="0"/>
Status	Disabled ▾
<input type="button" value="Apply"/>	
Show All System Log Servers	

Рисунок 4-35 Добавление сервера System Log

Параметр	Описание
Index	Номер записи, содержащей параметры ведения журнала событий на сервере (1-4).
Server IP	Введите IP-адрес сервера, который будет получать сообщения Syslog (журнала событий).
Severity	Выберите тип отправляемых на сервер сообщений: <i>Warning</i> (предупреждение), <i>Information</i> (информация) или <i>All</i> (все).
Facility	Некоторым процессам операционных систем присваивается значение Facility. Процессы, которым не присвоено явно значение Facility, могут использовать «локальные» значения Facility или «пользовательские» Facility. Распределенные значения Facility приведены ниже. Жирным шрифтом выделены поддерживаемые коммутатором значения Facility. Код Facility 0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog line printer subsystem 7 network news subsystem 8 UUCP subsystem 9 clock daemon 10 security/authorization messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon 16 local use 0 (local0) 17 local use 1 (local1) 18 local use 2 (local2) 19 local use 3 (local3) 20 local use 4 (local4) 21 local use 5 (local5) 22 local use 6 (local6) 23 local use 7 (local7)
UDP Port (514 or 6000 – 65535)	Введите номер порта UDP, используемого для отправки сообщений SysLog. Значение по умолчанию 514.

Status Можно включить (*Enabled*) или отключить (*Disabled*) данную функцию.

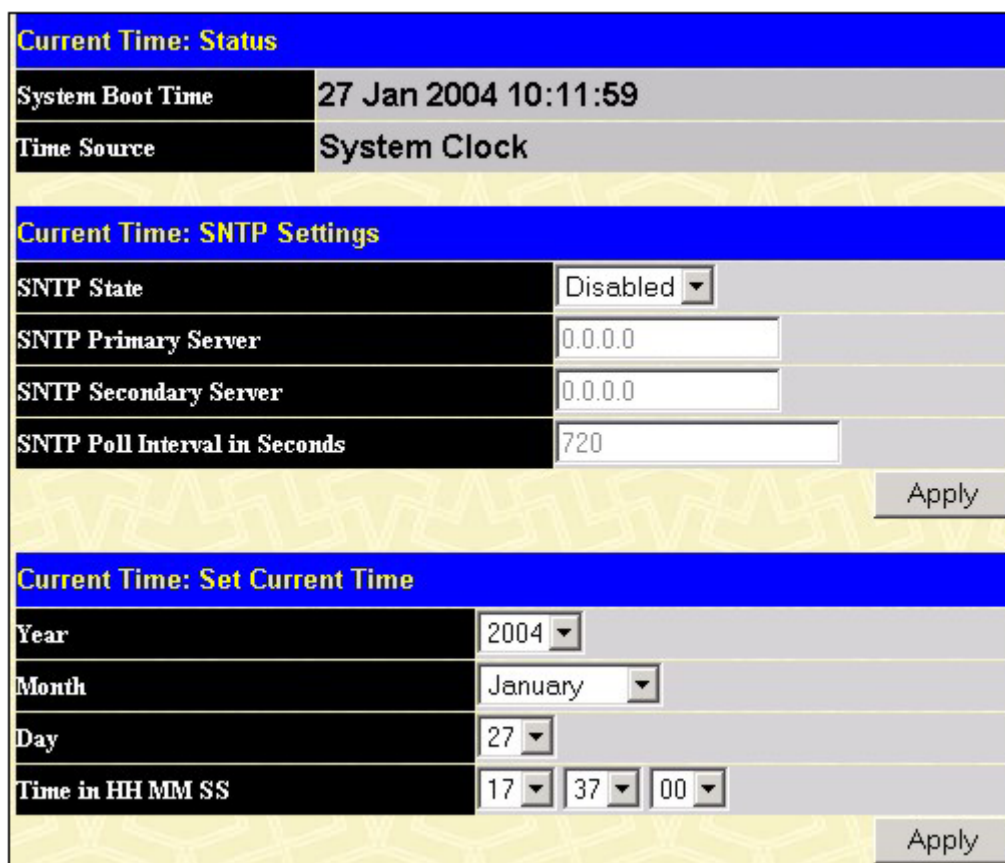
Нажмите *Apply*, чтобы изменения вступили в силу. Для удаления записи из списка серверов System Log нажмите  в колонке **Delete** рядом с удаляемой записью. Для возврата к списку серверов System Log в окне **Current System Log Servers** нажмите на ссылку [Show All System Log Servers](#).

Настройка параметров SNTP

Коммутатор DGS-3324SR позволяет настроить протокол SNTP (Simple Network Time Protocol, Простой протокол сетевого времени) {адаптированный протокол Network Time Protocol (NTP)}, используя следующие меню.

Настройка системного времени

Для настройки системного времени на коммутаторе в папке **Configuration** откройте папку **SNTP** и нажмите на ссылку **Time Setting**, появится следующее окно.



The screenshot shows a web-based configuration interface for SNTP settings. It is divided into three main sections:

- Current Time: Status**: Shows 'System Boot Time' as 27 Jan 2004 10:11:59 and 'Time Source' as System Clock.
- Current Time: SNTP Settings**: Contains four fields: 'SNTP State' (set to Disabled), 'SNTP Primary Server' (0.0.0.0), 'SNTP Secondary Server' (0.0.0.0), and 'SNTP Poll Interval in Seconds' (720). An 'Apply' button is at the bottom right.
- Current Time: Set Current Time**: Contains four fields: 'Year' (2004), 'Month' (January), 'Day' (27), and 'Time in HH MM SS' (17:37:00). An 'Apply' button is at the bottom right.

Рисунок 4-36 Меню настройки системного времени

Параметры для настройки:

Параметр	Описание
System Boot Time	Показывает время, прошедшее с момента последней загрузки.
Time Source	Источник настроек системного времени - SNTP или встроенные системные часы.
SNTP State	Включает (<i>Enabled</i>) или отключает (<i>Disabled</i>) сервис SNTP.
SNTP Primary Server	Введите IP-адрес основного сервера SNTP, который будет предоставлять необходимую информацию.
SNTP Secondary Server	Введите IP-адрес дополнительного сервера SNTP, который будет предоставлять необходимую информацию в случае недоступности основного сервера

SNTP Polling Interval	Задаёт интервал между запросами на обновление информации SNTP. Интервал опроса находится в пределах от 30 до 99 999 секунд.
Year	Выберите год для установки даты вручную.
Month	Выберите месяц для установки даты вручную.
Day	Выберите день для установки даты вручную.
Time in HH MM SS	Установите системное время в 24-х часовом формате.

Нажмите *Apply*, чтобы изменения вступили в силу.

Настройка часового пояса и автоматического перехода на летнее время

Следующее меню позволяет установить часовой пояс и настроить параметры автоматического перехода на летнее время для протокола SNTP. В папке **Configuration** откройте папку **SNTP** и нажмите на ссылку **Time Zone and DST**.

Time Zone and DST Settings

Daylight Saving Time State: Disabled

Daylight Saving Time Offset in Minutes: 60

Time Zone Offset from GMT in +/-HH:MM: + 00 00

DST Repeating Settings

From: Which Day: First

From: Day of Week: Sunday

From: Month: April

From: time in HH MM: 00 00

To: Which Day: Last

To: Day of Week: Sunday

To: Month: October

To: time in HH MM: 00 00

DST Annual Settings

From: Month: April

From: Day: 29

From: time in HH MM: 00 00

To: Month: October

To: Day: 12

To: Time in HH MM: 00 00

Apply

Рисунок 4-37 Настройка часового пояса и перехода на летнее время

Параметры для настройки:

Параметр	Описание
Daylight Saving Time State	Включает или отключает переход на летнее время.
Daylight Saving Time Offset in minutes	Сдвиг времени при переходе на летнее время – 30, 60, 90 или 120 минут.

Time Zone Offset from GMT in +/- HH:MM	Сдвиг времени (+/-) относительно GMT.
Меню DST Repeating Settings	
From: Which Day	Меню DST Repeating Settings позволяет настроить переход на летнее время по формуле повторяющегося перехода. Например, можно указать начало перехода на субботу второй недели апреля, а конец – на воскресенье последней недели октября. Должно быть From: Which Week . Выберите неделю месяца, когда начинается переход на летнее время.
From: Day of Week	Выберите день недели, когда начинается переход на летнее время.
From: Month	Выберите месяц, когда начинается переход на летнее время.
From: time HH:MM	Выберите время дня в 24-х часовом формате ЧЧ:ММ, когда начнется переход на летнее время.
To: Which Day	Должно быть To: Which Week . Выберите неделю месяца, когда начинается обратный переход.
To: Day of Week	Выберите день недели, когда начинается обратный переход.
To: Month	Выберите месяц, когда начинается обратный переход.
To: time HH:MM	Выберите время дня в 24-х часовом формате ЧЧ:ММ, когда начнется обратный переход.
Меню DST Annual Settings	
From: Month	Меню DST Annual Settings позволяет задать точную дату перехода на летнее время. Например, можно указать начало перехода на 3 апреля, а конец – на 14 октября. Выберите месяц, когда начинается ежегодный переход на летнее время.
From: Day	Выберите определенную дату (день месяца), когда начинается ежегодный переход на летнее время.
From: time HH:MM	Выберите время дня в 24-х часовом формате ЧЧ:ММ, когда начнется ежегодный переход на летнее время.
To: Month	Выберите месяц, когда начнется обратный ежегодный переход.
To: Day	Выберите определенную дату (день месяца), когда начинается обратный ежегодный переход.
To: time HH:MM	Выберите время дня в 24-х часовом формате ЧЧ:ММ, когда начнется обратный ежегодный переход.

Нажмите *Apply*, чтобы изменения вступили в силу.

Настройка таблицы профилей доступа

Профили доступа позволяют установить критерии, определяющие, какие виды пакетов принимать, а какие отбрасывать на основании информации, содержащейся в заголовке пакета. Эти критерии могут быть определены для таких признаков, как VLAN, MAC-адрес или IP-адрес.

Процесс создание профиля доступа делится на 2 основные части. Во-первых, указывается какую часть или части кадра будет проверять коммутатор, например, MAC-адрес источника или IP-адрес назначения. Во-вторых, вводится условие, которое коммутатор будет использовать для определения выполняемых над кадром действий (принять или отбросить). Весь процесс описан ниже.

Откройте папку **Configuration** и нажмите на ссылку **Access Profile Table**, появится окно **Access Profile Table**.

Access Profile Table			
Profile ID	Type	Access Rule	Delete
2	IP	Modify	X

Рисунок 4-38 Таблица профилей доступа

Для добавления новой записи в таблицу профилей доступа нажмите кнопку *Add*. Появится меню **Access Profile Configuration**, показанное ниже. Существует два вида меню **Access Profile Configuration** – для настройки профиля доступа **Ethernet** (на основе MAC-адреса) и для настройки профиля доступа по **IP-адресу**. Используя выпадающее меню **Type** можно выбрать необходимый тип профиля доступа. После настройки профиля доступа нажмите кнопку *Apply*. Ниже показано меню настройки профиля доступа **Ethernet**.

Рисунок 4-39 Настройка профиля доступа Ethernet.

Настройте следующие параметры маски профиля доступа:

Параметр	Описание
Profile ID (1-8)	Введите уникальный идентификационный номер данного профиля. ID может принимать значения от 1 до 8.
Type	Выберите тип профиля: <i>Ethernet</i> или <i>IP</i> . Вид меню изменится в соответствии с требованиями для выбранного типа профиля. Выберите опцию <i>Ethernet</i> , чтобы коммутатор исследовал часть заголовка 2-ого уровня каждого пакета. Выберите опцию <i>IP</i> , чтобы коммутатор исследовал IP-адрес в заголовке каждого кадра.
VLAN	Выберите эту опцию для того, чтобы коммутатор исследовал поле VLAN заголовка каждого пакета и использовал его в качестве критерия или части критерия при принятии решения о продвижении пакетов.
Source MAC	Source MAC Mask – введите маску MAC-адреса для MAC-адреса источника.
Destination MAC	Destination MAC Mask - введите маску MAC-адреса для MAC-адреса назначения.
802.1p	Выберите эту опцию для того, чтобы коммутатор исследовал значение приоритета 802.1p в заголовке каждого пакета и использовал его в качестве критерия или части критерия при принятии решения о продвижении пакетов.
Ethernet Type	Выберите эту опцию для того, чтобы коммутатор исследовал значение поля Ethernet Type в заголовке каждого кадра.
Port	Профиль доступа можно настроить на основе портов, введя значение в данное поле. Можно ввести <i>all</i> , что означает все порты всех коммутаторов стека, или ввести номер одного или нескольких портов. Диапазон портов задается указанием

порядкового номера первого коммутатора диапазона и номера начального порта на этом коммутаторе, разделяемых двоеточием. Затем следует номер последнего коммутатора диапазона и номер последнего порта на данном коммутаторе (также разделяются двоеточием). Начальный и конечный порты диапазона разделяются тире. Например, 1:3 задает коммутатор 1 и порт 3. 2:4 задает коммутатор 2 и порт 4. 1:3 – 2:4 определяет все порты между коммутатором 1 и его портом 3 и коммутатором 2 и его портом 4 – по порядку.

Ниже показано меню настройки профиля доступа по IP-адресу.

Рисунок 4-40 Настройка профиля доступа IP

Настройте следующие параметры маски профиля доступа:

Параметр	Описание
Profile ID (1-8)	Введите уникальный идентификационный номер данного профиля. ID может принимать значения от 1 до 8.
Type	Выберите тип профиля: <i>Ethernet</i> или <i>IP</i> . Вид меню изменится в соответствии с требованиями для выбранного типа профиля. Выберите опцию <i>Ethernet</i> , чтобы коммутатор исследовал часть заголовка 2-ого уровня каждого пакета. Выберите опцию <i>IP</i> , чтобы коммутатор исследовал IP-адрес в заголовке каждого кадра.
VLAN	Выберите эту опцию для того, чтобы коммутатор исследовал поле VLAN заголовка каждого пакета и использовал его в качестве критерия или части критерия при принятии решения о продвижении пакетов.
Source IP Mask	Введите маску IP-адреса для IP-адреса источника.
Destination IP Mask	Введите маску IP-адреса для IP-адреса назначения.
DSCP	Выберите эту опцию для того, чтобы коммутатор исследовал

Protocol

поле DiffServ Code Point (DSCP) в заголовке каждого пакета и использовал его в качестве критерия или части критерия при принятии решения о продвижении пакетов.

Выберите эту опцию для того, чтобы коммутатор исследовал поле типа протокола в заголовке каждого кадра.

Вы должны указать исследуемые протоколы, руководствуясь следующими принципами:

Выберите опцию **ICMP** для того, чтобы коммутатор исследовал поле ICMP (Internet Control Message Protocol) в заголовке каждого кадра.

Выберите **Type** для задания профиля доступа по значению типа ICMP-сообщения или выберите **Code** для задания профиля доступа по значению кода ICMP.

Выберите опцию **IGMP** для того, чтобы коммутатор исследовал поле IGMP (Internet Group Management Protocol) в заголовке каждого кадра.

Выберите **Type** для задания профиля доступа по значению типа IGMP.

Выберите опцию **TCP** для использования номера порта TCP, содержащегося в заголовке входящего пакета, в качестве критерия при принятии решения о продвижении пакета. Требуется также задать маску порта источника и/или маску порта назначения. Кроме того, можно указать, какие флаги пакета обрабатывать. Флаги – это часть пакета и определяют, какие действия нужно произвести с пакетом. Можно запретить определенные типы пакетов, выбрав необходимые флаги TCP. Доступны флаги **urg** (urgent), **ack** (acknowledgment), **psh** (push), **rst** (rest), **syn** (synchronize), **fin** (finish).

src port mask - укажите маску порта TCP для порта источника в шестнадцатеричном виде (hex 0x0-0xffff).

dest port mask - укажите маску порта TCP для порта приемника в шестнадцатеричном виде (hex 0x0-0xffff).

Выберите опцию **UDP** для использования номера порта UDP, содержащегося в заголовке входящего пакета, в качестве критерия при принятии решения о продвижении пакета. Требуется также задать маску порта источника и/или маску порта назначения.

src port mask - укажите маску порта UDP для порта источника в шестнадцатеричном виде (hex 0x0-0xffff)

dest port mask - укажите маску порта UDP для порта приемника в шестнадцатеричном виде (hex 0x0-0xffff)

protocol id – укажите маску порта 4-ого уровня для порта назначения в шестнадцатеричном виде (hex 0x0-0xffffffff)

Port

Профиль доступа можно настроить на основе портов, введя значение в данное поле. Можно ввести *all*, что означает все порты всех коммутаторов стека, или ввести номер одного или нескольких портов. Диапазон портов задается указанием порядкового номера первого коммутатора диапазона и номера начального порта на этом коммутаторе, разделяемых двоеточием. Затем следует номер последнего коммутатора диапазона и номер последнего порта на данном коммутаторе (также разделяются двоеточием). Начальный и конечный порты диапазона разделяются тире. Например, 1:3 задает коммутатор 1 и порт 3. 2:4 задает коммутатор 2 и порт 4. 1:3 – 2:4 определяет все порты между коммутатором 1 и его портом 3 и коммутатором 2 и его портом 4 – по порядку.

Создание правила для ранее определенного профиля доступа:

В папке **Configuration** нажмите на ссылку **Access Profile Table**, чтобы открыть таблицу профилей доступа **Access Profile Table**. Под заголовком **Access Rule** нажмите кнопку *Modify*, появится следующее окно.

Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	IP	1	View	

Рисунок 4-41 Таблица созданных правил доступа


Для создания нового правила нажмите кнопку *Add*. Для удаления правила доступа нажмите в колонке **Delete** рядом с удаляемой записью.

Рисунок 4-42 Настройка правила доступа (по профилю IP)

Задайте следующие параметры правила для профиля доступа:

Параметр	Описание
Profile ID	Идентификационный номер данного профиля доступа.
Mode	Выберите опцию Permit для того, чтобы коммутатор передавал пакеты, соответствующие профилю доступа. Выберите опцию Deny для того, чтобы коммутатор отбрасывал пакеты, не соответствующие профилю доступа.
Access ID	Введите уникальный идентификационный номер для данного правила доступа. Access ID может принимать значения от 1 до 50.
Type	Показывает тип данного профиля доступа: Ethernet или IP. По профилю Ethernet коммутатор проверяет заголовок 2-ого уровня в каждом кадре. По

Priority (0-7)	профилю IP коммутатор проверяет IP-адрес в заголовке каждого кадра. Выберите эту опцию для того, чтобы коммутатор использовал введенное в соседнем поле значение приоритета 802.1p для пакетов, которые удовлетворяют заданному критерию. Параметр Priority может принимать значения от 0 - наименьший приоритет - до 7 - наивысший приоритет.
Replace Dscp (0-63)	Выберите эту опцию для того, чтобы коммутатор заменял значение DSCP (в пакетах, удовлетворяющих заданному критерию) на значение, введенное в соседнем поле.
VLAN name	Позволяет ввести имя одной из ранее настроенных VLAN.
Source IP	Введите IP-адрес источника.
Destination IP	Введите IP-адрес назначения.
DSCP (0-63)	Позволяет ввести значение DSCP, которое коммутатор будет использовать в качестве критерия или части критерия при проверке поля DiffServ Code Point (DSCP) в заголовке каждого пакета и при принятии решения о продвижении пакета. Допустимые значения от 0 до 63.
Protocol	Позволяет изменить тип протокола, который был ранее указан при создании профиля доступа. В приведенном выше примере был выбран протокол IGMP, поэтому можно изменить параметры IGMP для данного профиля доступа.

Для просмотра параметров ранее созданного правила нажмите  в таблице профилей доступа, появится следующее окно:

Access Rule Display	
Profile ID	2
Access ID	1
Mode	Permit
Type	IP
Priority	-----
Replace Dscp	-----
Vlan Name	Trinity
Source IP	10.0.0.0
Destination IP	11.1.1.0
Dscp	7
Protocol	IGMP-- type:2
Show All Access Rule Entries	

Рисунок 4-43 Окно Access Rule Display (для профиля IP)

Для настройки правила доступа по профилю Ethernet откройте таблицу профилей доступа (окно **Access Profile Table**, показанное на рисунке 4-38) и нажмите *Modify* для записи с профилем Ethernet. Появится следующее окно:

Add

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	Ethernet	2	View	

[Show All Access Profile Entries](#)

Рисунок 4-44 Таблица созданных правил доступа

Для удаления правила доступа нажмите в колонке **Delete** рядом с удаляемой записью. Для создания нового правила нажмите кнопку *Add*:


Access Rule Configuration	
Profile ID	3
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID	1
Type	Ethernet
Priority(0-7)	<input type="checkbox"/> 0 <input type="checkbox"/> replace priority
Replace Dscp(0-63)	<input type="checkbox"/> 0
Vlan Name	
Source Mac	00-00-00-00-00-00
Destination Mac	00-00-00-00-00-00
802.1p(0-7)	0
Ethernet Type	0000
<input type="button" value="Apply"/>	
Show All Access Rule Entries	

Рисунок 4-45 Настройка правила доступа (по профилю Ethernet)

Задайте следующие параметры правила для профиля доступа и нажмите *Apply*:

Параметр	Описание
Profile ID	Идентификационный номер данного профиля доступа.
Mode	Выберите опцию Permit для того, чтобы коммутатор передавал пакеты, соответствующие профилю доступа. Выберите опцию Deny для того, чтобы коммутатор отбрасывал пакеты, не соответствующие профилю доступа.
Access ID	Введите уникальный идентификационный номер для данного правила доступа. Access ID может принимать значения от 1 до 50.
Type	Показывает тип данного профиля доступа: Ethernet или IP. По профилю Ethernet коммутатор проверяет заголовок 2-ого уровня в каждом кадре. По профилю IP коммутатор проверяет IP-адрес в заголовке каждого кадра.
Priority (0-7)	Выберите эту опцию для того, чтобы коммутатор использовал введенное в соседнем поле значение приоритета 802.1p для пакетов, которые удовлетворяют заданному критерию. Параметр Priority может принимать значения от 0 - наименьший приоритет - до 7 - наивысший приоритет.

Replace Dscp (0-63)	Выберите эту опцию для того, чтобы коммутатор заменял значение DSCP (в пакетах, удовлетворяющих заданному критерию) на значение, введенное в соседнем поле.
VLAN name	Позволяет ввести имя одной из ранее настроенных VLAN.
Source MAC	Введите MAC-адрес источника.
Destination MAC	Введите MAC-адрес назначения.
802.1p (0-7)	Позволяет ввести значение приоритета 802.1p, с которым коммутатор будет сравнивать приоритет 802.1p пакета, и в случае их совпадения будет применено данное правило доступа.
Ethernet Type	Указывает, что данное правило доступа будет применяться только к пакетам с таким шестнадцатеричным значением (0x0 – 0xffff) в поле Ethernet Type заголовка пакета. Значение Ethernet Type можно ввести в шестнадцатеричном виде 0x0 – 0xffff, т.е. любая комбинация из букв a-f и цифр 0-9.

Для просмотра параметров ранее созданного правила нажмите  в таблице профилей доступа, появится следующее окно:

Access Rule Display	
Profile ID	2
Access ID	2
Mode	Permit
Type	Ethernet
Priority	-----
Replace Dscp	-----
Vlan Name	Trinity
Source Mac	-----
Destination Mac	-----
802.1p	-----
Ethernet Type	-----
Show All Access Rule Entries	

Рисунок 4-46 Окно Access Rule Display (для профиля Ethernet)

Управление доступом

Управление доступом к сети IEEE 802.1x на основе портов

Коммутатор DGS-3324SR реализует серверную сторону управления доступом к сети IEEE 802.1x на основе портов. Этот механизм предполагает, что только авторизованные пользователи или сетевые устройства получают доступ к ресурсам сети.

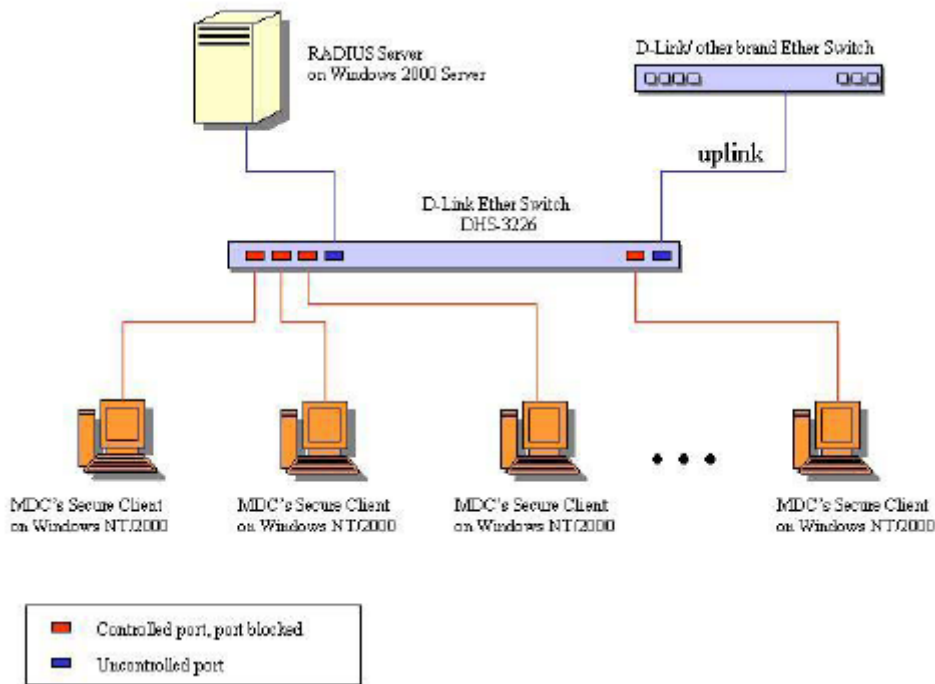


Рисунок 4-47 Типичная конфигурация 802.1x перед настройкой аутентификации пользователей

После прохождения пользователем процедуры аутентификации коммутатор разблокирует порт, к которому подключен пользователь, как показано на следующем рисунке.

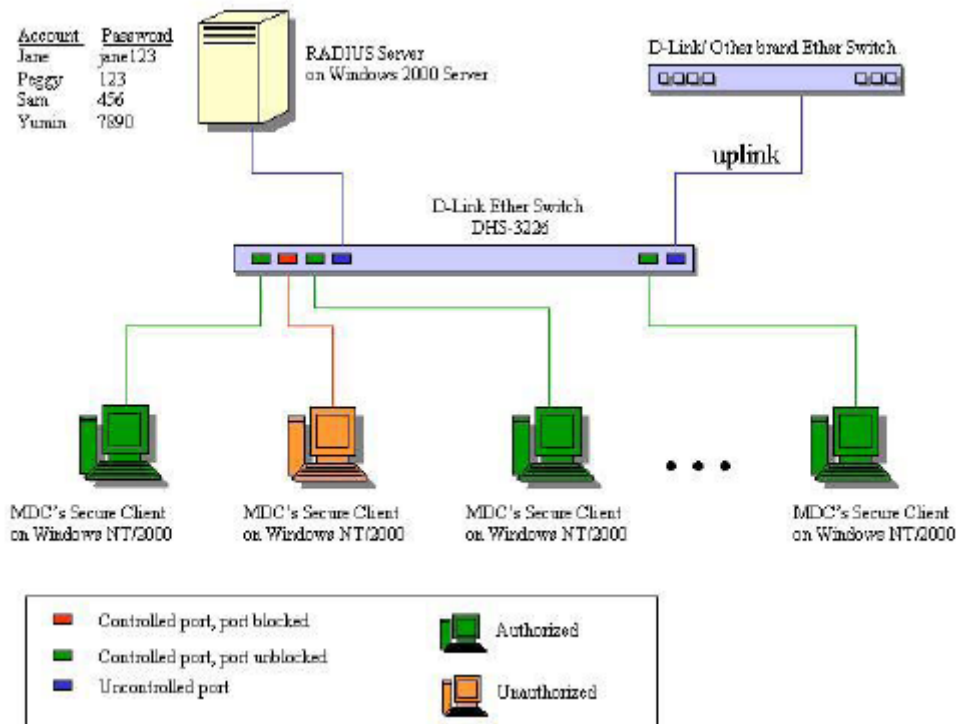


Рисунок 4-48 Типичная конфигурация 802.1x с аутентификацией пользователей

Информация о пользователе, включая учетную запись, пароль и некоторые параметры настройки, такие как IP-адрес и биллинговая информация, хранится на центральном сервере RADIUS.

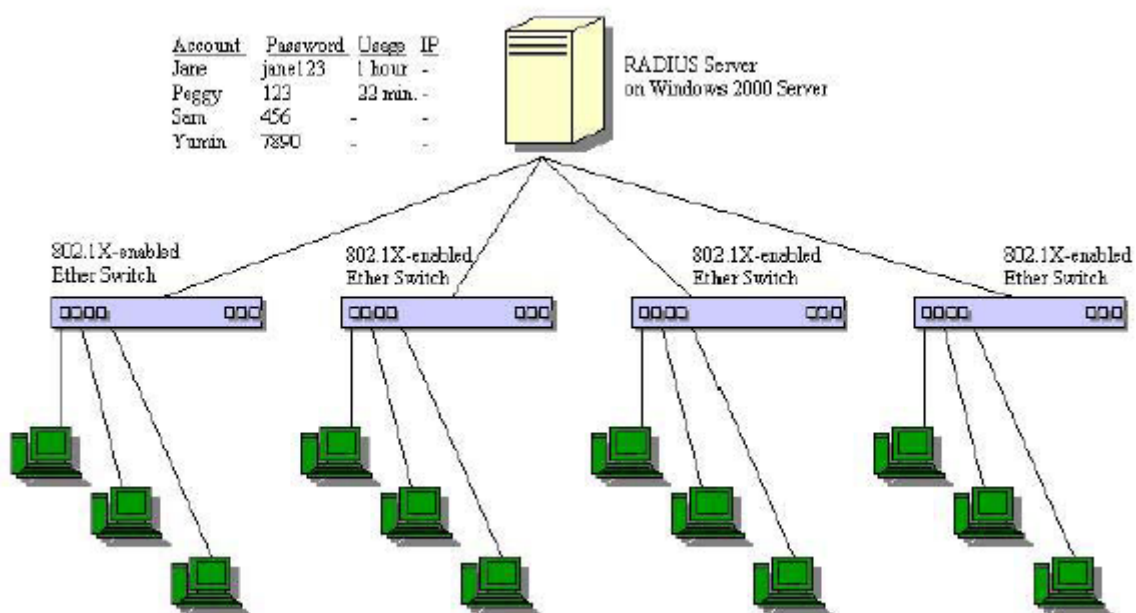


Рисунок 4-49 Типичная конфигурация сети с полной реализацией 802.1x

State Machine Name
Port Timers state machine
Authenticator PAE state machine
The Authenticator Key Transmit state machine
Reauthentication Timer state machine
Backend Authentication state machine
Controlled Directions state machine
The Receive state machine

Таблица 4-3 Соответствие стандарту IEEE 802.1x

Настройка аутентификации на коммутаторе

Для просмотра параметров аутентификации 802.1x на коммутаторе в папке **Configuration** откройте папку **Port Access Entity** и нажмите на ссылку **Configure Authenticator**, появится окно **802.1x Authenticator Settings**.

Unit: 1

802.1X Authenticator Settings

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

Рисунок 4-50 Таблица 802.1x Authenticator Settings

Для настройки аутентификации 802.1x на определенном порту нажмите на ссылку с номером порта под заголовком **Port**, появится следующее меню.

802.1X Authenticator Settings	
Unit	1
From	Port 1
To	Port 1
AdmDir	both
PortControl	forceAuthorized
TxPeriod	30
QuietPeriod	60
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled
Show Authenticators Setting for Unit 0 Apply	

Рисунок 4-51 Меню настройки аутентификации 802.1x на портах коммутатора

Параметры настройки 802.1x для порта:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке по его идентификатору Unit ID при объединении коммутаторов в стек.
From [] To [] AdmDir	Группа последовательно пронумерованных портов, подлежащих настройке. Выберите, будет ли неавторизованный порт осуществлять контроль над соединения только при приеме данных (<i>in</i>) или и при приеме, и передаче (<i>both</i>). Значение по умолчанию <i>both</i> .
Port Control	Показывает административный контроль над статусом авторизации порта. При выборе <i>forceAuthorized</i> порт переводится в состояние Authorized (авторизован), а при выборе <i>forceUnauthorized</i> в состояние Unauthorized (не авторизован). <i>Auto</i> означает, что в данном поле показывается результат процесса аутентификации – обмена пакетами аутентификации между клиентом, коммутатором и сервером аутентификации. Значение по умолчанию <i>forceAuthorized</i> .
Tx Period	Введите время ожидания ответа от пользователя перед отправкой пакетов EAP Request/Identity. Значение по умолчанию 30 секунд.
Quiet Period	Введите интервал времени между неудачной попыткой аутентификации и началом следующей попытки. Значение по умолчанию 60 секунд.
SuppTimeout	Введите время ожидания ответа от пользователя для всех пакетов EAP, кроме пакетов Request/Identity. Значение по умолчанию 30 секунд.
Server Timeout	Введите время ожидания ответа от сервера Radius. Значение по умолчанию 30 секунд.
Max Req	Введите максимальное количество попыток отправки пакетов пользователю. Значение по умолчанию 2.
ReAuthPeriod	Выберите интервал повторной аутентификации. Значение по умолчанию 3600 секунд.
ReAuth	Включите (<i>Enabled</i>) или отключите (<i>Disabled</i>) повторную аутентификацию.

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в таблицу **802.1x Authenticator Settings** нажмите на ссылку [Show Authenticators Settings for Unit](#).

Настройка учетных записей локальных пользователей

В папке **Configuration** откройте папку **Port Access Entity** и нажмите на ссылку **Local Users**, появится меню **802.1x Local User Table Configuration**. Данное меню позволяет настроить на коммутаторе учетные записи локальных пользователей.

802.1x Local User Table Configuration		
User Name	Password	Confirm Password
<input type="text"/>	<input type="text"/>	<input type="text"/>
		<input type="button" value="Apply"/>
Total Entries: 1		
802.1x Local User Table		
User Name	Password	Delete
Trinity	1	<input type="button" value="X"/>

Рисунок 4-52 Меню 802.1x Local User Table Configuration

Введите имя пользователя в поле **User Name**, пароль в поле **Password** и повторите ввод пароля в поле **Confirm Password**. Ниже в таблице **802.1x Local Users Table** показаны ранее настроенные учетные записи локальных пользователей.

Система контроля PAE

Настройка параметров аутентификации на портах

В следующем окне показаны текущие настройки 802.1x на портах, которые могут быть изменены.

В папке **Configuration** откройте папку **PAE Access Entity** и нажмите на ссылку **Port Capability Settings**, появится окно **802.1x Capability Settings**:

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

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

Рисунок 4-53 Меню настройки 802.1x на портах

Для настройки аутентификации 802.1x на основе портов выберите диапазон настраиваемых портов в полях **From To**. Затем из выпадающего меню **Capability** выберите *Authenticator*. Нажмите *Apply*, чтобы изменения вступили в силу.

Параметры для настройки:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке по его идентификатору Unit ID при объединении коммутаторов в стек.
From [] To []	Группа последовательно пронумерованных портов, подлежащих настройке.
Capability	Выберите одну из опций: <i>Authenticator</i> - пользователь должен будет пройти процесс аутентификации для получения доступа к сети. <i>None</i> - порт не будет использовать аутентификацию 802.1x

Инициализация портов

В папке **Configuration** откройте папку **PAE Access Entity** и нажмите на ссылку **Initialize Port(s)**, появится окно **802.1x Port Initial**:

Initialize Port

Unit	From	To	Apply
1	Port 1	Port 1	Apply

Initialize Port Table

Port	Auth PAE State	Backend_State	Port Status
1	ForceAuth	Success	Authorize d
2	ForceAuth	Success	Authorize d
3	ForceAuth	Success	Authorize d
4	ForceAuth	Success	Authorize d
5	ForceAuth	Success	Authorize d
6	ForceAuth	Success	Authorize d
7	ForceAuth	Success	Authorize d
8	ForceAuth	Success	Authorize d
9	ForceAuth	Success	Authorize d
10	ForceAuth	Success	Authorize d
11	ForceAuth	Success	Authorize d
12	ForceAuth	Success	Authorize d
13	ForceAuth	Success	Authorize d
14	ForceAuth	Success	Authorize d
15	ForceAuth	Success	Authorize d
16	ForceAuth	Success	Authorize d
17	ForceAuth	Success	Authorize d
18	ForceAuth	Success	Authorize d
19	ForceAuth	Success	Authorize d
20	ForceAuth	Success	Authorize d
21	ForceAuth	Success	Authorize d
22	ForceAuth	Success	Authorize d
23	ForceAuth	Success	Authorize d
24	ForceAuth	Success	Authorize d

Рисунок 4-54 Инициализация 802.1x на портах и текущее состояние аутентификации

Данное меню позволяет инициализировать 802.1x на портах, а в таблице ниже показано текущее состояние аутентификации на портах коммутатора после нажатия кнопки *Apply*.

Показаны следующие параметры:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке по его идентификатору Unit ID при объединении коммутаторов в стек.
From [] To []	Группа последовательно пронумерованных портов, подлежащих настройке.
Port	Порт коммутатора.

Auth PAE State	Показывает статус Authenticator PAE: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth</i> и <i>N/A</i> .
Backend State	Показывает статус Backend Authentication: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize</i> и <i>N/A</i> .
Port Status	Статус контролируемого порта: <i>authorized</i> (авторизован), <i>unauthorized</i> (не авторизован) и <i>N/A</i> .



Примечание: Вначале необходимо активизировать 802.1x глобально на коммутаторе через меню **Advanced Settings** в папке **Configuration**, прежде чем инициализировать аутентификацию 802.1x на портах. Информация об аутентификации в таблице **Initialize Ports Table** также не будет доступна до активизации 802.1x на коммутаторе.

Повторная аутентификация портов

Данное меню позволяет провести повторную аутентификацию портов. Выберите коммутатор в стеке в поле **Unit** и группу портов в полях **From** и **To** и нажмите *Apply*. После нажатия кнопки *Apply* в таблице **Reauthenticate Port Table** будет показано текущий статус портов.

В папке **Configuration** откройте папку **PAE Access Entity** и нажмите на ссылку **Reauthenticate Port(s)**, появится окно **Reauthenticate Port(s)**:

Reauthenticate Port			
Unit	From	To	Apply
1	Port 1	Port 1	Apply

Reauthenticate Port Table			
Port	Auth PAE State	BackendState	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized

Рисунок 4-55 Повторная аутентификация портов и таблица Reauthenticate Port Table

Показаны следующие параметры:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке по его идентификатору Unit ID при объединении коммутаторов в стек.
From [] To []	Группа последовательно пронумерованных портов, подлежащих настройке.
Auth State	Показывает статус Authenticator: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth</i> и <i>N/A</i> .
Backend State	Показывает статус Backend Authentication: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize</i> и <i>N/A</i> .
Port Status	Статус контролируемого порта: <i>authorized</i> (авторизован), <i>unauthorized</i> (не авторизован) и <i>N/A</i> .

Сервер RADIUS

Поддержка сервера RADIUS облегчает централизованное управление учетными записями пользователей и обеспечивает защиту от прослушивания сети и взлома.

В папке **Configuration** откройте папку **Radius Server** и нажмите на ссылку **Authentic Radius Server**, появится окно **Authentic Radius Server Setting**:

Authentic Radius Server Setting					
Succession	First				
Radius Server	10.53.13.94				
Authentic Port	1812				
Accounting Port	1813				
Key					
Confirm Key					
Status	Valid				
Apply					
Current Radius Server(s) Settings Table					
Succession	Radius Server	Auth UDP Port	Acct UDP Port	Status	Key
First	10.53.13.94	1812	1813	Valid	45
Second					
Third					

Рисунок 4-56 Настройка параметров сервера Radius

Параметры для настройки:

Параметр	Описание
Succession < First >	Выберите порядковый номер настраиваемого сервера RADIUS: <i>First</i> (первый), <i>Second</i> (второй), <i>Third</i> (третий).
Radius Sever < 10.53.13.94 >	Введите IP-адрес сервера RADIUS.
Authentic Port < 1812 >	Введите номер порта UDP, используемого для запросов аутентификации. Значение по умолчанию 1812.
Accounting Port < 1813 >	Введите номер порта UDP, используемого для запросов об учетных записях (если используется сервер учетных записей). Значение по умолчанию 1813.
Key	Введите ключ, используемый сервером RADIUS и коммутатором.
Confirm Key	Повторите ввод ключа, используемого сервером RADIUS и коммутатором.
Status	Позволяет активизировать (<i>Valid</i>) или отключить (<i>Invalid</i>) текущий сервер RADIUS.

Сетевое взаимодействие на 3-ем уровне

В папке **Configuration** откройте папку **Layer 3 IP Networking**. В ней содержатся ссылки на меню настройки сетевого взаимодействия на 3-ем уровне.

Общие настройки функций 3-его уровня

Меню **L3 Global Advanced Settings** позволяет включить или отключить функции коммутатора 3-его уровня. Полное описание функций и их параметров приведено далее в этом разделе. В папке **Configuration** откройте папку **Layer 3 IP Networking** и нажмите на ссылку **L3 Global Advanced Settings**, появится следующее окно:

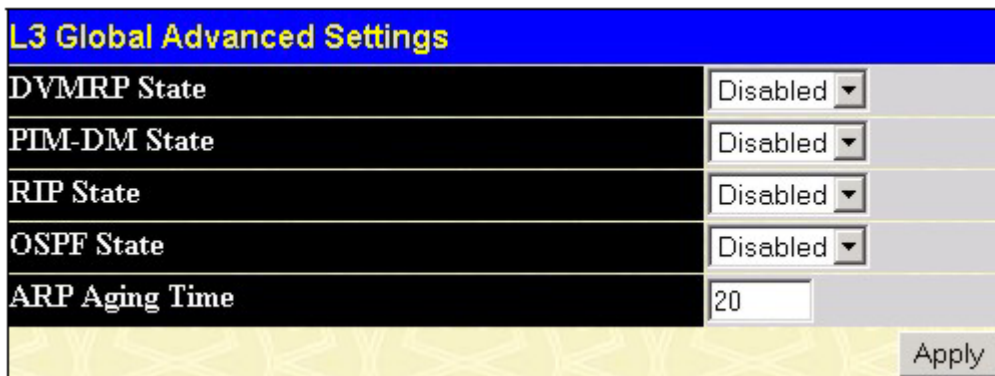


Рисунок 4-57 Меню L3 Global Advanced Settings

Параметры для настройки:

Параметр	Описание
DVMRP State	Позволяет глобально включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) протокол Distance Vector Multicast Routing Protocol (DVMRP).
PIM-DM State	Позволяет глобально включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) протокол Protocol Independent Multicast – Dense Mode (PIM-DM).
RIP State	Позволяет глобально включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) протокол Routing Information Protocol (RIP).
OSPF State	Позволяет глобально включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) протокол Open Shortest Path First (OSPF).
ARP Aging Time	Позволяет задать время хранения (в минутах) записи в ARP-таблице (Address Resolution Protocol, Протокол разрешения адресов) коммутатора при отсутствии обращений к этой записи.

Настройка IP-интерфейсов

Каждая из VLAN должна быть настроена прежде, чем будет произведена настройка соответствующих IP-интерфейсов VLAN.

Ниже приведен пример:

Имя VLAN	VID	Порты коммутатора
System (по умолчанию)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Таблица 4-4 Пример назначения портов в VLAN

В данном случае требуется 6 IP-интерфейсов, поэтому будет работать схема адресации 10.32.0.0/11 (или 11-бит) в нотации CIDR. Такая схема адресации определяет маску подсети 11111111.11100000.00000000.00000000 (в двоичном виде) или 255.224.0.0 (в десятичном виде).

При использовании IP-адреса вида 10.xxx.xxx.xxx в приведенном выше примере получаем 6 адресов сетей и 6 подсетей.

Можно выбрать любой IP-адрес из диапазона разрешенных IP-адресов для каждой в качестве IP-адреса интерфейса IP коммутатора.

В данном примере мы выбрали следующие IP-адреса и адреса сетей:

Имя VLAN	VID	Адрес сети	IP-адрес
System (по умолчанию)	1	10.32.0.0	10.32.0.1
Engineering	2	10.64.0.0	10.64.0.1
Marketing	3	10.96.0.0	10.96.0.1
Finance	4	10.128.0.0	10.128.0.1
Sales	5	10.160.0.0	10.160.0.1
Backbone	6	10.192.0.0	10.192.0.1

Таблица 4-5 Пример назначения IP-адресов в VLAN

Шесть IP-интерфейсов, каждый с IP-адресом (из таблицы) и маской подсети 255.224.0.0, можно настроить в меню **Setup IP Interface**.

Для настройки IP-интерфейсов на коммутаторе:

В папке **Configuration** откройте папку **Layer 3 IP Networking** и нажмите на ссылку **Setup IP Interfaces**. Появится следующее окно:

IP Interface Table					
Interface Name	IP Address	Subnet Mask	Vlan Name	Active	Delete
System	10.53.13.199	255.0.0.0	default	Enabled	<input type="checkbox"/>

Рисунок 4-58 Таблица IP-интерфейсов

Для настройки нового интерфейса нажмите кнопку *Add*. Для редактирования настроек IP-интерфейса нажмите на ссылку под заголовком **Interface Name** с именем нужного интерфейса. В обоих случаях появится следующее окно:

IP Interface Configuration	
Interface Name	System
IP Address	10.53.13.150
Subnet Mask	255.0.0.0
VLAN Name	default
State	Enabled
Link Status	Link UP

[Show All IP Interface Entries](#)

Рисунок 4-59 Настройка параметров IP-интерфейса

Введите имя нового интерфейса в поле **Interface Name** (при редактировании настроек интерфейса в данном поле будет показано его имя). Введите IP-адрес интерфейса и маску подсети в соответствующие поля. Из выпадающего меню **State** выберите *Enabled* и нажмите кнопку *Apply* для активизации интерфейса. Используйте меню **Save Changes** в папке **Basic Setup** для сохранения настроек в NV-RAM.

Для возврата в таблицу IP-интерфейсов **IP Interface Table** нажмите на ссылку [Show All IP Interface Entries](#).

Параметры для настройки:

Параметр	Описание
Interface Name	В данном поле показывается имя IP-интерфейса. IP-интерфейс по умолчанию называется System.
IP Address	Поле ввода IP-адреса, назначаемого IP-интерфейсу.
Subnet Mask	Поле ввода маски подсети для IP-интерфейса.
VLAN Name	Поле ввода имени VLAN, к которой относится данный интерфейс.
State <Disabled>	Можно активизировать (<i>Enabled</i>) или отключить (<i>Disabled</i>) интерфейс.
Link Status <Link UP>	Показывает текущее состояние IP-интерфейса коммутатора. <i>Link Up</i> указывает, что IP-интерфейс правильно настроен и работает. <i>Link Down</i> указывает, что IP-интерфейс не настроен и/или не активизирован.

Таблица ключей MD5

Меню **MD5 Key Table Configuration** позволяет ввести 16-символьный ключ Message Digest версии 5 (MD5), который будет использоваться для аутентификации каждого пакета между OSPF-маршрутизаторами. Ключ используется в качестве механизма обеспечения безопасности для ограничения обмена информацией о топологии сети в пределах домена OSPF-маршрутизации.

Создаваемые ключи MD5 будут использоваться в меню **OSPF Interface Configuration**, описанном ниже.

Для задания ключа MD5 нажмите на ссылку **MD5 Key**, появится следующее окно:

The screenshot shows two main sections. The first is 'MD5 Key Setting' with a table:

Key ID	Key
1	


Below this table is a yellow button labeled 'Add/Modify'. The second section is 'MD5 Key Table' with a table:

Key ID	Key	Delete
1	45	X

Рисунок 4-60 Настройка таблицы ключей MD5

Параметры для настройки:

Параметр	Описание
Key ID	Число от 1 до 255, используемое в качестве идентификатора ключа MD5.
Key	Символьная строка длиной от 1 до 16 символов, чувствительная к регистру символов, которая используется для генерации Message Digest, который в свою очередь используется для аутентификации пакетов OSPF в пределах домена маршрутизации OSPF.

Нажмите *Add/Modify* для создания нового ключа MD5 или изменения параметров записи с указанным Key ID. Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью.

Настройка перераспределения маршрутов

Функция перераспределения маршрутов позволяет маршрутизаторам сети – исполняющим различные протоколы маршрутизации – обмениваться маршрутной информацией. Это производится путем сравнения маршрутов, хранящихся в различных таблицах маршрутизации маршрутизатора, и назначения им подходящих метрик. Затем маршрутизаторы обмениваются данной информацией в соответствии со

своим текущим протоколом маршрутизации. DGS-3324SR может перераспределять маршрутную информацию между протоколами OSPF и RIP со всеми маршрутизаторами сети, исполняющими протоколы RIP или OSPF. Маршрутная информация, внесенная в таблицу статической маршрутизации на DGS-3324SR, также может перераспределяться.

Источниками маршрутной информации являются протокол OSPF и статическая таблица маршрутизации. Маршрутная информация будет адаптирована для протокола RIP. В следующей таблице приведен список допустимых значений метрик маршрутов и типов (или форм) маршрутной информации, которая может быть перераспределена.

Источник маршрутной информации	Метрика	Тип
OSPF	от 0 до 16	All Internal External ExtType1 ExtType2 Inter-E1 Inter-E2
RIP	от 0 до 16777214	Type 1 Type 2
Статическая таблица маршрутизации	от 0 до 16777214	Type 1 Type 2
Локальная информация	от 0 до 16777214	Type 1 Type 2

Таблица 4-6 Источники перераспределяемой маршрутной информации

Ввод комбинации типов – internal type_1 type_2 – эквивалентно all. Ввод комбинации типов type_1 type_2 эквивалентно external. Ввод комбинации external internal эквивалентно all.

Ввод метрики 0 определяет непосредственно подключенную сеть.

В папке **Configuration** откройте папку **Layer 3 IP Networking** и нажмите на ссылку **Route Redistribution Settings**, появится окно **Route Redistribution Table Configuration**:


The screenshot shows the 'Route Redistribution Settings' window. At the top, there's a blue header with the title. Below it is a table with four columns: 'Dest Protocol', 'Src Protocol', 'Type', and 'Metric'. Each column has a dropdown menu. The 'Dest Protocol' dropdown is set to 'RIP', 'Src Protocol' is also 'RIP', and 'Type' is 'All'. The 'Metric' column has an empty input field. Below this table is a yellow background area with an 'Add/Modify' button. Below that is another blue header for 'Route Redistribution Table', followed by a table with five columns: 'Src Protocol', 'Dest Protocol', 'Type', 'Metric', and 'Delete'.

Рисунок 4-61 Настройка функции перераспределения маршрутов

Параметры для настройки:

Параметр	Описание
Src Protocol	Позволяет выбрать протокол устройства-источника. Доступны опции <i>RIP</i> , <i>OSPF</i> , <i>Static</i> и <i>Local</i> .

Dest Protocol	Позволяет выбрать протокол устройства-назначения. Доступны опции <i>RIP</i> и <i>OSPF</i> .
Type	Позволяет выбрать один из шести методов вычисления значения метрики. Доступны опции <i>All</i> , <i>Internal</i> , <i>External</i> , <i>ExtType1</i> , <i>ExtType2</i> , <i>Inter-E1</i> , <i>Inter-E2</i> . В приведенной выше таблице описаны допустимые типы метрик для каждого протокола-источника.
Metric	Позволяет ввести метрику OSPF-интерфейса. Аналог количества переходов в протоколе RIP.

Нажмите *Apply*, чтобы изменения вступили в силу. Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью.



Примечание: В полях **Src Protocol** и **Dest Protocol** нельзя указывать один и тот же протокол.

Статическая таблица маршрутизации

Записи в адресной таблице коммутатора могут быть сделаны по MAC-адресу и IP-адресу. По IP-адресам формируется статическая таблица маршрутизации **Static IP Routing Table**.



Add						
Static/Default Route Settings						
IP Address	Subnet Mask	Gateway	Hops	Protocol	Backup State	Delete
10.0.0.0	255.0.0.0	10.254.254.251	1	Static	Primary	
Total Entries : 1						

Рисунок 4-62 Статическая таблица маршрутизации

Показаны следующие параметры:

Параметр	Описание
IP Address	IP-адрес статической записи в таблице маршрутизации.
Subnet Mask	Маска подсети, соответствующая введенному выше IP-адресу.
Gateway	IP-адрес шлюза по умолчанию, соответствующего введенному выше IP-адресу.
Hops	Метрика протокола маршрутизации для данного IP-интерфейса. Принимает значения от 1 до 65535 для протокола OSPF и от 1 до 16 для протокола RIP.
Protocol	Используемый протокол маршрутизации: OSPF, RIP, Static или Local.
Backup State	Показывает состояние маршрута: Primary (основной) или Backup (резервный).
Delete	Нажмите  для удаления записи из статической таблицы маршрутизации.

Для добавления новой записи в статическую таблицу маршрутизации коммутатора нажмите кнопку *Add*, появится следующее окно:

Рисунок 4-63 Добавление новой записи в статическую таблицу маршрутизации

Параметры для настройки:

Параметр	Описание
IP Address <0.0.0.0>	Позволяет ввести IP-адрес статической записи в таблице маршрутизации.
Subnet Mask <0.0.0.0>	Позволяет ввести маску подсети, соответствующую введенному выше IP-адресу.
Gateway <0.0.0.0>	Позволяет ввести IP-адрес шлюза для введенного выше IP-адреса.
Metric (1-65535) <1>	Позволяет ввести метрику протокола маршрутизации, представляющую собой количество промежуточных маршрутизаторов между коммутатором и устройством с данным IP-адресом.
Backup State <Primary>	Позволяет задать статус маршрута: <i>Primary</i> (основной) или <i>Backup</i> (резервный). Резервный маршрут активизируется в случае недоступности основного. Обратите внимание, что основной и резервный маршруты не должны проходить через один и тот же шлюз (Gateway).

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в статическую таблицу маршрутизации **Static/Default Route Settings** нажмите на ссылку [Show All Static/Default Route Entries](#).

Статическая ARP-таблица

Протокол ARP (Address Resolution Protocol, Протокол разрешения адресов) – это протокол стека TCP/IP, который преобразует IP-адреса в физические адреса. ARP-таблица позволяет просматривать, задавать, изменять и удалять ARP-информацию для указанных устройств.

В ARP-таблице можно создавать статические записи. После создания постоянная запись используется для трансляции IP-адреса в MAC-адрес.

В папке **Configuration** откройте папку **Layer 3 IP Networking** и нажмите на ссылку **Static ARP Table**, появится окно **Static ARP Table**.

Рисунок 4-64 Статическая ARP-таблица

Для добавления новой записи нажмите кнопку *Add*, появится следующее окно:

Рисунок 4-65 Добавление новой записи в статическую ARP-таблицу

Параметры для настройки:

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

После ввода IP-адреса и MAC-адреса статической записи ARP нажмите *Apply*, чтобы изменения вступили в силу. Для удаления всех записей из статической ARP-таблицы нажмите кнопку *Clear All*. Для возврата в ARP-таблицу **Static ARP Table** нажмите на ссылку [Show All Static ARP Entries](#).

Протокол RIP

Протокол RIP (Routing Information Protocol, Протокол маршрутной информации) является дистанционно-векторным протоколом маршрутизации. Существует два типа сетевых устройств, поддерживающих RIP – активные и пассивные. Активные устройства сообщают о своих маршрутах остальным устройствам посредством сообщений RIP, в то время как пассивные устройства только просматривают эти сообщения. И активные, и пассивные маршрутизаторы обновляют свои таблицы маршрутизации на основании сообщений RIP, которыми обмениваются активные маршрутизаторы. Только на маршрутизаторах RIP может работать в активном режиме.

Каждые 30 секунд маршрутизатор, исполняющий протокол RIP, широковещательно рассылает маршрутные обновления, содержащие набор пар из адреса сети и дистанции (представлена в виде количества переходов, или маршрутизаторов, между рассылающим маршрутизатором и удаленной сетью). Таким образом, вектором является адрес сети, а дистанция измеряется количеством промежуточных маршрутизаторов между локальным маршрутизатором и удаленной сетью.

Протокол RIP измеряет дистанцию целым числом переходов от одной сети до другой. Один переход – это непосредственно подключенный к сети маршрутизатор, сеть на расстоянии двух переходов может быть достигнута через маршрутизатор и т.д. Чем больше маршрутизаторов между источником и точкой назначения, тем больше дистанция RIP (или количество переходов).

Существует несколько правил для обновления маршрутных таблиц, помогающих повысить производительность и стабильность. Маршрутизатор не заменяет маршрут изученным новым, если новый маршрут содержит такое же количество переходов (иногда называемое «стоимостью» маршрута). Поэтому изученные маршруты сохраняются до тех пор, пока не будет найден маршрут с меньшим количеством переходов.

Когда найденные маршруты записываются в таблицу маршрутизации, включается таймер. Этот таймер перезапускается каждый раз, когда маршрут был обновлен. Если в течение некоторого периода времени (обычно 180 секунд) не было получено сообщение RIP, подтверждающее существование данного маршрута, то маршрут удаляется из таблицы маршрутизации.

Протокол RIP не имеет четко определенного метода обнаружения маршрутных петель. Многие реализации RIP включают механизм авторизации (по паролю) для предотвращения изучения маршрутизатором неверных маршрутов от неавторизованных маршрутизаторов.

Для повышения стабильности количество переходов, которыми RIP измеряет дистанцию, должно иметь наименьшее из максимальных значений. Бесконечность (означает, что сеть недостижима) определяется как 16 переходов. Другими словами, если сеть находится от источника дальше, чем 16 маршрутизаторов, локальный маршрутизатор будет полагать, что сеть недостижима.

RIP способен к медленной конвергенции маршрута (для удаления неверных, недостижимых маршрутов или маршрутов с петлями из таблицы маршрутизации), поскольку сообщения RIP распространяются по сети относительно медленно.

Проблема медленной конвергенции может быть решена использованием метода расщепления горизонта (split horizon), при котором маршрутизатор не распространяет информацию о маршруте по тому интерфейсу, по которому информация о данном маршруте была принята. Это уменьшает вероятность образования промежуточных маршрутных петель.

Метод задержки обновления (hold down) используется для принудительного игнорирования маршрутизатором обновления о новом маршруте в течение некоторого периода времени (обычно 60 секунд) после получения сообщения о новом маршруте. Это позволяет всем маршрутизаторам сети получить данное сообщение.

Маршрутизатор может отменить маршрут ("poison reverse"), добавив бесконечное (16) число переходов в сообщение обновления маршрута. Этот метод обычно используется вместе с триггерными обновлениями (triggered updates), которые заставляют маршрутизатор рассылать широковещательные сообщения, когда получено обновление о недостижимой сети.

Формат сообщения RIP версии 1

Существует два типа сообщений RIP: сообщения маршрутной информации и запросы на информацию. Для обоих типов используется одинаковый формат:

RIP Version 1 Message Format

Октейты				
0	1	2	3	4
Command	Version		Must be all zeros	
Family of Source Network		Must be all zeros		
IP Address of Source				
Must be all zeros				
Must be all zeros				
Distance to Source Network				
Family of Destination Network		Must be all zeros		
IP Address of Destination				
Must be all zeros				
Must be all zeros				
Distance to Destination Network				

Поле COMMAND указывает действие в соответствии со следующей таблицей:

Команда	Значение
1	Запрос на часть или всю маршрутную информацию
2	Ответ, содержащий пары чисел сеть-дистанция, от отправителя маршрутной информации
3	Включить режим отладки (устаревшее)
4	Выключить режим отладки (устаревшее)
5	Зарезервировано для внутреннего использования

	Sun Microsystem
9	Запрос на обновление
10	Ответ обновления
11	Подтверждение об обновлении

Таблица 4-7 Коды команд RIP

Поле VERSION содержит номер версии протокола (1 в данном случае) и используется получателем для проверки версии отправленного пакета RIP.

Сообщение RIP 1

Протокол RIP не ограничен стеком TCP/IP. Его формат адреса может поддерживать 14 байтные адреса (при использовании TCP/IP последние 10 байт должны быть равны 0). В поле Family of Source Network (род сети источника) могут быть указаны другие наборы сетевых протоколов (IP имеет значение 2). Этим определяется, как должно интерпретироваться поле адреса.

Протокол RIP определяет, что IP-адрес 0.0.0.0 обозначает маршрут по умолчанию.

Расстояния, измеренные в переходах, записываются в полях Distance to Source Network (расстояние до сети источника) и Distance to Destination Network (расстояние до сети назначения).

Интерпретация маршрута RIP 1

Протокол RIP был разработан для использования с классовой схемой адресации и не включает в себя явно маску подсети. Расширение версии 1 позволяет маршрутизаторам обмениваться адресами подсетей, но только если маска подсети, используемая сетью, совпадает с маской подсети, используемой адресом. Это означает, что RIP версии 1 не может быть использован для рассылки бесклассовых адресов.

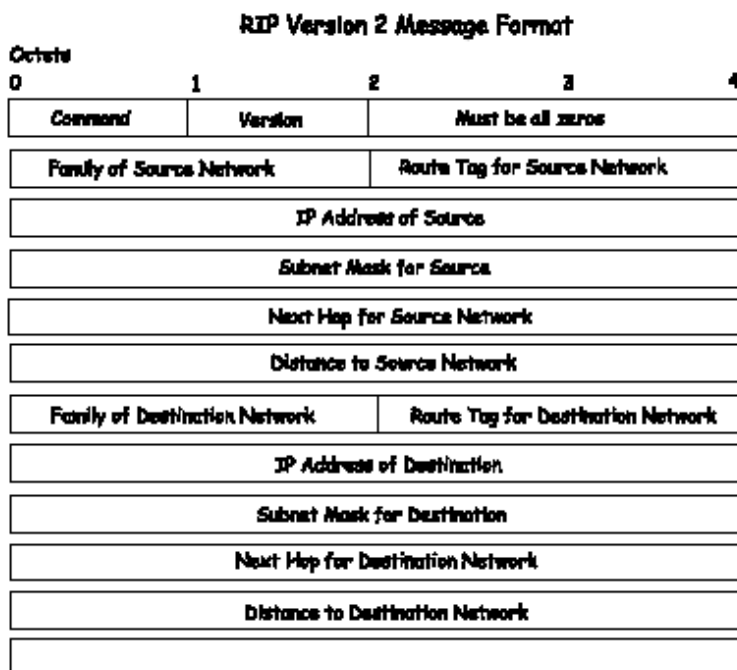
Маршрутизаторы, использующие RIP версии 1, должны отправлять различные сообщения об обновлении для каждого IP-интерфейса, к которому подключены. Интерфейсы, использующие ту же маску подсети, что и сеть маршрутизатора, могут содержать маршруты из нескольких подсетей, другие же интерфейсы не могут. Тогда маршрутизатор будет распространять информацию только об одном маршруте к сети.

Расширения RIP версии 2

Протокол RIP версии 2 содержит явное задание маски подсети, поэтому RIP версии 2 может быть использован для распространения информации об адресах подсетей различной длины или бесклассовых адресах в нотации CIDR. RIP версии 2 также добавляет поле для указания адреса следующего перехода, что ускоряет конвергенцию и помогает предотвратить образование маршрутных петель.

Формат сообщения RIP 2

Формат используемого протоколом RIP 2 сообщения является расширением формата RIP 1:



RIP версии 2 также добавляет 16-битный тег маршрута, который сохраняется и отправляется в маршрутном обновлении. Он может быть использован для идентификации исходного маршрута.

Поскольку номер версии протокола RIP 2 записывается в том же байте, что и RIP 1, обе версии протоколов могут быть использованы на одном маршрутизаторе одновременно без конфликта.

Настройка RIP

Прежде чем настраивать параметры протокола RIP на каждом IP-интерфейсе коммутатора, необходимо глобально активизировать протокол RIP. В папке **Configuration** откройте папку **Layer 3 IP Networking**, затем папку **RIP** и нажмите на ссылку **RIP Configuration**, появится следующее окно:



Рисунок 4-66 Окно RIP Global Setting

Для активизации протокола RIP на коммутаторе выберите **Enabled** и нажмите *Apply*.

Настройка RIP на интерфейсе

Параметры протокола RIP настраиваются на каждом IP-интерфейсе коммутатора. В папке **RIP** нажмите на ссылку **RIP Interface Settings**. В появившейся таблице будут показаны настройки всех IP-интерфейсов коммутатора. Для настройки RIP на интерфейсе нажмите на ссылку с именем нужного интерфейса в колонке **Interface Name**. Нажмите кнопку *Next* для просмотра следующей части таблицы.

RIP Interface Settings					
Interface Name	IP Address	Tx Mode	RX Mode	Auth.	State
System	10.53.13.150	Disabled	Disabled	Disabled	Disabled
					Next

Рисунок 4-67 Окно RIP Interface Settings

Для настройки RIP на интерфейсе нажмите на ссылку с именем нужного интерфейса, появится следующее меню:

RIP Interface Settings-Edit	
Interface Name	System
IP Address	10.53.13.144
Tx Mode	Disabled ▾
RX Mode	Disabled ▾
Authentication	Disabled ▾
Password	<input type="text"/>
State	Disabled ▾
Interface Metric	1
Apply	
Show All RIP Interface Entries	

Рисунок 4-68 Настройка параметров RIP на интерфейсе

Параметры для настройки:

Параметр	Описание
Interface Name	Имя IP-интерфейса, для которого производится настройка RIP. Данный интерфейс должен быть предварительно настроен на коммутаторе.
IP Address	IP-адрес данного IP-интерфейса.
Tx Mode <Disabled>	Доступны опции <i>Disabled</i> , <i>V1 Only</i> , <i>V2 Compatible</i> и <i>V2 Only</i> . Данное поле определяет, какая версия протокола RIP будет использоваться для распространения пакетов RIP. Опция <i>Disabled</i> запрещает передачу пакетов RIP.
Rx Mode <Disabled>	Доступны опции <i>Disabled</i> , <i>V1 Only</i> , <i>V2 Only</i> и <i>V1 and V2</i> . Данное поле определяет, какая версия протокола RIP будет использоваться для разбора полученных пакетов RIP. Опция <i>Disabled</i> запрещает прием пакетов RIP.
Authentication<Disabled>	При выборе опции <i>Enabled</i> маршрутизатор будет использовать введенный ниже пароль для аутентификации маршрутизатора, от которого была получена таблица маршрутизации. Опция <i>Disabled</i> отключает аутентификацию.
Password	Пароль, используемый для аутентификации взаимодействующих маршрутизаторов в сети.
State	Можно активизировать (<i>Enabled</i>) или отключить (<i>Disabled</i>) данный RIP-интерфейс на коммутаторе.
Interface Metric	Показывает метрику данного IP-интерфейса.

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в таблицу **RIP Interface Settings** нажмите на ссылку [Show All RIP Interface Entries](#).

Настройка протокола OSPF

Аутентификация OSPF

Пакеты OSPF могут быть аутентифицированы как входящие от доверенных маршрутизаторов путем использования предопределенных паролей. По умолчанию для маршрутизаторов аутентификация не используется.

Существует два других метода аутентификации – простая аутентификация по паролю (ключу) и аутентификация MD-5 (Message Digest).

Простая аутентификация по паролю

Пароль (или ключ) может быть настроен для каждой области. Маршрутизаторы из одной области, которая входит в домен маршрутизации, должны быть настроены с одним и тем же ключом. Данный метод уязвим от пассивных атак, когда простой анализатор пакетов используется для перехвата пароля.

Аутентификация MD-5

Аутентификация MD-5 является криптографическим методом защиты. Ключ (key) и идентификатор ключа (key-ID) настраиваются на каждом маршрутизаторе. Затем маршрутизатор использует определенный алгоритм для генерирования математического списка “message digest” на основе пакета OSPF, ключа и идентификатора ключа. Затем данный message digest (номер) прикрепляется к пакету. Ключ не передается по сети, а в пакеты помещаются неубывающие последовательные числа для предотвращения повторных атак.

Магистраль и область 0

Протокол OSPF ограничивает число требуемых обновлений состояния связей между маршрутизаторами путем определения областей, в пределах которых данный маршрутизатор функционирует. Если определено более одной области, то одна из областей назначается в качестве области 0 – также называемой магистралью.

Магистраль является центром всех остальных областей – все области сети имеют физическое (или виртуальное) соединение с магистралью через маршрутизатор. OSPF позволяет распространять маршрутную информацию путем передачи ее в область 0, из которой маршрутная информация может быть отправлена во все остальные области (и на все остальные маршрутизаторы) сети.

В ситуации, когда необходимо создать область, но нет возможности физически соединить ее с магистралью, настраивается виртуальная связь.

Виртуальная связь

Виртуальные связи создаются для достижения 2 целей:

Связь области с магистралью при отсутствии физического соединения между ними.

Связь участков магистрали в случае выхода из строя физического соединения в области 0.

Области, физически не подключенные к области 0

Все области в сети OSPF должны иметь физическое соединение с магистралью, но в некоторых случаях нет возможности создать физическую связь между удаленной областью и магистралью. Виртуальная связь – это логический маршрут между двумя пограничными маршрутизаторами, которые имеют общую область, и одним пограничным маршрутизатором, который непосредственно соединен с магистралью.

Разбиение магистрали

Протокол OSPF также позволяет настроить виртуальные связи для соединения частей магистрали, между которыми не существует связи. Это эквивалентно соединению различных областей 0 вместе, используя логический маршрут для каждой области 0. Кроме того, виртуальные связи можно добавить для резервирования каналов связи на случай сбоя в работе маршрутизатора. Виртуальная связь создается между двумя пограничными маршрутизаторами, каждый из которых имеет соединение со своей соответствующей областью 0.

Соседи

Маршрутизаторы, которые соединены с одной и той же областью или сегментом, становятся соседями в данной области. Соседи выбираются посредством пакетов Hello. Для рассылки пакетов Hello другим маршрутизаторам сегмента используется многоадресная рассылка. Маршрутизаторы становятся соседями, если они себя видят в списке пакета Hello, отправленного другим маршрутизатором данного сегмента. Таким образом, гарантируется возможность двустороннего взаимодействия между двумя любыми маршрутизаторами–соседями.

Прежде чем стать соседями, любые два маршрутизатора должны отвечать следующим условиям,:

Идентификатор области (Area ID) – два маршрутизатора должны иметь общий сегмент – их интерфейсы должны относиться к одной и той же области. И, конечно же, их интерфейсы должны относиться к одной подсети и иметь одну и ту же маску подсети.

Аутентификация (Authentication) – протокол OSPF позволяет настроить пароль для указанной области. Два маршрутизатора из одного сегмента и одной области должны также получить тот же пароль OSPF, прежде чем стать соседями.

Интервалы Hello и Dead – Интервал Hello задает интервал (в секундах) отправки маршрутизатором пакетов Hello по интерфейсу OSPF. Если по истечении интервала Dead (в секундах) от маршрутизатора не приходят пакеты Hello, то соседи объявляют его вышедшим из строя. OSPF-маршрутизаторы обмениваются пакетами Hello на каждом сегменте для подтверждения существования связи и для выбора выделенного маршрутизатора на магистрали. Протокол OSPF требует, чтобы данные интервалы совпадали у любых двух соседей. Если интервалы различны, то маршрутизаторы не станут соседями на данном сегменте.

Флаг тупиковой области (Stub Area) – Любые два маршрутизатора также должны иметь один и тот же флаг тупиковой области в пакетах Hello для того, чтобы стать соседями.

Отношения смежности

Смежные маршрутизаторы не обмениваются пакетами Hello и не участвуют в процессе обмена топологическими базами данных. Протокол OSPF выбирает один маршрутизатор в качестве выделенного маршрутизатора (Designated Router, DR) и второй маршрутизатор в качестве резервного выделенного маршрутизатора (Backup Designated Router, BDR) на магистрали автономной области (BDR работает в случае выхода из строя DR). Все остальные маршрутизаторы автономной области обращаются к DR за обновлениями топологической базы данных и при обмене сообщениями о состояниях связей. Это снижает трафик при пересылке обновлений состояния связей.

Выбор выделенного маршрутизатора (DR)

Выбор DR и BDR осуществляется посредством пакетов Hello. Маршрутизатор с наивысшим приоритетом OSPF на данной магистрали автономной области станет DR для данной автономной области. В случае равенства приоритетов нескольких маршрутизаторов выбирается маршрутизатор с наивысшим идентификатором Router ID. OSPF-приоритет по умолчанию равен 1. Приоритет, равный 0, означает, что маршрутизатор не может быть выбран в качестве DR.

Построение отношения смежности

Два маршрутизатора подвергаются многошаговому процессу построения отношения смежности. Далее приведено краткое описание требуемых шагов:

Нерабочее состояние (Down) – Нет принятой информации от какого-либо маршрутизатора автономной области.

Попытка (Attempt) – В нешироковещательных сетях (таких как Frame Relay или X.25) данное состояние указывает на то, что нет новой принятой информации от соседа. Должна быть предпринята попытка обращения к соседу путем отправки пакетов Hello с уменьшенной частотой, установленной интервалом Poll.

Инициализация (Init) – Интерфейс обнаружил пришедший от соседа пакет Hello, но двустороннее взаимодействие еще не установлено.

Двустороннее взаимодействие (Two-way) – Двустороннее взаимодействие с соседом установлено. Маршрутизатор увидел свой адрес в входящих от соседа пакетах Hello. В завершении данной стадии должен быть произведен выбор DR и BDR. В конце стадии Two-way маршрутизаторы решают, нужно ли перейти к процессу построения отношения смежности или нет. Решение основано на том, является ли один из маршрутизаторов DR или BDR, или связь является связью «точка-точка» (“point-to-point”) или виртуальной.

Начало обмена (Exstart, Exchange Start) – Маршрутизаторы устанавливают начальное число последовательности, которая будет использоваться в пакетах обмена информацией. Последовательность чисел гарантирует, что маршрутизаторы всегда будут получать самую свежую информацию. Один из маршрутизаторов станет первичным, а другой – вторичным. Первичный маршрутизатор будет периодически запрашивать информацию у вторичного.

Обмен (Exchange) – Маршрутизаторы полностью описывают свою топологическую базу данных путем отправки пакетов описания базы данных.

Загрузка (Loading) – Маршрутизаторы завершают обмен информацией. Маршрутизаторы составляют список запросов о состояниях связей и список повторной отправки запросов о состояниях связей. Если какая-либо информация выглядит неполной или устаревшей, то она помещается в список запросов. Любое отправленное обновление помещается в список повторных запросов до тех пор, пока не будет получено на него подтверждение.

Полное завершение (Full) – Построение отношения смежности завершено. Соседние маршрутизаторы полностью смежные. Смежные маршрутизаторы имеют одинаковую базу данных состояния связей.

Отношения смежности на интерфейсах «точка-точка»

OSPF-маршрутизаторы, которые соединены по интерфейсу «точка-точка» (например, связь через последовательные порты), всегда формируют отношение смежности. Концепции DR и BDR в данном случае не играют роли.

Форматы пакетов OSPF

Все типы пакетов OSPF начинаются со стандартного 24-байтового заголовка, и существуют 5 типов пакетов. Далее описан заголовок, а тип каждого из пакетов описан в последующих разделах.

Все пакеты OSPF (за исключением пакетов Hello) передают объявления о состоянии связей. Пакеты обновления состояния связей, например, распространяют объявления по всему домену маршрутизации OSPF.

Заголовок пакета OSPF

Пакет Hello

Пакет описания базы данных

Пакет с запросом о состоянии связей

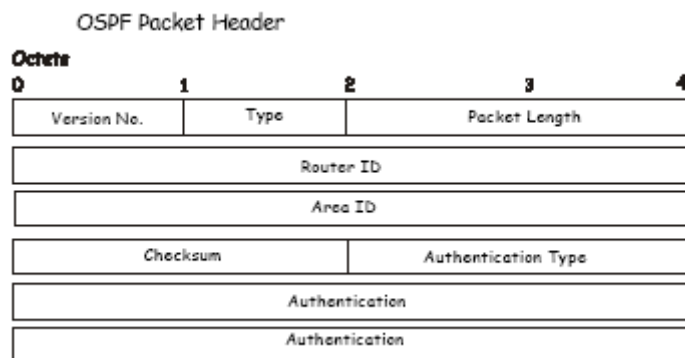
Пакет с обновлением состояния связей

Пакет с подтверждением получения сообщения о состоянии связей

Заголовок пакета OSPF

Каждый пакет OSPF предваряется общим 24-байтовым заголовком. На основании этой информации принявший пакет маршрутизатор принимает решение о дальнейшей обработке пакета.

Далее показан формат заголовка пакета OSPF:



Заголовок пакета OSPF

Поле	Описание												
Version No.	Номер версии OSPF												
Type	Тип пакета OSPF. Пакеты OSPF бывают следующих типов: <table style="margin-left: 20px; border: none;"> <tr> <td style="padding-right: 10px;">Тип</td> <td>Описание</td> </tr> <tr> <td>1</td> <td>Hello</td> </tr> <tr> <td>2</td> <td>Описание базы данных</td> </tr> <tr> <td>3</td> <td>Запрос состояния связей</td> </tr> <tr> <td>4</td> <td>Обновление состояния связей</td> </tr> <tr> <td>5</td> <td>Подтверждение приема сообщения о состоянии связей</td> </tr> </table>	Тип	Описание	1	Hello	2	Описание базы данных	3	Запрос состояния связей	4	Обновление состояния связей	5	Подтверждение приема сообщения о состоянии связей
Тип	Описание												
1	Hello												
2	Описание базы данных												
3	Запрос состояния связей												
4	Обновление состояния связей												
5	Подтверждение приема сообщения о состоянии связей												
Packet Length	Длина пакета в байтах. В длину включаются 24 байта заголовка.												
Router ID	Идентификатор маршрутизатора Router ID, отправившего пакет.												
Area ID	32-битное число, идентифицирующее область, к которой относится данный пакет. Все пакеты OSPF связаны с единственной областью. Пакеты, проходящие через виртуальную связь, связываются с магистралью, идентификатор Area ID которой равен 0.0.0.0.												
Checksum	Стандартная контрольная сумма IP, включающая все содержимое пакета за исключением 64-битного поля аутентификации Authentication.												
Authentication Type	Тип аутентификации, используемой для пакета.												
Authentication	64-битное поле, используемое схемой аутентификации.												

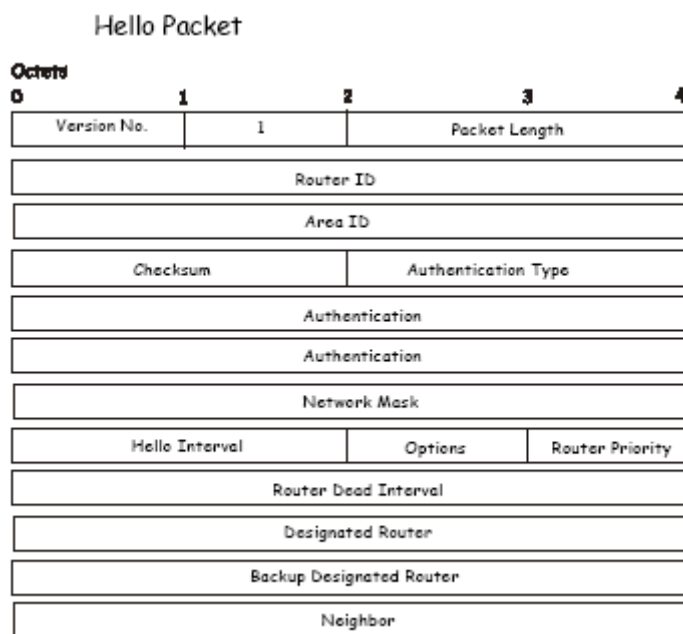
Таблица 4-8 Заголовок пакета OSPF

Пакет Hello

Пакеты Hello являются пакетами OSPF первого типа. Они периодически рассылаются по всем интерфейсам, включая виртуальные связи, для установления и поддержания отношений соседства. Кроме того, пакеты Hello являются многоадресными в тех сетях, которые обладают возможностью многоадресной или широковещательной рассылки и возможностью динамического обнаружения соседних маршрутизаторов.

Все маршрутизаторы, подключенные к общей сети, должны договориться о некоторых параметрах, таких как маска подсети, интервал Hello и интервал Router Dead. Данные параметры включаются в пакеты Hello, поэтому различия в их значениях сдерживают формирование отношения смежности.

Далее показан формат пакета Hello:



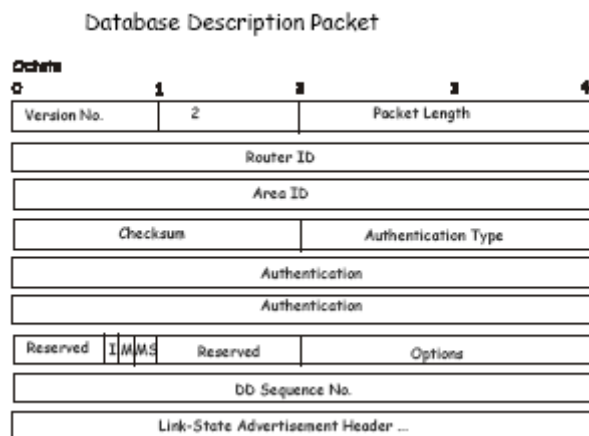
Формат пакета Hello

Поле	Описание
Network Mask	Сетевая маска, назначенная данному интерфейсу.
Options	Дополнительные возможности, поддерживаемые маршрутизатором.
Hello Interval	Интервал в секундах между отправкой данным маршрутизатором пакетов Hello.
Router Priority	Приоритет данного маршрутизатора. Параметр Router Priority используется при выборе DR и BDR. Если данное поле установлено в 0, то маршрутизатор не имеет право быть избранным DR или BDR.
Router Dead Interval	Интервал времени в секундах, по истечении которого маршрутизатор будет объявлен неработающим, если от него не было получено сообщений.
Designated Router	Идентификатор DR в данной сети с точки зрения маршрутизатора, рассылающего данные пакеты. DR идентифицируется по IP-адресу сетевого интерфейса.
Backup Designated Router	Идентификатор BDR в данной сети с точки зрения маршрутизатора, рассылающего данные пакеты. BDR идентифицируется по IP-адресу сетевого интерфейса. Данное поле равно 0.0.0.0, если нет BDR.
Neighbor	Идентификаторы всех маршрутизаторов, от которых были получены верные пакеты Hello в течение интервала Router Dead.

Таблица 4-9 Формат пакета Hello

Пакет описания базы данных

Пакеты описания базы данных (Database Description) являются пакетами OSPF второго типа. Данными пакетами обмениваются маршрутизаторы после установления между ними отношения смежности. Они описывают содержимое топологической базы данных. Для описания базы данных может быть использовано множество пакетов. С этой целью используется процедура запрос-ответ. Один из маршрутизаторов выбирается в качестве ведущего, а другой – в качестве ведомого. Ведущий отправляет пакеты описания базы данных (опрашивает другой маршрутизатор), на которые приходят подтверждения в качестве пакетов описания базы данных от ведомого маршрутизатора (отвечает). Ответы связаны с запросами через последовательные номера DD пакетов.



Пакет описания базы данных

Поле	Описание
Options	Дополнительные возможности, поддерживаемые маршрутизатором.
Бит I	Бит Initial. Если установлен в 1, то пакет является первым в последовательности пакетов описания базы данных.
Бит M	Бит More. Значение 1 означает, что последуют еще пакеты описания базы данных.
Бит MS	Бит Master Slave. Значение 1 означает, что маршрутизатор является ведущим в процессе обмена базами данных. Ведомый маршрутизатор имеет значение 0.
DD Sequence Number	Используется для отслеживания последовательности пакетов описания базы данных. Начальное значение (на него указывает бит I = 1) должно быть уникально. Значение DD Sequence Number инкрементируется, пока не будет отправлено полностью описание базы данных.

Таблица 4-10 Формат пакета описания базы данных

Оставшаяся часть пакета содержит список частей топологической базы данных. Каждое объявление о состоянии связей в базе данных описывается своим заголовком.

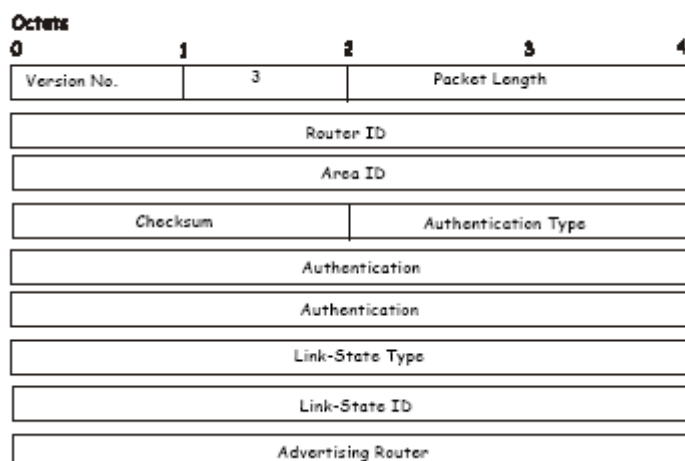
Пакет запроса состояния связей

Пакеты запросов состояния связей (Link State Request) являются пакетами OSPF третьего типа. После обмена пакетами описания базы данных с соседним маршрутизатором маршрутизатор может обнаружить, что часть его топологической базы данных устарела. Пакет запроса состояния связей используется для запроса части базы данных соседа, которая более нова. Для этого может понадобиться множество пакетов запроса состояния связей. Отправка пакетов запроса состояния связей является последним шагом в становлении отношения смежности.

Маршрутизатор, который отправляет пакеты запроса состояния связей, точно помнит запрос части базы данных, определяемый порядковым номером LS, контрольной суммой LS и возрастом LS, несмотря на то, что данные поля не определены в формате пакета запроса состояния связей. Маршрутизатор может получить в ответе даже большее количество состояний связей, чем запрашивал.

Далее показан формат пакета запроса состояния связей:

Link-State Request Packet



Формат пакета запроса состояния связей

Каждое запрашиваемое объявление о состоянии связей указывается в полях Link-State Type, Link-State ID и Advertising Router. Это уникально идентифицирует объявление, но не его экземпляр. Пакеты запроса состояния связей можно представить как запросы наиболее свежих экземпляров.

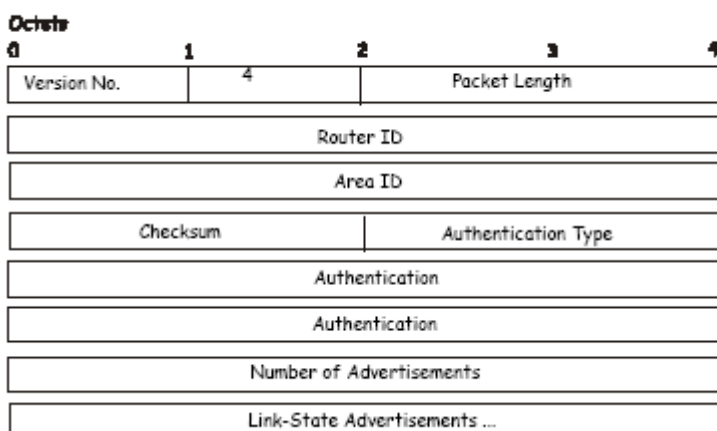
Пакет обновления состояния связей

Пакеты обновления состояния связей (Link-State Update) являются пакетами OSPF четвертого типа. Данные пакеты реализуют веерную рассылку объявлений о состояниях связей. Каждый пакет обновления состояния связей распространяет набор объявлений о состоянии связей на один переход вперед от маршрутизатора-источника. В один пакет может быть вложено несколько объявлений о состояниях связей.

Пакеты обновления состояния связей являются многоадресными пакетами в тех сетях, которые поддерживают многоадресную/широковещательную рассылку. Для того чтобы сделать процедуру рассылки надежной, распространяемые объявления подтверждаются пакетами Link-State Acknowledgment (подтверждение получения сообщения о состоянии связей). Если требуется повторная передача, то повторные объявления всегда отправляются в обычных одноадресных пакетах обновления состояния связей.

Далее показан формат пакета обновления состояния связей:

Link-State Update Packet



Формат пакета обновления состояния связей

Тело пакета обновления состояния связей состоит из списка объявлений о состоянии связей. Каждое объявление начинается с общего 20-байтового заголовка – заголовка объявления о состоянии связей. Во всем остальном формат каждого из пяти типов объявлений о состояниях связей различен.

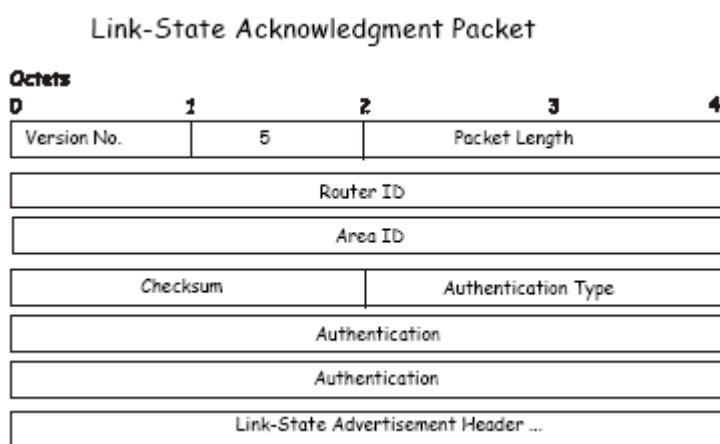
Пакет подтверждения получения сообщения о состоянии связей

Пакеты подтверждения получения сообщения о состоянии связей (Link-State Acknowledgement) являются пакетами OSPF пятого типа. Чтобы сделать рассылку объявлений о состояниях связей надежной, распространяемые объявления явно подтверждаются. Подтверждение выполняется путем отправки и приема пакетов Link-State Acknowledgment. Одним пакетом Link-State Acknowledgment может быть подтверждено получение нескольких объявлений о состояниях связей.

В зависимости от состояния отправляющего интерфейса и источника подтверждений получения объявлений пакет Link-State Acknowledgment отправляется или по групповому адресу AllSPFRouters, или по групповому адресу AllDRouters, или как обычный одноадресный пакет.

Формат этого пакета похож на формат пакета описания базы данных. Тело обоих пакетов является просто списком заголовков объявлений о состояниях связей.

Далее показан формат пакета Link-State Acknowledgment:



Формат пакета Link-State Acknowledgment

Каждое подтвержденное объявление о состоянии связей описано по своему заголовку. Он содержит всю информацию, необходимую для уникальной идентификации и объявления, и текущего экземпляра объявления.

Формат объявления о состоянии связей

Существует 5 различных типов объявлений о состоянии связей. Каждое объявление начинается со стандартного 20-байтового заголовка объявления о состоянии связей. В последующих разделах описываются все 5 типов объявлений.

Каждое объявление о состоянии связей описывает часть домена маршрутизации OSPF. Каждый из маршрутизаторов рассылает объявления о состоянии связей маршрутизатора. Кроме того, всякий раз, когда маршрутизатор выбирается в качестве DR, он рассылает объявление о состоянии связей сети. Также могут рассылаться и другие типы объявлений о состоянии связей. Надежный алгоритм веерной рассылки гарантирует, что все маршрутизаторы получают одинаковые наборы объявлений о состоянии связей. Набор объявлений называется базой данных состояния связей (топологической базой данных).

Каждый маршрутизатор на основании топологической базы данных строит дерево кратчайшего маршрута, выбирая себя в качестве корня. В результате он получает таблицу маршрутизации.

Все четыре типа объявлений имеют одинаковый заголовок, они перечислены далее:

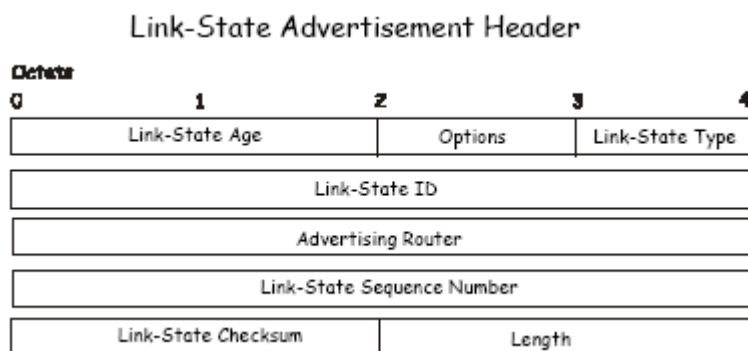
1. Объявление о связях маршрутизатора
2. Объявление о связях сети

- 3 и 4. Объявление о внешних связях области
- 5. Объявление о внешних связях автономной системы

Заголовок объявления о состоянии связей

Все объявления о состоянии связей начинаются с общего 20-байтового заголовка. Заголовок содержит достаточно информации для уникальной идентификации объявления (тип объявления, идентификатор и маршрутизатор - источник объявления). Одновременно в домене маршрутизации могут находиться множество объявлений о состоянии связей. Необходимо определить, какое из объявлений содержит самые последние данные. Это выполняется путем проверки полей возраста объявления о состоянии связи, его порядкового номера и контрольной суммы, которые также входят в заголовок объявления о состоянии связи.

Далее показан формат заголовка объявления о состоянии связей.



Формат заголовка объявления о состоянии связей

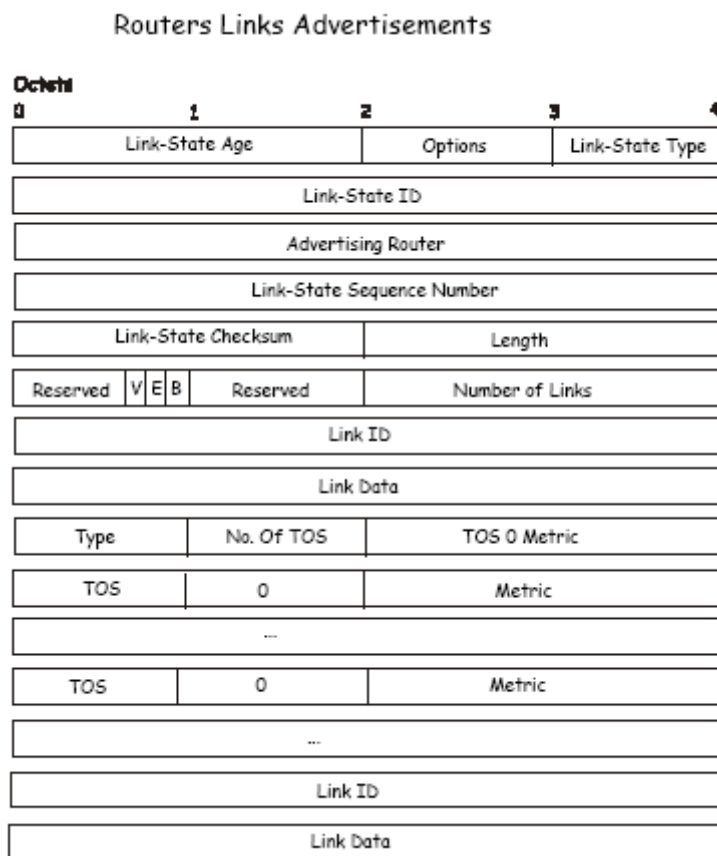
Поле	Описание												
Link State Age	Время (в секундах), прошедшее с момента отправки объявления												
Options	Дополнительные возможности, поддерживаемые описываемой частью домена маршрутизации												
Link State Type	Тип объявления о состоянии связей. Все типы объявлений имеют различные форматы. Допустимы следующие типы: <table style="width: 100%; border: none;"> <tr> <td style="width: 50px;">Тип</td> <td>Описание</td> </tr> <tr> <td>1</td> <td>Связи маршрутизатора</td> </tr> <tr> <td>2</td> <td>Связи сети</td> </tr> <tr> <td>3</td> <td>Внешние связи области (сети IP)</td> </tr> <tr> <td>4</td> <td>Внешние связи области (ASBR)</td> </tr> <tr> <td>5</td> <td>Внешняя связь автономной системы AS</td> </tr> </table>	Тип	Описание	1	Связи маршрутизатора	2	Связи сети	3	Внешние связи области (сети IP)	4	Внешние связи области (ASBR)	5	Внешняя связь автономной системы AS
Тип	Описание												
1	Связи маршрутизатора												
2	Связи сети												
3	Внешние связи области (сети IP)												
4	Внешние связи области (ASBR)												
5	Внешняя связь автономной системы AS												
Link State ID	Данное поле идентифицирует часть межсетевого окружения, которую описывает данное объявление. Содержимое данного поля зависит от типа объявления (поле Link State Type).												
Advertising Router	Идентификатор маршрутизатора, который отправил данное объявление о состоянии связей. Например, в объявлениях о состоянии связей сети в данном поле будет записан идентификатор выделенного маршрутизатора DR.												
Link State Sequence Number	Порядковый номер, используется для обнаружения устаревших или дублированных объявлений о состоянии связей. Следующее объявление о состоянии связей имеет следующий порядковый номер.												
Link State Checksum	Контрольная сумма вычисленная по алгоритму Fletcher для всего содержимого объявления о состоянии связей, включая заголовок, но без поля Link State Age.												
Length	Длина в байтах объявления о состоянии связей. Включает 20-байтовый заголовок.												

Таблица 4-11 Формат заголовка объявления о состоянии связей

Объявление о связях маршрутизатора

Объявления о связях маршрутизатора (Router Links Advertisements) являются объявлениями первого типа. Каждый маршрутизатор области генерирует объявления о своих связях. Объявление описывает состояние и метрику связей маршрутизатора к области. Все связи маршрутизатора к области должны быть описаны в одном объявлении о связях маршрутизатора.

Далее показан формат объявления о связях маршрутизатора:



Формат объявления о связях маршрутизатора

В объявлениях о связях маршрутизатора в поле Link State ID записывается идентификатор маршрутизатора OSPF. Бит T в поле Options устанавливается тогда и только тогда, когда маршрутизатор способен вычислять отдельные наборы маршрутов для различных типов сервиса IP (Type of Service, TOS). Объявления о связях маршрутизатора распространяются широкоэвещательно только в пределах области.

Поле	Описание
Бит V	Если установлен, то маршрутизатор является конечной точкой активной виртуальной связи которая используется описываемой областью в качестве транзитной области (V – конечная точка виртуальной связи (Virtual Link)).
Бит E	Если установлен, то маршрутизатор является пограничным маршрутизатором автономной области (E – внешний маршрутизатор (External)).
Бит B	Если установлен, то маршрутизатор является пограничным маршрутизатором области (B – пограничный маршрутизатор (Border)).
Number of Links	Количество связей маршрутизатора, описанных в данном объявлении. Должно равняться общему числу связей маршрутизатора к области.

Таблица 4-12 Формат объявления о связях маршрутизатора

Следующие поля используются для описания каждой связи маршрутизатора. Каждая связь имеет свой тип. В поле Type указывается тип описываемой связи. Это может быть связь с транзитной сетью, связь с

другим маршрутизатором или с тупиковой сетью. Значения в остальных полях описывают связь в зависимости от ее типа. Например, каждой связи сопоставлено 32-битное поле данных. Для связей к тупиковым сетям в данном поле указывается маска сети IP-адреса. Для остальных типов связей указывается соответствующий IP-адрес интерфейса маршрутизатора.

Поле	Описание										
Type	Классификация связей маршрутизатора: <table border="1"> <thead> <tr> <th>Тип</th> <th>Описание</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Соединение точка-точка с другим маршрутизатором</td> </tr> <tr> <td>2</td> <td>Соединение с транзитной сетью</td> </tr> <tr> <td>3</td> <td>Соединение с тупиковой сетью</td> </tr> <tr> <td>4</td> <td>Виртуальная связь</td> </tr> </tbody> </table>	Тип	Описание	1	Соединение точка-точка с другим маршрутизатором	2	Соединение с транзитной сетью	3	Соединение с тупиковой сетью	4	Виртуальная связь
Тип	Описание										
1	Соединение точка-точка с другим маршрутизатором										
2	Соединение с транзитной сетью										
3	Соединение с тупиковой сетью										
4	Виртуальная связь										
Link ID	Идентифицирует объект, к которому подключена данная связь. Значение зависит от типа связи. Если связь ведет к объекту, который также генерирует объявления о состоянии связей (например, маршрутизатор или транзитная сеть), то Link ID будет равно значению Link State ID соседнего объявления. Таким образом, предоставляется ключ для поиска объявления в базе данных состояния связей. <table border="1"> <thead> <tr> <th>Тип</th> <th>Link ID</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Идентификатор Router ID соседнего маршрутизатора</td> </tr> <tr> <td>2</td> <td>IP-адрес выделенного маршрутизатора</td> </tr> <tr> <td>3</td> <td>Номер сети/подсети IP</td> </tr> <tr> <td>4</td> <td>Идентификатор Router ID соседнего маршрутизатора</td> </tr> </tbody> </table>	Тип	Link ID	1	Идентификатор Router ID соседнего маршрутизатора	2	IP-адрес выделенного маршрутизатора	3	Номер сети/подсети IP	4	Идентификатор Router ID соседнего маршрутизатора
Тип	Link ID										
1	Идентификатор Router ID соседнего маршрутизатора										
2	IP-адрес выделенного маршрутизатора										
3	Номер сети/подсети IP										
4	Идентификатор Router ID соседнего маршрутизатора										
Link Data	Содержимое также зависит от значения в поле Type. Для соединений с тупиковыми сетями указывается маска сети IP-адреса. Для нумерованных соединений точка-точка указывается значение ifIndex MIB-II интерфейса. Для остальных типов связей указывается соответствующий IP-адрес интерфейса маршрутизатора. Последняя часть информации необходима в процессе построения таблицы маршрутизации при вычислении IP-адреса следующего перехода.										
No. of TOS	Количество различных метрик типов сервисов TOS для данной связи. В это число не входит метрика для TOS 0. Если не заданы дополнительные метрики TOS, то значение данного поля должно быть равно 0.										
TOS 0 Metric	Метрика данной связи для TOS 0.										

Таблица 4-13 Формат объявления о связях маршрутизатора - продолжение

Для каждой связи могут быть указаны различные метрики для каждого типа сервиса TOS. Метрика для TOS 0 всегда должна быть указана, это обсуждалось выше. Метрики для ненулевых TOS описаны ниже. Заметьте, что метрики для ненулевых значений TOS, которые не указаны, получают значения по умолчанию, равные TOS 0. Метрики должны быть указаны в порядке возрастания кода TOS. Например, метрика для TOS 16 должна следовать за метрикой TOS 8, если обе они указаны.

Поле	Описание
TOS Metric	Тип сервиса IP, к которому относится метрика. Метрика (стоимость использования) исходящей связи маршрутизатора для трафика указанного типа TOS.

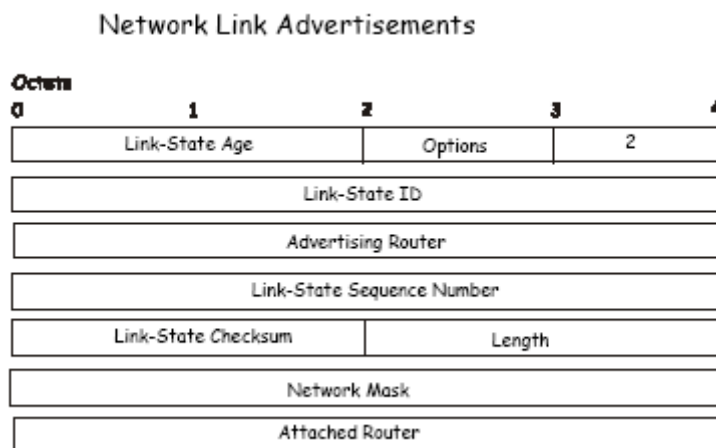
Таблица 4-14 Формат объявления о связях маршрутизатора - продолжение

Объявление о связях сети

Объявления о связях сети (Network Links Advertisements) являются объявлениями о состоянии связей второго типа. Объявления о связях сети генерируются для каждой транзитной сети в области. Транзитная сеть является сетью множественного доступа, к которой подключено более одного маршрутизатора. Объявления о связях сети генерируются выделенным маршрутизатором сети. В объявлении описываются все подключенные к сети маршрутизаторы, включая и сам выделенный маршрутизатор. В поле Link State ID объявления указывается IP-адрес интерфейса выделенного маршрутизатора.

Расстояния от сети до всех подключенных маршрутизаторов равняется 0 для всех TOS. По этой причине не нужно определять поля TOS и Metric в объявлении о связях сети.

Далее показан формат объявления о связях сети:



Формат объявления о связях сети

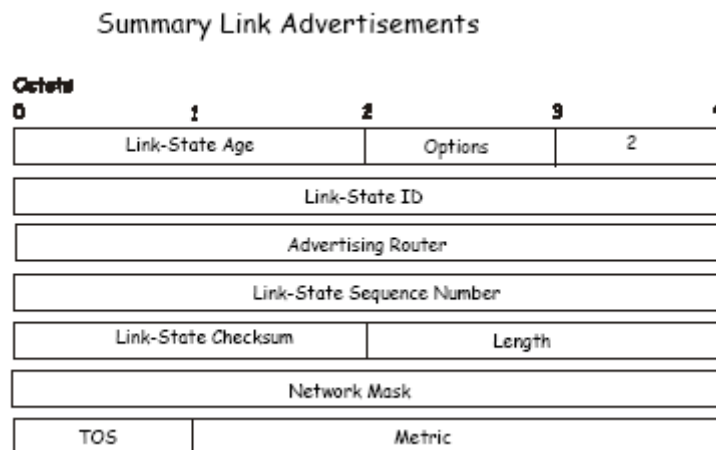
Поле	Описание
Network Mask	Маска сети IP-адреса.
Attached Router	Идентификатор Router ID каждого подключенного к сети маршрутизатора. Указываются только те маршрутизаторы, которые полностью смежны с выделенным маршрутизатором (DR). В список включается и сам DR.

Таблица 4-15 Формат объявления о связях сети

Объявление о внешних связях области

Объявления о внешних связях области (Summary Link Advertisements) являются объявлениями о состоянии связей третьего и четвертого типов. Данные объявления генерируются пограничным маршрутизатором области. Для каждой точки назначения в пределах автономной системы, но вне области, маршрутизатором генерируется отдельное объявление о внешних связях области.

Объявление о состоянии связей третьего типа используются, когда точкой назначения является сетью IP. В данном случае в поле Link State ID объявления записывается номер сети IP. Если точкой назначения является пограничный маршрутизатор автономной области, то используется объявление четвертого типа, а в поле Link State ID записывается идентификатор Router ID пограничного OSPF-маршрутизатора автономной области. В остальном формат объявления о состоянии связей третьего и четвертого типа одинаков.



Формат объявления о внешних связях области

Для тупиковых областей объявления о внешних связях области третьего типа также могут быть использованы для описания маршрута по умолчанию для каждой области. Вместо широковещательной рассылки описания всех внешних маршрутов отправляется информация об общем внешнем маршруте по умолчанию. При описании маршрута по умолчанию в поле Link State ID объявления всегда записывается набор значений Default Destination – 0.0.0.0 и Network Mask – 0.0.0.0.

Могут быть объявлены различные метрики для каждого из типов сервиса TOS. Помните, что метрика для TOS 0 должна всегда включаться в объявление и всегда указываться первой. Если бит T сброшен в поле Options объявления, то в объявлении описывается только маршрут для TOS 0. В противном случае, должны быть описаны маршруты для других значений TOS. Если метрика для некоторого TOS не задана, то она по умолчанию приравнивается к метрике для TOS 0.

Поле	Описание
Network Mask	В объявлениях о состоянии связей третьего типа в данном поле указывается маска сети назначения. Например, в объявлении о сети класса А значение маски равно 0xffff0000.
TOS	Тип сервиса TOS, для которого далее указана метрика.
Metric	Метрика данного маршрута. Измеряется в тех же единицах, что и метрика интерфейса в объявлении о связях маршрутизатора.

Таблица 4-16 Формат объявления о внешних связях области

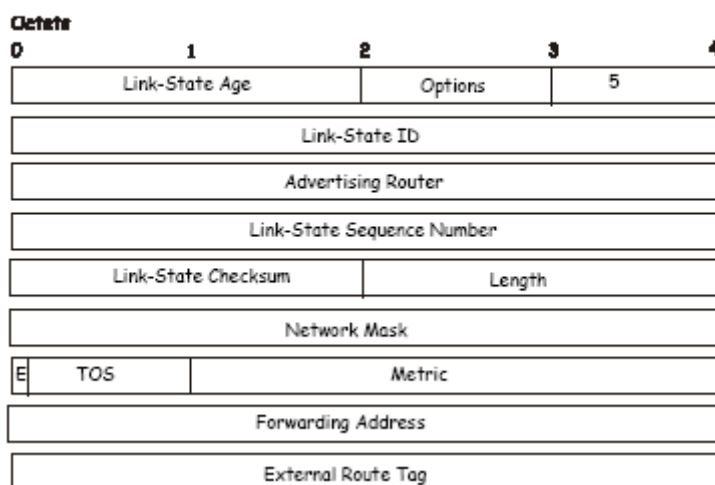
Объявление о внешних связях автономной системы

Объявления о внешних связях автономной системы (Autonomous System Link Advertisements) являются объявлениями о состоянии связей пятого типа. Данные объявления генерируются пограничными маршрутизаторами автономной системы. Для каждой точки назначения вне пределов автономной системы маршрутизатором генерируется отдельное объявление.

Объявления о внешних связях автономной системы обычно описывают часть внешних маршрутов. В этих объявлениях в поле Link State ID указывается номер сети IP. Кроме того, данные объявления используются для описания маршрута по умолчанию. Маршрут по умолчанию используется, когда не указан маршрут для определенной точки назначения. При описании маршрута по умолчанию в поле Link State ID всегда указываются значения Default Destination 0.0.0.0 и Network Mask 0.0.0.0.

Далее показан формат объявления о внешних связях автономной системы:

AS External Link Advertisements



Формат объявления о внешних связях автономной системы

Поле	Описание
Network Mask	Маска IP-адреса для объявляемой точки назначения.
Бит E	Тип внешней метрики. Если бит E установлен, то метрика указана как внешняя метрика второго типа. Это значит, что метрика полагается намного большей, чем метрика любой другой связи. Если бит E равен 0, то метрика указана как внешняя метрика первого типа. Это значит, что она сравнима с метрикой состояния связи.
Forwarding Address	Трафик для объявленной точки назначения будет передаваться по данному адресу. Если значение Forwarding Address равно 0.0.0.0, то трафик будет направляться по адресу источника данного объявления.
TOS	Тип сервиса TOS, для которого далее указана метрика.
Metric	Метрика данного маршрута. Интерпретация метрики зависит от типа внешней метрики (бит E).
External Router Tag	32-битное поле, прикрепленное к каждому внешнему маршруту. Протоколом OSPF не используется.

Таблица 4-17 Формат объявления о внешних связях автономной системы

Общие настройки OSPF

Меню **OSPF General Setting** позволяет активизировать или отключить протокол OSPF на коммутаторе – без изменения настроек OSPF на коммутаторе.

В папке **Layer 3 IP Networking** откройте папку **OSPF** и нажмите на ссылку **OSPF General Setting**. Для активизации работы OSPF вначале введите **OSPF Route ID** и выберите *Enabled* из выпадающего меню **State**, затем нажмите кнопку *Apply*.

Рисунок 4-69 Общие настройки OSPF

Параметры для настройки:

Параметр	Описание
OSPF Route ID	32-битное число (в формате IP-адреса – xxx.xxx.xxx.xxx), являющееся уникальным идентификатором коммутатора в домене OSPF. Часто в качестве идентификатора указывается наибольший из назначенных коммутатору (маршрутизатору) IP-адресов. В данном случае это должно быть значение 10.255.255.555, но можно указать и любое другое 32-битное число. Если указано значение 0.0.0.0, то наибольший из назначенных коммутатору IP-адресов станет идентификатором OSPF Route ID.
Current Route ID	Показывает текущий идентификатор Route ID коммутатора для удобства пользователя при изменении идентификатора.
State	Позволяет активизировать (<i>Enabled</i>) или отключить (<i>Disabled</i>) работу протокола OSPF на коммутаторе без изменения его настроек.

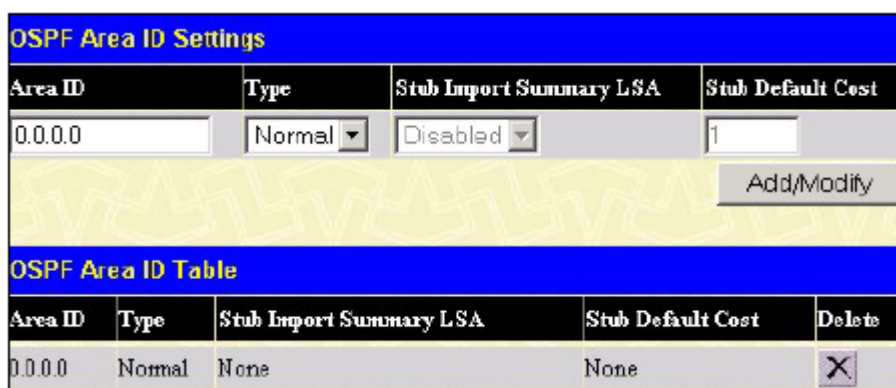


Примечание: Перед использованием данного меню необходимо глобально активизировать протокол OSPF, выбрав *Enabled* в поле **OSPF State** в меню **Layer 3 IP Networking > L3 Global Advanced Settings**.

Настройка областей OSPF

Данное меню позволяет настроить идентификаторы областей OSPF и определить области как обычные (**Normal**) или тупиковые (**Stub**). Обычные области OSPF позволяют рассылку объявлений о базе данных состояния связей (Link State Database, LSDB) от маршрутизаторов к сетям, являющимся внешними по отношению к области. Тупиковые области запрещают рассылку объявлений LSDB о внешних маршрутах. Тупиковые области используют внешний маршрут по умолчанию (0.0.0.0, или область Area 0) для достижения внешних точек назначения.

В папке **Layer 3 IP Networking** выберите папку **OSPF** и нажмите на ссылку **OSPF Area Setting**, появится следующее окно:




Area ID	Type	Stub Import Summary LSA	Stub Default Cost
0.0.0.0	Normal	Disabled	1

Add/Modify

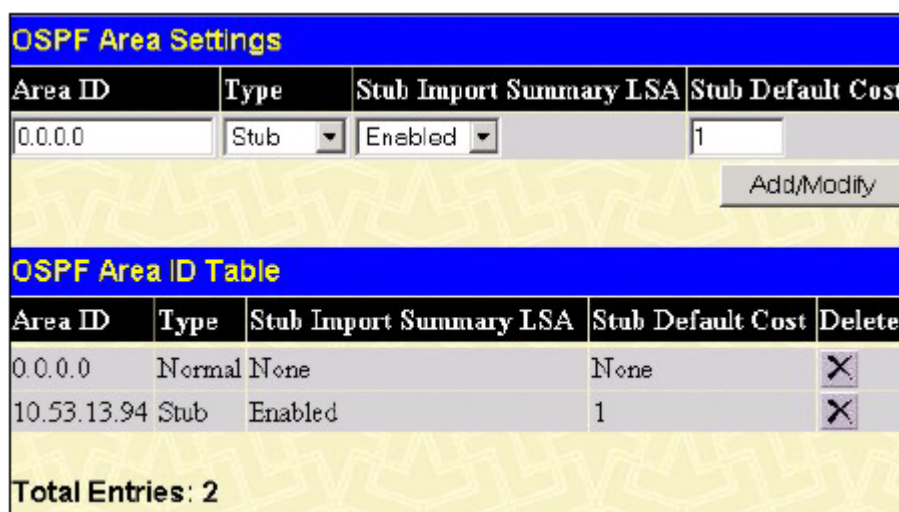
Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Delete
0.0.0.0	Normal	None	None	X

Рисунок 4-70 Настройка областей OSPF

Для добавления новой записи в таблицу введите уникальный идентификатор **Area ID**, выберите тип области в меню **Type**. Если выбран тип *Stub*, то в меню **Stub Import Summary LSA** выберите *Enabled* или *Disabled* и введите метрику **Stub Default Cost**. Нажмите кнопку *Add/Modify* для добавления записи в таблицу.

Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью.

Для изменения существующей записи введите **Area ID** изменяемой записи, внесите изменения и нажмите кнопку *Add/Modify*. Измененная запись появится в таблице **OSPF Area ID Table**.



Area ID	Type	Stub Import Summary LSA	Stub Default Cost
0.0.0.0	Stub	Enabled	1

Add/Modify

Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Delete
0.0.0.0	Normal	None	None	X
10.53.13.94	Stub	Enabled	1	X

Total Entries: 2

Рисунок 4-71 Пример настройки областей OSPF

Параметры для настройки:

Параметр	Описание
Area ID	32-битное число (в формате IP-адреса – xxx.xxx.xxx.xxx), являющееся уникальным идентификатором области OSPF в домене OSPF.
Type	Выбором опции <i>Normal</i> или <i>Stub</i> можно задать тип области OSPF: обычная (Normal) или тупиковая (Stub). При выборе Stub появляются дополнительные поля – Stub Import Summary LSA и Default Cost.
Stub Import Summary LSA	Показывает, позволит ли данная область импортировать объявления о внешних связях области (Summary Link State Advertisements) из других областей.
Stub Default Cost	Показывает метрику по умолчанию для маршрута к тупиковой области в пределах от 0 до 65 535. Значение по умолчанию 0.

Настройка OSPF на интерфейсе

Для настройки OSPF на интерфейсе нажмите на ссылку **OSPF Interface Settings**. В появившемся окне будут показаны настройки OSPF на всех IP-интерфейсах коммутатора. Если IP-интерфейсы не были настроены, то в списке появится только интерфейс по умолчанию System. Для изменения настроек OSPF на интерфейсе нажмите на ссылку с именем нужного интерфейса, появится следующее меню.

OSPF Interface Settings					
Name	IP Address	Area ID	Auth. Type	State	Metric
System	10.53.13.150	0.0.0.0	None	Disabled	1

Рисунок 4-72 Настройки OSPF на IP-интерфейсах коммутатора

OSPF Interface Settings - Edit	
Interface Name	System
IP Address	10.53.13.150(Link Up)
Network Medium Type	BROADCAST
Area ID	<input type="text" value="0.0.0.0"/>
Router Priority	<input type="text" value="1"/>
Hello Interval	<input type="text" value="10"/>
Dead Interval	<input type="text" value="40"/>
State	Disabled ▾
Auth. Type	None ▾
Auth. Key ID	<input type="text"/>
Metric	<input type="text" value="1"/>
DR State	DOWN
DR Address	0.0.0.0
Backup DR Address	0.0.0.0
transmit Delay	1
Retransmit Time	5
<input type="button" value="Apply"/>	
Show All OSPF Interface Entries	

Рисунок 4-73 Редактирование настроек OSPF на интерфейсе

После изменения настроек нажмите кнопку *Apply*. Измененная запись появится в таблице **OSPF Interface Configurations**. Для возврата в таблицу нажмите на ссылку [Show All OSPF Interface Entries](#).


Параметры для настройки:

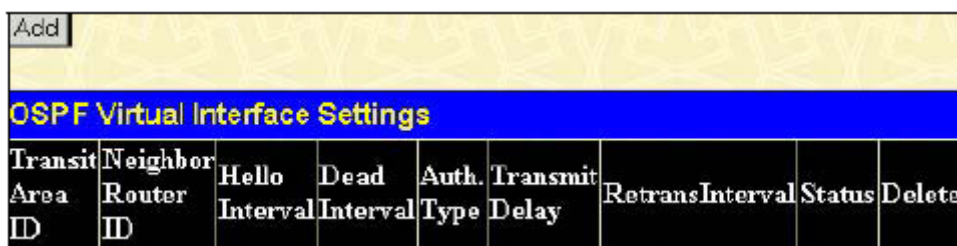
Параметр	Описание
Interface Name	Имя IP-интерфейса, предварительно настроенного на коммутаторе.
IP Address	IP-адрес интерфейса и его текущее состояние (<i>Link Up</i> или <i>Link Down</i>).
Network Medium Type	Тип сетевой среды. При настройке параметров OSPF отображается значение BROADCAST (широковещательная сеть).
Area ID	Позволяет ввести идентификатор области OSPF Area ID, определенный выше.
Router Priority	Позволяет ввести число от 0 до 255, представляющее собой приоритет коммутатора в выбранной области OSPF. Если значение Router Priority равно 0, то коммутатор не может быть выбран в качестве выделенного маршрутизатора сети.
Hello Interval	Позволяет задать интервал отправки пакетов Hello в пределах от 5 до 65 535 секунд. Значения Hello Interval, Dead Interval, Authorization Type и Authorization Key должны быть одинаковы для всех маршрутизаторов в одной сети.
Dead Interval	Если по истечении интервала времени Dead Interval от соседнего маршрутизатора не был получен пакет Hello, то данный маршрутизатор объявляется неработающим. Значение Dead Interval находится в пределах от 5 до 65 535 секунд и должно быть кратно значению Hello Interval.
State	Позволяет отключить (<i>Disabled</i>) интерфейс OSPF для выбранной области без изменения настроек области.

Auth Type	Доступны опции <i>None</i> , <i>Simple</i> и <i>MD5</i> . Позволяет выбрать схему авторизации для пакетов OSPF, передаваемых в пределах домена маршрутизации OSPF. При выборе <i>None</i> авторизация не будет осуществляться. При выборе <i>Simple</i> для авторизации OSPF-маршрутизатора, отправившего пакет, будет использоваться пароль. В этом случае поле Auth Key ID позволяет ввести 5-символьный пароль, который должен совпадать с паролем, заданным на соседнем маршрутизаторе. При выборе <i>MD5</i> для авторизации будет использоваться криптографический ключ, определенный в таблице ключей MD5 в меню MD5 Key Table Configuration. В этом случае поле Auth Key ID позволяет ввести идентификатор ключа Key ID из таблицы ключей MD5. Ключ MD5 должен совпадать с ключом, заданным на соседнем маршрутизаторе.
Auth Key ID	Введите пароль (длиной до 5 символов, чувствительный к регистру), если выше была выбрана схема авторизации <i>Simple</i> , или Key ID (длиной до 5 символов) ключа MD5, если выше была выбрана схема авторизации MD5.
Metric	Позволяет ввести число от 1 до 65 535, представляющее собой метрику OSPF для достижения выбранного интерфейса OSPF. Значение по умолчанию 1.
DR State	Это поле (только для чтения) описывает состояние выделенного маршрутизатора (DR) IP-интерфейса. Это поле может читать DR, если интерфейс является основным выделенным маршрутизатором или BDR, если интерфейс является резервным выделенным маршрутизатором. Интерфейс с наибольшим IP-адресом станет DR, как это определено протоколом OSPF Hello.
DR Address	IP-адрес вышеупомянутого выделенного маршрутизатора.
BDR Address	IP-адрес вышеупомянутого резервного выделенного маршрутизатора.
Transmit Delay	Показывает приблизительное время (в секундах) до отправки обновления состояния связей (Link State Update) через интерфейс.
Retransmit Delay	Показывает интервал (в секундах) повторной рассылки LSA через интерфейс.

Настройка виртуального интерфейса OSPF

Нажмите на ссылку **OSPF Virtual Interface Settings**, чтобы просмотреть текущие настройки виртуальных интерфейсов OSPF. По умолчанию виртуальные интерфейсы на коммутаторе не настроены, поэтому в таблице нет ни одной записи. Для добавления нового виртуального интерфейса нажмите кнопку *Add*. Появится показанное ниже меню. Для редактирования записи нажмите на ссылку с **Transit**

Area ID нужного интерфейса. Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью.



OSPF Virtual Interface Settings								
Transit Area ID	Neighbor Router ID	Hello Interval	Dead Interval	Auth. Type	Transmit Delay	Retransmit Interval	Status	Delete

Рисунок 4-74 Настройка виртуальных интерфейсов OSPF

В колонке **Status** показано текущее состояние каждого из интерфейсов.

OSPF Virtual Link Setting - Add	
Transit Area ID	<input type="text" value="0.0.0.0"/>
Neighbor Router ID	<input type="text" value="0.0.0.0"/>
Hello Interval(1-65535)	<input type="text" value="10"/>
Dead Interval(1-65535)	<input type="text" value="60"/>
Auth Type	None <input type="button" value="v"/>
Password/Auth. Key ID	<input type="text"/>
Transmit Delay	1
RetransInterval	5
<input type="button" value="Apply"/>	
Show All OSPF Virtual Link Entries	

Рисунок 4-75 Добавление/изменение параметров виртуального интерфейса OSPF

Параметры для настройки:

Параметр	Описание
Transit Area ID	Позволяет ввести идентификатор области OSPF Area ID - предварительно определенной на коммутаторе – которая позволит удаленной области взаимодействовать с магистралью (область 0). Транзитной областью не может быть тупиковая область или магистраль.
Neighbor Router ID	Идентификатор Router ID удаленного маршрутизатора. Это 32-битное число (в формате IP-адреса – xxx.xxx.xxx.xxx), являющееся уникальным идентификатором пограничного маршрутизатора удаленной области.
Hello Interval (1-65535)	Позволяет задать интервал отправки пакетов Hello в пределах от 5 до 65 535 секунд. Значения Hello Interval, Dead Interval, Authorization Type и Authorization Key должны быть одинаковы для всех маршрутизаторов в одной сети.
Dead Interval (1-65535)	Если по истечении интервала времени Dead Interval от соседнего маршрутизатора не был получен пакет Hello, то данный маршрутизатор объявляется неработающим. Значение Dead Interval находится в пределах от 5 до 65 535 секунд и должно быть кратным значению Hello Interval.
Auth Type	Доступны опции <i>None</i> , <i>Simple</i> и <i>MD5</i> . Позволяет выбрать схему авторизации для пакетов OSPF, передаваемых в пределах домена маршрутизации OSPF. При выборе <i>None</i> авторизация не будет осуществляться. При выборе <i>Simple</i> для авторизации OSPF-маршрутизатора, отправившего пакет, будет использоваться пароль. В этом случае поле Auth Key позволяет ввести 5-символьный пароль, который должен совпадать с паролем, заданным на соседнем маршрутизаторе. При выборе <i>MD5</i> для авторизации будет использоваться криптографический ключ, определенный в таблице ключей MD5 в меню MD5 Key Table Configuration. В этом случае поле Auth Key ID позволяет ввести идентификатор ключа Key ID из таблицы ключей MD5. Ключ MD 5 должен совпадать с ключом, заданным на соседнем маршрутизаторе.
Password/Auth. Key ID	Введите пароль (длиной до 5 символов, чувствительный к регистру), если выше была выбрана схема авторизации <i>Simple</i> , или Key ID (длиной до 5 символов) ключа MD5, если выше была выбрана схема авторизации MD5.
Transmit Delay	Поле, показывающее расчетное время (в секундах), требуемое для передачи обновления о состоянии связей через данный виртуальный интерфейс.
RetransInterval	Интервал (в секундах) повторной рассылки LSA на смежные с данным

виртуальным интерфейсом маршрутизаторы.

Для возврата в окно **OSPF virtual Interface Settings** нажмите на ссылку [Show All OSPF Virtual Link Entries](#).



Примечание: Для правильного функционирования протокола OSPF некоторые параметры должны быть одинаковыми на всех маршрутизаторах домена OSPF. В эти параметры входят интервалы Hello и Dead. В сетях, использующих авторизацию OSPF-маршрутизаторов, на всех маршрутизаторах должна быть выбрана одинаковая схема авторизации и пароль или ключ MD5.

Настройка агрегирования областей

Агрегирование областей позволяет агрегировать всю маршрутную информацию, которая относится к данной области, в обобщенное объявление LSDB, состоящее только из адреса сети и маски подсети. Это позволяет уменьшить размер трафика объявлений LSDB и объемы памяти коммутатора, отводимые под хранение таблиц маршрутизации.

Нажмите на ссылку **OSPF Area Aggregation Settings**, чтобы просмотреть текущие настройки. По умолчанию агрегирование областей OSPF не используется, поэтому в таблице нет ни одной записи. Для добавления новой записи об агрегировании областей нажмите кнопку *Add*. Для редактирования записи нажмите на ссылку с **Area ID** нужной области. Для удаления записи нажмите в колонке **Delete** рядом с удаляемой записью.

OSPF Area Aggregation Settings					
Area ID	Network Number	Network Mask	LSDB Type	Advertisement	Delete
10.0.0.128	10.0.0.0	255.0.0.0	Summary	Enabled	

Рисунок 4-76 Настройка агрегирования областей OSPF

Для добавления или редактирования записи используется следующее меню:

OSPF Aggregation Configuration - Add	
Area ID	<input type="text" value="0.0.0.0"/>
Network Number	<input type="text" value="0.0.0.0"/>
Network Mask	<input type="text" value="0.0.0.0"/>
LSDB Type	Summary ▾
Advertisement	Enabled ▾
<input type="button" value="Apply"/>	
Show All OSPF Aggregation Entries	

Рисунок 4-77 Добавление/изменение записи об агрегировании областей

После изменения настроек нажмите кнопку *Apply*. Измененная запись появится в таблице **OSPF Area Aggregation Settings**. Для возврата в таблицу нажмите на ссылку [Show All OSPF Aggregation Entries](#).


Параметры для настройки:

Параметр	Описание
Area ID	Позволяет ввести идентификатор области OSPF Area ID, для которой будет агрегироваться маршрутная информация. Область с данным идентификатором

	Area ID должна быть определена ранее.
Network Number	Иногда называется адресом сети. Это 32-битное число в формате IP-адреса, являющееся уникальным идентификатором сети, которая входит в состав заданной выше области OSPF.
Network Mask	Позволяет ввести маску сети, соответствующую указанному выше адресу сети. Каждый диапазон адресов определяется парой (адрес, маска), Оба значения должны быть введены корректно для правильной работы агрегирования OSPF.
LSDB Type	Опция <i>Summary</i> указывает коммутатору на необходимость рассылки в объявлении только адреса сети и маски сети. Последующие реализации коммутатора будут иметь возможность выбора различных типов LSDB.
Advertisement	Позволяет разрешить (<i>Enabled</i>) или запретить (<i>Disabled</i>) данной области OSPF рассылку обобщенных объявлений LSDB для этой области (Адрес сети и Маска сети).

Настройка маршрута OSPF к узлу

Маршруты OSPF к узлу работают аналогично маршрутам RIP, они применяются только для совместного использования информации OSPF с другими OSPF-маршрутизаторами.

Для настройки маршрутов OSPF к узлу нажмите на ссылку **OSPF Host Route Settings**. Для добавления нового маршрута OSPF нажмите кнопку *Add*. Появится меню настройки. Для изменения текущей записи нажмите на ссылку с нужным адресом узла **Host Address**. Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью.




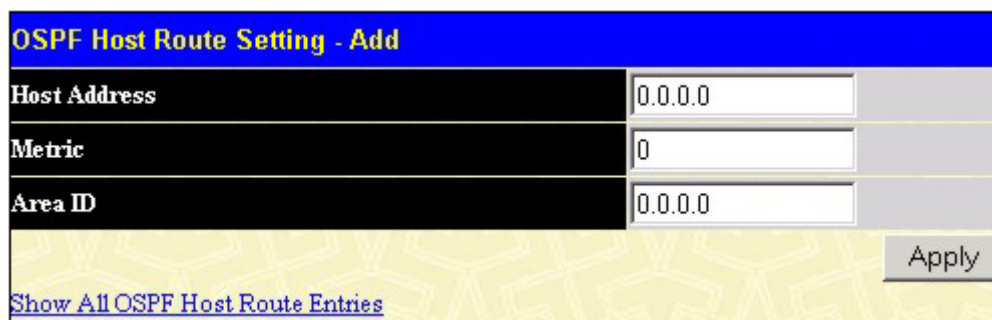
Add			
OSPF Host Route Settings			
Host Address	Metric	Area ID	Delete
10.53.13.144	2	10.1.1.1	

Рисунок 4-78 Настройка маршрута OSPF к узлу

Используйте следующее меню для настройки маршрута OSPF к узлу.



OSPF Host Route Setting - Add	
Host Address	<input type="text" value="0.0.0.0"/>
Metric	<input type="text" value="0"/>
Area ID	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/>	
Show All OSPF Host Route Entries	

Рисунок 4-79 Добавление/изменение маршрута OSPF к узлу

После изменения настроек нажмите кнопку *Apply*. Измененная запись появится в таблице **OSPF Host Route Setting**. Для возврата в таблицу нажмите на ссылку [Show All OSPF Host Route Entries](#).

Параметры для настройки:

Параметр	Описание
Host Address	IP-адрес узла.
Metric	Значение метрики маршрута в пределах от 1 до 65 535.
Area ID	32-битное число (в формате IP-адреса – xxx.xxx.xxx.xxx), являющееся уникальным идентификатором области OSPF в домене OSPF.

DHCP/BOOTP Relay

Протокол BOOTP позволяет задать ограничение количества переходов (промежуточных маршрутизаторов), через которые могут быть переданы сообщения BOOTP. Если счетчик переходов пакета превышает ограничение, то пакет отбрасывается. Максимальное количество переходов может быть установлено в пределах от 1 до 16, значение по умолчанию 4. Таймер Relay Time Threshold устанавливает минимальное время (в секундах), которое коммутатор будет выдерживать перед продвижением пакета BOOTPREQUEST. Если значение аналогичного поля пакета меньше, чем значение Relay Time Threshold, то пакет будет отброшен. Таймер Relay Time Threshold устанавливается в пределах от 0 до 65535 секунд, значение по умолчанию 0.

Информация DHCP/BOOTP Relay

Для активизации и настройки BOOTP или DHCP на коммутаторе в папке **Configuration** откройте папку **BOOTP/DHCP Relay** и нажмите на ссылку **BOOTP/DHCP Relay Information**:

Рисунок 4-80 Информация BOOTP/DHCP Relay

Параметры для настройки:

Параметр	Описание
BOOTP Relay Status <Disabled>	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) сервис BOOTP/DHCP Relay на коммутаторе. Значение по умолчанию <i>Disabled</i> .
BOOTP Hops Count Limit (1-16) <4>	Данное поле позволяет ввести максимальное количество промежуточных маршрутизаторов, через которые сообщения BOOTP могут быть переданы. Количество переходов должно находиться в пределах от 1 до 16, значение по умолчанию 4.
BOOTP/DHCP Relay Time Threshold (0-65535) <0>	Максимальное время маршрутизации пакета BOOTP/DHCP в пределах от 0 до 65535 секунд. Если введено значение 0, то коммутатор не будет обрабатывать поле времени жизни пакетов BOOTP или DHCP. Если введено ненулевое значение, то коммутатор будет использовать данное значение вместе с количеством переходов при принятии решения о продвижении пакета BOOTP или DHCP.

Настройка DHCP/BOOTP Relay

Для настройки параметров DHCP/BOOTP Relay нажмите на ссылку **BOOTP/DHCP Relay Settings**:

DHCP/Bootp Relay Settings				
Interface	Server IP			Apply
<input type="text"/>	<input type="text" value="0.0.0.0"/>			<input type="button" value="Add"/>
Bootp Relay Table				
Interface	Server 1	Server 2	Server 3	Server 4
System	<input checked="" type="checkbox"/> 10.53.13.94			

Рисунок 4-81 Меню настройки BOOTP/DHCP Relay

Параметры для настройки:

Параметр	Описание
Interface	Имя IP-интерфейса, которому принадлежат серверы BOOTP или DHCP.
Server IP<0.0.0.0>	Позволяет ввести до четырех IP-адресов серверов BOOTP или DHCP.

Нажмите *Apply*, для записи строки в таблицу **BOOTP Relay Table**. Для удаления записи нажмите .

DNS Relay

Пользователи обычно предпочитают использовать текстовые имена компьютеров, с которыми они хотят установить соединение. Сами компьютеры требуют 32-битные IP-адреса. Где-либо в сети должна быть размещена база данных текстовых имен сетевых устройств и соответствующих им IP-адресов.

Система доменных имен (DNS, Domain Name System) используется для отображения имен на IP-адреса по всей сети Интернет и была адаптирована для работы в пределах внутренней сети.

Для того чтобы два DNS-сервера могли взаимодействовать между собой через различные подсети, нужно использовать функцию коммутатора DGS-3324SR **DNS Relay**. DNS-серверы идентифицируются по IP-адресам.

Отображение доменных имен на адреса

Трансляция имя–адрес выполняется программой, называемой сервер имен (Name Server). Клиентская программа называется распознаватель имен (Name Resolver). Для распознавателя имен может возникнуть необходимость связаться с несколькими серверами имен для трансляции имени в адрес.

Система доменных имен организована в иерархическом виде. Часто один сервер содержит имена для одной сети и подключен к корневому DNS-серверу, обычно обслуживаемому провайдером услуг Интернет (ISP).

Разрешение доменных имен

Система доменных имен может быть использована посредством связи с серверами имен по одному за раз или запросом ко всей системе доменных имен для полной трансляции имени. Клиент делает запрос, содержащий имя, требуемый тип ответа и код, указывающий, должна ли система доменных имен выполнить полную трансляцию имени или просто вернуть адрес следующего DNS-сервера, если принявший запрос сервер не может разрешить имя.

Когда DNS-сервер получает запрос, он проверяет, входит ли имя в его поддомен. Если это так, сервер транслирует имя, добавляет ответ к запросу и отправляет его обратно клиенту. Если DNS-сервер не может транслировать имя, он определяет, какой тип разрешения имени запросил клиент. Полная трансляция имени называется рекурсивным разрешением и требует, чтобы сервер связывался с другими серверами до полного разрешения имени. Итерационное разрешение определяет, что если сервер не может дать ответ, то он возвращает адрес следующего DNS-сервера, с которым клиент должен связаться.

Каждый клиент должен иметь возможность связаться как минимум с одним DNS-сервером, и каждый DNS-сервер должен иметь возможность связаться как минимум с одним корневым сервером.

Адрес узла, обеспечивающей сервис доменных имен, часто предоставляется серверами DHCP или BOOTP, или может быть задан вручную и настраиваться операционной системой при загрузке.

Настройка DNS Relay

Для настройки DNS Relay на коммутаторе в папке **Configuration** откройте папку **DNS Relay** и нажмите на ссылку **DNS Relay Information**, появится следующее окно:

DNS Relay Information	
DNS Relay Status	Disabled
Primary Name Server	0.0.0.0
Secondary Name Server	0.0.0.0
DNSR Cache Status	Disabled
DNSR Static Table Status	Disabled
Apply	

Рисунок 4-82 Настройка DNS Relay

Параметры для настройки:

Параметр	Описание
DNS Relay State <Disabled>	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) сервис DNS Relay на коммутаторе. Значение по умолчанию <i>Disabled</i> .
Primary Name Server <0.0.0.0>	Позволяет ввести IP-адрес основного сервера доменных имен (DNS).
Secondary Name Server <0.0.0.0>	Позволяет ввести IP-адрес дополнительного сервера доменных имен (DNS).
DNSR Cache Status <Disabled>	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) кэш DNS Relay на коммутаторе. Значение по умолчанию <i>Disabled</i> .
DNSR Static Table Status <Disabled>	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) использование статической таблицы DNS на коммутаторе. Значение по умолчанию <i>Disabled</i> .

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


Статическая таблица DNS Relay

Для просмотра статической таблицы DNS Relay (**DNS Relay Static Table**) в папке **Configuration** откройте папку **DNS Relay** и нажмите на ссылку **DNS Relay Static Table**, появится следующее меню.

DNS Relay Static Settings		
Domain Name	IP Address	Apply
Trinity	10.53.13.94	Add

DNS Relay Static Table		
Domain Name	IP Address	Delete
Trinity	10.53.13.94	X

Рисунок 4-83 Статическая таблица DNS Relay

Для добавления новой записи в статическую таблицу DNS Relay введите доменное имя и соответствующий IP-адрес и нажмите *Add*. В таблице появится новая запись. Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью.

Многоадресная рассылка

Поддерживаемые коммутатором функции многоадресной рассылки находятся в папке **IP Multicast Routing Protocol**, которая становится доступна при выборе папки **Layer 3 IP Networking**.

На коммутаторе можно активизировать или отключить протоколы **IGMP**, **DVMRP** и **PIM-DM** без изменения настроек каждого из протоколов.

Настройка IGMP на интерфейсе

Протокол IGMP (Internet Group Management Protocol, Межсетевой протокол управления группами) может быть настроен на коммутаторе для каждого IP-интерфейса. В папке **Configuration** откройте папку **IP Multicast Routing Protocol** и нажмите на ссылку **IGMP Interface Settings**. В появившейся таблице **IGMP Interface Table** будут показаны все настроенные на коммутаторе IP-интерфейсы. Для настройки IGMP на отдельном интерфейсе нажмите на ссылку с именем нужного интерфейса, появится меню настройки IGMP:

IGMP Interface Table							
Interface Name	IP Address	Version	Query	Max Response Time	Robustness Value	Last Member Query Interval	State
System	10.53.13.144	2	125	10	2	1	Disabled

Рисунок 4-84 Таблица IGMP Interface Table

IGMP Interface Configuration	
Interface Name	System
IP Address	10.53.13.144
Version	2
Query Interval(1-65535)	125
Max Response Time(1-25)	10
Robustness Variable(1-255)	2
Last Member Query Interval(1-25)	1
State	Disabled
<input type="button" value="Apply"/>	
Show All IGMP Interface Entries	

Рисунок 4-85 Меню настройки IGMP на интерфейсе

С помощью данного меню можно настроить параметры IGMP на каждом из IP-интерфейсов коммутатора. Используемую версию протокола IGMP (1 или 2) можно выбрать в поле **Version**. Интервал запросов в пределах от 1 до 65500 секунд позволяет ввести поле **Query Interval**. Максимальное время, на которое узел может задержать IGMP-отчет, указывается в поле **Max Response Time**.

Поле **Robustness Variable** позволяет «подстроить» протокол IGMP для тех подсетей, где ожидается большое количество потерянных пакетов. Наибольшее значение **Robustness Variable** (255) указывается для сетей с очень большим процентом потерянных пакетов, а наименьшее (2) – для сетей с небольшими потерями.

Параметры для настройки:

Параметр	Описание
Interface Name <System>	Показывает имя IP-интерфейса, для которого настраивается протокол IGMP.
IP Address Version <2>	Показывает IP-адрес, соответствующий IP-интерфейсу. Выберите версию протокола IGMP (1 или 2), которая будет использоваться для интерпретации IGMP-запросов на интерфейсе.
Query Interval (1-65535) <125>	Позволяет ввести интервал времени между IGMP-запросами; может принимать значения от 1 до 65535 секунд, значение по умолчанию 125 секунд.
Max Response Time (1-25) <10>	Максимальное время ожидания коммутатором IGMP-отчета; может принимать значения от 1 до 25 секунд, значение по умолчанию 10 секунд.
Robustness Variable (1-255) <2>	Переменная, позволяющая настроить протокол IGMP для подсетей, где ожидается большое количество потерь пакетов; можно установить значение от 1 до 255, причем это значение должно быть больше для тех подсетей, где ожидается большее количество потерянных пакетов. Допускается ввод значения 1, но это может привести к проблемам, и поэтому не рекомендуется. Значение по умолчанию 2.
Last Member Query Interval (1-25) <1>	Укажите максимальный интервал времени между запросами о вхождении в группу, включая те, которые отправляются в ответ на запрос о намерении покинуть группу. Может принимать значения от 1 до 25 секунд, значение по умолчанию 1 секунда.
State <Disabled>	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) IGMP на интерфейсе коммутатора. Значение по умолчанию <i>Disabled</i> .

Настройка DVMRP на интерфейсе

Протокол **DVMRP** (Distance Vector Multicast Routing Protocol, Дистанционно-векторный протокол маршрутизации многоадресной рассылки) - это метод построения деревьев многоадресной рассылки от источника рассылки ко всем узлам сети, в качестве метрики учитывающий количество промежуточных маршрутизаторов. Поскольку ветви дерева рассылки «обрезаны» для сетей, где нет получателей групповой рассылки, и построены по кратчайшим путям для сетей, где такие получатели есть, то протокол DVMRP достаточно эффективен. Так как информация о членстве в группах многоадресной рассылки распространяется по дистанционно-векторному алгоритму, то ее распространение идет медленно. DVMRP оптимизирован для сетей с низкой пропускной способностью и большими задержками и может считаться протоколом многоадресной рассылки с «доставкой по возможности» (“best effort”).

DVMRP похож протокол RIP, но расширен для доставки многоадресной рассылки. Он полагается на количество переходов по протоколу RIP при вычислении кратчайшего пути обратно к источнику многоадресного сообщения, но определяет метрику маршрута для вычисления того, какие ветви дерева должны быть «обрезаны» - после построения дерева многоадресной рассылки.

Когда источник инициирует групповую рассылку, DVMRP вначале предполагает, что все узлы сети захотят получать многоадресные сообщения. Когда смежный маршрутизатор получает сообщение, он проверяет свою обычную таблицу маршрутизации для определения интерфейса, который ведет по кратчайшему маршруту обратно к источнику. Если групповое сообщение было принято по кратчайшему пути, то смежный маршрутизатор заносит информацию в свои таблицы и передает сообщение дальше. В противном случае, маршрутизатор отбрасывает сообщение.

Метрика маршрута – это число, которое использует протокол DVMRP для определения ветвей дерева, подлежащих удалению. Метрика считается относительно метрик других маршрутов всей сети.

Чем больше метрика маршрута (его стоимость), тем меньше вероятность, что данный маршрут будет выбран в качестве активной ветви дерева многоадресной рассылки (не будет «обрезан») – если существуют альтернативные маршруты.

Общая настройка DVMRP

Чтобы активизировать протокол DVMRP глобально на коммутаторе, выберите меню **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > DVMRP Configuration**. Появится следующее окно:



Рисунок 4-86 Окно DVMRP Global Setting

Для активизации протокола DVMRP на коммутаторе выберите **Enabled** и нажмите *Apply*.

Параметры DVMRP на интерфейсе

Нажмите **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > DVMRP Interface Settings**. В появившейся таблице **DVMRP Interface Settings** будут показаны все настроенные на коммутаторе IP-интерфейсы. Для настройки параметров DVMRP на отдельном интерфейсе нажмите на ссылку с именем нужного интерфейса, появится меню настройки DVMRP:

DVMRP Interface Settings					
Interface Name	IP Address	Neighbor Timeout	Probe	Metric	State
System	10.53.13.150	35	10	1	Disabled

Рисунок 4-87 Таблица DVMRP Interface Table

Рисунок 4-88 Меню настройка DVMRP на интерфейсе

Параметры для настройки:

Параметр	Описание
Interface Name <System>	Показывает имя IP-интерфейса, для которого настраивается протокол DVMRP. Это должен быть предварительно настроенный на коммутаторе интерфейс.
IP Address	IP-адрес, соответствующий IP-интерфейсу.

Neighbor Timeout Interval (1-65535 sec) <35>	Если в течении интервала времени Neighbor Timeout Interval от соседних маршрутизаторов не были получены отчеты, то протокол DVMRP генерирует сообщения об отмене маршрутов (poison route). Интервал может быть установлен в пределах от 1 до 65 535 секунд. Значение по умолчанию 35 секунд.
Probe Interval (1-65535 sec) <10>	Позволяет задать интервал рассылки «пробных» групповых сообщений в пределах от 1 до 65 535 секунд. Значение по умолчанию 10 секунд.
Metric (1-31) <1>	Позволяет задать метрику маршрута на данном интерфейсе в пределах от 1 до 31. Метрика маршрута DVMRP – это число, показывающее реальную стоимость использования маршрута при построении дерева многоадресной рассылки. Данная метрика похожа на количество переходов в протоколе RIP, но ею не является. Значение по умолчанию 1.
State <Disabled>	Позволяет включить (Enabled) или отключить (Disabled) протокол DVMRP на IP-интерфейсе коммутатора. Значение по умолчанию Disabled.

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в таблицу **DVMRP Interface Settings** нажмите на ссылку [Show All DVMRP Interface Entries](#).

Настройка PIM-DM на интерфейсе

Протокол PIM-DM должен использоваться в сетях с малыми задержками и высокой пропускной способностью, поскольку он оптимизирован для надежной доставки пакетов групповой рассылки, а не для уменьшения накладных расходов.

Протокол маршрутизации многоадресной рассылки PIM-DM предполагает, что все нижестоящие маршрутизаторы хотят получать многоадресные сообщения, и полагается на сообщения rпune («обрезать» ветвь) от нижестоящих маршрутизаторов для удаления ветвей дерева многоадресной рассылки, которые не содержат членов группы многоадресной рассылки.

PIM-DM не имеет явного сообщения join (присоединить). Он полагается на периодическую веерную рассылку многоадресных сообщений по всем интерфейсам и затем или ждет истечения таймера (**Join/Prune Interval**), или получения сообщений rпune от нижестоящих маршрутизаторов, указывающих, что в соответствующих ветвях больше нет членов группы многоадресной рассылки. Затем PIM-DM удаляет эти ветви («обрезает» - rпune) из дерева многоадресной рассылки.

Поскольку узел «обрезанной» ветви дерева многоадресной рассылки может захотеть присоединиться к группе, протокол периодически удаляет информацию об «обрезанных» ветвях дерева из своей базы данных и верно рассылает многоадресные сообщения по всем интерфейсам данной ветви. Интервал удаления информации об удаленных ветвях задается таймером **Join/Prune Interval**.

Общая настройка PIM-DM

Чтобы активизировать протокол PIM-DM глобально на коммутаторе, выберите меню **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM > PIM-DM Configuration**. Появится следующее окно:



Рисунок 4-89 Окно PIM-DM Global Setting

Для активизации протокола PIM-DM на коммутаторе выберите **Enabled** и нажмите *Apply*.

Параметры PIM-DM на интерфейсе

Нажмите **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM > PIM-DM Interface Settings**. В появившейся таблице **PIM-DM Interface Settings** будут показаны все настроенные

на коммутаторе IP-интерфейсы. Для настройки PIM-DM на отдельном интерфейсе нажмите на ссылку с именем нужного интерфейса, появится меню настройки PIM-DM:

PIM-DM Interface Settings				
Interface Name	IP Address	Hello Interval	Join/Prune Interval	State
System	10.53.13.150	30	60	Disabled

Рисунок 4-90 Таблица PIM-DM Interface Settings

PIM-DM Interface Configuration	
Interface Name	System
IP Address	10.53.13.199
Hello Interval(1-18724 sec)	<input type="text" value="30"/>
Join-Prune Interval(1-18724 sec)	<input type="text" value="60"/>
State	Disabled ▾
<input type="button" value="Apply"/>	

Рисунок 4-91 Меню настройки PIM-DM на интерфейсе

Параметры для настройки:

Параметр	Описание
Interface Name	Показывает имя IP-интерфейса, для которого настраивается протокол PIM-DM. Это должен быть предварительно настроенный на коммутаторе интерфейс.
IP Address	IP-адрес, соответствующий IP-интерфейсу.
Hello Interval (1-18724 sec) <30>	Позволяет задать интервал отправки пакетов Hello в пределах от 1 до 18724 секунд. Значение по умолчанию 30 секунд.
Join/Prune Interval (1-18724 sec) <60>	Позволяет задать интервал времени Join/Prune в пределах от 1 до 18724 секунд, по истечении которого маршрутизатор автоматически удалит информацию об «обрезанной» ветви дерева многоадресной рассылки и начнет веерно рассылать многоадресные сообщения по ветвям дерева. Значение по умолчанию 60 секунд.
State <Disabled>	Позволяет включить (<i>Enabled</i>) или отключить (<i>Disabled</i>) протокол PIM-DM на IP-интерфейсе коммутатора. Значение по умолчанию <i>Disabled</i> .

Нажмите *Apply*, чтобы изменения вступили в силу.

Раздел 5

SNMP-управление

Настройка SNMP

Таблица SNMP User Table

Таблица SNMP View Table

Таблица SNMP Group Table

Таблица SNMP Community Table

Таблица SNMP Host Table

SNMP Engine ID

Настройка SNMP

Протокол SNMP (Simple Network Management Protocol, Простой протокол сетевого управления) – это протокол уровня 7 модели OSI, используемый для удаленного контроля и настройки сетевых устройств. SNMP позволяет станциям сетевого управления просматривать и изменять настройки шлюзов, маршрутизаторов, коммутаторов и других сетевых устройств. Используйте SNMP для настройки системы, контроля производительности и обнаружения потенциальных проблем в коммутаторе или группе коммутаторов.

Управляемые устройства, поддерживающие SNMP, содержат программу (называемую «агентом»), которая работает локально на коммутаторе. Определенный набор переменных (управляемые объекты) обслуживается SNMP-агентом и используется для управления устройством. Данные объекты определены в MIB (Management Information Base, информационная база управления), которая обеспечивает стандартное представление информации, управляемой встроенным SNMP-агентом. SNMP определяет формат MIB и протокола, используемого для доступа к данной информации по сети.

DGS-3324SR поддерживает SNMP версии 1, 2с и 3. Можно указать версию SNMP, используемую для управления коммутатором и мониторинга его работы. Три версии SNMP отличаются в обеспечиваемом уровне безопасности между станцией управления и сетевым устройством.

В SNMP v.1 и SNMP v.2 авторизация пользователя выполняется посредством «строки сообщества» - Community String, которая действует как пароль. Удаленная пользовательская программа SNMP и агент SNMP должны использовать одни и те же Community Strings. Пакеты SNMP от любой станции, которая не была авторизована, игнорируются (отбрасываются).

По умолчанию определены следующие Community Strings, используемые для управления по SNMP v.1 и v.2:

public – позволяет авторизованным станциям управления получать объекты MIB.

private – позволяет авторизованным станциям управления получать и изменять объекты MIB.

SNMP v.3 использует более сложный процесс авторизации, который разделяется на две части. Первая часть используется для поддержания списка пользователей и их атрибутов, которым разрешено управлять по протоколу SNMP. Вторая часть описывает, что каждый пользователь из данного списка может делать при управлении по SNMP.

Коммутатор позволяет указывать и настраивать группы пользователей в данном списке с одинаковым набором привилегий. Для указанных групп может быть установлена версия SNMP. Таким образом, можно создать группу SNMP, которой разрешено просматривать информацию, предназначенную только для чтения, или получать сообщения traps, используя SNMP v.1, в то время как другой группе назначен более высокий уровень безопасности, предоставляющий привилегии чтения/записи, посредством SNMP v.3.

Используя SNMP v.3 можно позволить или запретить индивидуальным пользователям или группам SNMP-менеджеров выполнять конкретные функции SNMP-управления. Разрешенные или запрещенные функции определяются с помощью идентификатора объекта Object Identifier (OID), ассоциированного с

конкретной MIB. Дополнительным уровнем безопасности SNMP v.3 является возможность шифрования SNMP-сообщений. За дополнительной информацией о настройке SNMP v.3 обращайтесь к разделу *Управление*.

Traps

Traps – это сообщения, которые предупреждают о произошедших событиях при работе коммутатора. События могут быть как серьезными типа перезагрузки (кто-то случайно отключил питание коммутатора), так и менее серьезными типа изменения состояния порта. Коммутатор генерирует traps и посылает их станции сетевого управления. Типичными сообщениями traps являются сообщения Authentication Failure, Topology Change, Broadcast/Multicast Storm.

MIB

Управляющая информация и параметры коммутатора хранятся в информационной базе управления (Management Information Base, MIB). Коммутатор использует стандартный модуль информационной базы управления MIB-II. Следовательно, значения входящих в MIB объектов могут быть получены с помощью любых средств сетевого управления, основанных на SNMP. Кроме стандарта MIB-II, коммутатор также поддерживает собственную MIB в виде расширенной информационной базы управления. Объекты этой MIB также могут быть получены путем указания менеджером OID MIB (Object Identifier, идентификатор объекта MIB). Значения объектов MIB могут быть как открытыми только для чтения (read-only), так и для чтения, и для записи (read-write).

DGS-3324SR включает в себя гибкую систему SNMP-управления для обслуживания коммутатора. Система SNMP-управления может быть настроена в соответствии с требованиями сети и предпочтениями сетевого администратора. Используйте меню SNMP V3 для выбора версии SNMP под определенные задачи.

Коммутатор DGS-3324SR поддерживает протокол SNMP (Simple Network Management Protocol, Простой протокол сетевого управления) - версий 1, 2с и 3. Администратор может определить версию протокола SNMP, используемого для управления коммутатором и наблюдения за ним. Три версии SNMP отличаются предоставляемым уровнем безопасности соединения между станцией управления и сетевым устройством.

SNMP можно настроить через различные меню, расположенные в папке SNMP V3 Web-браузера. Можно ограничить круг станций сети, которым будет предоставляться привилегированный доступ к коммутатору, используя меню Management Station IP Address.

Таблица SNMP User Table

В таблице SNMP User Table показаны все SNMP-пользователи коммутатора.


В папке **SNMP Manager** нажмите на ссылку **SNMP User Table**, появится таблица **SNMP User Table**:



The screenshot shows a web interface for managing SNMP users. At the top left is an 'Add' button. Below it, the text reads 'Total Entries: 1 (Note: Maximum of 10 entries.)'. A blue header bar contains the title 'SNMP User Table'. Below the header is a table with four columns: 'User Name', 'Group Name', 'SNMP Version', and 'Delete'. The first row contains the values 'initial', 'initial', 'V3', and a delete icon (an 'X' in a square).

User Name	Group Name	SNMP Version	Delete
initial	initial	V3	

Рисунок 5-1 Таблица SNMP User Table

Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью. Для просмотра подробной информации об SNMP-пользователе нажмите на ссылку с именем пользователя в колонке **User Name**. Появится окно **SNMP User Table Display**:

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

Рисунок 5-2 Подробная информация о пользователе

Показываемые параметры:

Параметр	Описание
User Name	Символьная строка длиной до 32 символов, идентифицирующая SNMP-пользователя.
Group Name	Символьная строка длиной до 32 символов, идентифицирующая SNMP-группу, в которую назначается SNMP-пользователь.
SNMP Version	V1 – используется SNMP v1 V2 – используется SNMP v2 V3 – используется SNMP v3
Auth-Protocol	None – протокол аутентификации не используется. MD5 – используется протокол аутентификации HMAC-MD5-96 SHA – используется протокол аутентификации HMAC-SHA
Priv-Protocol	None – протокол аутентификации не используется. DES – используется шифрование 56-бит DES на основе стандарта CBC-DES (DES-56)

Для возврата в окно **SNMP User Table** нажмите на ссылку [Show All SNMP User Table Entries](#).

Для добавления нового SNMP-пользователя нажмите кнопку *Add*, появится меню **SNMP User Table Configuration**.

SNMP User Table Configuration	
User Name	<input type="text"/>
Group Name	<input type="text"/>
SNMP Version	V1 <input type="checkbox"/> encrypted
Auth-Protocol	MD5 Password <input type="text"/>
Priv-Protocol	DES Password <input type="text"/>
<input type="button" value="Apply"/>	
Show All SNMP User Table Entries	

Рисунок 5-3 Меню SNMP User Table Configuration

Параметры для настройки:

Параметр	Описание
User Name	Символьная строка длиной до 32 символов, идентифицирующая SNMP-пользователя.
Group Name	Символьная строка длиной до 32 символов, идентифицирующая SNMP-группу, в которую назначается SNMP-пользователь.
SNMP Version	В данном меню выберите: V1 - для использования SNMP v1 V2 - для использования SNMP v2 V3 - для использования SNMP v3
Auth-Protocol	Из выпадающего меню выберите: None – протокол аутентификации не используется. MD5 – используется протокол аутентификации HMAC-MD5-96 SHA – используется протокол аутентификации HMAC-SHA
Priv-Protocol	Из выпадающего меню выберите: None – протокол аутентификации не используется. DES – используется шифрование 56-бит DES на основе стандарта CBC-DES (DES-56)
encrypted	Только для SNMP v3. Выберите, будет ли использоваться шифрование.

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в окно **SNMP User Table** нажмите на ссылку [Show All SNMP User Table Entries](#).

Таблица SNMP View Table

Таблица **SNMP View Table** используется для задания наборов объектов MIB, определяющих, какие объекты MIB будут доступны при управлении через SNMP-менеджер. Для просмотра таблицы **SNMP View Table** в папке **SNMP Manager** нажмите на ссылку **SNMP View Table**:

Add			
Total Entries:8 (Note:Maximum of 30 entries.)			
SNMP View Table			
View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	
restricted	1.3.6.1.2.1.11	Included	
restricted	1.3.6.1.6.3.10.2.1	Included	
restricted	1.3.6.1.6.3.11.2.1	Included	
restricted	1.3.6.1.6.3.15.1.1	Included	
CommunityView	1	Included	
CommunityView	1.3.6.1.6.3	Excluded	
CommunityView	1.3.6.1.6.3.1	Included	

Рисунок 5-4 Таблица SNMP View Table

Для удаления записи нажмите в колонке **Delete** рядом с удаляемой записью. Для создания новой записи нажмите кнопку *Add*, появится следующее меню:

Рисунок 5-5 Меню SNMP View Table Configuration

Параметры для настройки:

Параметр	Описание
View Name	Введите символьную строку длиной не более 32 символов. Она используется для идентификации созданного набора объектов SNMP.
Subtree	Введите идентификатор объекта поддерева - Object Identifier (OID) Subtree. OID идентифицирует объект дерева MIB, который включается или исключается из числа доступных SNMP-менеджеру.
View Type	Выберите <i>Included</i> для включения данного объекта в список доступных SNMP-менеджеру. Выберите <i>Excluded</i> для исключения данного объекта из списка доступных SNMP-менеджеру.


Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в окно **SNMP View Table** нажмите на ссылку [Show All SNMP View Table Entries](#).

Таблица SNMP Group Table

Созданная в данной таблице SNMP-группа объединяет SNMP-пользователей, определенных в таблице SNMP User Table, и назначает им заданные в предыдущем меню наборы объектов MIB для просмотра или изменения. Для просмотра таблицы **SNMP Group Table** в папке **SNMP Manager** нажмите на ссылку **SNMP Group Table**:

Group Name	Security Model	Security Level	Delete
public	SNMPv1	NoAuthNoPriv	✕
public	SNMPv2	NoAuthNoPriv	✕
initial	SNMPv3	NoAuthNoPriv	✕
private	SNMPv1	NoAuthNoPriv	✕
private	SNMPv2	NoAuthNoPriv	✕
ReadGroup	SNMPv1	NoAuthNoPriv	✕
ReadGroup	SNMPv2	NoAuthNoPriv	✕
WriteGroup	SNMPv1	NoAuthNoPriv	✕
WriteGroup	SNMPv2	NoAuthNoPriv	✕

Рисунок 5-6 Таблица SNMP Group Table

Для удаления записи нажмите  в колонке **Delete** рядом с удаляемой записью. Для просмотра подробной информации об SNMP-группе нажмите на ссылку с именем группы в колонке **Group Name**. Появится окно **SNMP Group Table Display**:

SNMP Group Table Display	
Group Name	initial
Read View Name	restricted
Write View Name	
Notify View Name	restricted
Security Model	SNMPv3
Security Level	NoAuthNoPriv
Show All SNMP Group Table Entries	

Рисунок 5-7 Подробная информация о SNMP-группе

Для добавления новой SNMP-группы нажмите кнопку *Add*, появится меню **SNMP Group Table Configuration**:

SNMP Group Table Configuration	
Group Name	<input type="text"/>
Read View Name	<input type="text"/>
Write View Name	<input type="text"/>
Notify View Name	<input type="text"/>
Security Model	SNMPv1 ▾
Security Level	NoAuthNoPriv ▾
<input type="button" value="Apply"/>	
Show All SNMP Group Table Entries	

Рисунок 5-8 Меню SNMP Group Table Configuration

Параметры для настройки:

Параметр	Описание
Group Name	Введите символьную строку длиной не более 32 символов. Она используется для идентификации созданной SNMP-группы SNMP-пользователей.
Read View Name	Укажите набор объектов MIB, определяющий, какие объекты MIB может запрашивать данная SNMP-группа для чтения
Write View Name	Укажите набор объектов MIB, определяющий, для каких объектов MIB у данной SNMP-группы будут права на изменение их значений.
Notify View Name	Укажите набор объектов MIB, определяющий, для каких объектов MIB SNMP-агент коммутатора будет генерировать уведомляющие сообщения (traps) для данной SNMP-группы.
Security Model	Используйте данное меню для выбора версии SNMP: SNMPv1 - задает использование SNMP версии 1 SNMPv2 - задает использование SNMP версии 2с. SNMP v2с поддерживает как централизованную систему управления сетью, так и распределенную. Он добавляет некоторые усовершенствования в структуру управляющей

Security Level	<p>информации - Structure of Management Information (SMI) - и некоторые функции обеспечения безопасности.</p> <p>SNMPv3 - задает использование SNMP версии 3. SNMP v3 обеспечивает безопасный доступ к устройству посредством обмена по сети пакетами аутентификации и их шифрованием.</p> <p>Используйте данное меню для выбора уровня безопасности (только для SNMPv3):</p> <p>NoAuthNoPriv - определяет, что коммутатор и удаленный SNMP-менеджер не будут обмениваться пакетами авторизации и зашифровывать пакеты при передаче.</p> <p>AuthNoPriv - требуется авторизация, но пакеты не будут зашифровываться при передаче их между коммутатором и удаленным SNMP-менеджером.</p> <p>AuthPriv - требуется авторизация, и передаваемые между коммутатором и удаленным SNMP-менеджером пакеты будут зашифровываться.</p>
----------------	--

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в окно **SNMP Group Table** нажмите на ссылку [Show All SNMP Group Table Entries](#).

Настройка таблицы SNMP Community Table

Используйте данную таблицу для задания «строки сообщества» SNMP - Community String - определяющей отношение между менеджером и агентом SNMP. Community string действует как пароль при получении доступа к агенту коммутатора. Следующие параметры могут быть связаны с Community String:

- Список IP-адресов SNMP-менеджеров, которым позволено использовать Community String для получения доступа к SNMP-агенту коммутатора.
- Набор объектов MIB, определяющий доступное подмножество всех объектов MIB.
- Возможность чтения/записи или только чтения при обращении к доступным объектам MIB.

Для создания записей SNMP Community , откройте папку **SNMP Manager** и нажмите на ссылку **SNMP Community Table**:

SNMP Community Table Configuration			
Community Name	View Name	Access Right	
<input type="text"/>	<input type="text"/>	Read_Only ▾	
<input type="button" value="Apply"/>			
Total Entries:2 (Note:Maximum of 10 entries.)			
SNMP Community Table			
Community Name	View Name	Access Right	Delete
private	CommunityView	Read_Write	<input type="button" value="X"/>
public	CommunityView	Read_Only	<input type="button" value="X"/>

Рисунок 5-9 Таблица SNMP Community Table

Введите следующие параметры новой записи:

Параметр	Описание
Community Name	Введите символьную строку длиной до 33 символов, которая используется для идентификации членов SNMP-группы. Данная строка используется как пароль при получении доступа удаленным SNMP-менеджером к объектам MIB агента коммутатора.

View Name	Введите символьную строку длиной до 32 символов, которая используется для идентификации набора объектов MIB, доступных для удаленного SNMP-менеджера. Набор объектов с таким же идентификатором View Name должен существовать в таблице SNMP View Table.
Access Right	Используйте данное меню для выбора прав доступа: read_only - определяет, что при использовании заданной выше Community String можно только читать содержимое MIB коммутатора. read_write - определяет, что при использовании заданной выше Community String можно читать и изменять содержимое MIB коммутатора.



Нажмите *Apply*, чтобы изменения вступили в силу. Для удаления записи из таблицы **SNMP Community Table** нажмите  в колонке **Delete** рядом с удаляемой записью.

Таблица SNMP Host Table

Используйте таблицу **SNMP Host Table** для задания IP-адресов станций, которые будут получать уведомляющие сообщения traps.

В папке **SNMP Manager** нажмите на ссылку **SNMP Host Table**, появится таблица **SNMP Host Table**, показанная далее.

Для удаления записи из таблицы **SNMP Host Table** нажмите  в колонке **Delete** рядом с удаляемой записью.

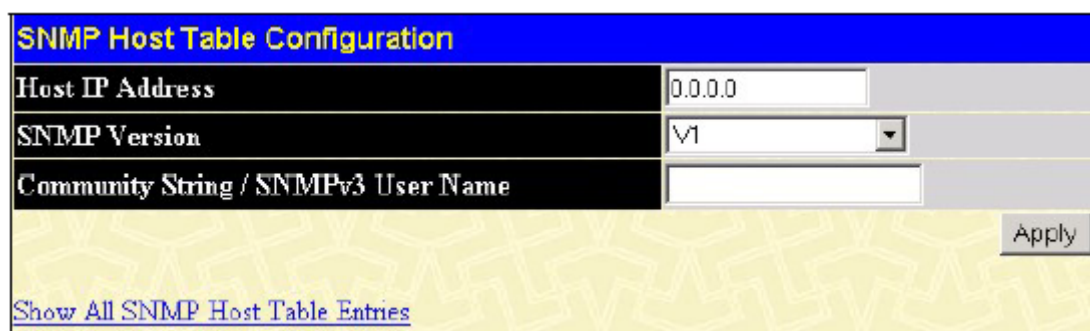
Для просмотра текущих записей таблицы **SNMP Group Table** нажмите на ссылку с IP-адресом SNMP-станции управления в колонке **Host IP Address**.



Add			
Total Entries:0 (Note:Maximum of 10 entries.)			
SNMP Host Table			
Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete

Рисунок 5-10 Таблица SNMP Host Table

Для добавления новой записи в таблицу нажмите кнопку *Add*, появится меню **SNMP Host Table Configuration**:



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

Рисунок 5-11 Меню SNMP Host Table Configuration

Параметры для настройки:

Параметр	Описание
IP Address	Введите IP-адрес удаленной станции управления, которая будет получать сообщения traps от SNMP-агента коммутатора.

SNMP Version	В данном меню выберите: V1 - для использования SNMP v1. V2 - для использования SNMP v2. V3-NoAuth-NoPriv - для использования SNMP v3 с уровнем безопасности NoAuth-NoPriv (без авторизации, без шифрования). V3-Auth-NoPriv - для использования SNMP v3 с уровнем безопасности Auth-NoPriv (с авторизацией, без шифрования). V3-Auth-Priv - для использования SNMP v3 с уровнем безопасности Auth-Priv (с авторизацией, с шифрованием).
Community String or SNMP V3 User Name	Введите Community String или подходящее имя пользователя SNMP V3.

Нажмите *Apply*, чтобы изменения вступили в силу. Для возврата в таблицу **SNMP Host Table** нажмите на ссылку [Show All SNMP Host Table Entries](#).

SNMP Engine ID

Engine ID - это уникальный идентификатор, используемый в реализациях SNMP V3.

Для просмотра SNMP Engine ID коммутатора в папке **SNMP Manager** нажмите на ссылку **SNMP Engine ID**, появится окно **SNMP Engine ID Configuration**:

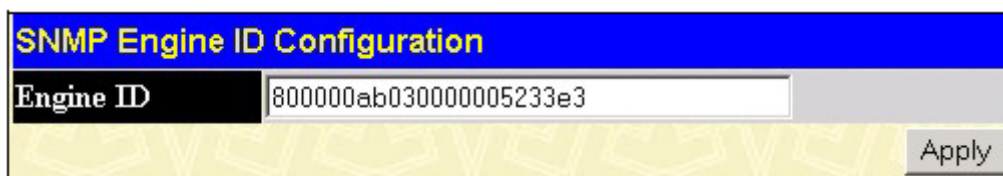


Рисунок 5-12 Окно SNMP Engine ID Configuration

Для изменения **Engine ID** введите новое значение **Engine ID** и нажмите кнопку *Apply*.

Раздел 6

Сетевой мониторинг

- Загрузка портов*
- Пакеты*
- Ошибки*
- Размер пакетов*
- Информация о стеке*
- Состояние коммутатора*
- Таблица MAC-адресов*
- Журнал событий коммутатора*
- Таблица IGMP Snooping*
- Порты Router Port*
- Управление доступом на портах*
- Мониторинг функций 3-его уровня*

Загрузка портов

В окне **Port Utilization** отображается использование полосы пропускания в процентном отношении для данного порта. Статистику загрузки портов также можно посмотреть в виде графика или таблицы.

Для просмотра загрузки портов в папке **Monitoring** нажмите на ссылку **Port Utilization**:

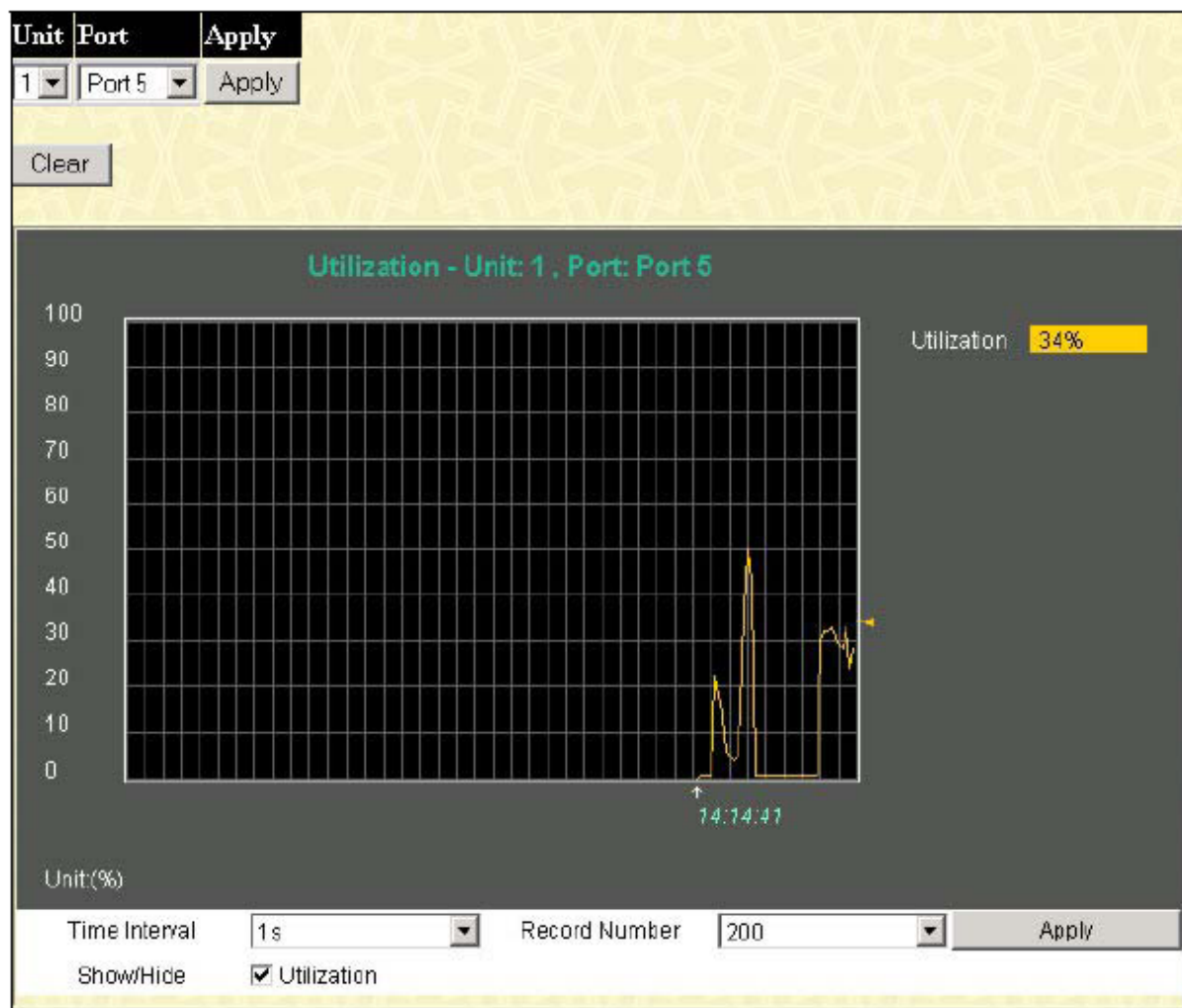


Рисунок 6-1 График загрузки портов

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
Unit	Позволяет выбрать коммутатор в стеке по его идентификатору Unit ID при объединении коммутаторов в стек. 15 указывает, что коммутатор работает в автономном режиме.
Port	Порт коммутатора, для которого показывается статистика. Нажмите <i>Apply</i> для просмотра статистики для выбранного порта.
Time Interval	Выберите значение между 1s и 60s (s – секунды). Значение по умолчанию 1.
Record Number	Определите, сколько раз за интервал Time Interval коммутатор будет снимать показания. Значение находится в пределах от 20 до 200, по умолчанию 200.

Пакеты

Web-интерфейс управления позволяет просмотреть различную статистику о пакетах в виде графика или таблицы.

Принятые пакеты

В папке **Monitoring** откройте папку **Packets** и нажмите на ссылку **Received(Rx)**, появится график количества принятых коммутатором пакетов.

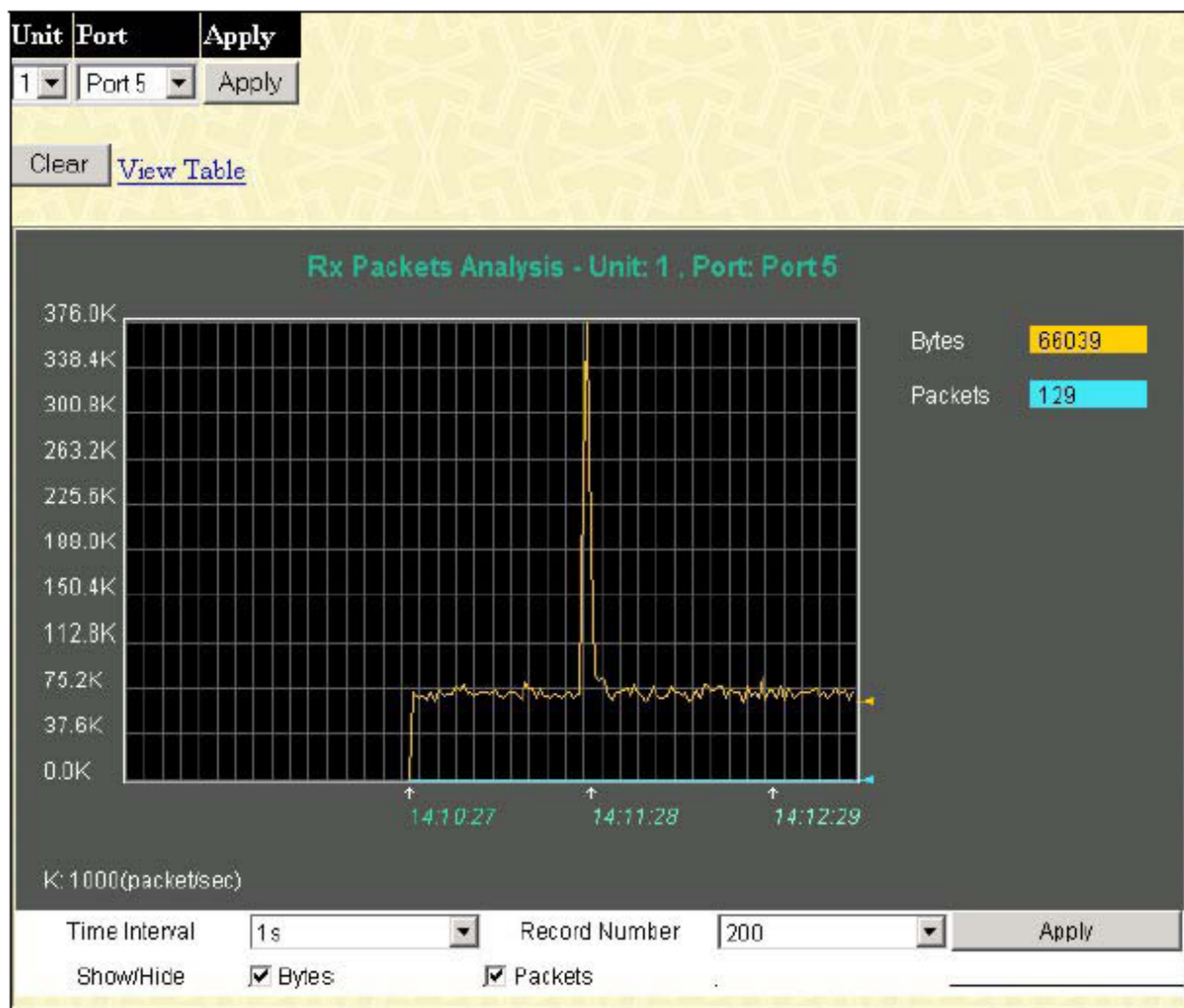


Рисунок 6-2 Статистика принятых пакетов (график в байтах и пакетах)

Для просмотра статистики в виде таблицы нажмите на ссылку [View Table](#):

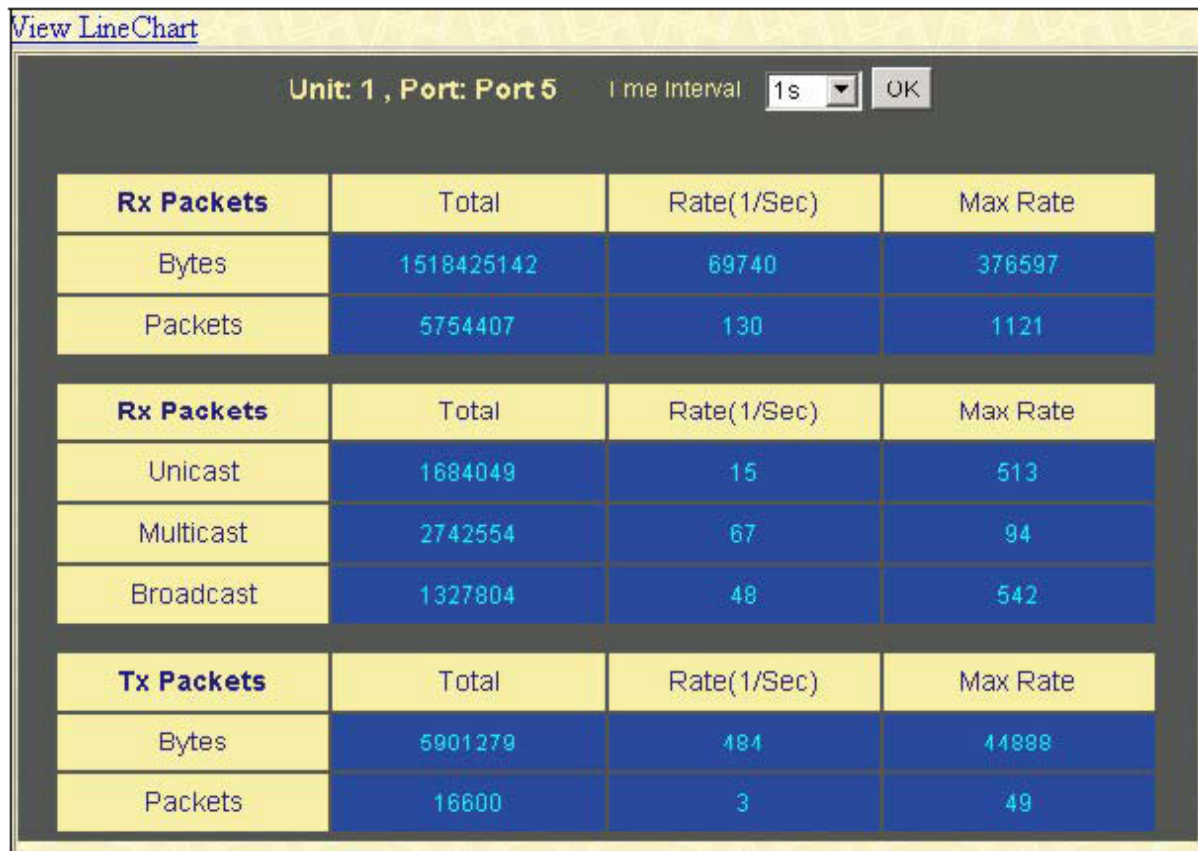


Рисунок 6-3 Статистика принятых пакетов (таблица в байтах и пакетах)

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
Time Interval [1s]	Выберите значение между 1s и 60s (s – секунды). Значение по умолчанию 1.
Record Number [200]	Определите, сколько раз за интервал Time Interval коммутатор будет снимать показания. Значение находится в пределах от 20 до 200, по умолчанию 200.
Bytes	Количество байт, принятых данным портом.
Packets	Количество пакетов, принятых данным портом.
Show/Hide	Можно отключить показ счетчиков Bytes и Packets.
Clear	Нажмите для сброса накопленной статистики.
View Table	Нажмите для перехода в режим таблицы.
View Line Chart	Нажмите для перехода в режим графика.

Принятые одноадресные/групповые/широковещательные пакеты (UMB_cast)

В папке **Monitoring** откройте папку **Packets** и нажмите на ссылку **UMB_cast(Rx)**, появится график количества принятых пакетов различных типов (UMB cast).



Рисунок 6-4 Статистика принятых пакетов (график для одноадресных, групповых и широковещательных пакетов)

Для просмотра статистики в виде таблицы нажмите на ссылку [View Table](#):

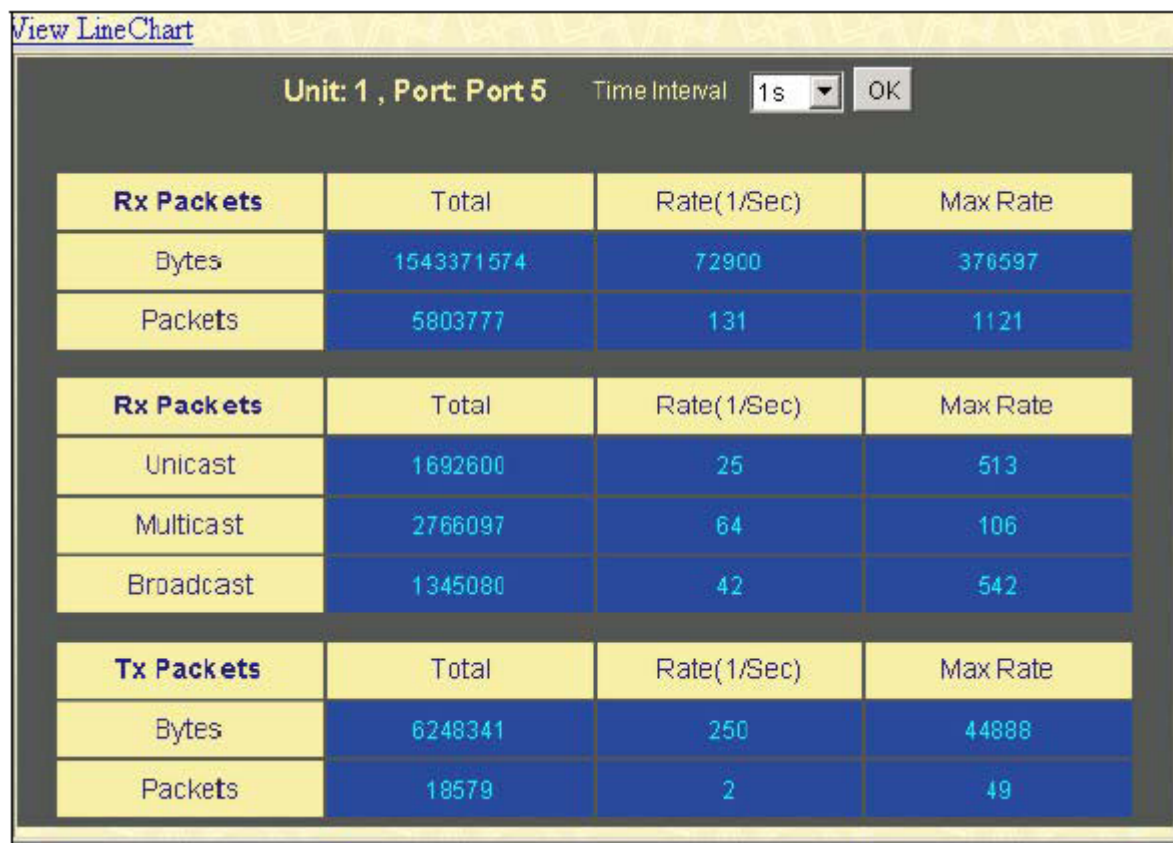


Рисунок 6-5 Статистика принятых пакетов (таблица для одноадресных, групповых и широковещательных пакетов)

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
Time Interval [1s]	Выберите значение между 1s и 60s (s – секунды). Значение по умолчанию 1.
Record Number [200]	Определите, сколько раз за интервал Time Interval коммутатор будет снимать показания. Значение находится в пределах от 20 до 200, по умолчанию 200.
Unicast	Общее количество правильно сформированных одноадресных пакетов, принятых данным портом.
Multicast	Общее количество правильно сформированных многоадресных пакетов, принятых данным портом.
Broadcast	Общее количество правильно сформированных широковещательных пакетов, принятых данным портом.
Show/Hide	Можно отключить показ счетчиков Unicast, Multicast и Broadcast.
Clear	Нажмите для сброса накопленной статистики.
View Table	Нажмите для перехода в режим таблицы.
View Line Chart	Нажмите для перехода в режим графика.

Отправленные пакеты

В папке **Monitoring** откройте папку **Packets** и нажмите на ссылку **Transmitted (Tx)**, появится график количества отправленных коммутатором пакетов.

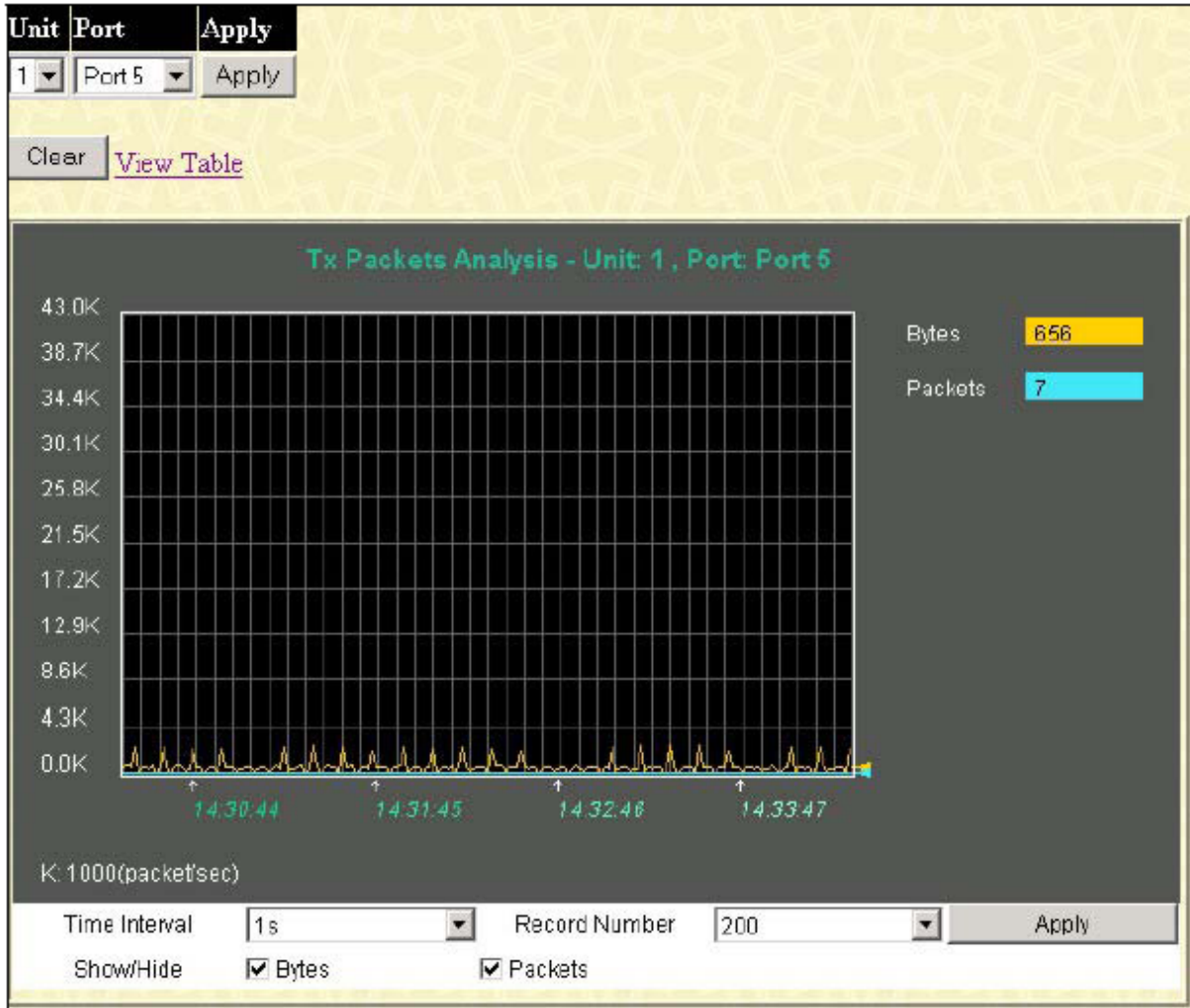


Рисунок 6-6 Статистика отправленных пакетов (график в байтах и пакетах)

Для просмотра статистики об отправленных пакетах различного типа в виде таблицы нажмите на ссылку [View Table](#):

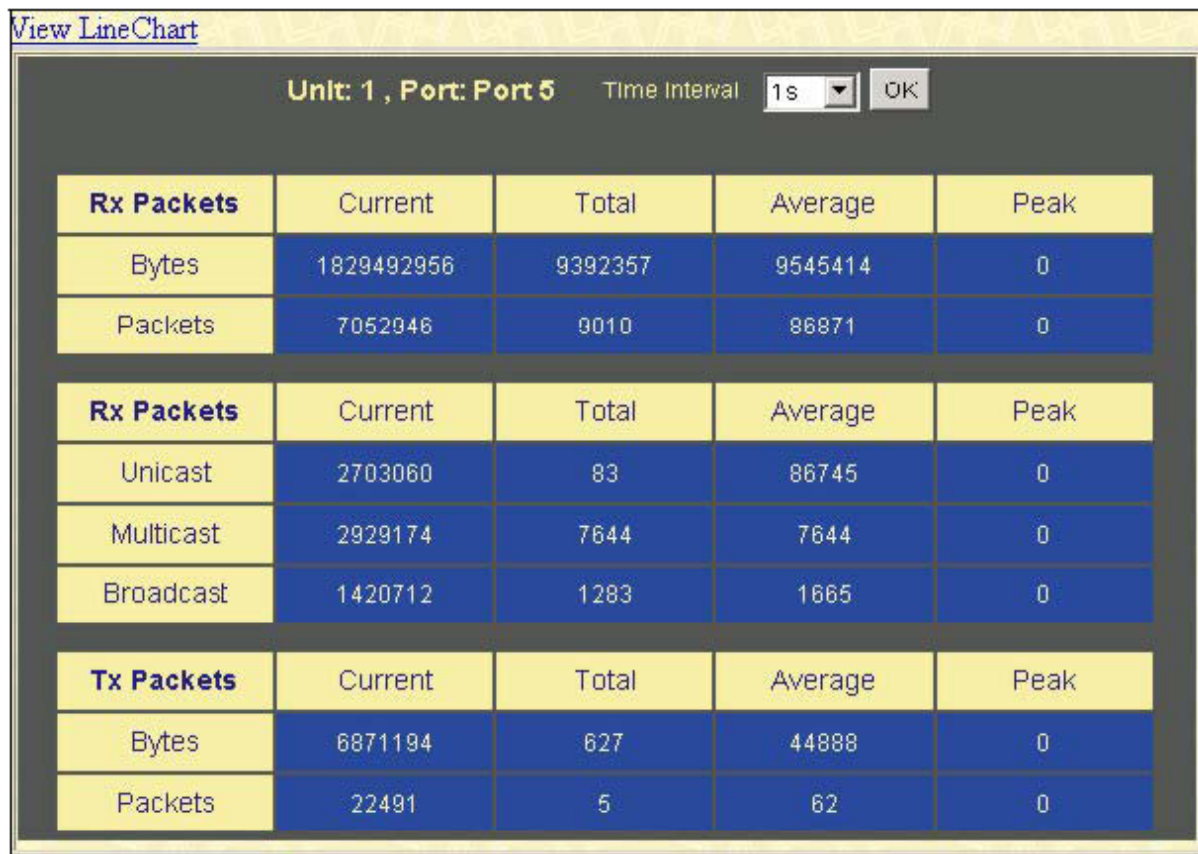


Рисунок 6-7 Статистика отправленных пакетов (таблица в байтах и пакетах)

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
Time Interval [1s]	Выберите значение между 1s и 60s (s – секунды). Значение по умолчанию 1.
Record Number [200]	Определите, сколько раз за интервал Time Interval коммутатор будет снимать показания. Значение находится в пределах от 20 до 200, по умолчанию 200.
Bytes	Количество байт, отправленных данным портом.
Packets	Количество пакетов, отправленных данным портом.
Show/Hide	Можно отключить показ счетчиков Bytes и Packets.
Clear	Нажмите для сброса накопленной статистики.
View Table	Нажмите для перехода в режим таблицы.
View Line Chart	Нажмите для перехода в режим графика.

Ошибки

Web-интерфейс управления позволяет просмотреть статистику об ошибках на портах в виде графика или таблицы.

Принятые пакеты

В папке **Monitoring** откройте папку **Errors** и нажмите на ссылку **Received(Rx)**, появится график количества принятых коммутатором пакетов с ошибками.

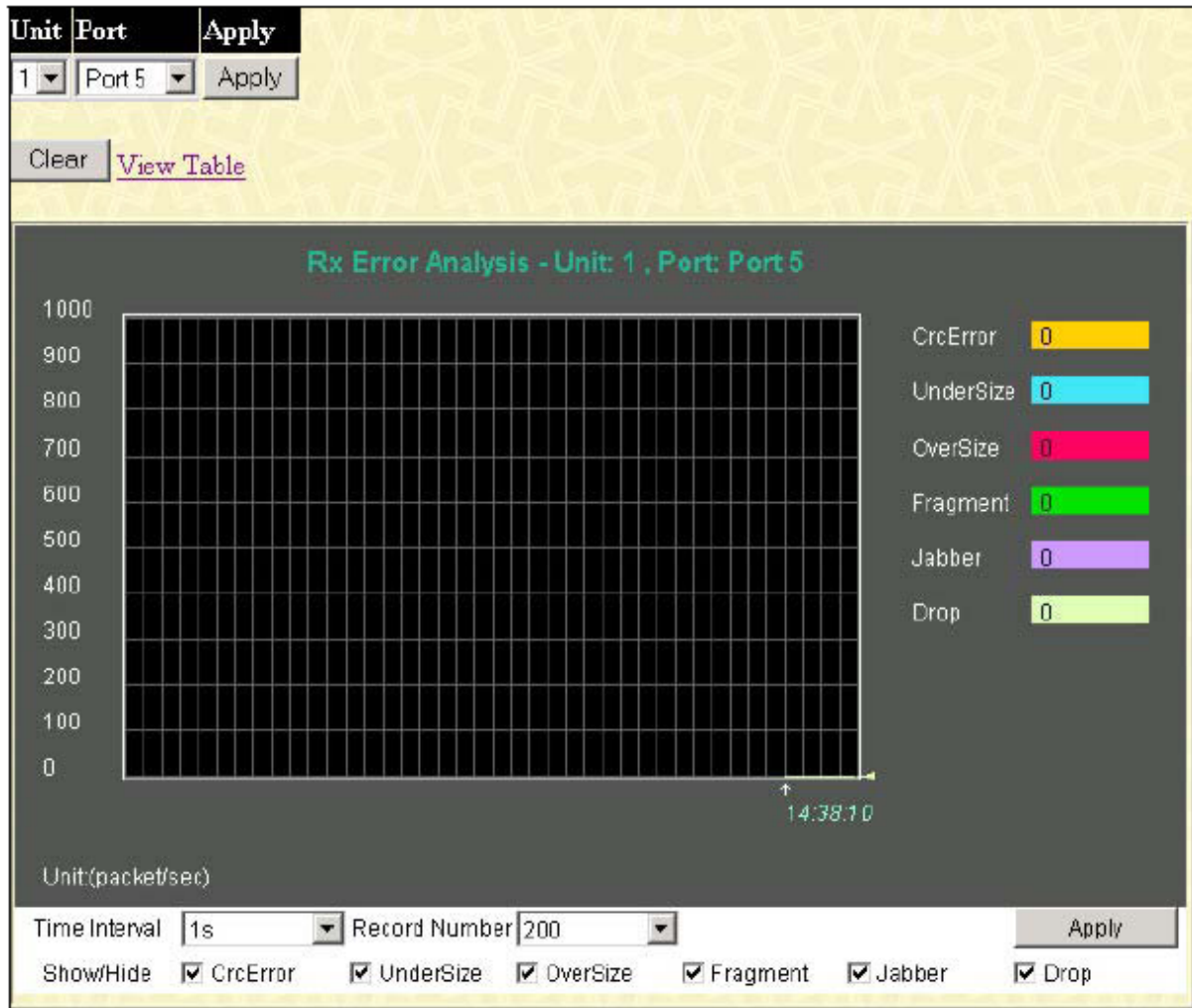


Рисунок 6-8 Статистика принятых пакетов с ошибками (график)

Для просмотра статистики в виде таблицы нажмите на ссылку [View Table](#):

View LineChart

Unit: 1 , Port: Port 5 Time Interval 1s OK

Rx Error	Tctal	Rate(1/Sec)	Max Rate
CrcError	71	0	0
UnderSize	0	0	0
OverSize	0	0	0
Fragment	0	0	0
Jabber	9	0	0
Drop	131	1	1

Рисунок 6-9 Статистика принятых пакетов с ошибками (таблица)

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
Time Interval [1s]	Выберите значение между 1s и 60s (s – секунды). Значение по умолчанию 1.
Record Number [200]	Определите, сколько раз за интервал Time Interval коммутатор будет снимать показания. Значение находится в пределах от 20 до 200, по умолчанию 200.
CrcError	Количество правильно сформированных пакетов, но контрольная сумма которых неверна.
UnderSize	Количество принятых кадров размером меньше минимального разрешенного в 64 байт, но имеющих верную сумму CRC. Такие кадры обычно указывают на возникновение коллизии – обычное явление в сети.
OverSize	Количество принятых кадров размером больше 1518 байт (или с тегом VLAN – 1522 байт) и меньше, чем значение MAX_PKT_LEN. Внутреннее значение MAX_PKT_LEN равно 1522 байт.
Fragment	Количество принятых кадров длиной менее 64 байт и содержащих ошибки FCS или ошибки выравнивания. Это обычно результат коллизии.
Jabber	Количество принятых кадров размером больше значения MAX_PKT_LEN. Внутреннее значение MAX_PKT_LEN равно 1522 байт.
Drop	Количество кадров, отброшенных портом с момента последней перезагрузки коммутатора.
Show/Hide	Можно отключить показ счетчиков CrcError, UnderSize, OverSize, Fragment, Jabber и Drop.
Clear	Нажмите для сброса накопленной статистики.
View Table	Нажмите для перехода в режим таблицы.
View Line Chart	Нажмите для перехода в режим графика.

Отправленные пакеты

В папке **Monitoring** откройте папку **Error** и нажмите на ссылку **Transmitted (Tx)**, появится график возникших при отправке пакетов ошибок.

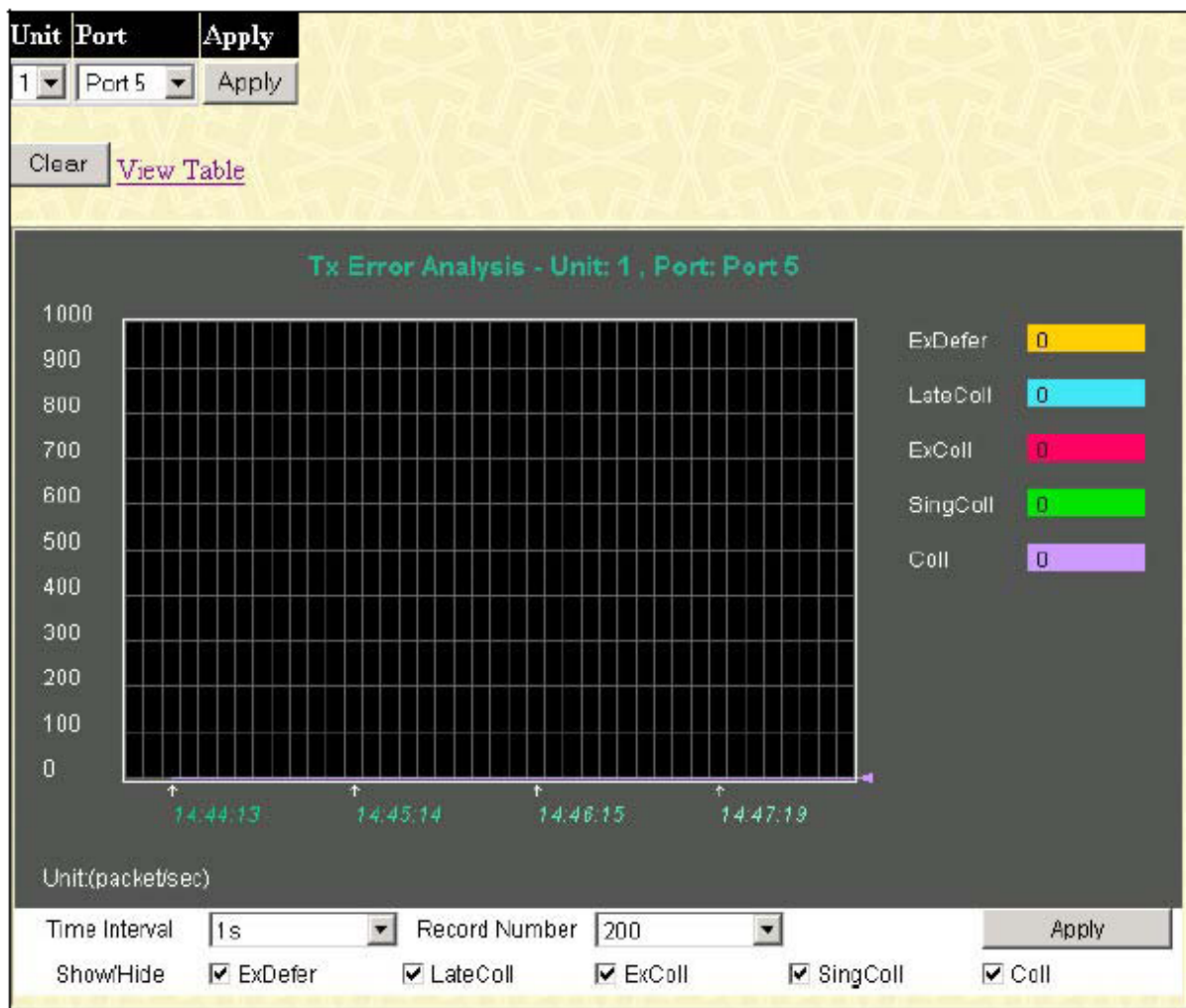


Рисунок 6-10 Статистика возникших ошибок при отправке пакетов (график)

Для просмотра статистики в виде таблицы нажмите на ссылку [View Table](#):

Tx Error	Total	Rate (1/Sec)	Max Rate
ExDefer	0	0	0
LateColl	0	0	0
ExColl	0	0	0
SingColl	0	0	0
Coll	0	0	0

Рисунок 6-11 Статистика возникших ошибок при отправке пакетов (таблица)

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
Time Interval [1s]	Выберите значение между 1s и 60s (s – секунды). Значение по умолчанию 1.
Record Number [200]	Определите, сколько раз за интервал Time Interval коммутатор будет снимать показания. Значение находится в пределах от 20 до 200, по умолчанию 200.
ExDefer	Количество кадров, первая попытка передачи которых была отложена по причине занятости среды передачи.
LateColl	Количество случаев обнаружения коллизии при передаче пакета позднее, чем 512 битовых интервала.
ExColl	Количество кадров, передача которых завершилась неудачей по причине чрезмерных коллизий.
SingColl	Количество удачно переданных кадров, передача которых была задержана более чем одной коллизией.
Coll	Общее число установленных в данном сегменте сети коллизий.
Show/Hide	Можно отключить показ счетчиков ExDefer, LateColl, ExColl, Coll и SingColl.
Clear	Нажмите для сброса накопленной статистики.
View Table	Нажмите для перехода в режим таблицы.
View Line Chart	Нажмите для перехода в режим графика.

Размер пакетов

Web-интерфейс управления позволяет просмотреть статистику о размере принятых коммутатором пакетов, разбитых на 6 групп, в виде графика или таблицы.



Рисунок 6-12 Статистика размера принятых пакетов (график)

Для просмотра статистики в виде таблицы нажмите на ссылку [View Table](#):

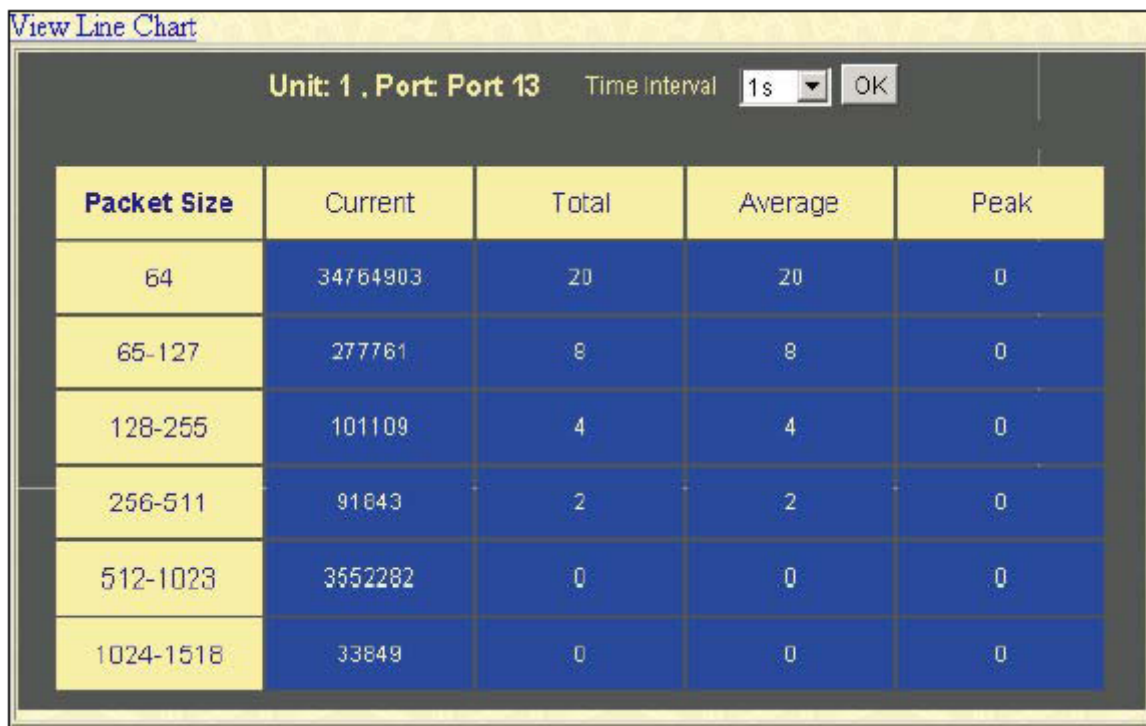


Рисунок 6-13 Статистика размера принятых пакетов (таблица)

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
Time Interval [1s]	Выберите значение между 1s и 60s (s – секунды). Значение по умолчанию 1.
Record Number [200]	Определите, сколько раз за интервал Time Interval коммутатор будет снимать показания. Значение находится в пределах от 20 до 200, по умолчанию 200.
64	Общее количество принятых пакетов (включая неверно сформированные), длина которых составляет 64 байта (без преамбулы, но с контрольной суммой FCS).
65-127	Общее количество принятых пакетов (включая неверно сформированные), длина которых находится в пределах от 65 байт до 127 байт (без преамбулы, но с контрольной суммой FCS).
128-255	Общее количество принятых пакетов (включая неверно сформированные), длина которых находится в пределах от 128 байт до 255 байт (без преамбулы, но с контрольной суммой FCS).
256-511	Общее количество принятых пакетов (включая неверно сформированные), длина которых находится в пределах от 256 байт до 511 байт (без преамбулы, но с контрольной суммой FCS).
512-1023	Общее количество принятых пакетов (включая неверно сформированные), длина которых находится в пределах от 512 байт до 1023 байт (без преамбулы, но с контрольной суммой FCS).
1024-1518	Общее количество принятых пакетов (включая неверно сформированные), длина которых находится в пределах от 1024 байт до 1518 байт (без преамбулы, но с контрольной суммой FCS).
Show/Hide	Можно отключить показ счетчиков 64, 65-127, 128-255, 256-511, 512-1023, 1024-1518.
Clear	Нажмите для сброса накопленной статистики.
View Table	Нажмите для перехода в режим таблицы.
View Line Chart	Нажмите для перехода в режим графика.

Информация о стеке

Для изменения параметров стека по умолчанию (например, порядка коммутаторов в стеке) используйте меню **Box Information** в папке **Configuration**.

Количество коммутаторов в составе стека (максимально 12) показывается в правом верхнем углу Web-браузера. Значки устройств следуют в порядке присвоенных коммутаторам Unit ID (порядковый номер устройства в стеке), поэтому коммутатор с Unit 1 соответствует самому левому значку в группе.

Когда коммутаторы правильно объединены в стек при помощи дополнительных модулей стекирования, то информация о стеке отображается в меню **Stack Information**.

Для просмотра информации о стеке в папке **Monitoring** нажмите на ссылку **Stacking Information**.

Stacking Information								
Box ID	User Set	Type	Exist	Start Port	Priority	Prom version	Runtime version	H/W version
1	1	DGS-3224SR	exist	1	16	1.00-B03	1.10-B22	2A1
2	---	USR-NOT-CFG	no					
3	---	USR-NOT-CFG	no					
4	---	USR-NOT-CFG	no					
5	---	USR-NOT-CFG	no					
6	---	USR-NOT-CFG	no					
7	---	USR-NOT-CFG	no					
8	---	USR-NOT-CFG	no					
9	---	USR-NOT-CFG	no					
10	---	USR-NOT-CFG	no					
11	---	USR-NOT-CFG	no					
12	---	USR-NOT-CFG	no					
Topology :		DUPLEX_CHAIN						
My Box ID :		1						
Current state :		MASTER						
Box count :		1						

Рисунок 6-14 Информация о стеке коммутаторов

Показываемые параметры:

Параметр	Описание
Box ID	Порядковый номер коммутатора в стеке.
User Set	Порядковый номер может быть назначен автоматически (Auto) или статически. По умолчанию Auto.
Type	Модель соответствующего коммутатора в стеке.
Exist	Показывает, находится ли коммутатор в стеке или нет.
Start Port	Показывает порядковый номер первого порта коммутатора среди всех портов в составе стека.
Priority	Показывает приоритет коммутатора. Меньшее значение указывает на больший приоритет. Коммутатор с наименьшим значением приоритета в стеке является мастер-коммутатором стека.
Prom Version	Версия PROM коммутатора. Может отличаться от показанной на рисунке.

Runtime Version	Версия firmware коммутатора. Может отличаться от показанной на рисунке.
H/W Version	Аппаратная версия коммутатора. Может отличаться от показанной на рисунке.

Состояние коммутатора

В папке **Monitoring** нажмите на ссылку **Device Status**, появится окно **Device Status**. Оно показывает состояние физических компонентов коммутатора, включая источник питания и вентиляторы.

Device Status				
ID	Internal Power	External Power	Side Fan	Back Fan
1	Active	Fail	OK	OK
2	Active	Fail	OK	OK

Рисунок 6-15 Окно Device Status

Показываемые параметры:

Параметр	Описание
ID	Порядковый номер коммутатора в стеке.
Internal Power	Текущее состояние внутреннего источника питания. <i>Active</i> указывает, что источник питания работает нормально. <i>Fail</i> указывает на сбой в работе источника питания.
External Power	Текущее состояние внешнего источника питания. <i>Active</i> указывает, что источник питания работает нормально. <i>Fail</i> указывает на сбой в работе источника питания.
Side Fan	Показывает состояние вентилятора на боковой панели коммутатора.
Back Fan	Показывает состояние вентилятора на задней панели коммутатора.

Таблица MAC-адресов

В данном меню можно просмотреть динамически создаваемую таблицу MAC-адресов. Когда коммутатор изучил соответствие между MAC-адресом и номером порта, то создает запись в своей адресной таблице. В дальнейшем эти записи используются коммутатором для продвижения пакетов.

Для просмотра адресной таблицы в папке **Monitoring** нажмите на ссылку **MAC Address**, появится следующее окно:

VLAN Name Find Delete
 MAC Address Find Delete
 Unit - Port Find Delete

MAC Address Table

VID	Vlan Name	MAC Address	Unit	Port	Type
1	default	00-00-00-44-73-01	1	1	Dynamic
1	default	00-00-00-44-73-02	1	1	Dynamic
1	default	00-00-00-44-73-03	1	1	Dynamic
1	default	00-00-00-53-97-89	1	1	Dynamic
1	default	00-00-33-48-49-00	System	--	Self
1	default	00-00-5e-00-01-01	1	1	Dynamic
1	default	00-00-81-05-00-01	1	1	Dynamic
1	default	00-00-81-05-02-33	1	1	Dynamic
1	default	00-00-81-9a-f2-f4	1	1	Dynamic
1	default	00-00-e2-4f-57-03	1	1	Dynamic
1	default	00-00-e2-54-de-9a	1	1	Dynamic
1	default	00-00-e2-7f-6b-53	1	1	Dynamic
1	default	00-00-e8-67-97-72	1	1	Dynamic
1	default	00-01-02-03-04-00	1	1	Dynamic
1	default	00-01-02-03-10-01	1	1	Dynamic
1	default	00-01-06-30-10-63	1	1	Dynamic
1	default	00-01-27-35-26-01	1	1	Dynamic
1	default	00-01-27-35-26-02	1	1	Dynamic
1	default	00-01-30-12-13-02	1	1	Dynamic
1	default	00-01-30-fa-5f-00	1	1	Dynamic

Total Entries: 603

Рисунок 6-16 Таблица MAC-адресов

Следующие параметры можно просмотреть или настроить:

Параметр	Описание
VLAN ID	Позволяет выбрать для просмотра записи по VLAN ID (VID).
MAC Address	Позволяет выбрать для просмотра записи по MAC-адресу.
Unit – Port	Позволяет выбрать для просмотра записи по порядковому номеру коммутатора в стеке и номеру порта.
Find	Поиск записей по указанным значениям VLAN ID, MAC Address и Unit – Port.
VID	Идентификатор VLAN, членом которой является данный порт.
MAC Address	MAC-адрес, занесенный в адресную таблицу.
Unit	Порядковый номер коммутатора в составе стека.
Port	Порт коммутатора, к которому подключено устройство с данным MAC-адресом.
Learned	Как коммутатор изучил данный MAC-адрес. Возможные значения <i>Dynamic(динамически)</i> , <i>Self(собственный MAC-адрес порта)</i> и <i>Static(статически)</i> .

Next

Нажмите для просмотра следующей части адресной таблицы

Журнал событий коммутатора

Web-интерфейс управления позволяет просмотреть журнал событий коммутатора.

Switch History		
Sequence	Time	Log Text
21	2003-12-02, 11:45:15	Topology changed
20	2003-12-02, 11:42:12	Unit 1, Console session timed out (Username: Anonymous)
19	2003-12-02, 11:32:42	Successful login through Web (Username: Anonymous)
18	2003-12-02, 11:31:26	Unit 1, Configuration saved to flash (Username: Anonymous)
17	2003-12-02, 11:30:51	Unit 1, Successful login through Console (Username: Anonymous)
16	2003-12-02, 11:30:30	Port 1:15 link up, 100Mbps FULL duplex
15	2003-12-02, 11:30:30	Unit 1, System started up
14	2003-12-02, 11:26:38	Unit 1, Configuration saved to flash (Username: Anonymous)
13	2003-12-02, 11:26:38	Unit 1, Configuration saved to flash (Username: Anonymous)
12	2003-12-02, 11:26:20	Unit 1, Successful login through Console (Username: Anonymous)
11	2003-12-02, 11:25:49	Unit 1, Firmware upgraded successfully (Username: Anonymous)
10	2003-12-02, 10:50:09	Unit 1, Console session timed out (Username: Anonymous)
9	2003-12-02, 10:42:00	Successful login through Web (Username: Anonymous)
8	2003-12-02, 10:41:35	Port 1:15 link up, 100Mbps FULL duplex
7	2003-12-02, 10:40:06	Unit 1, Successful login through Console (Username: Anonymous)
6	2003-12-02, 10:39:21	Unit 1, System started up
5	2003-11-26, 10:42:59	Unit 1, Configuration saved to flash (Username: Anonymous)
4	2003-11-26, 10:42:14	Unit 1, Successful login through Console (Username: Anonymous)
3	2003-11-26, 10:40:39	Port 1:13 link up, 100Mbps FULL duplex
2	2003-11-26, 10:40:39	Unit 1, System started up

Clear Next

Рисунок 6-17 Журнал событий коммутатора

Показываемые параметры:

Параметр	Описание
Sequence	Порядковый номер системного события.
Time	Показывает время системного события.
Log Text	Краткое описание системного события.

Next	Нажмите для просмотра следующей части журнала событий коммутатора.
Clear	Нажмите для очистки журнала событий.

Таблица IGMP Snooping

Функция IGMP Snooping позволяет коммутатору просматривать в проходящих через него пакетах IGMP групповой IP-адрес и соответствующий MAC-адрес. Количество просмотренных IGMP-отчетов показывается в поле **Reports**.

Для просмотра таблицы **IGMP Snooping** в папке **Monitoring** нажмите на ссылку **IGMP Snooping Group**:

Total Entries : 1																								
IGMP Snooping Table																								
VLAN ID	Multicast Group											MAC Address								Queries	Reports			
0	0.0.0.0											00:00:00:00:00:00								Disabled	0			
Unit	Port Map																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1																								
2																								
3																								
4																								
5																								
6																								
7																								
8																								
9																								
10																								
11																								
12																								

Рисунок 6-18 Таблица IGMP Snooping

Показываемые параметры:

Параметр	Описание
VLAN ID	Идентификатор VLAN ID группы многоадресной рассылки.
Multicast Group	IP-адрес группы многоадресной рассылки.
MAC Address	MAC-адрес группы многоадресной рассылки.
Queries	Статус Querier State. <i>Disabled</i> означает, что коммутатор не передает пакеты IGMP Snooping Query, иначе <i>Enabled</i> .
Reports	Общее количество отчетов, принятых коммутатором от данной группы.



Примечание: Для настройки IGMP Snooping на коммутаторе DGS-3324SR в папке **Configuration** нажмите на ссылку **IGMP**. Информацию о настройке и иную информацию относительно функции IGMP Snooping смотрите в Разделе 4 данного руководства.

Порты Router Port

В данном меню можно посмотреть, какие порты коммутатора настроены как Router Ports. Порты Router Ports, настроенные пользователем (через консоль или Web-интерфейс), отображаются как статические Router Ports и помечены символом **S**. Порты Router Ports, настроенные коммутатором динамически, помечены символом **D**.

Browse Router Port																								
VLAN ID												VLAN Name												
1												default												
Unit	Ports																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1																								
2																								
3																								
4																								
5																								
6																								
7																								
8																								
9																								
10																								
11																								
12																								

Рисунок 6-19 Порты Router Port

Управление доступом на портах

Следующие меню позволяют просмотреть данные об аутентификации 802.1x на коммутаторе по портам. Доступ к ним можно получить по ссылке **Port Access Control** в папке **Monitoring**. Статистика показывается в 5 различных окнах.

Состояние аутентификации на коммутаторе

В меню **Authenticator State** можно просмотреть состояние аутентификации портов коммутатора. Записи в таблице показывают состояние аутентификации каждого порта, поддерживающего функцию аутентификации. Выберите **Monitoring > Port Access Control > Authenticator Statistics**, появится следующее окно:

Port	Frames Rx	Frames Tx	Rx Start	TxReqID	RxLogOff	TxReq	RxRespId	RxResp	RxInvalid	RxError	Last Version	Last Source
1	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
2	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
3	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
4	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
5	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
6	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
7	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
8	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
9	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
10	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
11	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
12	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
13	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
14	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
15	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
16	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
17	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
18	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
19	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
20	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
21	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
22	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
23	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
24	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00

Рисунок 6-20 Состояние аутентификации портов

Поле **Unit** позволяет выбрать коммутатор в составе стека по его Unit ID. В поле **Time Interval** можно указать интервал обновления данных от 1s до 60s (“s” – секунды). По умолчанию данные обновляются один раз в секунду.

Показываемые параметры:

Параметр	Описание
Port	Порт коммутатора.
Frames Rx	Количество принятых портом правильных кадров EAPOL.
Frames Tx	Количество отправленных портом кадров EAPOL.
Rx Start	Количество принятых портом кадров EAPOL Start.
TxReqID	Количество отправленных портом кадров EAP Req/Id.
RxLogOff	Количество принятых портом кадров EAPOL Logoff.
TxReq	Количество отправленных портом кадров EAP Request (всех, кроме Req/Id).
RxRespId	Количество принятых портом кадров EAP Resp/Id.
RxResp	Количество принятых портом правильных кадров EAP Response (всех, кроме Resp/Id).
RxInvalid	Количество принятых портом кадров EAPOL, тип которых не был распознан.
RxError	Количество принятых портом кадров EAPOL, в которых поле Packet Body Length не верно.
Last Version	Версия протокола в большинстве недавно принятых кадров EAPOL.
Last Source	MAC-адрес источника в большинстве недавно принятых кадров EAPOL.

Статистика сессий аутентификации

В меню **Authenticator Session Statistics** можно просмотреть статистические данные о сессиях аутентификации по портам коммутатора. Записи в таблице показывают статистику для каждого порта, поддерживающего функцию аутентификации. Выберите **Monitoring > Port Access Control > Authenticator Session Statistics**, появится следующее окно:

Port	Octets Rx	Octets Tx	Frames Rx	Frames Tx	ID	Authentic Method	Time	Terminate Cause	User Name
1	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
2	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
3	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
4	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
5	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
6	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
7	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
8	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
9	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
10	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
11	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
12	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
13	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
14	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
15	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
16	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
17	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
18	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
19	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
20	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
21	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
22	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
23	0	0	0	0	10A	Remote Authentic Server	0	MA	MA
24	0	0	0	0	10A	Remote Authentic Server	0	MA	MA

Рисунок 6-21 Статистика по сессиям аутентификации на портах

Поле **Unit** позволяет выбрать коммутатор в составе стека по его Unit ID. В поле **Time Interval** можно указать интервал обновления данных от 1s до 60s (“s” – секунды). По умолчанию данные обновляются один раз в секунду.

Показываемые параметры:

Параметр	Описание
Port	Порт коммутатора.
Octets Rx	Счетчик байт, принятых портом в кадрах пользовательских данных в течение сессии.
Octets Tx	Счетчик байт, отправленных портом в кадрах пользовательских данных в течение сессии.
Frames Rx	Счетчик принятых портом кадров пользовательских данных в течение сессии.
Frames Tx	Счетчик отправленных портом кадров пользовательских данных в течение сессии.
ID	Уникальный идентификатор сессии в форме печатной строки ASCII, длиной как минимум 3 символа.
Authentic Method	Метод аутентификации, используемый для установления сессии. Возможные методы: (1) Remote Authentic Server – используется внешний сервер аутентификации. (2) Local Authentic Server – используется встроенный сервер аутентификации.
Time	Длительность сессии в секундах.
Terminate Cause	Причина завершения сессии. Возможны 8 причин завершения сессии: 1) Supplicant Logoff – завершение работы клиента. 2) Port Failure – сбой порта. 3) Supplicant Restart – перезагрузка клиента. 4) Reauthentication Failure – сбой повторной аутентификации. 5) AuthControlledPortControl set to ForceUnauthorized – параметр AuthControlledPortControl был установлен в значение ForceUnauthorized 6) Port re-initialization – повторная инициализация порта. 7) Port Administratively Disabled – порт административно отключен. 8) Not Terminated Yet – сессия еще не завершена.
User Name	Имя пользователя, идентифицирующее личность клиента.

Диагностика аутентификации

В меню **Authenticator Diagnostics** доступна диагностическая информация об аутентификации по портам коммутатора. Записи в таблице показывают данные для каждого порта, поддерживающего функцию аутентификации. Выберите **Monitoring > Port Access Control > Authenticator Diagnostics**, появится следующее окно:

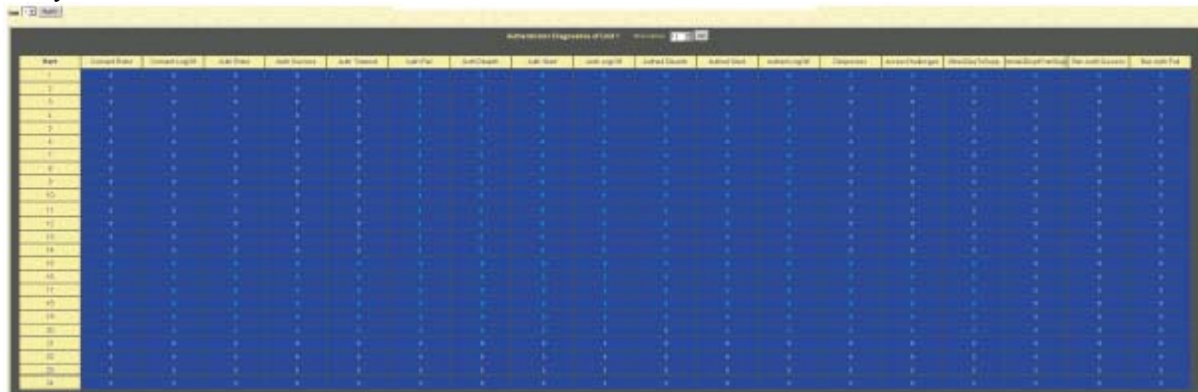


Рисунок 6-22 Диагностика аутентификации

Поле **Unit** позволяет выбрать коммутатор в составе стека по его Unit ID. В поле **Time Interval** можно указать интервал обновления данных от 1s до 60s (“s” – секунды). По умолчанию данные обновляются один раз в секунду.

Показываемые параметры:

Параметр	Описание
Port	Порт коммутатора.
Connect Enter	Количество переходов state machine (машины состояний) в состояние CONNECTING из любого другого состояния.
Connect LogOff	Количество переходов state machine из состояния CONNECTING в DISCONNECTED в результате получения сообщения EAPOL-Logoff.
Auth Enter	Количество переходов state machine из состояния CONNECTING в AUTHENTICATING в результате получения от клиента сообщения EAPOL-Response/Identity.
Auth Success	Количество переходов state machine из состояния AUTHENTICATING в AUTHENTICATED в результате того, что Backend Authentication state machine показал успешную аутентификацию клиента (authSuccess=TRUE).
Auth Timeout	Количество переходов state machine из состояния AUTHENTICATING в ABORTING в результате того, что Backend Authentication state machine показал тайм-аут аутентификации (authTimeout=TRUE).
Auth Fail	Количество переходов state machine из состояния AUTHENTICATING в HELD в результате того, что Backend Authentication state machine показал сбой аутентификации (authFail =TRUE).
Auth Reauth	Количество переходов state machine из состояния AUTHENTICATING в ABORTING в результате запроса на повторную аутентификацию (reAuthenticate=TRUE).
Auth Start	Количество переходов state machine из состояния AUTHENTICATING в ABORTING в результате получения от клиента сообщения EAPOL-Start.
Auth LogOff	Количество переходов state machine из состояния AUTHENTICATING в ABORTING в результате получения от клиента сообщения EAPOL-Logoff.
Authed Reauth	Количество переходов state machine из состояния AUTHENTICATED в CONNECTING в результате запроса на повторную аутентификацию (reAuthenticate=TRUE).
Authed Start	Количество переходов state machine из состояния AUTHENTICATED в CONNECTING в результате получения от клиента сообщения EAPOL-Start.
Authed LogOff	Количество переходов state machine из состояния AUTHENTICATED в DISCONNECTED в результате получения от клиента сообщения EAPOL-Logoff.

Responses	Количество отправленных state machine начальных пакетов Access-Request на сервер аутентификации (например, выполняет команду sendRespToServer при входе в состояние RESPONSE). Указывает, что коммутатор пытался связаться с сервером аутентификации.
AccessChallenges	Количество принятых state machine начальных пакетов Access-Challenge от сервера аутентификации (например, параметр aReq становится равным TRUE в результате выхода из состояния RESPONSE). Указывает, что сервер аутентификации взаимодействовал с коммутатором.
OtherReqToSupp	Количество отправленных state machine пакетов EAP-Request (кроме сообщений Identity, Notification, Failure или Success) клиенту (например, выполняет команду txReq при входе в состояние REQUEST). Указывает, что коммутатор выбрал метод аутентификации EAP.
NonNakRespFromSupp	Количество принятых state machine от клиента ответов на начальный пакет EAP-Request, и при этом ответом не являлся пакет EAP-NAK (например, параметр gxResp становится равным TRUE в результате перехода state machine из состояния REQUEST в RESPONSE, и ответом не является EAP-NAK). Указывает, что клиент может отвечать на выбранный коммутатором метод аутентификации EAP.
Vac Auth Success	Количество принятых state machine сообщений Accept от сервера аутентификации (например, параметр aSuccess становится равным TRUE в результате перехода из состояния RESPONSE в SUCCESS). Указывает, что клиент успешно прошел аутентификацию на сервере аутентификации.
Vac Auth Fail	Количество принятых state machine сообщений Reject от сервера аутентификации (например, параметр aFail становится равным TRUE в результате перехода из состояния RESPONSE в FAIL). Указывает, что клиент не прошел аутентификацию на сервере аутентификации.

Аутентификация на сервере RADIUS

В таблице **RADIUS Authentication** содержится информация относительно активности клиента протокола аутентификации RADIUS. Записи в таблице показывают данные для каждого сервера аутентификации RADIUS, с которым работают клиенты. Выберите **Monitoring > Port Access Control > RADIUS Authentication**, появится следующее окно:

Рисунок 6-23 Информация о серверах RADIUS

В поле **Time Interval** можно указать интервал обновления данных от 1s до 60s (“s” – секунды). По умолчанию данные обновляются один раз в секунду. Для сброса накопленной статистики нажмите кнопку *Clear*.

Показываемые параметры:

Параметр	Описание
Server Index	Идентификационный номер, назначенный каждому серверу аутентификации RADIUS, с которым работают клиенты.
InvalidServerAddr	Количество пакетов RADIUS Access-Response, принятых с неизвестных адресов.
Identifier	Идентификатор NAS-Identifier клиента аутентификации RADIUS. (Не так обязательно, как sysName в MIB-II.)
AuthServerAddr	Список серверов RADIUS, с которыми работает клиент.
ServerPortNumber	Порт UDP, который использует клиент для отправки запросов на сервер.
RoundTripTime	Интервал (в сотнях секунд) между последним пакетом Access-Replay/Access Challenge и соответствующим ему пакетом Access-Request от сервера.

Access Requests	Количество отправленных на данный сервер RADIUS пакетов Access-Request. В это число не входят повторно переданные пакеты.
Access Retrans	Количество повторно отправленных на данный сервер RADIUS пакетов Access-Request.
AccessAccepts	Количество принятых от данного сервера RADIUS пакетов Access-Accept (правильных или неправильных).
AccessRejects	Количество принятых от данного сервера RADIUS пакетов Access-Reject (правильных или неправильных).
AccessChallenges	Количество принятых от данного сервера RADIUS пакетов Access-Challenge (правильных или неправильных).
AccessResponses	Количество принятых от данного сервера RADIUS пакетов Access-Response, которые были неверно сформированы. В число неверно сформированных пакетов входят пакеты неверной длины. Пакеты с неверными атрибутами или типами Authenticator или Signature сюда не включаются.
BadAuthenticators	Количество принятых от данного сервера RADIUS пакетов Access-Response, которые содержат неверные атрибуты Authenticator или Signature.
PendingRequests	Количество пакетов Access-Request, предназначенных данному серверу RADIUS, время ожидания ответа которых еще не истекло, и еще не был получен ответ. Эта переменная инкрементируется при каждой отправке пакета Access-Request и декрементируется при приеме пакета Access-Accept, Access-Reject или Access-Challenge или по истечении времени ожидания, или при повторной передаче.
Timeouts	Количество таймаутов аутентификации для данного сервера. По истечении таймаута клиент может повторить попытку запроса на данный сервер, отправить запрос на другой сервер или прекратить попытки аутентификации. Повторный запрос на тот же сервер учитывается как повторная передача, так же как и истечение таймаута. Отправка запроса на другой сервер учитывается как обычный запрос, так же как и истечение таймаута.
Unknown Types	Количество принятых через порт аутентификации от данного сервера RADIUS пакетов неизвестного типа.
PacketsDropped	Количество принятых через порт аутентификации от данного сервера RADIUS пакетов и затем отброшенных по другим причинам.

Ведение учетных записей на сервере Radius

В таблице **Radius Accounting** содержится информация об объектах, используемых для управления учетными записями клиентов на сервере RADIUS, и текущие статистические данные, с ними связанные. Записи в таблице показывают данные для каждого сервера аутентификации RADIUS, с которым работают клиенты. Выберите **Monitoring > Port Access Control > Radius Accounting**, появится следующее окно:

ServerName	ValidServerName	Method	ServerAddress	ServerPort	RadiusType	Requests	AccessAccepts	AccessRejects	AccessChallenges	AccessResponses	PendingRequests	Timeouts	UnknownTypes	PacketsDropped
1	192.168.1.1	radius	192.168.1.1	1812	radius	100	100	0	0	0	0	0	0	0
2	192.168.1.2	radius	192.168.1.2	1812	radius	100	100	0	0	0	0	0	0	0
3	192.168.1.3	radius	192.168.1.3	1812	radius	100	100	0	0	0	0	0	0	0

Рисунок 6-24 Таблица Radius Accounting

В поле **Time Interval** можно указать интервал обновления данных от 1s до 60s (“s” – секунды). По умолчанию данные обновляются один раз в секунду. Для сброса накопленной статистики нажмите кнопку **Clear**.

Показываемые параметры:

Параметр	Описание
Server Index	Идентификационный номер, назначенный каждому серверу учетных записей RADIUS, с которым работают клиенты.
InvalidServerAddr	Количество пакетов RADIUS Accounting-Response, принятых с неизвестных адресов.
Identifier	Идентификатор NAS-Identifier клиента аутентификации RADIUS. (Не так обязательно, как sysName в MIB-II.)
ServerAddress	Список серверов учетных записей RADIUS, с которыми работает клиент.
ServerPortNumber	Порт UDP, который использует клиент для отправки запросов на сервер.
RoundTripTime	Интервал между последним пакетом Accounting-Response и соответствующим ему пакетом Accounting-Request от сервера.
Requests	Количество отправленных на данный сервер учетных записей RADIUS пакетов Accounting-Request. В это число не входят повторно переданные пакеты.
Retransmissions	Количество повторно отправленных на данный сервер учетных записей RADIUS пакетов Accounting-Request. В их число входят повторные пакеты, в которых параметры Identifier и Acct-Delay были обновлены, также как и те пакеты, в которых эти параметры остались прежними.
Responses	Количество принятых от данного сервера RADIUS пакетов через порт запросов учетных записей.
MalformedResponses	Количество принятых от данного сервера RADIUS пакетов Accounting-Response, которые были неверно сформированы. В число неверно сформированных пакетов входят пакеты неверной длины. Пакеты с неверными атрибутами Authenticator или неизвестных типов сюда не включаются.
BadAuthenticators	Количество принятых от данного сервера RADIUS пакетов Accounting-Response, которые содержат неверные атрибуты Authenticator.
PendingRequests	Количество пакетов Accounting-Request, отправленных на данный сервер RADIUS, время ожидания ответа которых еще не истекло, и еще не был получен ответ. Эта переменная инкрементируется при каждой отправке пакета Accounting-Request и декрементируется при приеме пакета Accounting-Response, по истечении времени ожидания или при повторной передаче.
Timeouts	Количество таймаутов учетных записей для данного сервера. По истечении таймаута клиент может повторить попытку запроса на данный сервер, отправить запрос на другой сервер или прекратить попытки запроса учетной записи. Повторный запрос на тот же сервер учитывается как повторная передача, так же как и истечение таймаута. Отправка запроса на другой сервер учитывается как запрос Accounting-Request, так же как и истечение таймаута.
Unknown Types	Количество принятых через порт запроса учетных записей от данного сервера RADIUS пакетов неизвестного типа.
PacketsDropped	Количество принятых через порт запроса учетных записей от данного сервера RADIUS пакетов и затем отброшенных по другим причинам.



Примечание: Для настройки аутентификации 802.1x на коммутаторе DGS-3324SR в папке Configuration нажмите на ссылку **Port Access Entity**. Информацию о настройке и иную информацию относительно аутентификации 802.1x смотрите в Разделе 4 данного руководства.

Мониторинг функций 3-его уровня

В меню **Layer 3 Feature** можно просмотреть информацию о функциях коммутатора, настроенных через меню **Layer 3 IP Networking** в папке **Configuration**. Они были ранее описаны в Разделе 4 в параграфе *Сетевое взаимодействие на 3-ем уровне*.

Таблица IP-адресов

По ссылке **Monitoring > Layer 3 Feature > Browse IP Address** доступна таблица **IP Address Table**, которая содержит изученные коммутатором IP-адреса. Для поиска определенного IP-адреса введите нужный IP-адрес в поле **IP Address** и нажмите кнопку *Find*. Нажмите *Next* для просмотра следующей части таблицы.

IP Address		<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>
IP Address Table			
Interface	IP Address	Port	Learned
System	10.0.0.1	15	Dynamic
System	10.0.0.121	15	Dynamic
System	10.0.25.1	15	Dynamic
System	10.0.34.1	15	Dynamic
System	10.0.46.1	15	Dynamic
System	10.0.51.1	15	Dynamic
System	10.0.58.4	15	Dynamic
System	10.0.85.168	15	Dynamic
System	10.1.1.101	15	Dynamic
System	10.1.1.102	15	Dynamic
System	10.1.1.103	15	Dynamic
System	10.1.1.152	15	Dynamic
System	10.1.1.158	15	Dynamic
System	10.1.1.161	15	Dynamic
System	10.1.1.162	15	Dynamic
System	10.1.1.163	15	Dynamic
System	10.1.1.164	15	Dynamic
System	10.1.1.166	15	Dynamic
System	10.1.1.167	15	Dynamic
System	10.1.1.168	15	Dynamic

Total Entries: 766

Рисунок 6-25 Таблица IP-адресов

Таблица маршрутизации

По ссылке **Monitoring > Layer 3 Feature > Browse Routing Table** доступна таблица **Routing Table** – текущая таблица маршрутизации коммутатора. Для поиска определенного маршрута введите IP-адрес назначения в поле **Destination Address**, маску подсети в поле **Mask** и нажмите кнопку *Find*.

Destination Address	<input type="text" value="0.0.0.0"/>				
Mask	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>			
Routing Table					
IP Address	Netmask	Gateway	Interface	Cost	Protocol
10.0.0.0	255.0.0.0	0.0.0.0	System	1	Local
Total Entries: 1					

Рисунок 6-26 Таблица маршрутизации

ARP-таблица

По ссылке **Monitoring > Layer 3 Feature > Browse ARP Table** доступна таблица **ARP Table** – ARP-таблица коммутатора. Для поиска определенной записи ARP введите имя интерфейса в поле **Interface Name** или IP-адрес в поле **IP Address** и нажмите кнопку *Find*.

Interface Name	<input type="text"/>		
IP Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>	
ARP Table			
Interface Name	IP Address	Mac Address	Type
System	10.0.0.0	ff-ff-ff-ff-ff-ff	Local/Broadcast
System	10.0.0.100	00-a0-c5-15-3b-6e	Dynamic
System	10.0.25.1	00-d0-59-a9-2a-c4	Dynamic
System	10.0.34.1	00-0c-6e-6e-14-13	Dynamic
System	10.0.46.1	00-80-c8-91-15-eb	Dynamic
System	10.0.51.1	00-80-c8-4c-69-fb	Dynamic
System	10.0.58.4	00-0c-6e-43-13-ae	Dynamic
System	10.0.85.168	00-50-ba-11-08-e4	Dynamic
System	10.1.1.1	00-08-74-3d-5e-91	Dynamic
System	10.1.1.4	00-ff-7f-47-d9-42	Dynamic
System	10.1.1.66	00-05-5d-0d-34-24	Dynamic
System	10.1.1.99	00-08-02-54-10-0f	Dynamic
System	10.1.1.100	00-05-5d-84-ae-75	Dynamic
System	10.1.1.101	00-50-ba-15-48-56	Dynamic
System	10.1.1.102	00-50-ba-97-d7-c0	Dynamic
System	10.1.1.103	00-50-ba-97-d7-c9	Dynamic
System	10.1.1.158	00-50-ba-f5-a5-55	Dynamic
System	10.1.1.161	00-50-ba-70-e4-89	Dynamic
System	10.1.1.162	00-50-ba-70-e4-5a	Dynamic
System	10.1.1.163	00-50-ba-70-e4-55	Dynamic
Total Entries: 712			<input type="button" value="Next"/>

Рисунок 6-27 ARP-таблица коммутатора

Таблица маршрутизации многоадресной рассылки

По ссылке **Monitoring > Layer 3 Feature > Browse IP Multicast Forwarding Table** доступна таблица **IP Multicast Forwarding Table** – таблица маршрутизации многоадресной рассылки. Для поиска определенной записи введите IP-адрес группы многоадресной рассылки в поле **Multicast Group** или IP-адрес источника рассылки в поле **Source IP** и нажмите кнопку *Find*.

Multicast Group	<input type="text" value="0.0.0.0"/>				
Source IP	<input type="text" value="0.0.0.0"/>			<input type="button" value="Find"/>	
IP Multicast Forwarding Table					
Multicast Group	Source IP Address	Source Mask	Upstream Neighbor	Expire Time	Protocol
Total Entries: 0					

Рисунок 6-28 Таблица маршрутизации многоадресной рассылки

Таблица IGMP-групп

По ссылке **Monitoring > Layer 3 Feature > Browse IGMP Group Table** доступна таблица **IGMP Group Table** – таблица IGMP-групп. Для поиска определенной IGMP-группы введите имя интерфейса в поле **Interface Name** или IP-адрес группы многоадресной рассылки в поле **Multicast Group** и нажмите кнопку *Find*.

Interface Name	<input type="text"/>			
Multicast Group	<input type="text" value="0.0.0.0"/>		<input type="button" value="Find"/>	
IGMP Group Table				
Interface Name	Multicast Group	Last Reporter IP	Querier IP	Expire
Total Entries: 0				

Рисунок 6-29 Таблица IGMP-групп

Мониторинг OSPF

Расположенные в папке **OSPF Monitoring** ссылки предоставляют доступ к таблицам **OSPF LSDB Table**, **OSPF Neighbor Table** и **OSPF Virtual Neighbor Table**, которые содержат различную информацию о протоколе OSPF.

Таблица состояния связей OSPF

По ссылке **Monitoring > Layer 3 Feature > OSPF Monitor > Browse OSPF LSDB** доступна таблица **OSPF LSDB Table**, показывающая состояние связей OSPF для каждой области OSPF.

Area ID	<input type="text" value="0.0.0.0"/>				
Advertise Router ID	<input type="text" value="0.0.0.0"/>				
LSDB Type	<input type="text" value="ALL"/>	<input type="button" value="Find"/>			
LSDB Table					
Area ID	LSDB Type	Adv. Router ID	Link State ID	Cost	Sequence
Total Entries: 0					

Рисунок 6-30 Таблица состояния связей OSPF

Возможен поиск в таблице определенной записи по следующим полям:

Поле *Area ID* позволяет задать для поиска IP-адрес, идентифицирующий область OSPF.

Поле *Advertise Router ID* позволяет задать для поиска IP-адрес, идентифицирующий маршрутизатор, который является источником рассылки объявлений LSDB.

Поле *LSDB Type* позволяет задать для поиска тип объявлений о состоянии связей (*RtrLink*, *NetLink*, *Summary*, *ASSummary* и *ASExtLink*).

Для поиска записи с указанными параметрами нажмите *Find*.

Показываемые параметры:

Параметр	Описание										
Area ID	Идентификатор области OSPF Area ID.										
LSDB Type	Показывает тип объявления о состоянии связей, из которого информация о данной связи была получена коммутатором: связи маршрутизатора (<i>RTRLINK</i>), связи сети (<i>NETLink</i>), внешние связи области (<i>Summary</i>), внешние связи автономной системы (<i>ASSummary</i>), внешняя связь автономной области (<i>ASExternal</i>).										
Adv. Router ID	Идентификатор Router ID маршрутизатора, отправившего данное объявление.										
Link State ID	Идентификатор части межсетевой среды, которую описывает данное объявление. Содержимое поля зависит от типа объявления.										
	<table border="1"> <thead> <tr> <th>LSDB Type</th> <th>Link State ID</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Идентификатор Router ID маршрутизатора, отправившего данное объявление.</td> </tr> <tr> <td>2</td> <td>IP-адрес интерфейса выделенного маршрутизатора.</td> </tr> <tr> <td>3</td> <td>IP-адрес сети назначения.</td> </tr> <tr> <td>4</td> <td>Идентификатор Router ID описываемого пограничного маршрутизатора автономной системы.</td> </tr> </tbody> </table>	LSDB Type	Link State ID	1	Идентификатор Router ID маршрутизатора, отправившего данное объявление.	2	IP-адрес интерфейса выделенного маршрутизатора.	3	IP-адрес сети назначения.	4	Идентификатор Router ID описываемого пограничного маршрутизатора автономной системы.
LSDB Type	Link State ID										
1	Идентификатор Router ID маршрутизатора, отправившего данное объявление.										
2	IP-адрес интерфейса выделенного маршрутизатора.										
3	IP-адрес сети назначения.										
4	Идентификатор Router ID описываемого пограничного маршрутизатора автономной системы.										
Cost	Метрика данной связи.										
Sequence	Показывает, сколько раз данная связь была объявлена как изменившаяся.										

Таблица OSPF-соседей

Таблица OSPF-соседей доступна по ссылке **Monitoring > Layer 3 Feature > OSPF Monitor > Browse OSPF Virtual Neighbor**. Маршрутизаторы, подключенные к одной и той же области или сегменту, становятся соседями в данной области. Соседи выбираются посредством протокола Hello. Многоадресная рассылка используется для отправки пакетов Hello остальным маршрутизаторам сегмента. Маршрутизаторы становятся соседями, когда они видят себя в списке в пакете Hello, который был отправлен другим маршрутизатором того же сегмента. Таким образом, гарантируется возможность двустороннего взаимодействия между двумя любыми соседними маршрутизаторами. Данная таблица показывает OSPF-соседей коммутатора.

IP Address	<input type="text" value="0.0.0.0"/>	Find			
OSPF Neighbor Table					
IP Address	Neighbor Router ID	Option	Priority	State	Events
Total Entries: 0					

Рисунок 6-31 Таблица OSPF-соседей

Таблица виртуальных OSPF-соседей

По ссылке **Layer 3 Feature > OSPF Monitor > Browse OSPF Virtual Neighbor** доступна таблица **OSPF Virtual Neighbor Table**, содержащая список виртуальных OSPF-соседей коммутатора. Возможен поиск в таблице определенной записи по следующим полям:

Параметр	Описание
Transit Area ID	Идентификатор Area ID транзитной области. Транзитной областью не может быть тупиковая область или магистраль.
Neighbor ID	Идентификатор Router ID удаленного маршрутизатора. Этот IP-адрес уникально идентифицирует пограничный маршрутизатор удаленной области.

Transit Area ID	<input type="text" value="0.0.0.0"/>				
Neighbor ID	<input type="text" value="0.0.0.0"/>	Browse			
OSPF Virtual Neighbor Table					
Transit Area ID	Virtual Neighbor ID	IP Address	Virtual Neighbor Option	Virtual Neighbor State	State Changes
Total Entries: 0					

Рисунок 6-32 Таблица виртуальных OSPF-соседей

Мониторинг DVMRP

Расположенные в папке **DVMRP Monitoring** ссылки предоставляют доступ к таблицам **DVMRP Routing Table**, **DVMRP Neighbor Address Table** и **DVMRP Routing Next Hop Table**, которые содержат различную информацию о протоколе OSPF. Описание протокола DVMRP и его функций относительно DGS-3324SR можно посмотреть в Разделе 4 в параграфе *Многоадресная рассылка*.

Таблица маршрутизации DVMRP

Информация о маршрутизации многоадресной рассылки по протоколу DVMRP хранится в таблице маршрутизации DVMRP, которая доступна по ссылке **Monitoring > Layer 3 Feature > DVMRP Monitoring > Browse DVMRP Routing Table**. Каждая запись в таблице содержит информацию об одном маршруте (одной подсети). Маршрутная информация используется протоколом DVMRP для доставки многоадресной рассылки. Для поиска определенной записи введите IP-адрес источника в поле **Source IP Address**, маску подсети в поле **Source Mask** и нажмите кнопку *Browse*.

Source IP Address	<input type="text" value="0.0.0.0"/>					
Source Mask	<input type="text" value="0.0.0.0"/>	<input type="button" value="Browse"/>				
DVMRP Routing Table						
Source IP Address	Source Mask	Upstream Neighbor	Metric	Learned	Interface Name	Expire
Total Entries: 0						

Рисунок 6-33 Таблица маршрутизации DVMRP

Таблица адресов DVMRP- соседей

По ссылке **Monitoring > Layer 3 Feature > DVMRP Monitoring > Browse DVMRP Neighbor Address Table** доступна таблица **DVMRP Neighbor Address Table**, содержащая информацию о DVMRP-соседах коммутатора. Для поиска определенной записи введите имя интерфейса в поле **Interface Name** или IP-адрес соседа в поле **Neighbor Address** и нажмите кнопку *Find*. Найденные записи появятся в таблице.

Interface Name	<input type="text"/>		
Neighbor Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>	
DVMRP Neighbor Table			
Interface Name	Neighbor Address	Generation ID	Expire Time
Total Entries: 0			

Рисунок 6-34 Таблица DVMRP-соседей

Таблица переходов DVMRP

По ссылке **Monitoring > Layer 3 Feature > DVMRP Monitoring > Browse DVMRP Routing Next Hop Table** доступна таблица **DVMRP Routing Next Hop Table**, содержащая информацию относительно следующего перехода (выходного интерфейса коммутатора) при маршрутизации многоадресных пакетов. Каждая запись в таблице указывает выходной интерфейс для данного адреса источника многоадресной рассылки. Для поиска определенной записи введите имя интерфейса в поле **Interface Name** или IP-адрес источника рассылки **Source IP Address** и нажмите кнопку *Find*.

Interface Name	<input type="text"/>		
Source IP Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>	
DVMRP Routing Next Hop Table			
Source IP Address	Source Mask	Interface Name	Type
Total Entries: 0			

Рисунок 6-35 Таблица переходов DVMRP

Мониторинг PIM

Маршрутизаторы многоадресной рассылки используют протокол PIM для определения того, каким образом другие маршрутизаторы должны принимать многоадресные пакеты. Описание протокола PIM и его функций относительно DGS-3324SR можно посмотреть в Разделе 4 в параграфе *Многоадресная рассылка*.

Таблица адресов PIM-соседей

По ссылке **Monitoring > Layer 3 Feature > PIM Monitor > PIM Neighbor Address Table** доступна таблица **PIM Neighbor Address Table**, содержащая информацию о PIM-соседах коммутатора. Для поиска определенной записи введите имя интерфейса в поле **Interface Name** или IP-адрес соседа в поле **Neighbor Address** и нажмите кнопку *Find*. Найденные записи появятся в таблице.

Interface Name	<input type="text"/>	
Neighbor Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>
PIM Neighbor Table		
Interface Name	Neighbor Address	Expire Time
Total Entries: 0		

Рисунок 6-36 Таблица PIM-соседей

Раздел 7

Обслуживание коммутатора

Сервисы TFTP

Ping-тест

Сохранение настроек

Сброс к заводским установкам

Перезагрузка

Выход из системы

Сервисы TFTP

Протокол TFTP позволяет обновлять ПО коммутатора путем загрузки файла нового ПО с сервера TFTP на коммутатор. Также можно загрузить конфигурационный файл коммутатора с сервера TFTP или сохранить его и журнал событий на сервере TFTP.

Обновление ПО коммутатора с сервера TFTP

Для обновления ПО коммутатора с сервера TFTP в папке **Maintenance** откройте папку **TFTP Services** и нажмите на ссылку **Download Firmware**:

Рисунок 7-1 Загрузка ПО с сервера TFTP

В поле **Unit Number** выберите порядковый номер коммутатора в стеке, для которого Вы хотите обновить ПО (если установлены дополнительные модули стекирования, и коммутаторы объединены в стек), или выберите **All** для обновления ПО на всех коммутаторах стека.

Введите IP-адрес TFTP-сервера в поле **Server IP Address**.

TFTP-сервер должен быть включен, и должен находиться той же подсети, что и коммутатор. ПО сервера TFTP является частью многих пакетов ПО сетевого управления - таких как NetSight - или может быть получено отдельно.

Введите путь к файлу ПО и его название в поле **Filename**.

Нажмите кнопку *Start*, чтобы начать процедуру загрузки файла.

Загрузка конфигурационного файла с сервера TFTP

Для загрузки конфигурационного файла на коммутатор с сервера TFTP в папке **Maintenance** откройте папку **TFTP Services** и нажмите на ссылку **Download Configuration File**:

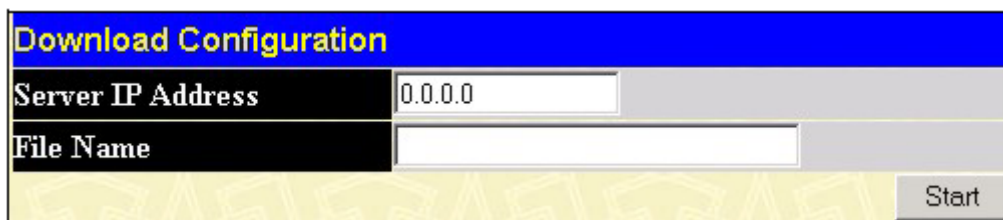


Рисунок 7-2 Загрузка конфигурационного файла с сервера TFTP

Введите IP-адрес TFTP-сервера и укажите расположение конфигурационного файла коммутатора на сервере.

Нажмите кнопку *Start*, чтобы начать процедуру загрузки файла.

Сохранение конфигурационного файла на сервере TFTP

Для сохранения конфигурационного файла коммутатора на сервере TFTP в папке **Maintenance** откройте папку **TFTP Services** и нажмите на ссылку **Save Settings**:

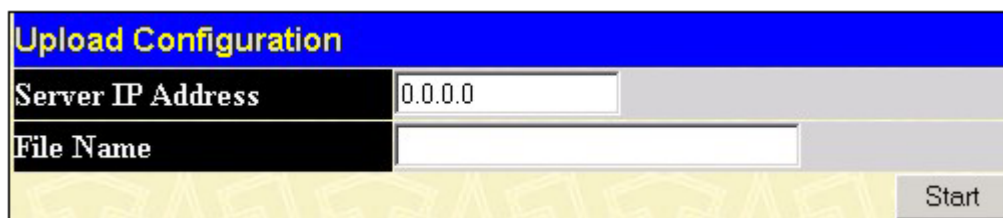


Рисунок 7-3 Сохранение конфигурационного файла на сервере TFTP

Введите IP-адрес TFTP-сервера и укажите расположение конфигурационного файла коммутатора на сервере.

Нажмите кнопку *Start*, чтобы начать процедуру сохранения файла.

Сохранение файла журнала коммутатора на сервере TFTP

Для сохранения файла журнала коммутатора на сервере TFTP в папке **Maintenance** откройте папку **TFTP Services** и нажмите на ссылку **Upload Log**:

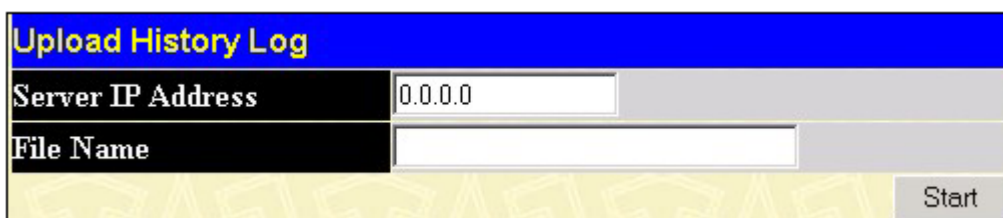


Рисунок 7-4 Сохранение файла журнала коммутатора на сервере TFTP

Введите IP-адрес TFTP-сервера и укажите расположение файла журнала коммутатора на сервере.

Нажмите кнопку *Start*, чтобы начать процедуру сохранения файла.

Ping - тест

Ping - это небольшая программа, которая отправляет пакеты по указанном IP-адресу. Затем узел назначения возвращает пакеты коммутатору. Программу полезно использовать для проверки соединения между коммутатором и остальными узлами сети.

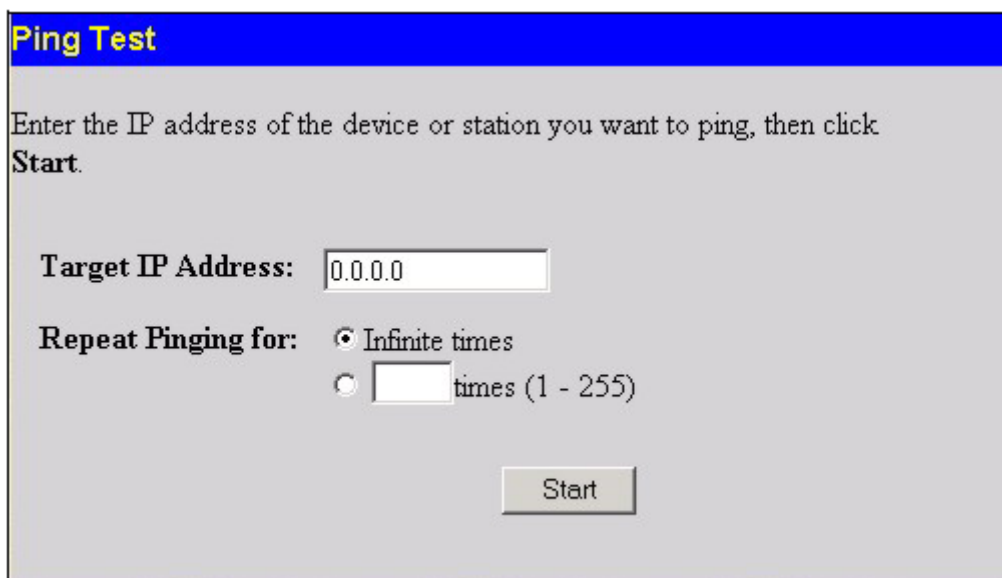


Рисунок 7-5 Ping-тест

Опция **Infinite times** в поле **Repeat Pinging for** определяет, что программа ping будет отправлять пакеты ICMP Echo по указанному IP-адресу до тех пор, пока ее работа не будет прервана. Можно указать точное число отправляемых пакетов, нажав на радио-кнопку и введя в соседнем поле нужное значение. Поле **Target IP Address** позволяет ввести адрес узла, который тестируется. Нажмите *Start* для запуска ping-теста.

Сохранение настроек

Коммутатор имеет два уровня памяти: обычное ОЗУ (RAM) и постоянную память, или NV-RAM. Изменения в настройках вступают в силу по нажатию кнопки *Apply*. После этого изменения немедленно применяются к ПО Коммутатора, загруженному в ОЗУ, и немедленно вступят в силу.

Однако некоторые изменения в настройках коммутатора требуют перезагрузки. При перезагрузке все настройки в ОЗУ стираются и загружаются последние сохраненные в NV-RAM настройки. Таким образом, необходимо сохранять настройки коммутатора в NV-RAM.

Для сохранения настроек в постоянной памяти коммутатора нажмите кнопку **Save** на странице **Save Changes**, которая показана ниже:

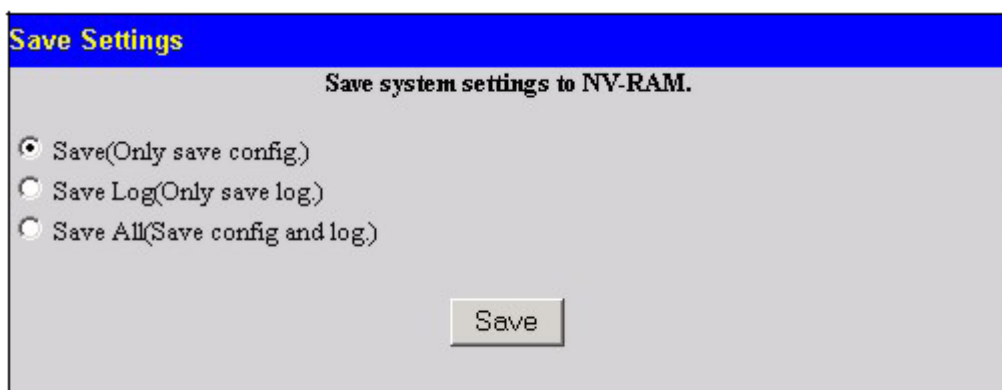


Рисунок 7-6 Окно Save Changes

Доступны следующие опции:

Параметр	Описание
Save (Only save config)	Сохранение только текущего конфигурационного файла коммутатора в NV-RAM.
Save Log(Only save log)	Сохранение только текущего файла журнала коммутатора в NV-RAM.
Save All (Save config and log)	Сохранение и текущего конфигурационного файла коммутатора в NV-RAM, и текущего файла журнала.

Как только настройки сохранены в NV-RAM, они становятся настройками коммутатора по умолчанию, и будут использоваться каждый раз, когда коммутатор перезагружается. В параграфе *Сброс к заводским установкам* описаны другие варианты изменения параметров, сохраненных в NV-RAM.

Сброс к заводским установкам

Функция **Reset** (сброс к заводским установкам) имеет несколько опций. Некоторые текущие настройки могут быть сохранены, в то время как все остальные настройки сбрасываются к заводским установкам по умолчанию.



Примечание: Только опция **Reset System** сохраняет заводские установки в NV-RAM коммутатора. Все остальные опции применяют заводские установки к текущей конфигурации, но не сохраняют ее. Опция **Reset System** вернет коммутатор к настройкам, определенным на заводе.

Reset - сброс всех настроек к заводским установкам по умолчанию, кроме учетных записей пользователей и журнала событий. Если сброс был выполнен с этой опцией, и не выполнялась команда **Save Changes**, то после перезагрузки коммутатор восстановит последнюю сохраненную в NV-RAM конфигурацию.

Reset Config - сброс всех настроек к заводским установкам по умолчанию, но без их сохранения и перезагрузки коммутатора. Если сброс был выполнен с этой опцией, и не выполнялась команда **Save Changes**, то после перезагрузки коммутатор восстановит последнюю сохраненную в NV-RAM конфигурацию.

Reset System – сброс всех настроек к заводским установкам по умолчанию и сохранение их в NV-RAM коммутатора. Затем коммутатор будет перезагружен. После перезагрузки будет восстановлена конфигурация коммутатора, установленная на заводе. Эквивалентно сбросу с опцией **Reset Config** и последующему выполнению команды **Save Changes**.

Factory Reset to Default Value

Reset All parameters are reset to default settings except IP address, user account and history log.

Reset Config All parameters are reset to default settings.

Reset System All parameters are reset to default settings. Then the switch will do factory reset, save, reboot.

Рисунок 7-7 Сброс к заводским установкам

Перезагрузка коммутатора

В папке **Maintenance** нажмите на ссылку **Reboot Device**, появится следующее меню.

Нажмите **Yes** для того, чтобы коммутатор сохранил текущие настройки в NV-RAM перед перезагрузкой.

Нажмите **No**, если не хотите, чтобы коммутатор сохранял текущие настройки в NV-RAM перед перезагрузкой. Все изменения в настройках, произведенные с момента последнего исполнения команды **Save Changes**, будут потеряны.

Нажмите кнопку **Restart** для перезагрузки коммутатора.

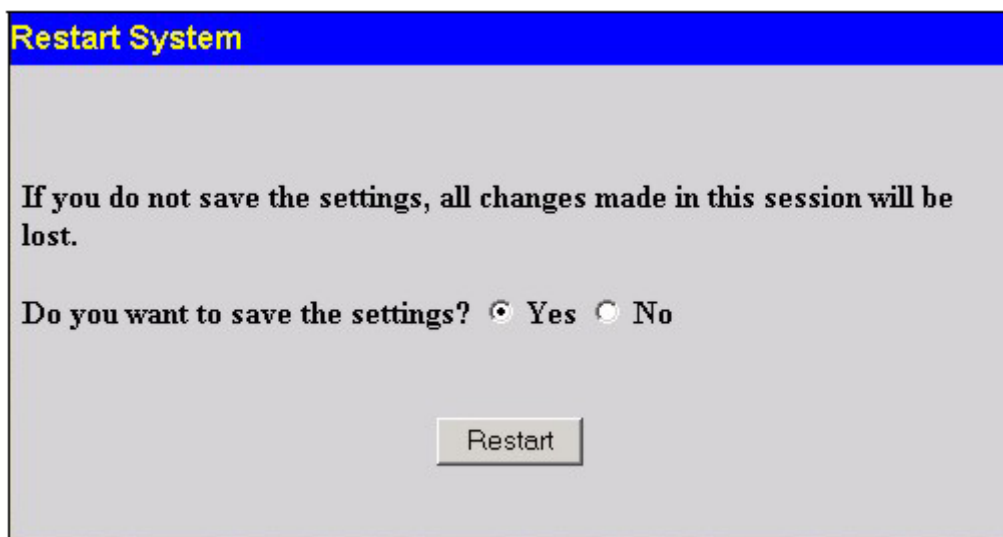


Рисунок 7-8 Меню перезагрузки коммутатора

Выход из системы

Для выхода из Web-интерфейса управления на странице **Logout** нажмите кнопку **Log Out**.

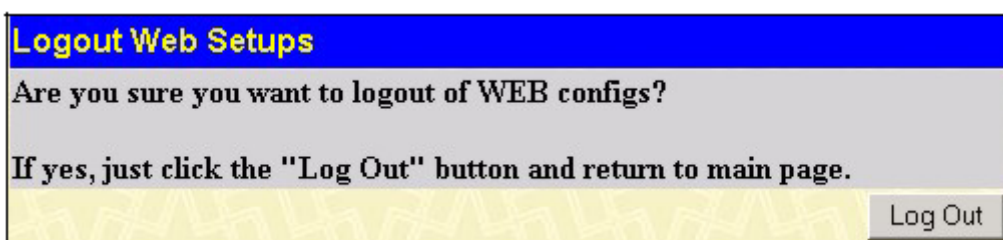


Рисунок 7-9 Страница Logout

Приложение А

Технические характеристики

Общие	
Стандарты	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1P/Q VLAN IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation
Протокол	CSMA/CD
Скорость подключения	Полу-дуплекс Полный дуплекс
Ethernet	10Мбит/с 20 Мбит/с
Fast Ethernet	100 Мбит/с 200 Мбит/с
Gigabit Ethernet	2000 Мбит/с
Оптический кабель	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 или кольцо
Кабели	UTP Кат. 5, Кат. 5е для 1000 Мбит/с UTP Кат. 5 100 Мбит/с UTP Кат. 3,4,5 для 10 Мбит/с EIA/TIA- 568 100-Ом экранированная витая пара STP (100 м)

Физические и климатические	
Питание (поддержка внешнего резервного источника питания)	100 - 240 В, 50/60 Гц (внутренний универсальный источник питания)
Потребляемая мощность	90 Ватт максимум
Вентиляция	2 встроенных вентилятора размером 40 x 40 x10 мм; 1 встроенный вентилятор размером 60 x 60 x18 мм
Температура хранения	От -25°до 55° С
Рабочая температура	От 0°до 40° С
Влажность	Рабочая: 5% - 95% без конденсата Хранения: 0% - 95% без конденсата
Размеры	441 x 207 x 44 мм, для установки в 19" стойку
Вес	3,15 кг
Электромагнитное излучение	FCC Part 15 Class A/ ICES-003 Class (Canada) EN55022 Class A / EN55024
Безопасность	CSA International

Производительность	
Метод коммутации	Store-and-forward
Буфер RAM	2 Мб на устройство
Адресная таблица	16К MAC-адресов на устройство
Скорость фильтрации/продвижения пакетов	На полной скорости соединения. 148,810 pps на порт (для 100 Мбит/с) 1,488,100 pps на порт (для 1000 Мбит/с)
Изучение MAC адресов	Автоматическое обновление.
Время жизни записей в таблице коммутации	Макс.: 10 – 1 000 000 секунд По умолчанию: 300 секунд

Глоссарий

100BASE-FX Реализация 100 Мбит/с Ethernet для оптического кабеля.

100BASE-TX Реализация 100 Мбит/с Ethernet для витой пары категории 5 типа 1.

10BASE-T Спецификация IEEE 802.3 Ethernet для неэкранированной витой пары (Unshielded Twisted Pair, UTP).

ageing (устаревание) Автоматическое удаление динамических записей из таблицы коммутации, время жизни которых истекло, и они больше не действительны.

ATM (Asynchronous Transfer Mode, Асинхронный режим передачи) Протокол с коммутацией каналов, основанный на ячейках фиксированной длины (пакетах). ATM был разработан для передачи всех видов пользовательского трафика, включая голос, данные и видео.

auto-negotiation (автосогласование) Функция порта, которая позволяет ему сообщать о поддерживаемых скоростях работы, режимах дуплекса и методах управления потоком. При подключении к конечной станции, также поддерживающей автосогласование, соединение само определяет оптимальные параметры взаимодействия.

backbone port (магистральный порт) Порт, который не изучает адреса устройств и принимает все кадры с неизвестными адресами. Магистральные порты обычно используются для подключения коммутатора к магистрали сети. Обратите внимание, что раньше магистральные порты были известны как выделенные порты downlink (designated downlink ports).

backbone (магистраль) Часть сети, используемая в качестве основного маршрута передачи трафика.

Backbone (Магистраль) Часть сети, используемая в качестве основного маршрута передачи трафика между сегментами сети.

bandwidth (полоса пропускания) Объем трафика в битах, который канал способен передать за секунду. Полоса пропускания Ethernet равна 10 Мбит/с, полоса пропускания Fast Ethernet равна 100 Мбит/с.

baud rate (скорость в бодах) Скорость коммутации линии связи. Также известна как *line speed (скорость линии связи)* между сегментами сети.

BOOTP Протокол BOOTP позволяет автоматически назначать IP-адрес устройству с определенным MAC-адресом каждый раз, когда устройство начинает работать. Кроме того, протокол позволяет назначать маску подсети и шлюз по умолчанию.

bridge (мост) Устройство, соединяющее локальную и удаленную сети и не зависящее от протокола верхнего уровня. Мосты формируют единую логическую сеть с централизованным управлением.

broadcast (широковещательная рассылка) Сообщение, отправленное всем узлам сети.

broadcast storm (широковещательный шторм) Множество одновременно отправленных широковещательных сообщений, обычно поглощающих доступную пропускную способность сети, что может привести к отказу сети.

console port (консольный порт) Порт коммутатора, к которому подключается терминал или модем. Он преобразует параллельное представление данных, используемое в компьютере, в последовательные сигналы для передачи по соединению. Данный порт чаще всего используется для локального управления.

CSMA/CD Метод доступа к среде передачи, используемый стандартами Ethernet и IEEE 802.3, который позволяет устройствам передавать данные только после того, как они обнаружили, что среда передачи свободна в течении некоторого периода времени. Если два устройства начинают передачу одновременно, то возникает коллизия, и конфликтующие устройства откладывают передачу данных на случайный промежуток времени.

data center switching (центр коммутации данных) Точка агрегирования соединений внутри корпоративной сети, в которой коммутатор обеспечивает высокую производительность для подключения серверов, высокоскоростных магистралей и контроль управления и безопасности.

Ethernet Стандарт LAN, совместно разработанный Xerox, Intel и Digital Equipment Corporation. Сеть Ethernet работает на скорости 10 Мбит/с, используя метод доступа к среде передачи CSMA/CD.

Fast Ethernet Технология 100 Мбит/с, основанная на методе доступа к сети Ethernet/CD.

Flow Control (Управление потоком) (IEEE 802.3z) Способ задержки пакетов на передающем порту конечной станции. Предотвращает потери пакетов на загруженном порту коммутатора.

forwarding (продвижение) Процесс передачи пакета по адресу назначения устройством, объединяющим несколько сетей.

full duplex (полный дуплекс) Система, позволяющая одновременно передавать и принимать пакеты, что приводит к удвоению потенциальной пропускной способности канала связи.

half duplex (полудуплекс) Система, позволяющая передавать и принимать пакеты, но не одновременно. Противоположность режиму *полного дуплекса*.

IP address (IP-адрес) Адрес протокола Интернет (Internet Protocol). Уникальный идентификатор устройства, подключенного к сети TCP/IP. Этот адрес записывается в виде 4 байт, разделенных точками, состоит из адреса сети, дополнительного адреса подсети и адреса узла.

IPX Протокол Internetwork Packet Exchange. Протокол взаимодействия в сети NetWare.

LAN Local Area Network, Локальная сеть. Сеть, состоящая из связанных между собой вычислительных ресурсов (таких как, ПК, принтеры, серверы) и занимающая относительно небольшую географическую область (обычно не больше чем этаж или здание). Характеризуется высокими скоростями передачи данных и низким процентом ошибок.

latency (задержка) Интервал времени между моментом приема устройством пакета и передачей его на порт назначения.

line speed (скорость линии связи) См. *baud rate (скорость в бодах)*.

main port (основной порт) Порт в устойчивом канале связи, который передает трафик при обычных условиях работы.

MDI Medium Dependent Interface, Зависящий от среды передачи интерфейс. Соединение Ethernet, при котором передатчик одного устройства подключается к приемнику другого устройства.

MDI-X Medium Dependent Interface Cross-over, Зависящий от среды передачи перекрестный интерфейс. Соединение Ethernet, в котором внутренние передающая и принимающая линии перекрещиваются.

MIB Management Information Base, База данных управляющей информации. Содержит переменные для управления устройством и его параметры. MIB используются протоколом SNMP (Simple Network Management Protocol, Простой протокол сетевого управления) для поддержания атрибутов управляемой системы. Коммутатор DGS-3324SR содержит собственную внутреннюю MIB.

multicast (многоадресная рассылка) Одиночные пакеты, которые копируются на указанный диапазон сетевых адресов. Эти адреса указаны в поле адреса назначения пакета.

protocol (протокол) Набор правил для взаимодействия между устройствами в сети. Правила устанавливают формат пакетов и данных, временные соотношения, планирование и методы обнаружения ошибок.

resilient link (устойчивый канал связи) Пара портов, настроенных так, что один из них берет на себя передачу данных другого при его выходе из строя. См. также *main port(основной порт)* и *standby port(резервный порт)*.

RJ-45 Стандартный 8-контактный разъем для сети IEEE 802.3 10BASE-T.

RMON Remote Monitoring, Удаленный мониторинг. Подмножество SNMP MIB II, которое предоставляет возможности мониторинга и управления посредством адресации до 10 различных информационных групп.

RPS Redundant Power System, Резервный источник питания. Устройство, которое обеспечивает резервное питание при подключении к коммутатору.

server farm (группа серверов) Кластер серверов в одной комнате, обслуживаемый большим количеством персонала.

SLIP Serial Line Internet Protocol, Протокол Интернет на последовательной линии. Протокол, позволяющий протоколу IP работать на последовательном соединении.

SNMP Simple Network Management Protocol, Простой протокол сетевого управления. Протокол, специально разработанный для управления в сетях TCP/IP. В настоящее время протокол SNMP реализован в широком диапазоне сетевого оборудования и компьютеров и может быть использован для управления многим аспектами сети и работой конечных станций.

Spanning Tree Protocol (Протокол покрывающего дерева) (STP) Система, обеспечивающая устойчивость сети к сбоям связей между мостами. STP позволяет создавать параллельные маршруты для сетевого трафика и гарантирует, что резервные маршруты будут отключены, если основные работают, и активизируются при их сбое.

stack (стек) Группа сетевых устройств, объединенных в единое логическое устройство.

Standby port (резервный порт) Порт в устойчивом канале связи, который берет на себя передачу данных основного порта в случае его сбоя.

switch (коммутатор) Устройство, которое фильтрует, продвигает и веерно рассылает пакеты на основании адреса назначения пакета. Коммутатор изучает адреса, связанные с каждым портом коммутатора и строит таблицу по этой информации, используемую в дальнейшем для принятия решения о продвижении пакетов.

TCP/IP Многоуровневый набор коммуникационных протоколов, обеспечивающих эмуляцию терминала Telnet, сервис передачи файлов FTP и многие другие сервисы, которые позволяют широкому диапазону компьютерного оборудования взаимодействовать между собой.

Telnet Протокол стека TCP/IP уровня приложения, обеспечивающий сервис виртуального терминала и позволяющий пользователю регистрироваться в другой компьютерной системе и получать доступ к другому узлу так, если бы пользователь был непосредственно подключен к этому узлу.

TFTP Trivial File Transfer Protocol, Простой протокол передачи файлов. Позволяет передавать файлы (например, обновление ПО) с удаленного устройства, используя возможности локального управления коммутатором.

UDP User Datagram Protocol, Протокол пользовательских дейтаграмм. Стандартный протокол Интернет, позволяющий прикладной программе на одном устройстве отправлять дейтаграммы другому приложению на другом устройстве.

VLAN Virtual LAN, Виртуальная локальная сеть. Группа узлов, объединенных логически в независимости от их расположения и топологии сети и взаимодействующих так, будто они находятся в одной физической сети.

VLT Virtual LAN Trunk, транк VLAN. Канал связи между коммутаторами, который передает трафик всех VLAN на каждом из коммутаторов.

VT100 Тип терминала, который использует символы ASCII. Экран терминала имеет текстовый вид.

Ограниченная гарантия

Аппаратные средства:

D-Link гарантирует отсутствие производственных дефектов и неисправностей в своих аппаратных средствах в случае их эксплуатации в нормальных условиях и правильном обслуживании в течение следующего периода, исчисляемого с момента его приобретения у D-Link или его авторизованного продавца:

<u>Тип продукции</u>	<u>Гарантийные период</u>
Изделие	Один год
Комплекующие к нему	90 дней

Годовая гарантия на изделие действует в том случае, если приложенная Регистрационная карточка была полностью заполнена и отправлена на адрес офиса D-Link в течение 90 дней с момента его приобретения по почте, факсу или e-mail. В случае нарушения этого условия гарантия автоматически ограничивается 90 днями с момента приобретения. Адреса офисов D-Link прилагаются к Регистрационной карточке.

Если устройство стало неработоспособным в течение гарантийного периода, D-Link осуществит ремонт или замену данного устройства. D-Link оставляет за собой право осуществлять ремонт или замену, в последнем случае заменяющее устройство может быть как новым, так и восстановленным. Заменяющее устройство должно соответствовать аналогичной или лучшей спецификации, но не обязательно таким же. Любое подвергшееся ремонту со стороны D-Link устройство или его комплектующие имеют гарантийный период не менее 90 дней с момента проведения ремонта, даже если ранее этого срока срок базовой гарантии закончился. Если D-Link осуществляет замену, то неисправное устройство становится собственностью D-Link.

Запрос на Гарантийное обслуживание осуществляется обращением в Представительство D-Link в оговоренный срок для получения номера RMA (Return Material Authorization). Если Регистрационная карточка на изделие не была отправлена D-Link, то необходимо предоставить документы, подтверждающие его приобретение у авторизованных продавцов. Если у Заказчика имеются особые условия, связанные с гарантийным обслуживанием, то при оформлении RMA необходимо указать их и D-Link может учесть их.

После получения номера RMA неисправное устройство должно быть упаковано для предотвращения повреждений при транспортировке как в исходную фирменную, так и стороннюю упаковку, причем номер RMA должен быть указан на снаружи. После этого устройство необходимо отправить в адрес D-Link с оплатой транспортировки и страховки Заказчиком. D-Link не отвечает за потерю информации Заказчика, которая содержалась в возвращаемом по гарантии устройстве.

Любая упаковка, возвращаемая на D-Link без номера RMA, не принимается и не несет за них ответственность.

В случае неправильного или некорректного оформления RMA Заказчиком D-Link оставляет за собой право не признать соответствующий случай гарантийным.

Программное обеспечение:

Гарантийное обслуживание по программному обеспечению можно получить связавшись с офисом D-Link в оговоренный гарантийный период. Список офисов D-Link приведен на последней странице данного Руководства, а также вместе с Регистрационной карточкой. Если Регистрационная карточка не была отправлена на адрес офиса D-Link, то для гарантийного обслуживания требуется документальное подтверждение факта покупки у авторизованного продавца. Термин «покупка» в отношении программного обеспечения означает факт приобретения и получение

D-Link гарантирует, что его программное обеспечение будет работать в строгом соответствии с прилагаемым к нему D-Link документацией в девяносто (90) дней с момента его приобретения у D-Link или авторизованного продавца. D-Link предоставляет гарантию на носитель, на котором поставляется программное обеспечение, в виде отсутствия потери им информации на тот же гарантийный срок. Данная гарантия имеет отношение только к приобретенному программному обеспечению или его замене по гарантии, и не касается любых обновлений или замен, которые получены по Internet или бесплатно.

Ответственность D-Link по обеспечению гарантии программного обеспечения состоит в замене его на новое, которое выполняет перечисленные в прилагаемой документации функции. Ответственность Заказчика состоит в выборе соответствующего приложения, программной платформы/системы и дополнительных материалов. D-Link не отвечает за работоспособность программного обеспечения вместе с любыми аппаратными средствами, и/или программными платформами/системами, которые поставляются третьими сторонами, если совместимость с ними они не оговорены в прилагаемой к продукции D-Link документации. Согласно данной гарантии, D-Link старается обеспечить разумную совместимость своей продукции, но D-Link не несет ответственность, если с аппаратными или программными средствами третьих фирм происходят сбои. D-Link не гарантирует, что работа программного обеспечения будет непрерывна и в процессе не будут происходить ошибки, а также то, что все дефекты в программном продукте с или без учета документации на него, будут исправлены.

ОГРАНИЧЕНИЯ ГАРАНТИЙ

Если оборудование D-LINK не было использовано в соответствии с приведенными выше условиями, то, по мнению D-LINK, ответственность по ремонту или замене будет целиком лежать только на самом заказчике. Вышеупомянутые гарантии и замечания являются исключительными и соответствуют всем прочим гарантиям, объявленным или подразумеваемых, которые даются в явном виде или в соответствии с законодательством, установленных законами или в другом виде, включая гарантии на сам товар и его пригодность для стандартных целей. D-LINK никогда не допускает или принимает на себя прочую ответственность связанную с продажами, поддержкой инсталляции или использования продукции D-LINK.

D-LINK никогда не несет ответственность по гарантии, если проводимое им тестирование и анализ определяет, что заявленный дефект в изделии не был обнаружен или он был вызван неверным использованием заказчиком или третьей стороной, невнимательной или неправильной инсталляцией или тестированием, попыткой неавторизованного ремонта или чем-либо еще не предусмотренном в назначении изделия типа несчастного случая, огня, пожара и других бедствий.

ОГРАНИЧЕНИЯ ОТВЕСТВЕННОСТИ

Ни в каком случае D-LINK не несет ответственность за любые убытки, включая потерю данных, потерю прибыли, стоимости покрытия или других случайных, последовательных или непрямых убытков, являющихся следствием инсталляции, сопровождения, использования, производительности, неисправности или временной неработоспособности D-LINK. Эти ограничения действуют даже если D-LINK был предупрежден о возможности такого убытка.

Если изделие D-LINK было заказано в США, то некоторые штаты не допускают ограничения или исключения ответственности для случайных или последовательных убытков, в связи с чем указанные выше ограничения они не относятся к Вам.

Офисы D-Link для регистрации и гарантийного обслуживания

Регистрационная карточка, прилагаемая на обратной стороне Руководства, должна быть отправлена в офис D-Link. Для получения номера RMA в целях гарантийного обслуживания аппаратных средств или получения гарантийного сервиса для программного обеспечения свяжитесь с ближайшим офисом D-Link. Список адресов/ телефонов/ факсов офисов D-Link содержится на обратной стороне данного Руководства.